

Take Control

of Your 802.11n AirPort Extreme Network

by Glenn Fleishman

Table of Contents (1.2)

Read Me First	2
Introduction	5
AirPort Networking Quick Start	6
Quick Troubleshooting Guide	8
Key Glossary Terms	10
Learn Wireless and AirPort Basics.....	13
Put Your Base Station into Action.....	25
Set Up Your Network	54
Connect Your Computers	70
Connect Multiple Base Stations	86
Mix Legacy, New N Networks.....	97
Reach Your Network Remotely.....	101
Set Up a Shared USB Printer	113
Set Up a Shared USB Disk.....	121
Secure Your Network.....	132
Overcome Interference.....	146
Appendix A: Stream Media with AirPort.....	150
Appendix B: Setting up a Software Base Station ..	158
Appendix C: Advanced Extreme Features	161
Appendix D: What's New in Leopard	167
About This Book.....	179



READ ME FIRST

Welcome to *Take Control of Your 802.11n AirPort Extreme Network*, version 1.2. This book helps you install and get the most out of an 802.11n Wi-Fi network. This book was written by Glenn Fleishman, edited by Tonya Engst, and published by TidBITS Publishing Inc.

Copyright © 2008 Glenn Fleishman. All rights reserved.

The price of this ebook is \$10. If you want to share it with a friend, please do so as you would a physical book. [Click here](#) to give your friend a discount coupon. Discounted [classroom copies](#) are also available.

Updates

You may not have the latest version of this PDF. To find out if there's a new version, click the Check for Updates link on the [cover](#). Once you click the link, you'll be taken to a Web page where you can learn about any available or planned updates, and sign up to be notified about updates to the PDF via email. You may also find minor update information directly on that Web page.

Who Needs This Book

I wrote this book for people who have purchased or are considering buying the thoroughly overhauled, 802.11n AirPort Extreme Base Station, released in January 2007 with new software, and updated with new hardware and revised software in August 2007. My goal is to help you configure this base station model to meet your needs, and to use it with existing and new networking equipment and computers.


Who Doesn't Need This Book

If you're not yet using a 2007-or-later, 802.11n AirPort Extreme Base Station, this book would be worthwhile only for background research if you are considering buying that new base station. If you use earlier networking hardware on a Mac, consider purchasing [Take Control of Your AirPort Network](#), which covers gear released before 2007.

Basics

In reading this book, you may get stuck if you don't know certain basic facts about Mac OS X or if you don't understand Take Control

syntax for things like working with menus or finding items in the Finder. Please note the following:

- **Path syntax:** I occasionally use a *path* to show the location of a file or folder in your file system. Path text is formatted in bold type. For example, the Airport Utility gets installed into the Utility folder, which is located inside the Applications folder. The path to AirPort Utility is: **/Applications/Utilities/AirPort Utility**.
- **Menus:** When I describe choosing a command from a menu in the menu bar, I use an abbreviated description. For example, the abbreviated description for the menu command that creates a new folder in the Mac OS X Finder is “File > New Folder.”
- **Finding preference panes:** I sometimes refer to Mac OS X preferences that you may want to adjust, such as the Network preference pane. To reach this pane, open System Preferences by clicking its icon in the Dock or choosing System Preferences from the  menu. You access a particular preference pane by way of its icon, or the View menu. For example, to see “the Network preference pane,” you would launch System Preferences and then click the Network icon or choose View > Network. To see “the AirPort view of the Network preference pane,” you would do the same thing, and then click AirPort.
- **Configuring a base station:** Throughout the book, I refer to using a program called AirPort Utility to configure a base station. To configure a base station in almost all cases, you launch or switch to AirPort Utility, select the base station in a left-hand list of base stations, and then choose Base Station > Manual Setup (Command-L) to proceed.

What's New in Version 1.2

Leopard shipped several weeks after the 1.1 version of this book, and there was nothing to be done but wait to see what shook out—and boy did a lot shake out, including Apple’s release of Time Capsule, an updated AirPort Express, and another overhaul of their AirPort Utility. As a result, this updated version 1.2 features an extensive appendix documenting changes in Leopard. An upcoming new book, tentatively titled *Take Control of Your Draft N AirPort Network in Leopard*, will thoroughly address all the new backup and network options separately.

See [Appendix D: What's New in Leopard](#) (p. 167) for the rundown on how the Network preference pane changed, how the new AirPort menu works, and how to configure a host of small tweaks that have moved since Tiger.



Also, in areas of the book where the new appendix has important information about Leopard, I've added a leopard spot (🐆) in the margin. If you see the spot, you can click it to view the appendix. If you find yourself moving around a lot due to clicking the spots, you may find it handy to use a keyboard shortcut to quickly return to the previous location. Look in the menus to find the shortcut for your PDF software.

What Was New in Version 1.1

At first, this revision was intended to be a 1.0.1 update, to cover the changes in the AirPort Extreme Base Station with 802.11n that Apple introduced in August 2007. After reviewing reader mail and spending many hours working with the gigabit model, I wound up making a number of changes and additions that should help with setting up regular networks and those with multiple base stations.

In this update, I added the following:

- An updated discussion of the state of 802.11n. See [Extreme N Details](#) (p. 18).
- More information about [Third-party adapters](#) for 802.11n (p. 22).
- A new section, [Connect Multiple Base Stations](#) (p. 86), which explains in detail how to use Ethernet and Wi-Fi links to build a network of two or more base stations to cover a greater area or increase the speed of the network.
- For mixed networks using older 802.11 standards with 802.11n, I recommend that you attach USB printers to an Extreme N Base Station. See [Put Printers in the Right Place](#) (p. 99).
- Updated information about NAT-PMP and wide-area Bonjour, Apple technologies for extending access to local network resources.
- To the section on coping with interference, I added more specific advice. See [Eliminate Conflicting Signals](#) (p. 146).

INTRODUCTION

Apple introduced integrated wireless networking to the world with AirPort in 1999. Although corporations had already 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 products shot off the shelves due to their relatively low initial price, simple configuration interface, and excellent performance.

AirPort came out of the same approach that allowed Apple to ship the iMac the year before: combining available, standard parts in a unique package that provided more value as a whole.

The AirPort Card fit into a special slot in Macintoshes; its stand-alone, central coordinating hub was called the AirPort Base Station. Apple replaced the original AirPort line with AirPort Extreme: first, in 2003 with a somewhat faster flavor (known as 802.11g), then again in 2007, with a substantially faster version (802.11n). Today, AirPort Extreme is built into every Mac, except the Mac Pro, for which it is an add-on option, and the Xserve, which is designed for server rooms.

Despite Apple's 8-year history with wireless networking and the general excellence of their software and support, setting up a wireless network isn't always a snap. This book helps you set up a wireless network and offers tips to help save time, improve security, extend range, and enjoy a technical edge when working with AirPort.

Although the title of this book references 802.11n AirPort Extreme networks, I also cover compatibility and connections with older hardware, as well as connecting to a new network using Mac OS X, Windows XP, and Windows Vista.

I start with wireless basics, move through installation and configuration, explain how to share printers and hard disks, tell you how to connect to a Wi-Fi network, give advice on extending a network's range and quality, look at adding devices like an Apple TV or AirPort Express, and finish with how-to information on security for those who want their AirPort networks safe from freeloaders and intruders.

AIRPORT NETWORKING QUICK START

If you read this book in order, you'll be guided through the steps shown below—unpacking an 802.11n AirPort Extreme Base Station, configuring the gateway, and getting on the Internet. The book also guides you through adding devices like printers, hard disks, and Apple TV, and securing the network.

Need a quick solution? *If you are reading this book in order to solve a particular problem, flip ahead two pages to the [Quick Troubleshooting Guide](#), also, you may especially wish to consult [Eliminate Conflicting Signals](#) (p. 146).*

Learn wireless basics:

- Get a quick grounding in wireless terminology and technology. See [Key Glossary Terms](#) (p. 10) and [Learn Wireless and AirPort Basics](#) (p. 13).

Set up your network:

- [Unpack and power your base station](#) (p. 25), and [Install new software](#) (p. 27).
- [Handle initial setup](#) (p. 32) for the base station. This might be all you need to get on the Internet.
- Learn about options and tradeoffs for which frequency band and channel to use, in [Configure the Spectrum and Channel](#) (p. 47).
- Place your gateway in the right place for optimum coverage. See [Pick the Right Place for Your Base Station](#) (p. 49).
- Hook your AirPort Extreme into the Internet or a larger network, while learning the difference between public and private network addresses, and static and dynamic addresses in [Get a WAN Address](#) (p. 55).
- Set up your local network connections for computers to connect wirelessly and via Ethernet to the base station. Read [Hand Out LAN Addresses](#) (p. 61).

- Control how your computers connect to the network with [Connect Your Computers](#) (p. 70), which covers Mac OS X, Windows XP Service Pack 2, and Windows Vista.
- Open your local network up to the wider world in limited ways for gaming, remote control, and Web servers. See [Reach Your Network Remotely](#) (p. 101).
- Add printers and external drives to your base station to share across the network—or the Internet. See [Set Up a Shared USB Printer](#) (p. 113) and [Set Up a Shared USB Disk](#) (p. 121).
- Stream media on your network through an [Apple TV](#) (p. 150) or with [AirPort Express and AirTunes](#) (p. 154).

Extend your network with more routers:

- Add access points to your network with the right settings to create seamless roaming. See [Connect Multiple Base Stations](#) (p. 86).
- Don't throw away your old gear: combine old and new for the best of both worlds. See [Mix Legacy, New N Networks](#) (p. 97).
- Extend your network over your home electrical system. Read the sidebar [Extend with HomePlug](#) (p. 90).
- [Bridge Wirelessly](#) among access points, in order to avoid wiring (p. 91).

Secure your network:

- Decide if you need encryption. Read [Likelihood, Liability, and Lost Opportunity](#) (p. 132).
- Avoid security tricks that don't work, while using a new method that does. See [Simple Tricks That Don't Work](#) (p. 134).
- Apply encryption using the best—and often simplest—method. See [Use Built-In Encryption](#) (p. 137).

If you need quick help, here's the starting point.

Reset the Base Station from a Lock-Up

If your AirPort Extreme Base Station can't be seen over the network via AirPort Utility (see [Install new software](#), p. 27), and you cannot connect to the base station or the Internet via a Wi-Fi-enabled computer, try these steps in order:

- 1. Check a local connection:** Make sure that the computer running AirPort Utility is on the same local network as the base station. Try connecting the computer via Ethernet to one of the base station's LAN ports. Try AirPort Utility again.
- 2. Failing a direct Ethernet connection, try power cycling:** Pull the power adapter's plug out of the wall socket or remove the end that plugs into the base station. Wait 10 seconds. Plug it back in, and try to connect via AirPort Utility. Everything may be back to normal.
- 3. Failing power cycling, try a factory reset:** This step erases any the custom settings you've made (I recommend backing up settings using AirPort Utility; see [Create and manage profiles](#), p. 38). To reset the base station, straighten one end of a paperclip, and with the base station plugged into power, hold down the base station's reset button with the paperclip end. The reset button is recessed in the rear right of the base station below the reset symbol: a white arrow reversed out of a gray circle.
- 4. Failing power cycling, try to reset another way:** Unplug the base station from power, push in the reset button and hold it down, plug the base station into power, and keep the reset button pressed for at least 20 seconds.
- 5. Failing factory reset:** Call Apple for return instructions.

Printer Problems

Printer on 802.11g part of network won't print

You'll need to connect it to your Extreme N base station. [Put Printers in the Right Place](#) explains how (p. 99).

Can't print to a USB-connected printer

See [Troubleshoot an Unavailable Shared USB Printer](#) (p. 120).

Other Troubleshooting

Can't see base station's network from all computers

Did you set the base station to the 5 gigahertz (GHz) band? Only newer Macs with 802.11n built in can connect. See [Configure the Spectrum and Channel](#) (p. 42).

Can't connect to base station's network; get an error instead

If you can see its network name, try these fixes:

- Did you inadvertently set the base station to allow 802.11n only connections in the 2.4 GHz band? See [Connect Your Computers](#) (first Warning, page 70). It's also possible that access control is preventing access. See [Mac address filtering](#) (p. 135).
- It's possible that interference in your area from other networks is preventing you from connecting. You may need to change the base station's channel. See [Eliminate Conflicting Signals](#) (p. 146).

Error occurs after connecting to the base station with the correct encryption key

Are you using a Mac with the older AirPort Card with your base station set up with WPA2 encryption? See [Turning on WPA/WPA2 with AirPort Extreme](#) (p. 141).

Firmware update makes base station act erratically

Try to [Revert to Older Firmware](#) (p. 161).

Network works erratically

Another network might be interfering with yours. See [Eliminate Conflicting Signals](#) (p. 146).

Conflicting signals seem to cause network problems

See [Eliminate Conflicting Signals](#) (p. 146).

KEY GLOSSARY TERMS

In this section, I've defined a few terms that you'll encounter over and over in this book. Read the list below to become familiar with any new terms and refresh your memory on the rest. I also define these terms where they occur. I've presented the concepts below in the order you need to understand them, building one on top of the other.

Wi-Fi: The set of wireless networking standards that encompasses all of Apple's AirPort products, and thousands of wireless networking products made by other firms. The in-progress 802.11n standard used in the latest AirPort Extreme Base Station is slated to become part of Wi-Fi in third quarter 2007.

Ethernet: A set of standards for connecting computers by wire, typically at speeds of 10 megabits per second (Mbps), 100 Mbps, and 1,000 Mbps. 1,000 Mbps Ethernet is commonly called *gigabit* Ethernet.

Local Area Network (LAN): A *LAN* comprises computers connected via Ethernet and/or Wi-Fi into a small or large group. A LAN's computers are in close physical proximity, usually in an area as small as a home office or as large as an entire office building. A LAN is typically thought of as a single network, especially when considering local network resources like file servers.

Wide Area Network (WAN): A router, like the AirPort Extreme Base Station, connects its own LAN to a wider network that's known as a *WAN*. A WAN, from the perspective of a base station, is often simply the Internet; or it might be a network connecting several offices run by the same company in different cities.

Access point: A wireless networking device that accepts connections from clients or other access points in order to move network traffic over the air.

Base station, router, gateway: These three terms are used somewhat interchangeably to refer to the central Wi-Fi hub that connects a LAN to a WAN. *Routers*, often called *gateways*, connect different kinds of networks and allow devices on each network to communicate with each other. Apple calls its combination of an access point and gateway a *base station*; other companies call these *Wi-Fi gateways* or *Wi-Fi routers*.

MAC (Media Access Control) address: The MAC address is a unique number assigned by a manufacturer to each network adapter, including Ethernet adapters and Wi-Fi adapters. The MAC address is used to identify an adapter on a LAN. (*Media* here is the plural of medium, as in the access medium: the physical means over which data flows.) To learn how to find a device’s MAC address, see the sidebar [What and Where is a MAC Address?](#) (p. 59).

Larger LAN: A base station often creates a LAN for computers connected to it. But in larger networks, the base station is connected via its WAN port to a “larger LAN”—despite the name of the port, this is a local network, but it typically has services that are passed through to the base station-connected computers. The larger LAN handles functions that an Internet service provider (ISP) would.

Often, the settings for an Apple base station are different when you connect it to a broadband modem and the Internet—a simple WAN connection—than when you connect the base station to a larger LAN.

Internet Protocol (IP) address: An *IP address* is a number assigned to a network interface, like an Ethernet card or a Wi-Fi radio, that allows it to be identified uniquely on a local network or the Internet. A device needs an IP address in order to interact with Internet services such as an email server or a Web site.

Private IP addresses: *Private IP addresses*, also called simply *private addresses*, are assigned in LANs from a pool of globally reserved IP address prefixes. Private addresses are not reachable or routable from outside the LAN without extra work: Internet-connected computers can’t directly address private IP addresses, and require an intermediary to help (see Network Address Translation, below).

Public IP addresses: *Public IP addresses*, also frequently called *public addresses*, are drawn from the global pool of IP addresses that can be routed, or reached, from any other computer on the Internet. These are colloquially called *real IPs*. (Public addresses access can be restricted through firewalls, however.)

Network Address Translation (NAT): *NAT* provides a work-around that lets computers outside a LAN reach privately addressed computers inside a LAN. NAT maps outgoing connections from computers within the LAN to an address on the WAN side of a router,

allowing a response to that outgoing connection, like a Web page being requested and retrieved. NAT can also map in the other direction. I discuss how this mapping can be safely controlled in [Map Ports for Remote Access](#). A NAT gateway is not a firewall, although it's often marketed as one.

Dynamic Host Configuration Protocol (DHCP): DHCP is used to assign IP addresses to computers and other equipment on a network. Any device that can connect to a network has a DHCP client built in, and that client can request and retrieve an address from the network gateway.

The AirPort base station has a DHCP server to provide this function. The base station also has a DHCP client that operates on its WAN port to request an address—if necessary—from the higher-level network to which it is connected.

In some cases, the DHCP server in the base station is redundant and needs to be turned off to avoid interfering with other elements of a network. In other cases, you might disable a computer's DHCP client so that you could enter a fixed IP address. DHCP and NAT are often used together: NAT allows a private address to reach the Internet; DHCP assigns that private address to a computer or other networked device.

LEARN WIRELESS AND AIRPORT BASICS

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

Access Points and Adapters

AirPort and Wi-Fi networks need two connected parts: a wireless adapter and an access point. The wireless adapter is part of a computer or mobile device, while the *access point*, in many ways, works just like an Ethernet switch. An access point that's coupled with a router is called a *wireless gateway*; Apple's wireless gateway is called a *base station*.

NOTE You might have heard of 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 connotes *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.

NOTE An *AirPort network* is a Wi-Fi network with some Apple extras that may work only with Apple software—under Mac OS X, or Windows XP or Vista—or in conjunction with other AirPort equipment. Examples of such features include streaming audio, hard-drive sharing, and base-station-to-base-station connections.

The wireless adapter uses client software on the computer or hand-held device to connect to a specific base station (or set of affiliate base stations) after a user selects a network name from a list or manually enters the network's name. Mac OS X allows network selection from the AirPort menu in the menu bar, the AirPort pane of the Internet Connect program (located in the Applications folder), and the AirPort view in the Network preference pane.

When a wireless adapter connects—technically, *associates*—with a base station, the device to which the adapter is attached can send data to and from the base station. If the base station has encryption enabled, then an encryption key must be provided before the base station allows the device access to any networks to which it connects.

Depending on your setup, the key, a series of characters, must be entered exactly as it was entered on the base station. A stored key can be sent without a person having to re-enter it.

Avoid entering an encryption key manually: *The AirPort Extreme also now supports a simpler method that avoids key entry altogether. See [Use WPS](#).*

Once an adapter connects to a base station and the encryption key is accepted, the computer's operating system can carry out the next steps, such as automatically requesting an Internet protocol (IP) address using DHCP and sending data over the wireless network.

The Spectrum Part of Wi-Fi

Wi-Fi networks use *unlicensed spectrum*, so called because regulatory agencies don't require users to obtain a license to use those airwaves, and everyone may use that spectrum; cellular telephone companies, by contrast, pay huge amounts for the exclusive geographic rights to certain frequencies.

Unlicensed *bands*—specified ranges of frequencies—are divided into smaller upper and lower bounds called *channels*, which allow many devices to use the same band within “hearing” distance of each other, but without overlapping any or all the frequencies they employ. However, unlicensed bands are intended for broad use by individuals and businesses, and there's no guarantee that you and other people won't produce interfering signals, reducing the speeds you can achieve.

The rule is that in these unlicensed bands, devices use extremely low signal power, but they also must be quite robust in order to cope with lots of interference while still functioning.

In the United States and in most countries, the 2.4 GHz (gigahertz) and 5 GHz bands are available for use. (The 900 MHz [megahertz] band is also unlicensed in the United States, but it is not employed for wireless LANs.) The precise frequencies and channels vary enormously by country. Older AirPort equipment could work only in the 2.4 GHz band; the 2007 version of the AirPort Extreme and the 802.11n protocol can use either the 2.4 or 5 GHz band.

Warning! *Apple and other manufacturers limit the usable channels and power output levels of Wi-Fi devices to what's legal in the country in which the gear is sold. Using that equipment outside the country of purchase without first checking on what's legal could result in fines or jail time.*

NOTE In some countries, the 4.9 GHz band is used instead of the 5 GHz band; in the United States, 4.9 GHz is a restricted band, partly devoted to fire, emergency, and police digital communications.

Wi-Fi and AirPort Flavors

AirPort hardware has gone through many transformations since its original 1999 introduction. Each major flavor of Wi-Fi that Apple has built into AirPort gear relies on industry standards created by the IEEE, the Institute of Electrical and Electronics Engineers. The IEEE has groups that work on many different kinds of standards. Their 802 group handles local area networks (LANs), and a working group in that area, numbered 11, covers wireless LANs (WLANs). This is called the 802.11 Working Group.

Each successive update to the standard produced by the 802.11 group is lettered and defines a particular set of codified ideas. For instance, the original popular flavor of Wi-Fi was known as 802.11b or just “B” for short. The current fastest generation is known as 802.11n or “N,” and is still being finalized even as Apple and others have released equipment that uses a draft of the standard, often called “Draft N” (see [Not yet finished](#), for more detail).

The Wi-Fi Alliance takes those IEEE standards and builds tests that allow different makers to ensure that they are creating equipment that works with all the other manufacturers' equipment and that carries out a common set of tasks in the same way.

Since the original AirPort in 1999, Apple has released three major versions of AirPort hardware, which correspond to three major revisions of the IEEE 802.11 standards (**Table 1**, next page). Every older version can be used with even the newest flavors. Let's look at those older flavors, briefly, and then focus on Apple's newer 802.11n gear.

Table 1: Wi-Fi Standards in Apple Hardware			
Standard	Apple Equipment (introduced, discontinued)	Raw Speed	Maximum Throughput
802.11b (B)	<ul style="list-style-type: none"> • AirPort (1999, discontinued 2003) • AirPort Card (1999, discontinued 2004) 	11 Mbps	5.5 Mbps
802.11g (G)	<ul style="list-style-type: none"> • AirPort Extreme (2003, discontinued 2007) • AirPort Extreme Card (2003, superceded by built-in adapters, but not discontinued at this writing) • AirPort Express (2004) • Built-in 802.11g adapter in Macs (2005) • iPhone (June 2007) 	54 Mbps	25 Mbps
802.11n* (N or Draft N)	<ul style="list-style-type: none"> • AirPort Extreme (Feb. 2007) • Apple TV (Feb. 2007) • AirPort Extreme with gigabit Ethernet (Aug. 2007) • Built-in 802.11n adapter in all current model desktop, laptop Macs (late 2006)** 	300 Mbps	90 Mbps (with Feb. 2007 base station) 140 Mbps (with gigabit model)
<p>* Current draft became a tested part of Wi-Fi in June 2007; final version is due in September 2008 in a very similar form.</p> <p>** Intel Core 2 Duo Macs except discontinued 1.83 GHz iMac and all Mac minis; optional adapter for the Mac Pro.</p>			

Original AirPort (1999)

The original AirPort system uses 802.11b, and it comprises an AirPort Card, which fits into a card slot in all AirPort-capable Macs released through 2002; and an AirPort Base Station, which resembles a small, gray (“graphite” original) or white (“snow” revision) flying saucer.

The graphite base station has a single Ethernet port and a built-in modem; you couldn’t connect the graphite model to an Ethernet LAN and WAN at the same time. The snow base station added a second Ethernet port, which increased security and flexibility by allowing

you to separate a LAN from a broadband or wide area network (WAN) connection via a cable or DSL modem.

AirPort Extreme (2003)

AirPort Extreme 2003 uses the 802.11g standard. AirPort Extreme originally appeared in two components: the AirPort Extreme Card that fit into a new kind of internal card slot, and the AirPort Extreme Base Station. The Base Station has the previous generation's spaceship shape, is translucent white, and has three white LEDs for status on the front.

Apple started adding the Extreme card slot to Macs released starting in January 2003, and completed the transition by September 2003. By 2006, all Macs included AirPort Extreme as a built-in feature except for the Intel Xeon Mac Pro, which has the option to be factory equipped with Wi-Fi, and the Xserve, which is designed for server rooms. (Bluetooth came to be included in all but those two models, too, by 2006.)

Apple quietly added 802.11a—which uses a different frequency band and is explained later—to the Intel line of Macintoshes, but never explicitly advertised this fact or offered support. See [Apple's version of 802.11n](#) for why this is useful.

***Card or built-in?** Apple moved from offering Macintoshes with an AirPort Extreme card slot to including Wi-Fi onboard—but they still call the technology AirPort Extreme, and they still sell the standalone card for older Macs.*

AirPort Express (2004)

The AirPort Express Base Station, which started shipping in July 2004, is similar to the AirPort Extreme Base Station, but it supports fewer users and can stream music to a stereo. A single yellow/green LED shows the unit's status. The Express is still sold as this book goes into production.

AirPort Extreme (2007)

At Macworld Expo 2007, Apple quietly moved the AirPort Extreme Base Station from 802.11g to 802.11n. They announced that most current Macs could have 802.11n enabled through a firmware update, and they revealed a new AirPort Extreme that started shipping in February 2007. This unit had just 10/100 Mbps Ethernet built in.

In August 2007, Apple released an updated unit, keeping the same name but adding gigabit Ethernet.

Because Apple has unfortunately kept the name the same for both of these new units, to avoid confusion, I call the new base station models collectively “Extreme N” where Ethernet speed doesn’t matter. When Ethernet makes a difference in performance or features, I call the February 2007 model “Extreme N (original)” and the August 2007 model “Extreme N (gigabit).”

This new base station has a square footprint, is squat, and is designed to be stacked, making it easy to distinguish visually from the spaceship shape of previous base stations.

Extreme N Details

Let’s learn more about the new Extreme N base station and Extreme N AirPort adapters.

802.11n technology

802.11n is up to seven times faster than G in typical circumstances when measuring real data passed over a network. N uses several antennas, with at least two receiving and two transmitting data, as well as multiple radios. Each radio can transmit data while varying the amount of power on each transmitting antenna, thus steering the radio beam. This allows signals to go farther, and allows multiple simultaneous data streams—each radio sending a unique set of data at the same time over the same frequencies!

Each incoming signal is “heard” by two or more antennas, making it easier to pick up more distant transmissions and to tease out the wheat (data) from lots of chaff (other, interfering signals and background noise).

These techniques allow 802.11n to have a raw data rate of 300 Mbps in a basic version and up to 600 Mbps in advanced versions. The Extreme N and other consumer gateways will almost all use the 300 Mbps speed, which can pass as much as 150 Mbps in real data.

The speed drops when other Wi-Fi networks are in use in the vicinity, when older 802.11 devices are used on the same network, or when N adapters are far enough away from the base station to require slower transmission rates.

Not yet finished

An important proviso when discussing 802.11n is that the standard isn't finished. As with some earlier 802.11 standards, the work has taken so long in the IEEE 802.11n task group that companies and the Wi-Fi Alliance have moved forward while the details are being settled. That led to a lot of equipment working at its best speeds only when exchanging data with other devices made by the same company *and* using the same Wi-Fi chips.

Draft N, as it's known, spent 2006 in limbo, while companies and engineers engaged in horse trading in order come up with something the whole industry liked. Draft 2.0 was accepted by the IEEE's wireless networking group in March 2007, and the Wi-Fi Alliance developed a set of interim interoperability tests in June 2007 to certify equipment as complying with Draft 2.0.

Most major hardware vendors have had pre-production versions of their Draft N hardware approved by the Wi-Fi Alliance to carry their Draft N seal of approval. However, the testing happens on engineering models; firmware still must move into production and then be released as updates by hardware makers.

In early September 2007, Apple released its certified Draft N firmware update for Extreme N. By the time you read this book, many other companies' products should also have certified Draft 2.0 firmware available for download. That new firmware should, in turn, allow the highest possible speeds among all Draft 2.0 gear.

Apple's version of 802.11n

The Extreme N is the first base station released by Apple that supports both major frequency bands for Wi-Fi: 2.4 gigahertz (GHz) and 5 GHz. While 2.4 GHz is better known, and has been used by the original plain 802.11 spec, as well as B and G, the 5 GHz band has been available for some time, waiting for the right technology to make use of its wide-open spectrum.

NOTE A little-used 802.11 protocol known as 802.11a, or “A,” was famously declared dead by Steve Jobs in January 2003. The A protocol never took off because while it had the advantage of using the 5 GHz band, it wasn’t backward compatible with the popular B protocol, which is still in wide use. Some organizations chose to use A for voice over IP (VoIP) for that very reason: they could use the 5 GHz band with little interference.

Apple slipped 802.11a into the Intel versions of its Macs without advertising the fact because the Intel chips Apple used included 802.11a at essentially no additional cost. Since there were so few 802.11a base stations available—almost none for consumers—the fact seemed unimportant.

The 5 GHz band in the United States offers 23 non-overlapping channels for 802.11a/n; whereas the 2.4 GHz band offers only 11 staggered, overlapping channels for 802.11b/g. Further, the 5 GHz band has many fewer users.

***Tune in tomorrow:** Apple has chosen to allow use of just eight of those 5 GHz channels at present, but future firmware could easily up the total to 23. The company told me in August 2007 that they are investigating adding more channels but had no specific plans nor timetable. When and if that happens, I’ll post information on this book’s update page; click the [Check for Updates](#) link on the [cover](#) to visit that page.*

***Warning!** Apple sells specifically tailored versions of its Extreme N for different parts of the world. This is especially significant due to how the 5 GHz band is regulated in each country. If you buy a North American Extreme N and take it to, say, France, as one of my colleagues did, when you power it up, you’re likely in violation of local law. If you happened to tread on local uses, including military purposes, you could be found (via triangulation) and spend some years in jail.*

Apple could have supported just 2.4 GHz in the new 802.11n gear for backward compatibility, but instead the new gear supports both bands, which offers a lot of potential for maximizing the speed of a network, even in the home. (See [Mix Legacy, New N Networks](#).)

Physical features

The latest base station (**Figure 1**) is square, designed for stacking, with the same footprint as a Mac mini (6.5 inches/16.5 cm square), and a smaller footprint than the Apple TV (7.7 inches/19.7 cm square). (The Apple TV is 1.1 inches/2.8 cm tall; the Mac mini, 2 inches/5.1 cm; and the Extreme N, 1.3 inches/3.4 cm.)

FIGURE 1



The tilted front view (left) and straight-on back view (right) of the AirPort Extreme Base Station introduced in 2007. The back ports are, left to right, power, USB, one WAN Ethernet jack, three LAN Ethernet jacks, and a security slot for physical lock-down.

The Extreme N base station is the first to offer an Ethernet switch; Apple included four Ethernet ports, three of which are used for the LAN and one for the WAN. The Extreme N (original) included 10/100 Mbps Ethernet. The N standard can outstrip 100 Mbps Ethernet, which achieves somewhere over 90 Mbps of real throughput. That's the reason why in August 2007, Apple released the Extreme N (gigabit) with 1,000 Mbps Ethernet on all four ports. In the process, Apple improved throughput in nearly every configuration I tested.

Hardware, not software: *Before you ask, the earlier Extreme Ns can't be upgraded to support gigabit Ethernet. Okay, it's a reasonable question, given that Apple's 802.11n was included but not turned on, in some Macs. To add gigabit Ethernet, Apple used different chips in the second model of the Extreme N.*

Fastest method: *If you really need speed, gigabit Ethernet is far faster and simpler than Wi-Fi, with the only downside being the requirement for wires. Ethernet switches can deliver nearly seven times the throughput of N between any two connected gigabit Ethernet devices in both directions. In contrast, Wi-Fi is limited to half its maximum speed when transmitting data between two Wi-Fi devices on the same network.*

Adapters in Macs

Starting around the end of the third quarter of 2006, Apple began introducing new Mac models that secretly included 802.11n wireless chips. Apple didn't tell customers or enable the faster N mode, so the Macs behaved like they had a G card inside. Apple was apparently waiting for the standard's progress to be clear before switching on the new 802.11n capabilities. (Clever buyers who cracked their Macs open figured this out long before Apple made it official.)

This set of computers comprises:

- All Macs with Wi-Fi adapters and Intel Core 2 Duo processors—except the 17-inch, 1.83 GHz iMac , which was discontinued in August 2007, and the Mac mini. (Those exceptions have 802.11a, however.)
- The Xeon Mac Pro, if you chose the wireless add-on option.

Enable your Mac! *Apple didn't start enabling 802.11n on Macs until as late as third-quarter 2007. So, depending on when your Mac entered the retail channel, it may, or may not, need you to enable 802.11n. (Find out if your Mac needs to be enabled in the sidebar [Do You Need the 802.11n Enabler?](#))*

To enable a Mac, you must install the AirPort Extreme 802.11n Enabler for Mac. You can install it from the CD that ships with the Extreme N, as I describe in [Install new software](#). You can also buy it from the Apple Store separately for \$1.99. Once you own a copy of the enabler, you can use it on “all computers under your ownership or control,” as Apple's licensing terms put it.

Third-party adapters

Apple didn't offer—and never will offer—N on the separately installable AirPort Extreme Card. About 3 years ago, Apple began including the 802.11g AirPort Extreme as a basic design feature on new Macs. Without Wi-Fi being on a separate card, Apple had little motivation to provide an upgrade. They'd rather you buy a newer computer, if you really need 802.11n.

Third parties are starting to step up to the plate, however, with QuickerTek the first out of the gate and Other World Computing following at their heels.

QuickerTek

The company has released several adapters in its nQuicky series and under other names (<http://www.quickertek.com/>). Some options remain expensive (at this writing) because of the higher engineering cost and higher chip costs associated with N right now. Expect prices to drop. The nQuicky models and the nNano all support just 2.4 GHz, which reduces potential throughput.

The nNano is a \$59.95 USB adapter that works with all Macs running Mac OS X 10.3 or higher; they're also offering the \$49.95 Nano, which is 802.11g only, useful for Macs that could otherwise operate only at 802.11b speeds with a hard-to-obtain original AirPort Card.

The nQuicky USB (\$149.95), nQuicky PCI (\$99.95), and nQuicky CardBus (\$64.95) all require Mac OS X 10.3.9 or later. The USB model works with any Mac, and it has a much higher-gain antenna than the nNano; the PCI works with all Power Macs (G3, G4, and G5) except the G5 models that use DDR2 (double data rate, 2nd version) memory; and the CardBus adapter supports any PowerBook.

For Intel Macs issued without Draft N hardware, QuickerTek offers hardware updates that require opening a case and messing about. They'll also perform the upgrade for you. Prices for the kit and the mail-in install (exclusive of return shipping) are: MacBook or MacBook Pro, \$99.95/\$149.95; Mac mini or iMac, \$179.95/\$199.95.

Finally, if you have a Mac mini, QuickerTek offers a kit and mail-in install (\$149.95/\$199.95) that swaps in 802.11a for 5 GHz and 802.11n for 2.4 GHz. It's an odd option, but could be useful.

Other World Computing

Other World Computing has also released a set of 802.11n adapters that work in the 2.4 GHz band: a PCI Card for Power Macs, a PC Card for PowerBooks, and a USB adapter for any Mac that can run Mac OS X 10.3 or later (<http://eshop.macsales.com/shop/wireless/>). All three adapters in their Edimax nMax series cost \$67.99, and work with Windows XP/2000 and later, too.

A unique aspect to the Edimax adapters is that they support wide channels in 2.4 GHz. Because Apple doesn't offer wide 2.4 GHz channels, you would need a Wi-Fi gateway from another company to take advantage of that option, which isn't considered particularly advantageous in 2.4 GHz, anyway.

More coming soon

I expect that other vendors will add Mac OS X drivers, too, as many have with each previous generation of Wi-Fi hardware. Belkin, a stalwart provider of Wi-Fi and other peripherals with Mac OS X drivers, told me fairly strongly that Mac OS X drivers are coming for their equipment. Ralink is likely, too, as are firms that resell products using Atheros chips (Atheros is Apple's chip supplier for Wi-Fi).

Compatibility among AirPort Generations

Each AirPort generation is backward compatible with all previous generations, although backward compatibility can be turned off. While the original AirPort handled just 802.11b, AirPort Extreme 2003 added 802.11g, which incorporates B with full support. Likewise, Extreme N's 802.11n handles the older A, B, and G standards.

However, transfer speeds between an adapter and a base station running different 802.11 standards can't exceed the speed supported by the slower of the two 802.11 flavors that both devices share. A B device connecting to an N base station communicates at B speeds, meaning that each packet of data a B device pushes through the network occupies the equivalent of 10 to 20 N packets.

While most of the loss in throughput happens only while older devices are taking up airtime (and newer devices are cooling their heels), simply enabling backward compatibility shaves at least 10 percent off the maximum throughput of the network. This overhead comes from the fact that every computer on the network must send extra traffic that's designed for older devices to interpret.

NOTE Wi-Fi gateways can force older adapters to talk less. In one method, an 802.11n gateway would use an existing mechanism that all the standards understand to grab an equal amount of time as a B device, rather than an equal amount of data. These mechanisms aren't standardized yet, and it's unclear if Apple has implemented any of them. In the future, it's likely that we'll see this kind of protection against older devices hogging a network.

One way to avoid bogging down an N network is to set the N network up as a new, separate entity, leaving an older, slower B or G network in place. I discuss how to set this up in [Mix Legacy, New N Networks](#).

PUT YOUR BASE STATION INTO ACTION

You're ready to set up your network, so let's get unpacking! This section focuses on initial setup, and in many cases it will take you to a working Wi-Fi network. But, if you need to go beyond the basics, you can keep reading beyond this section to learn about special cases in configuring your local and wider network connections. Also, note that [Connect Your Computers](#), later, explains how to connect via Wi-Fi from any computer in the vicinity to the newly set up base station.

TIP MULTIPLE HOPS TO THE INTERNET

Although one base station must be connected with Ethernet to your Internet connection, you can connect AirPort Extreme—both G and N models—and AirPort Express Base Stations wirelessly back to that main base station. For setting up these satellites, see [Bridge Wirelessly](#) for step-by-step details.

Set Up Your Base Station

Let's get that base station out of its box, plugged in, and ready to connect to the Internet.

Unpack and power your base station

The Extreme N comes with fewer parts than any previous Apple base station. Unpack the base station to determine what you have and if you need any additional hardware:

- **Remove your base station from its box and check the parts.** The Extreme N box includes just a few necessary parts: The square base station, a CD containing utility and enabler software, and a power adapter and its corresponding AC power cord. The base station no longer comes with a wall-mounting bracket; it's designed to work horizontally.
- **Is the power cord long enough?** The power cord's length—17 feet/5.2 m—should aid in placement; in the American version, the AC end of the cord terminates in a non-polarized two-prong plug—both prongs are the same width—which can work in any outlet in either orientation. That still may not be long enough, so plan on purchasing a lightweight extension cord if you need to place the base station more than 17 feet/5.2 m from an outlet.

This model doesn't have a wall-mounting bracket because it works best level on a table or floor. (For now, your goal is to plug the base station in where you can set it up, though you may wish to skip ahead and read [Pick the Right Place for Your Base Station](#) before you continue.)

- **Get Ethernet cables.** The Extreme N, unlike its predecessors, comes with no network cables. Configuring your base station may be simpler if you hook it to your computer or existing LAN with an Ethernet cable, and you need at least one Ethernet cable in the likely case that you plan to connect the base station to a broadband router or other network. The Extreme N has auto-sensing, auto-switching Ethernet, which means you needn't buy particular kinds of Ethernet cables. I recommend [Cyberguys.com](http://www.cyberguys.com/) as a good online source for cables (<http://www.cyberguys.com/>).

Configuration Computer: *You'll be using AirPort Utility to configure your base station, and the steps I give shortly show screenshots taken on a Macintosh. To configure from a Mac, you must be running Mac OS X 10.4.8 or later. However, AirPort Utility can also be installed under Windows XP or Vista, and the steps are the same.*

Now it's time to power up. Plug your base station into an electrical outlet, and plug an Ethernet cable from your computer into any of the three LAN ports. If you'd rather have mobility while configuring, you can also set up the base station via Wi-Fi, but you will have to keep reconnecting after each configuration change if you change password and naming options.

Flashy: *In a neat addition, all the Ethernet ports on an Extreme N have a tiny green LED that lights up when an Ethernet cable is connected to the port and there is a live connection on the other end of the cable; the LED flashes to indicate activity. A front green/amber LED shows the status of the base station, including activity (green) or trouble (amber).*

I recommend not connecting your base station via the WAN (Wide Area Network) port to a broadband modem or the rest of your network until you've carried out more of the setup, especially the very next part.

Install new software

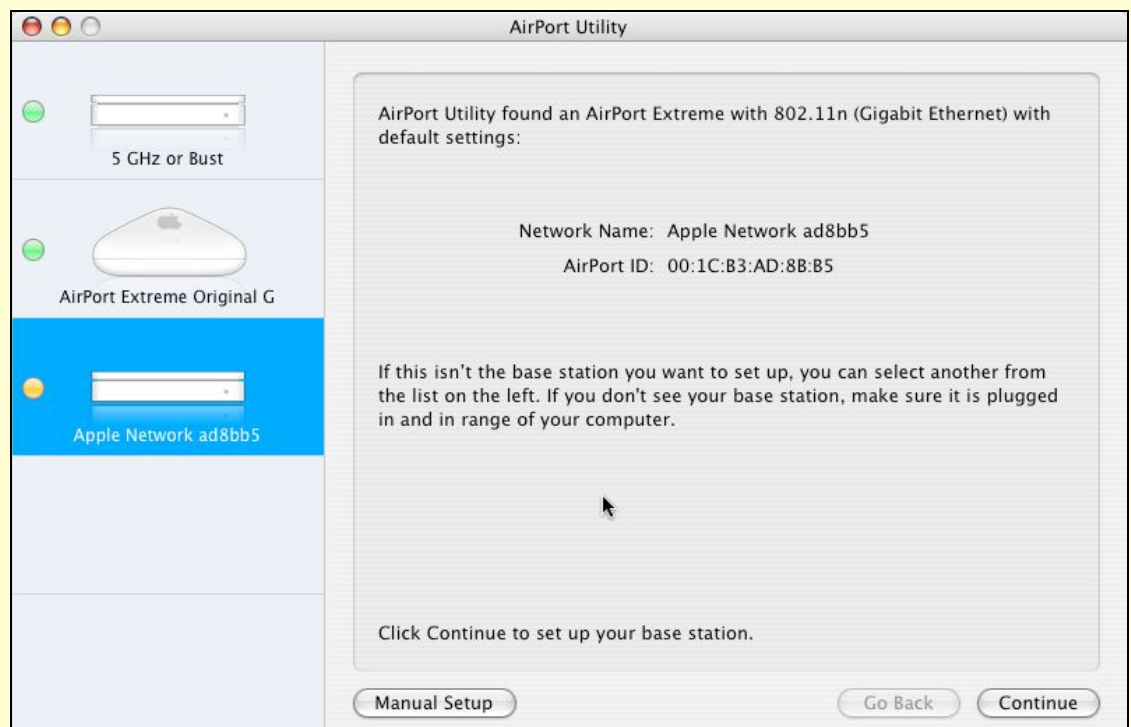


The Extreme N comes with a CD full of software: AirPort Utility, AirPort Disk Utility, and the 802.11n enabler for appropriately equipped Macs. The software isn't—at this writing—available for download from Apple's Web site. AirPort Utility replaces the hoary AirPort Admin Utility, which dates back to 1999; the new AirPort Utility combines a set of assistants with advanced configuration options (**Figure 2**). It can configure any AirPort Extreme or AirPort Express base station.

No advantage for older base stations: *AirPort Utility is different, not better, than the older AirPort Admin Utility. There's no particular reason for those of you without an Extreme N to use the newer software.*

TIP If you're still using an old graphite or snow base station, the AirPort Admin Utility isn't deleted; it's renamed AirPort Admin Utility for Graphite and Snow (find it in **/Applications/Utilities**).

FIGURE 2



The main screen of the new AirPort Utility.

On a Mac running Mac OS X 10.4.8 or later, or with Windows XP or Vista, run the installer on the CD.

While installing, on the Installation Type screen, you can click the Customize button to install individual utilities or components. The full installation includes:

- AirPort Utility, which you need to configure your Extreme N base station.
- AirPort Disk Utility (called AirPort Disk on the Custom Install screen), which lets you mount hard disks and partitions that are connected via USB to an Extreme N.
- AirPort Base Station Agent, a monitoring program that can alert you when there's a problem with an Extreme N on the local network.
- The 802.11n enabler, (it's called AirPort Extreme Drivers on the Custom Install Screen), which turns on the N support in Macs that have the correct chips. It's installed only on computers that need it. All newly purchased Macs that were described as including 802.11n are already enabled for that flavor of Wi-Fi; if you bought a Mac before August 2007, see the sidebar [Do You need the 802.11n Enabler?](#), next page.

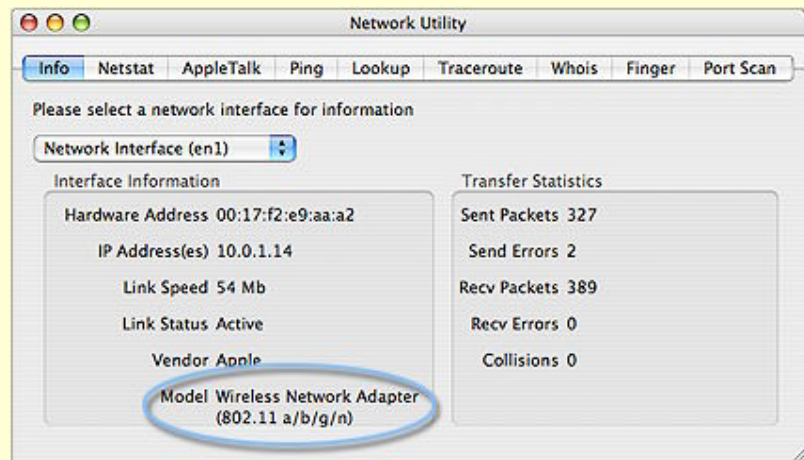
The last step of the installation is to restart the computer.

DO YOU NEED THE 802.11N ENABLER?

You can check if you need to install the enabler on your Mac by launching Network Utility from **/Applications/Utilities** and choosing the appropriate interface from the pop-up menu at the top of the Info pane, usually “Network Interface (en1)”. If the computer doesn’t require the update, “(802.11a/b/g/n)” appears under Wireless Network Adapter at the bottom (**Figure 3**).

If only “(802.11a/b/g)” is shown, run the enabler and restart, and then check Network Utility again.

FIGURE 3



Network Utility shows that the 802.11n enabler isn’t needed.

After restarting, you can find AirPort Utility and AirPort Disk Utility in **/Applications/Utilities**.

Run the installer on every computer on your network that has an 802.11n adapter that needs to be upgraded, from which you want to mount hard disks connected to the base station, or with which you want to configure the base station.

Launch AirPort Utility and let’s get this AirPort on the air!

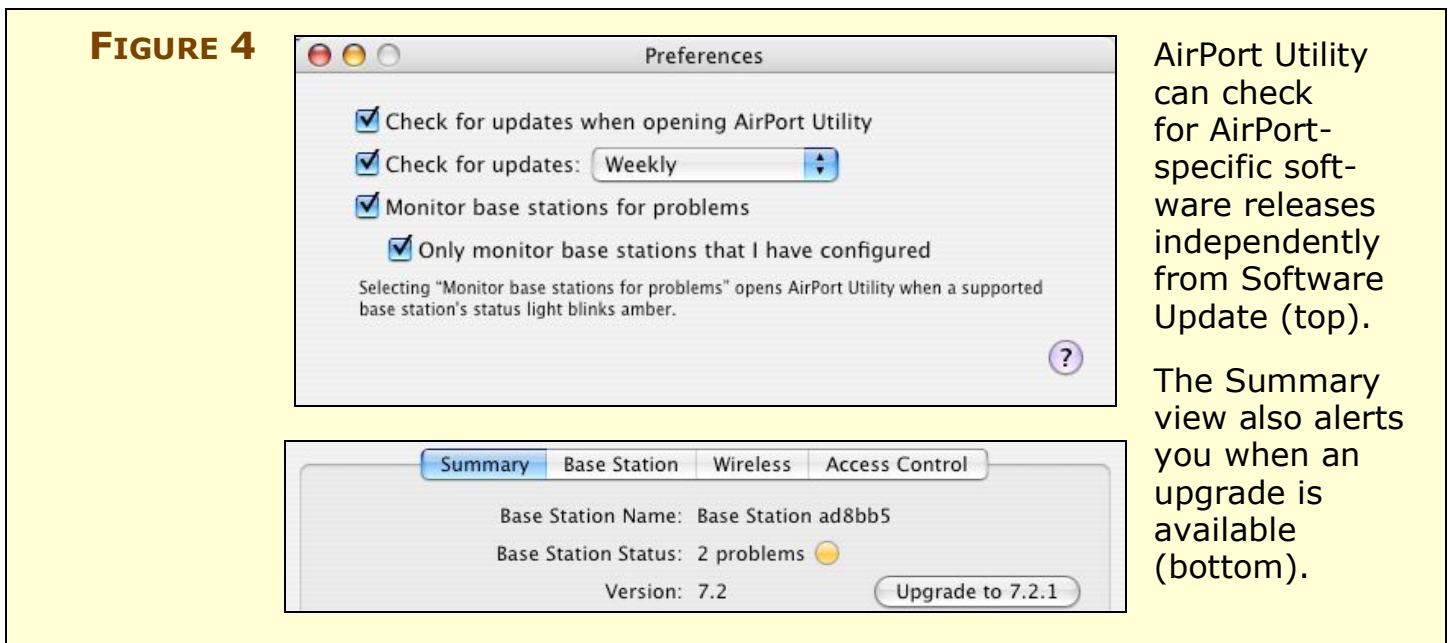
Keep up to date

The first time you run AirPort Utility, it prompts you to choose whether or not to check for updates automatically. Although Mac OS X’s Software Update feature (Apple > Software Update) will also alert you to install AirPort software and firmware releases, Apple set

up this separate update conduit to make it more likely that you would apply security, stability, and compatibility upgrades that you might otherwise ignore for a while in Software Update.

This update notification works whether or not you have AirPort Utility launched. The AirPort Base Station Agent, added as part of the AirPort Base Station Update 2007-002 (for Mac and Windows) in August 2007, monitors at the frequency you specify for updates, and then launches AirPort Utility if an update is available.

You can adjust the frequency for which updates are checked in AirPort Utility's Preferences dialog (**Figure 4**).

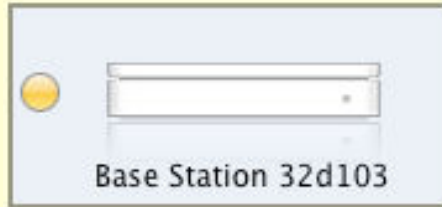


Connect to your base station

AirPort Utility is your one-stop shop for setting up the base station's parameters. But, first, you need to make a network connection to your base station so that AirPort Utility can access it. With AirPort Utility launched, use one of these three methods to find your base station; the methods are listed in order of simplicity:

- **Connect via LAN:** In the simplest case, you use an Ethernet cable to plug your computer into one of the three LAN Ethernet ports on the Extreme N. The unconfigured base station should appear in the left column of AirPort utility (**Figure 5**), confirming that you've made the connection.

FIGURE 5



An unconfigured base station appears in AirPort Utility's base station list named uniquely with the last six digits of its AirPort ID (see the note, "Default Network Names," below). (Dig the subtle reflection!)

- **Connect via a larger network:** For larger LANs, in which the base station is just a piece of the network, you can connect the base station to your larger LAN through the base station's WAN port, connecting an Ethernet cable from it to any port on an Ethernet switch on your network. Because the base station uses Apple's *Bonjour*, a way for devices to advertise their availability across a network, you should be able to spot the new base station in AirPort Utility even though it hasn't been configured. Failing that, try configuring with Wi-Fi.
- **Connect via Wi-Fi:** Slightly trickier is connecting via Wi-Fi, because many configuration changes require that you apply new settings by clicking Update in AirPort Utility. This restarts the base station and thus you have to reconnect to it.

From the factory, Extreme N is set to 2.4 GHz, so you can initially configure it via Wi-Fi from any computer. An unconfigured base station shows up with a default Wi-Fi network name in the AirPort menu (see "Default Network Names," below).

NOTE DEFAULT NETWORK NAMES

The default Wi-Fi network name for Extreme N base stations—as well as previous base station models—is **AirPort Network 0033FF** where **0033FF** is replaced with the last six digits of the AirPort ID of the wireless adapter in the Extreme N. The default Ethernet network name is **Base Station** plus a space and then the last six digits of the AirPort ID. That ID is printed on the underside of an Extreme N.

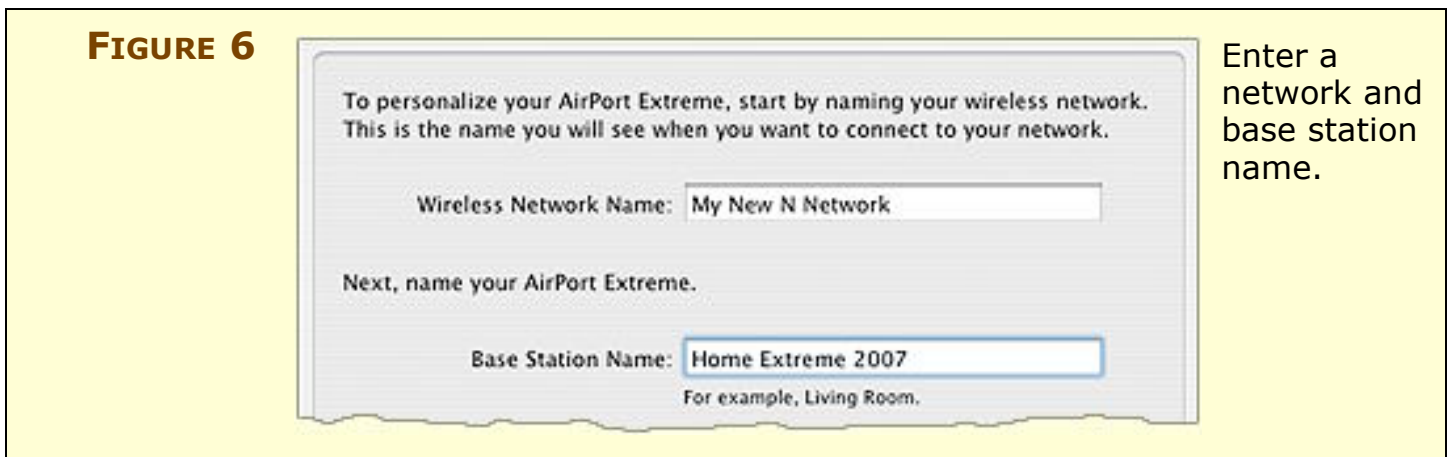
The AirPort ID is a MAC (Media Access Control) address. See [What and Where Is a MAC Address?](#) (p. 59) for more information about MAC addresses.

Handle initial setup

The simplest way to configure a base station is to use AirPort Utility's built-in assistant, which walks you through assigning a name to the base station, changing its administrative password, and turning on encryption. (If you are reconfiguring a base station, see [Reconfiguring a base station](#), ahead.)

Follow these steps to configure your base station:

1. In AirPort Utility, select the base station from the list of base stations at the left.
2. On the “Welcome to AirPort Utility” screen, click Continue to open the first Network Setup screen (**Figure 6**).

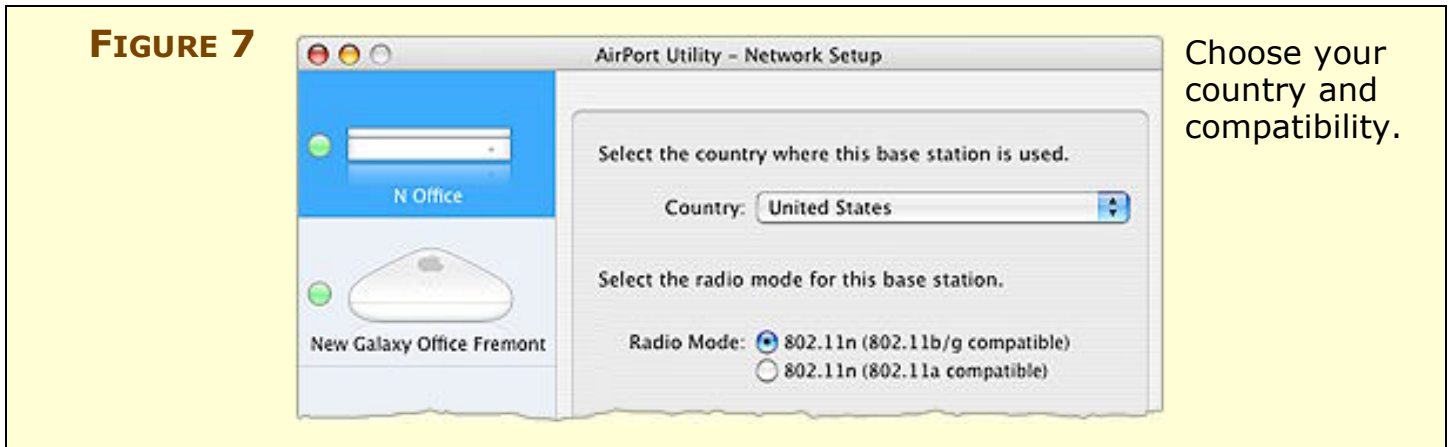


Screen names: *The assistant screens lack unique names; look in the title bar of each window for the name of the screen. I'll give you other cues, too.*

3. Enter a network name and base station name:
 - The network name will be “advertised” to Wi-Fi adapters that scan for networks to connect to; for instance, on a Macintosh the network name will appear in the AirPort status menu at the right of the menu bar. Multiple base stations may share the same network name to create a network with a larger area or more available bandwidth.
 - The base station name will be used to identify the base station in AirPort Utility.

Once you've entered both names, click Continue.

4. On the second Network Setup screen (**Figure 7**), choose the country in which the base station will operate and the backward compatibility you need, and click Continue.



Almost anyone reading this book will want to choose United States or Puerto Rico, and leave the radio button next to Radio Mode set to “802.11n (802.11b/g compatible)”. (For more about spectrum and country choices, see [Configure the Spectrum and Channel](#).)

Warning! Do not use the AirPort Extreme in a country that’s not listed in the Country pop-up menu. It’s not just a suggestion; national regulators monitor for misuse and you could wind up in the pokey, or worse.

5. On the third Network Setup screen (**Figure 8**), select the level of security you want to use:
 - WEP allows the oldest Wi-Fi adapters to connect to a network.
 - WPA2 is actually mixed WPA/WPA2 security, which allows Macs running Mac OS 10.3 Panther or later and computers with Windows XP SP2 or later to connect.
 - No security allows all connections.

Warning! Apple’s explanation on this screen about how WPA and WPA2 work is a little breezy, and it could frustrate you when trying to connect some older Macs to the network. The [Use Built-In Encryption](#) section can help you avoid that frustration.

Select your security option, and click Continue.

FIGURE 8

Select the level of security you want to use to protect your wireless network.

WEP (Transitional Security Network)
Provides security that is compatible with older WEP clients, but allows newer clients to join the network using WPA and WPA2. You must enter a password of exactly 13 characters.

WPA2 Personal (more secure)
Provides the maximum level of wireless security. Computers that support WPA or WPA2 will be able to join this network. You must enter a password between 8 and 63 characters.

No security
Any wireless computer can join your network without entering a password.

Wireless Network Password: [password field]

Verify Password: [password field]

Remember this password in my keychain

Set security to prevent unwanted users.

6. The first Internet Setup screen lets you choose how addresses are assigned on your network (**Figure 9**). The four options cover the major scenarios, which you then configure in the next step:

- **DSL or cable modem with static IP address or DHCP:** This is the right choice in almost every case.

Most broadband providers use DHCP to assign your base station an address automatically. (DHCP and the corresponding NAT feature are explained in detail in [Hand Out LAN Addresses](#).)

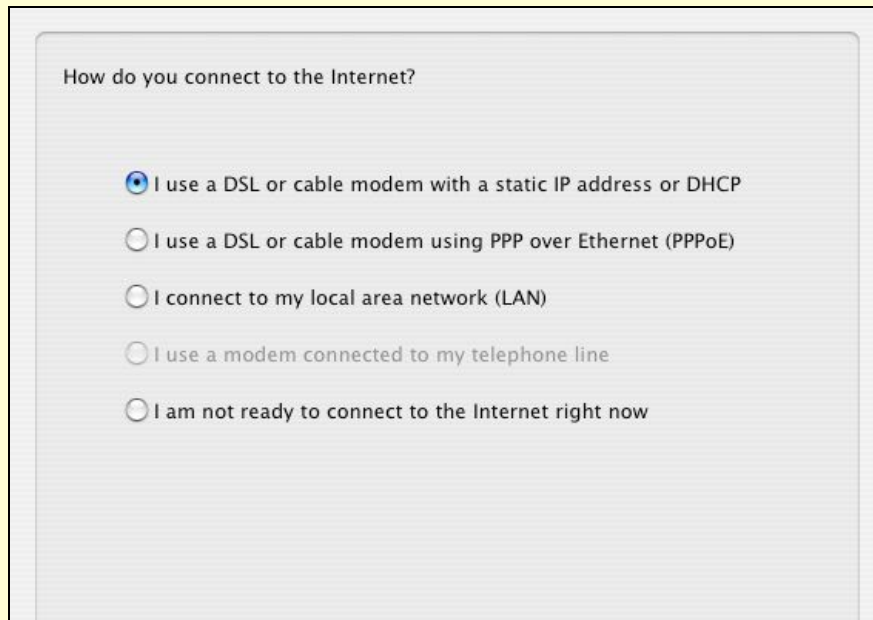
A static IP address requires additional manual entry. (A *static IP address* is a fixed IP address that your service provider provides to you.)

- **DSL or cable modem with PPPoE:** This option works with ISPs that use a special log in that the base station has to handle. The login process lets an ISP server assign an address (static or dynamic) to your base station.
- **LAN:** For larger networks, this is the right option, because you'll set up networking values based on what you chose yourself or use those provided by a network administrator.

- **Not ready:** Apple provides this choice so you can configure the rest of the settings without having to gather details for the Internet setup.
- **Modem:** A modem option appears but is dimmed for Extreme N base stations. If you're configuring an older Extreme G with a modem, that option's available.

Confirm your selection and click Continue.

FIGURE 9



Choose the kind of connection that's exactly or close to your set up.

7. In the second Internet Setup screen, configure the TCP/IP connection that allows your base station to access the Internet:
 - If you chose the first (DSL/cable with static or DHCP address) or third (LAN) option in the previous step, you have two choices:
 - ◇ If you aren't sure, or your ISP told you to, choose Using DHCP from the Configure IPv4 pop-up menu. This option is what most people choose.
 - ◇ If your base station is assigned a static address, with details provided by your ISP or network administrator, choose Manually from the Configure IPv4 pop-up menu.

- If your provider uses PPPoE, enter the account name, password, and optionally the service provider's name, while choosing to have the connection always on (default), automatic (connects when needed), or manual (connects when you choose).

For more details, see [Set Up Your Network](#). Click Continue.

8. The USB Peripherals Setup screen lets you set your initial password configuration for attached hard disks that can be shared via the Extreme N. For details on these choices, see [Set Up a Shared USB Disk](#). The preselected options are fine; click Continue.
9. On the AirPort Extreme Setup screen, set up a base-station password. This password is unrelated to network data encryption and protection, but it's vital to set the password to prevent unwanted access by others to the base station. The default base station passwords for all Wi-Fi routers are well known. Use a password that is simple, but hard to guess.

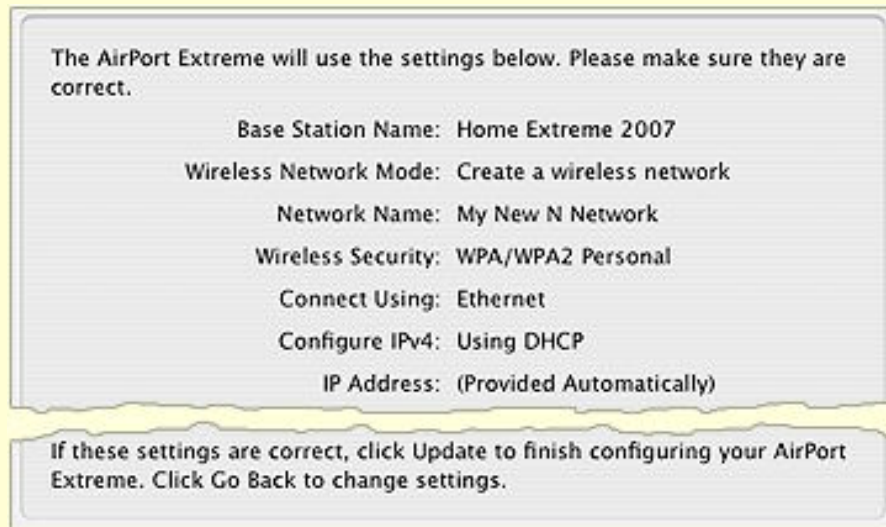
I recommend checking the Remember the Password in My Keychain option so that you can invent a password here and have the system store it.

Click Continue when you are ready to move to the next screen.

10. The Summary screen shows all your choices (**Figure 10**). You can click Go Back repeatedly to change options, or Update to store your options and restart the base station with those new settings. If you've forgotten the passwords you entered, click the Show Passwords button first to see them in plain text so you can copy them or write them down.

NOTE Whenever you click Update in AirPort Utility, the program sends your configuration changes to the base station, which burns those changes into non-volatile memory. Removing power from the base station doesn't cause it to lose these settings.

FIGURE 10



A summary appears, showing the choices you made during setup.

Reconfiguring a base station

You can reconfigure a base station that's already set up by selecting the base station in AirPort Utility and choosing Base Station > Assist Me.

NOTE HOW TO RETURN TO THE FACTORY DEFAULTS

You can reset an Extreme N to its factory settings at any time through software or hardware. Resetting the Extreme loses all settings you've applied, including passwords. If you save a configuration (see [Export and import configuration profiles](#)), you can load that configuration after resetting the base station.

Via software, launch AirPort Utility, select your base station, and choose Manual Setup or press Command-L. From the Base Station menu, choose Restore Default Settings. Click Restore in the dialog that appears and wait for the base station to restart.

If you can't connect to the base station or prefer the hardware approach, use a ballpoint pen or the tip of a straightened end of a paperclip to press the reset button for at least 5 seconds. The tiny reset button is on the Ethernet connection end of the Extreme, beneath a white right-pointing arrow in a field of gray.

Create and manage profiles

The Extreme N carries over a feature, first found in the AirPort Express, which allows you to define and *store* multiple *profiles*. A profile is a complete set of configuration parameters; each profile resides on the base station in non-volatile memory.

Stored versus exported profile: *I call this form of profile a “stored” profile to distinguish it from the “exported” profile described just below.*


These profiles can be useful when you’re sorting out precisely what options you want for your network and want to create different scenarios to test. Stored profiles are also useful if you take the base station to different locations.

I suggest starting with a base profile that you can duplicate to test other options, and then you can simply revert to it whenever you like.

Since you created the equivalent of a profile in following the steps (just previously) for initial setup of an Extreme N, you can rename that first profile to something descriptive and then duplicate it:

1. Select the base station in AirPort Utility, and then choose Base Station > Manual Setup (Command-L).
2. Choose Base Station > Manage Profiles.

The screen that appears lets you create, activate, and delete profiles.

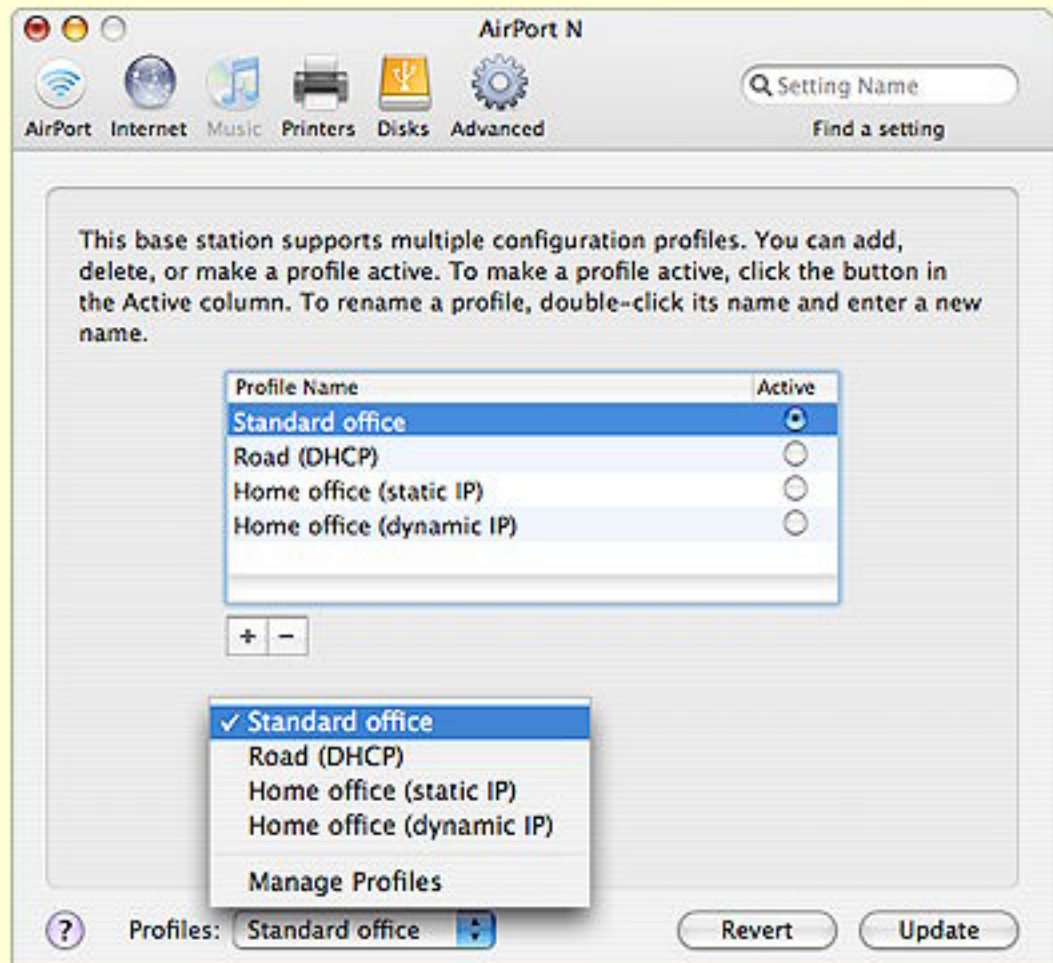
3. Click the  button to copy the current configuration to a new profile.

You should now see another profile in the list. The AirPort Utility also adds a Profile pop-up menu at the bottom of the screen.

4. Name the new profile: double-click the profile name to activate the edit field, and then type a new name. Press Return to accept the new name.

You can switch among profiles by choosing them from the Profiles pop-up menu at the bottom of the manage profiles screen (**Figure 11**). You must click Update to activate a given profile, or to save changes that you make to the active profile.

FIGURE 11



AirPort Utility lists stored profiles for a base station. To switch to a different profile, choose the profile's name from the Profiles pop-up menu and click Update to restart the base station and load that profile's settings.

Export and import configuration profiles

There's one more way you can work with profiles that you set up in AirPort Utility: you can export current settings to a file that can be imported later, for the same base station or for a different one. This is useful when you want to create a model configuration with the same network name, password, and other details, and then use it to configure many base stations.

Warning! Unlike stored profiles, these exported profiles do not reside on the base station. However, profiles can be exported and imported from any AirPort Extreme or AirPort Express base station; stored profiles are available only with the Extreme N and AirPort Express.

Management utilities will return: AirPort Management Tools lets you manage several base stations at once, including applying a model configuration file to them. However, it hasn't been updated at this writing for Extreme N. Apple told me it will be updated at some point—although they told me that in February 2007, and the tools hadn't returned when we published this edition in September 2007.

To export a profile:

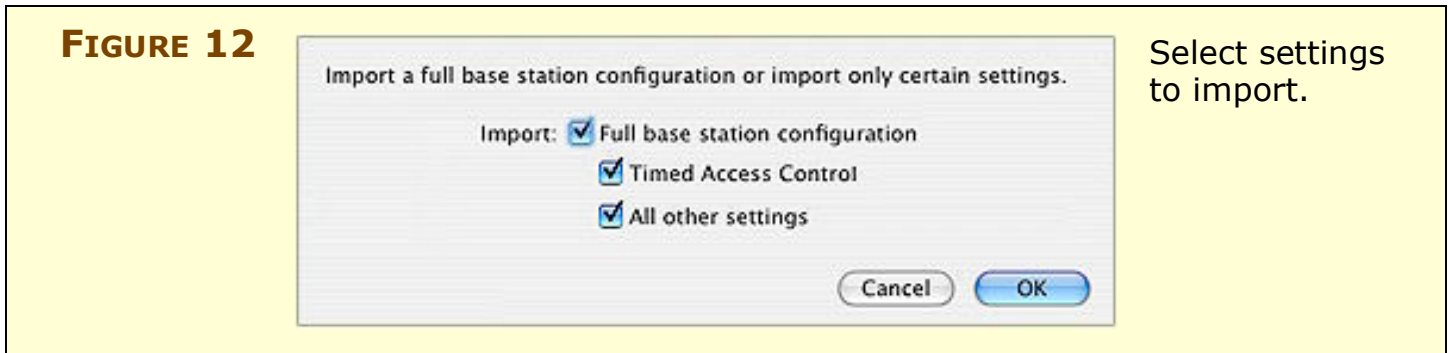
1. In AirPort Utility, select the base station from the list at the left, and choose Base Station > Manual Setup (Command-L).
2. Choose File > Save a Copy As, and name the file descriptively, as there will be few other clues that help you identify the file. (Apple should have named this option Export Profile, since that's the action the menu item carries out.)

After you've exported a configuration file, you can open it within AirPort Utility to examine the file's list of settings without applying those settings to an active base station. The settings appear in what looks like a standalone AirPort Utility configuration window, but you can't apply the settings against a base station from that window.

If you want to restore a base station to the settings in a file or configure a different base station in the same way, follow these steps to import the exported profile:

1. In AirPort Utility, select the base station from the list at the left, and choose Base Station > Manual Setup.
2. Choose File > Import. (See? For symmetry's sake, you'd like Apple to call the opposite operation Export!)
3. Select the configuration file and click Open.
4. Choose which options you want to import and click OK.

Extreme N includes timed settings, which can restrict access to given computers at given times of the day or week, and you can choose to import just those restrictions, all settings, or all settings except restrictions (**Figure 12**).



5. Click Update to apply the imported profile's settings.

Once the profile is imported, the settings replace your current base station settings. This could confuse you if you're also using stored profiles: the imported profile modifies the active stored profile. These changes take effect when you click Update.

TIP Importing just Timed Access Control settings lets you apply the same restrictions for use across all base stations on a network, while just setting those restrictions on a single base station.

Connecting remotely

You may want to set up remote access to your AirPort, so that you can configure it via its WAN port—either from a larger network to which the gateway is connected or elsewhere on the Internet. While there are some risks associated with that, remote connections also mean you can help, say, relatives, friends, or remote offices keep their networks running.

To allow remote access, follow these steps:

1. In AirPort Utility, select the base station from the list at the left, and choose Base Station > Manual Setup.
2. Click the Base Station button in the AirPort pane.
3. Check Allow Configuration over Ethernet WAN Port.

With remote access on, AirPort Utility can now access a remote Extreme N via its IP address or through a domain name if you've assigned that name through DNS (Domain Name Service). To make the connection, choose File > Configure Other and enter the IP address or domain name.

Secure connection: *I didn't know if AirPort Utility creates a secure, encrypted connection when you configure locally or remotely. I looked at a packet dump of raw data while configuring a unit, and saw nothing intelligible, which typically means that encryption is employed. I asked Apple, and they assured me that they did the right thing: you can enter a base-station password and configure over a local or remote network without fear of interception.*

Configure the Spectrum and Channel

With the Extreme N, you're faced with a choice: 2.4 GHz or 5 GHz? That choice makes a huge difference in the overall performance of your network, and how well it works with older machines.

Warning! *With all the talk of Extreme N supporting two frequency bands, you might have thought that the base station could work in both bands simultaneously. Not so; that would require duplicating the whole radio function. Instead, you could set up two separate, connected networks, one on each band; see [Mix Legacy, New N Networks](#).*

Consider your spectrum choices

The 2.4 GHz band is crowded with other Wi-Fi networks, Bluetooth devices, and other uses; 5 GHz is relatively empty—in the United States, the band has almost seven times the amount of frequency available in the 2.4 GHz band. Further, Apple restricts the use of so-called *wide channels* to the 5 GHz band. Wide channels use twice the standard amount of spectrum and thus can achieve twice the data throughput. Apple does this in order to avoid treading on older networks in 2.4 GHz.

In my tests comparing the two bands' *throughput*—the net amount of data passed over a network—I found that the 5 GHz band offered very consistent throughput as high as 140 Mbps (N to Ethernet LAN) and 90 Mbps (N to N) because there were few other variables to control, like other users or uses of the channels I tested. With 2.4 GHz, however, throughput was all over the place. I could test the same network setup over and over again, and sometimes see the highest rates (about 70 Mbps, N to Ethernet LAN), and other times see rates drop to 10–30 Mbps. See **Table 2** for specifics.

Higher Wi-Fi rates require Extreme N (gigabit): To achieve the highest speeds from the Extreme N, you must have the newer gigabit Ethernet model.

Table 2: Throughput Based on Band Choice (Best Speeds)		
Connection	2.4 GHz (regular channel)	5 GHz (wide channel)
Draft N to Draft N (same Extreme N)	Up to 35 Mbps (from one computer to another), but varies enormously	Up to 90 Mbps (from one computer to another); up to 50 Mbps with two computers transmitting to each other
Draft N to wired 100 Mbps Ethernet (LAN)	Up to 70 Mbps, but varies enormously	Over 90 Mbps
Draft N to gigabit Ethernet (LAN)		Over 140 Mbps
Draft N to any Ethernet (WAN) with NAT	Up to 50 Mbps*	
Any Ethernet (LAN) to any Ethernet (WAN)	Up to 70 Mbps*	
100 Mbps Ethernet LAN to same LAN	94 Mbps	
Gigabit Ethernet LAN to same LAN	900 Mbps	
* With NAT turned off, speeds are the same as Ethernet LAN.		

OTHER USES OF THE 2.4 AND 5 GHz BANDS

The 2.4 GHz and 5 GHz bands weren't empty before Wi-Fi networking came along. 2.4 GHz is known as a "junk band" because it's full of other approved uses that can conflict at times. Industrial sealers, for instance, use heating processes that emit 2.4 GHz radiation. Home microwave ovens use the principle that water molecules are dipolar (have two oppositely charged ends), and they switch the fields 2.45 billion times a second to cause friction which heats the food. (If your friends think microwaves "leak" radiation, create ionizing radiation, or "irradiate" food, please have them read this excellent Q&A page:

http://rabi.phys.virginia.edu/HTW/microwave_ovens.html.)

Problems with AirPort networks often stem from your own or neighbors' use of conflicting technology, which can include 2.4 GHz cordless phones, the above-mentioned microwave ovens, nearby industrial sites, or wireless cameras. The 5 GHz band has many fewer approved uses; primarily, 5.8 GHz cordless phones will be your enemy.

The rising interest in a new wireless standard called WiMax could be problematic. While WiMax will largely use licensed spectrum, there's plenty of interest and many early deployments that use the 5.8 GHz band to carry data from one central transmitter to many roof-mounted antennas.

You would think that the choice of using 5 GHz is obvious, right? Not so fast. If you have any 802.11b or g devices on your network—like Macs with the original AirPort Extreme built in—they can't connect. Or if a visitor were to show up with an older adapter, she would be out of luck. On the other hand, if you have all Intel Macs, you could use 5 GHz and mix A and N, which would provide much better performance than mixing G and N in the 2.4 GHz band. See **Table 3** (next page) for a comparison of the tradeoffs.

You can get the best of both worlds if you have an existing 802.11b/g network and want to add to the network, rather than replace it. See [Mix Legacy, New N Networks](#).

Table 3: Comparing the 2.4 GHz and 5 GHz Bands

Band	Pros	Cons
2.4 GHz	<ul style="list-style-type: none">• Backward compatible with 802.11b/g devices• Longer range than 5 GHz• Best for a network with a mix of B or G, and N Wi-Fi adapters• Third-party N adapters already available for Macs, but only in 2.4 GHz	<ul style="list-style-type: none">• Relatively crowded with other users, purposes, including 2.4 GHz cordless phones, Bluetooth• Maximum data rate is about 70 Mbps (Wi-Fi to wired) or 50 Mbps (Wi-Fi to Wi-Fi) only in the best conditions• Throughput can be very poor, connection erratic
5 GHz	<ul style="list-style-type: none">• Allows wide channels for higher throughput• Maximum data rate is 140 Mbps (Wi-Fi to wired) or 90 Mbps (Wi-Fi to Wi-Fi) in normal conditions• Relatively uncrowded, very large band, with lots of room to move to other channels• Backward compatible with 802.11a found in Intel Macs and some Windows laptops• No need to slow down for B devices• Best for all-new network with no visitors expected	<ul style="list-style-type: none">• Can't work with 802.11b/g devices• Higher <i>attenuation</i> than 2.4 GHz means signal strength drops faster when passing through walls, floors, even people• 5.8 GHz cordless phones and some unlicensed WiMax networks can interfere, reducing the number of possible channels

Second to choosing your spectrum is choosing a channel. The regular and wide channels I mentioned earlier are schemes to allow many networks to work together in overlapping locations. Regular channels use 20 MHz of spectrum; wide channels use 40 MHz.

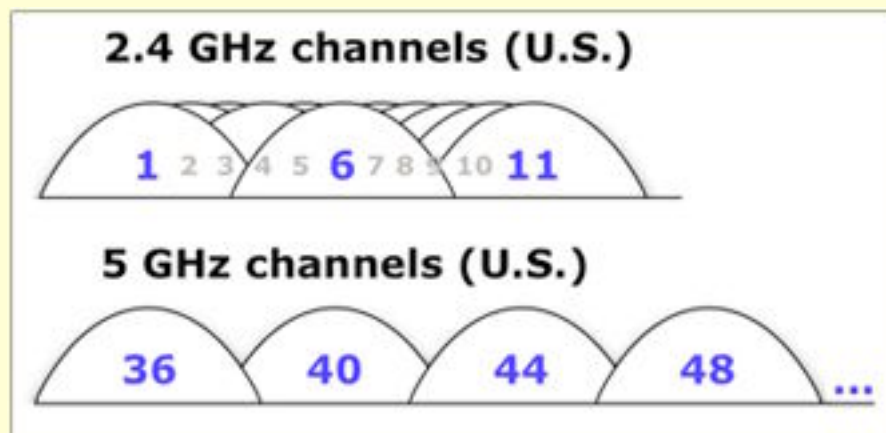
MHz and Mb: Megahertz does, in fact, correlate to megabits per second. Shannon's Law, a bit of information theory, says that there's a direct relationship that ties the width of a channel and the ratio of signal to noise to the achievable data rate. Twice the channel width means up to twice the raw data.

In case you were wondering, the formula is: maximum bit rate equals channel width in hertz multiplied by \log_2 multiplied by the sum of 1 + signal divided by noise.

In the United States, 802.11 standards can use any of 11 numbered, staggered channels in the 2.4 GHz band (**Figure 13**). Because these channels are staggered and overlap, only channels 1, 6, and 11 in the United States can be used in networks that overlap their coverage area when you want the least interference. (In some countries, the 2.4 GHz band is slightly wider, allowing for four non-overlapping channels.)

Also, due to the overlapping, staggered nature of the channels, there is room for only a single unique 40 MHz channel and a single 20 MHz channel to be used at the same time—and then only in ideal cases. This is why Apple didn't want wide channels in 2.4 GHz.

FIGURE 13



2.4 GHz 802.11 channels are staggered, with channels 1, 6, and 11 having the least overlap. 5 GHz 802.11 channels are meant to have little overlap; only the four lowest channels of 23 are shown.

By contrast, the 5 GHz band can be divided into 23 channels for 802.11a or n. The regular-width channels are the same 20 MHz width as 2.4 GHz band channels; or you can use 11 wide channels that are

40 MHz wide. These channels overlap only at the fringes, and thus allow many different networks to work in the same space with little interference.

NOTE Unlike the 2.4 GHz channels, which are numbered sequentially—1 to 11 in the United States—5 GHz channels jump by an increment of four and don't proceed sequentially. Why? Two reasons:

- First, 802.11 channels—for A, B, G, and N—increase by 1 for each unit of 5 MHz. Because 802.11a/n channels don't overlap, you get four numbers (20 MHz) between each regular-width channel.
- Second, there are four separate hunks of allotted unlicensed 5 GHz bandwidth. The first two (which comprise channels 36 through 64) are contiguous; we then jump to channels 100 to 136, and finish in 149 to 161. There's a 24th channel, 165, that's not supported in 802.11a or n.

Unfortunately, for reasons that are still not publicly stated, Apple has chosen to offer only 8 of the 23 possible 5 GHz 802.11a/n channels for use. The 15 that they aren't supporting have specific restrictions on use.

A few years ago, the IEEE developed 802.11h to allow the A spec to work in Europe. This 802.11h addition allows better co-existence between some existing uses of 5 GHz, like military radar, and it's become a necessary part of N as well. More recently, a compromise between the electronics industry and the military opened up 255 MHz of additional spectrum in the 5 GHz band—11 A/N regular channels—but using the additional spectrum requires that you use 802.11h not only for those new channels but also for four of the existing ones. Between European restrictions and the availability of more channels, it's even more peculiar that Apple has released a worldwide product without fully taking advantage of all the possible channels.

Apple's Wi-Fi chip suppliers support this co-existence. One chip vendor told me that Apple could add the missing channels through a simple firmware upgrade. Apple told me in August 2007 that they were actively investigating adding additional channels, but had no timetable or specific plan to do so.

Set a band and a channel

To configure which band you use, and what backward compatibility your base station offers, launch AirPort Utility, connect to your base station, and choose Base Station > Manual Setup. Click the AirPort icon to open the AirPort pane, and then click the Wireless button.

The Radio Mode pop-up menu offers four choices:

- **802.11n (802.11b/g compatible):** This mode allows full backward compatibility in 2.4 GHz, while allowing N to work at about 70 percent of its full speed in regular-width channels.
- **802.11n (2.4 GHz):** With this choice, your base station supports only N devices, and B and G devices can't connect to it.
- **802.11n (802.11a compatible):** This 5 GHz mode could be useful if you have all Intel Macs on your network and you want the advantages of 5 GHz's free-and-clear spectrum. You lose some speed when mixing A and N, but if you have the right set of machines, it's the best choice, unless you want to operate two networks. (See [Mix Legacy, New N Networks](#).)
- **802.11n only (5 GHz):** The best choice for 5 GHz networks.

Additional options: *If you hold down the Option key while choosing from Radio Mode, you see four additional options: 802.11b only, 802.11b/g compatible, 802.11g only, and 802.11a. These are provided in the interest of providing the most complete support for older networking gear, I'll wager.*

The Channel pop-up menu lets you choose a channel based on the band you selected. You are best off setting it to Automatic when you use the 2.4 GHz band. The Automatic option is the only apparent choice for 5 GHz. Choosing Automatic causes the base station to pick the least occupied channel when the base station starts up or restarts, but the base station doesn't change the channel while running—only after it has been restarted. To bypass Apple's Automatic mode for 5 GHz channels, hold down the Option key as you pop up the Channel menu.

Warning! “Least occupied” (previous paragraph) means least occupied by other Wi-Fi networks. In testing, even apparently “empty” channels were sometimes full of interference from other causes. While I couldn’t determine the cause, switching channels alleviated problems, but it required choosing a channel rather than relying on the Automatic setting.

Pick the Right Place for Your Base Station

When you walk around with a cell phone, the number of bars showing signal strength varies with the quality of the signal that the phone receives. 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 when you connect a computer to 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 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.

While the Extreme N uses MIMO technology—multiple sets of receiving and transmitting antennas—to cover a much greater area than its predecessors, the base station still has its limits. It’s just much closer to covering the area of a typical home than earlier units.

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 provide a name and a signal.

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 want to provide network access (see [Testing from base station to client](#), below). Also write down 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.

TIP The AirPort menu lists networks alphabetically. Hold down the Option key and select the menu, and Mac OS X re-orders the list by signal strength, from strongest at the top to weakest at the bottom.

- 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 Apple designed the base station to have its strongest performance parallel to the horizon. It doesn't come with a mounting bracket, perhaps Apple's way of emphasizing that you should keep it in a horizontal orientation.

NOTE All flavors of Wi-Fi work at speeds below their maximum rates as an adapter becomes more distant from the access point.

Testing from base station to client

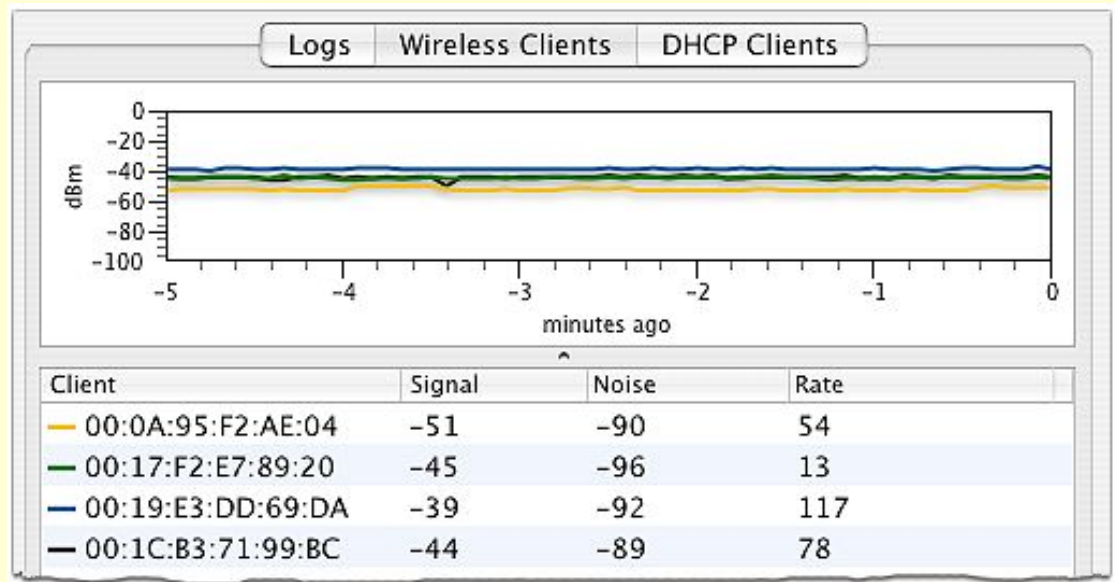
AirPort Utility now incorporates what was a separate Apple utility to monitor the performance of wireless adapters connected to a base station.

To view this monitoring tool:

1. Launch AirPort Utility, connect to your base station, and choose Base Station > Manual Setup.
2. At the top of the window, click the Advanced icon.
3. In the Advanced pane, on the Logging & SNMP view, click the Logs and Statistics button (located near the bottom).
4. Click the Wireless Clients button.

You can now check the performance of any devices connected to your base station (**Figure 14**). This nifty readout provides ongoing monitoring of the signal rate for each connected device. Each device is assigned a different color in the Client list beneath the graph, and that color corresponds to a line that tracks signal strength over time.

FIGURE 14



The graph at top shows the signal strength for each client. The bottom lists each client by MAC address, with the actual measurements for signal and noise, and the raw data rate.

The Client list shows connected devices by their unique adapter number. (For more on adapter numbers, see [What and Where Is a MAC Address?](#) on p. 59.)

For each client, the utility shows the signal and noise rates. The signal-to-noise ratio is an absolute measure of potential throughput. Signal and noise levels are measured in such a way that a negative number means below a certain threshold, rather than an absence of a signal or noise. Noise has a large absolute value, like -100; the larger the absolute value, the less noise. The signal should be negative, too, but have a lower absolute value, approaching 0; the closer to 0, the better the signal.

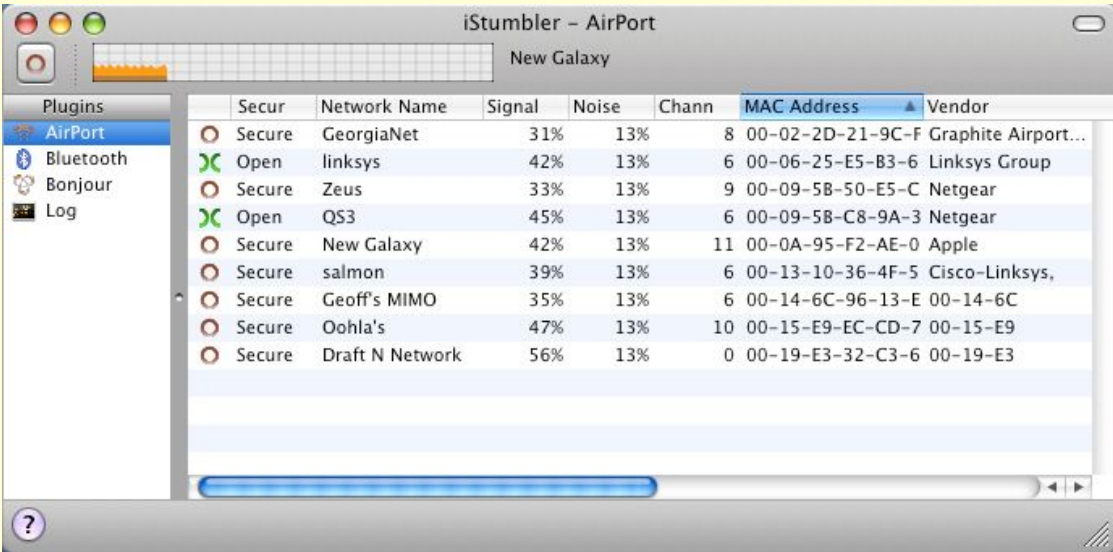
NOTE The label *dBm* on the left of the graph means *decibels below one milliwatt* (mW). Decibels are a logarithmic measure of power, and dBm defines how much signal strength was received below the nominal strength of 1 mW, a useful starting point for these kinds of signals.

The Rate column, however, has the most useful information: It shows the raw data rate, in Mbps, at which the client is connected. This is useful to know because you can have decent signal strength but be connected at a lower speed than the raw 54 or 300 Mbps maximum for 802.11g or 802.11n, respectively. The lower the connection speed, the more likely you need to tweak the base station's—or the computer's—position.

Testing from client to base station

The flip side when testing connections is measuring how strong your base station is from the computer you're trying to connect from. iStumbler (<http://www.istumbler.com/>) is my detector of preference. iStumbler provides a continuous scan with information about signal and noise for all the networks in your vicinity (**Figure 15**).

FIGURE 15



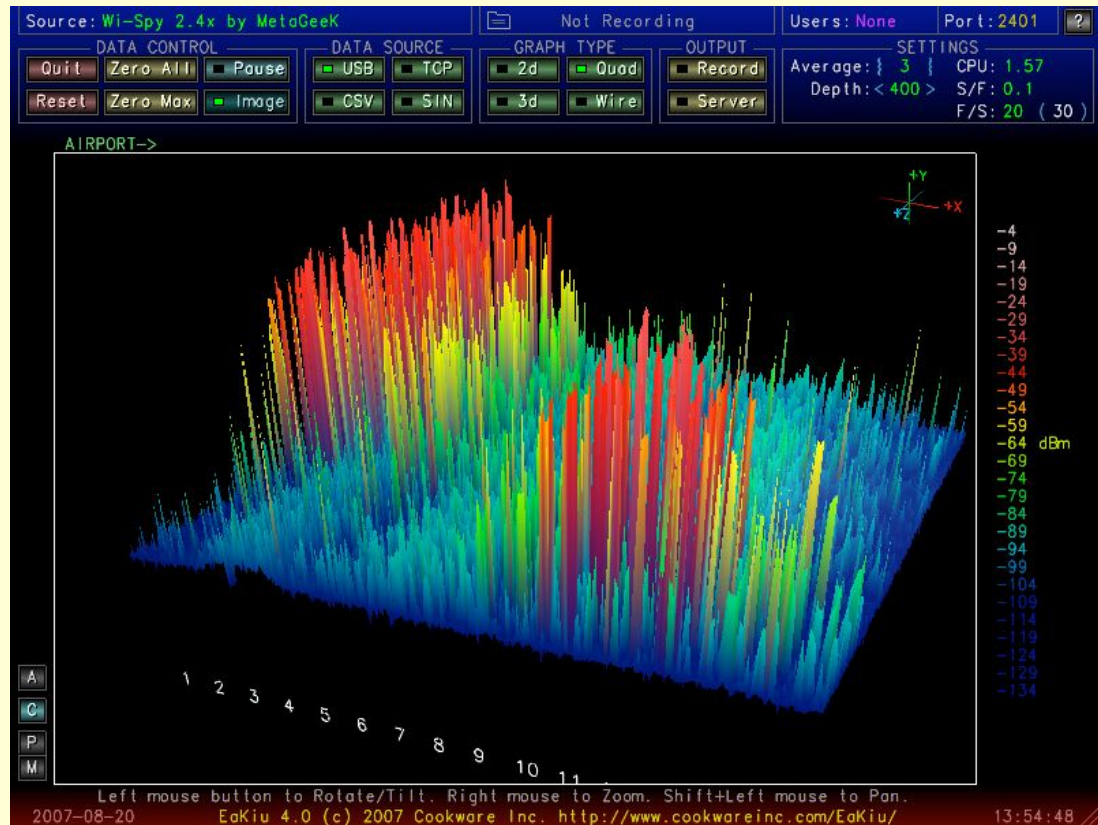
Secur	Network Name	Signal	Noise	Chann	MAC Address	Vendor
Secure	GeorgiaNet	31%	13%	8	00-02-2D-21-9C-F	Graphite Airport...
Open	linksys	42%	13%	6	00-06-25-E5-B3-6	Linksys Group
Secure	Zeus	33%	13%	9	00-09-5B-50-E5-C	Netgear
Open	QS3	45%	13%	6	00-09-5B-C8-9A-3	Netgear
Secure	New Galaxy	42%	13%	11	00-0A-95-F2-AE-0	Apple
Secure	salmon	39%	13%	6	00-13-10-36-4F-5	Cisco-Linksys,
Secure	Geoff's MIMO	35%	13%	6	00-14-6C-96-13-E	00-14-6C
Secure	Oohla's	47%	13%	10	00-15-E9-EC-CD-7	00-15-E9
Secure	Draft N Network	56%	13%	0	00-19-E3-32-C3-6	00-19-E3

iStumbler shows nearby networks. I made this scan in my office, which is in the middle of a building in Seattle with a window off to one side. Imagine a scan made in Manhattan.

If you're truly frustrated with finding a good connection, you could make an expensive purchase—or perhaps pool your dollars with friends or colleagues—and get a spectrum analyzer. The Wi-Spy and Wi-Spy 2.4x from MetaGeek run \$199 and \$399, respectively, and provide a live analysis of the signals passing in the air around you.

A spectrum analyzer constantly measures the strength of signals in hunks of frequency, and produces an output that software can read and display (**Figure 16**). The more energy or more spikes in a given channel, the more likelihood that Wi-Fi won't work there.

FIGURE 16



Wi-Spy and Wi-Spy 2.4x capture signal strength over time at frequencies in the 2.4 GHz band and relay them to software like EaKiu, which displays the results graphically. (Wi-Spy 2.4x data pictured.)

SET UP YOUR NETWORK

The next steps in setting up your AirPort network involve configuring the LAN (local area network) and WAN (wide area network). For many of us, this configuration is as simple as plugging in a couple of cables—or maybe even one cable. But for more complicated networks, a few more steps are involved to make sure the computers connecting via the Extreme N can access the Internet, or the rest of a local network, without you pulling out your hair.

More than one base station: *If you're building or re-building a network with more than one base station, read this section first for how to set up the base station that connects directly to your broadband service provider. Then read [Connect Multiple Base Stations](#).*

Simplest Case: Plug and Go

Before getting into more exotic scenarios, let me give you the rundown on the simplest possible case, which has two parts:

- You have a broadband cable or DSL modem that doesn't require any special login or restrictions in order to access the Internet. (If you're not sure, see [Log in via PPPoE over broadband DSL](#) and [Deal with MAC-address-restricted cable broadband](#).)
- You plan to share the Internet connection coming in from the broadband connection among computers and devices that connect to the Extreme N via Wi-Fi or Ethernet.

Here's how to get your connection up and running:

1. Plug an Ethernet cable from the LAN port of your broadband modem into the WAN port of the Extreme N.
2. Connect the computers on your network via Wi-Fi or Ethernet to the Extreme N.

That's it! This setup relies on the factory settings that an Extreme N has when it's first powered up. If this simplified setup appears to be working, and you have no reason to think that it shouldn't do the job, then skip ahead to [Connect Your Computers](#).

If this simplified setup doesn't work, or you know you have a more complicated situation, read through the rest of this section to find your scenario.

Get a WAN address

The more complicated scenarios start with getting a WAN address for your base station; you'll then move to LAN configuration.

To communicate with the rest of the world, you need to hook the wide area network (WAN) port of your Extreme N into either a broadband modem; or, if you have an existing Ethernet LAN to which you are connecting the base station, into that larger network.

In either case, start with an Ethernet cable and plug the cable into the Extreme N's WAN port. Next, plug the other end into the LAN port of your broadband modem, or into a port on an Ethernet switch for a larger network.

Auto-sensing: *Extreme N has auto-sensing, auto-switching Ethernet, which means you can use either type of Ethernet cable—straight-through or crossover—successfully. The Ethernet ports also automatically adjust speed to the highest available rate.*

Now that you've made the physical connection, you can configure your base station to handle the connection. The many different possible configurations can be broken down into two categories: those that use *dynamic addressing* and those that use *static addressing*:

- If your Internet connection is a home broadband connection, you'll probably use dynamic addressing; you may need to ask your ISP for more information if you're not sure whether they provide you with a dynamic address or not.
- A static address is more typical for small and large offices.

Dynamic addressing

A *dynamic address* is an Internet protocol (IP) address that is assigned through Dynamic Host Configuration Protocol (DHCP), a relatively old Internet technology. With DHCP, your Extreme N requests an IP address via its WAN port, acting as a *DHCP client*. A *DHCP server* on the other end of the Internet connection (typically at your service provider) receives the requests and provides an address. And that's as complex as it has to be.

A dynamically assigned address can be a *private* address, one that's restricted to the ISP's own network; that network is hard for anyone to reach making your network even more inaccessible; or a *publicly routable* address, which is part of the global numbering system for IP addresses.

The Extreme N is set to act as a DHCP Client if back in Step 7 of [Handle initial setup](#), you chose Using DHCP. No additional steps should be needed (**Figure 17**).

FIGURE 17

The screenshot shows a configuration window with three tabs: "Internet Connection", "DHCP", and "NAT". The "DHCP" tab is selected. The configuration includes the following fields and values:

- Connect Using: Ethernet
- Configure IPv4: Using DHCP
- IP Address: 192.168.2.148
- Subnet Mask: 255.255.255.0
- Router Address: 192.168.2.1
- DNS Server(s): 192.168.2.1
- Domain Name: sea1.dsl.speakeasy.net
- DHCP Client ID: (empty)
- Ethernet WAN Port: Automatic (Default)
- Connection Sharing: Share a public IP address

Below the fields, there is a note: "Select if you want this base station to share a single IP address with wireless clients using DHCP and NAT, distribute a range of static IP addresses using only DHCP, or act as a bridge."

The simplest way to get an Extreme N on the Internet.

In some limited cases, you might need to enter the DNS (Domain Name Service) IP addresses manually. Your ISP should tell you those addresses if you need them. DNS IP addresses are entered in the DNS Server(s) fields (**Figure 17**, above).

TIP HANDLE DNS RESOLUTION WITH OPENDNS

I recommend using OpenDNS to handle your DNS resolution instead of DNS server information provided by an ISP. OpenDNS has a few neat features that improve on normal DNS resolution. First, they're much faster than most ISPs, making the Web seem snappier. Second, they can fix typos, for instance, when you enter an address that doesn't exist—`flickr.cmo` becomes `flickr.com`. Third, they offer a custom account that lets you set DNS shortcuts so that when you type a word into a browser's Location field, you control what domain name is looked up.

See <http://www.opendns.com/> for more details, including their two nameservers' IP addresses.

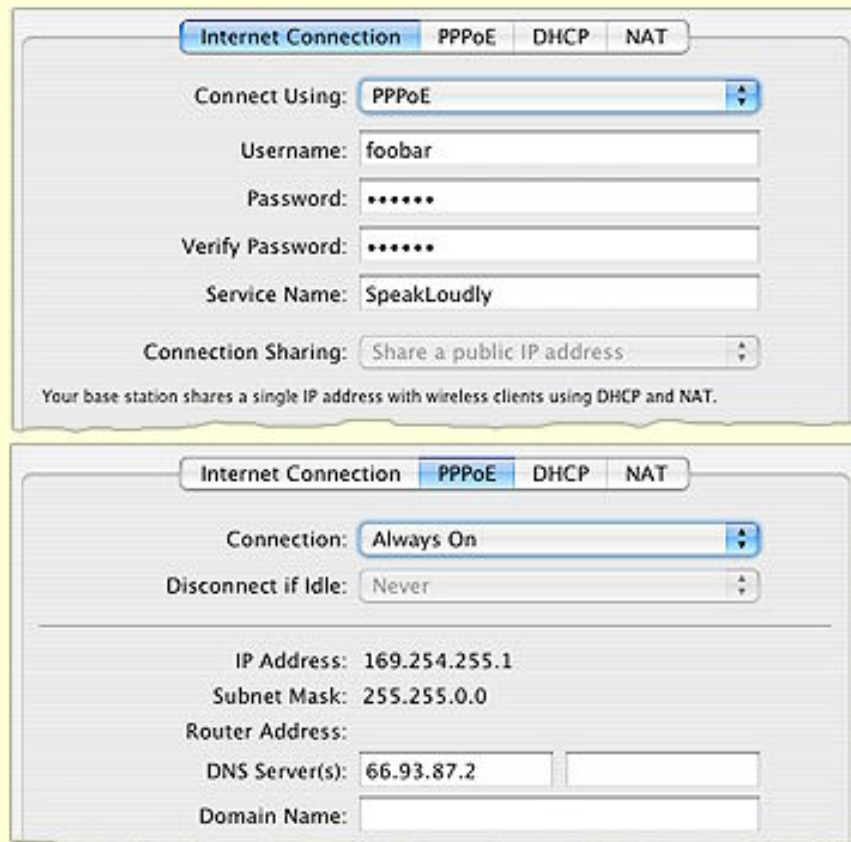
Some ISPs require you to jump through additional hoops to connect to their networks: a login process or a way to restrict access to a single computer. The former is used mostly by DSL providers; the latter, by cable firms.

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 pane of AirPort Utility in the Internet Connection and PPPoE views (**Figure 18**). The base station connects per the setting you choose in the Connection pop-up menu in the PPPoE view: Always On is the most likely choice.

FIGURE 18



PPP over Ethernet connects using a login name and password.

Deal with MAC-address-restricted cable broadband

To prevent multiple machines from accessing a single cable-modem connection, some providers restrict access to a single MAC address (see [What and Where Is a MAC Address?](#) next page). ISPs use two common methods for restricting access by MAC address:

- In the less annoying method, the cable modem powers up and locks on to the MAC address of the device connected to it. You can switch between devices by unplugging and reconnecting the cable modem after you connect your Extreme N.
- In the more annoying method, you register the MAC address with the ISP manually or through an automatic process. You may need to call your cable provider—which may want to charge an additional monthly fee—to register the MAC address of your Extreme N's WAN port. (The WAN port's MAC address is printed on the underside of the Extreme N, as the Ethernet ID.)

Warning! A feature in non-Apple Wi-Fi gateways, called MAC cloning or spoofing, lets you enter any MAC address for the WAN port. No AirPort base station firmware version has this common feature.

WHAT AND WHERE IS A MAC ADDRESS?

The MAC, or *Media Access Control*, address is a unique, factory-assigned 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 0C:F2:33:01:02:FC. (*Hexadecimal*, or *hex*, is the base 16 number system, with values running from 0 to 9, and then from A to F for 10 to 15.)

The first three numbers are assigned to a manufacturer; Apple has at least two common ranges, which begin with 00:0a:95 and 00:03:93. MAC addresses are frequently used for filtering, authentication, and WDS, often without requiring direct entry.

Here's how to find MAC addresses for Apple's devices:

- **Extreme N:** Look on the bottom of the base station to find the MAC addresses of the WAN Ethernet port and the Wi-Fi adapter. Or, in AirPort Utility, select a base station at the left to see its MAC addresses on the right:
 - ◇ The AirPort ID is the device's wireless MAC address.
 - ◇ The Ethernet ID is the WAN port's MAC address.
- **Computers connected to an Extreme N:** In AirPort Utility, select the base station and choose Base Station > Manual Setup. Click the Advanced icon, and then—on the Logging and SNMP view—click the Logs and Statistics button. Click the DHCP Client button and a list of MAC addresses appears. You can turn your computer's Wi-Fi adapter off and on to see which MAC address corresponds to your computer.
- **Wi-Fi adapter in a Mac:** In Mac OS X, 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 view.)
- **Wi-Fi adapter under Windows:** In Windows XP or Vista, view the connection status of the adapter and click Details below the Connection Status section. The Physical Address is the MAC address.



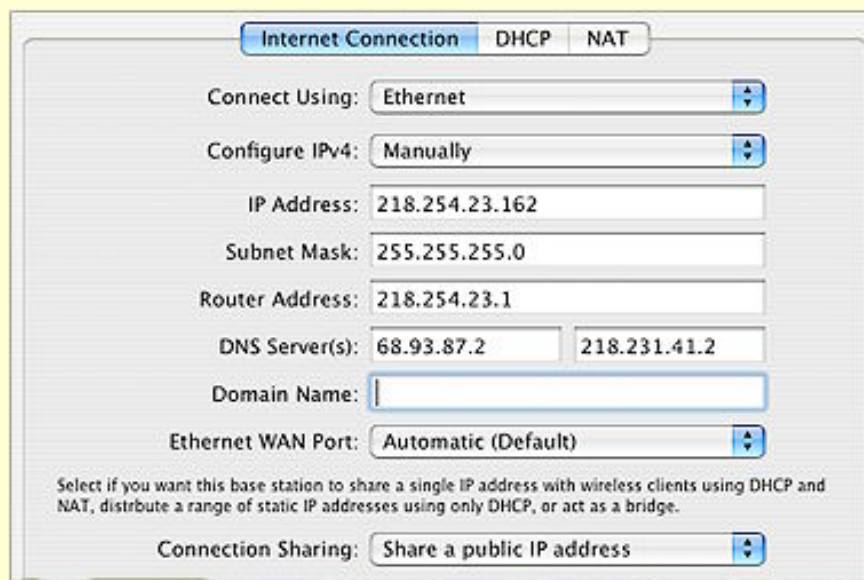
Static addressing

A *static address* is an IP address that is entered manually and is fixed over time. A static address could be private or public. To enter a static address, you need details provided either by your ISP or, for an office network, by a network administrator. You need:

- **The static IP address:** This address could be from an internal private range or a public address reachable from the Internet.
- **The subnet mask:** A number full of mystery, the *subnet mask* merely defines the size of the local network in which the static address comes from, with “size” expressed as the number of addresses in that local range.
- **The router address or gateway:** This is the address to which any traffic that’s not bound for other machines on the local network is sent, to be *routed* to higher-level networks, such as a larger office LAN or the Internet.
- **DNS server or servers:** You need at least one DNS server, which handles turning domain names into IP addresses. Two is better; that avoids slowdowns if the first DNS server is unavailable or overloaded.

To enter these values, click the Internet icon at the top of the AirPort Utility window; click the Internet Connection button, and choose Manually from the Configure IPv4 pop-up menu (**Figure 19**).

FIGURE 19



The screenshot shows the 'Internet Connection' window in AirPort Utility. The 'Internet Connection' tab is selected, with 'DHCP' and 'NAT' tabs also visible. The 'Connect Using' dropdown is set to 'Ethernet'. The 'Configure IPv4' dropdown is set to 'Manually'. The fields are filled with the following values: IP Address: 218.254.23.162, Subnet Mask: 255.255.255.0, Router Address: 218.254.23.1, DNS Server(s): 68.93.87.2 and 218.231.41.2, Domain Name: (empty), Ethernet WAN Port: Automatic (Default), and Connection Sharing: Share a public IP address. A note at the bottom states: 'Select if you want this base station to share a single IP address with wireless clients using DHCP and NAT, distribute a range of static IP addresses using only DHCP, or act as a bridge.'

Configure the Internet connection manually by entering the static values provided by your ISP or network administrator.

NOTE WHAT'S IPv4?

The other element of mystery in setting an IP address is what, exactly, is IPv4? *IP* stands for Internet Protocol, but *v4* means “version 4,” the form of IP used in Internet networking for decades. That distinction has become important with the availability of IPv6 (version 6), which Apple supports in Mac OS X and Extreme N, among other products. IPv6 isn't widely available, but it is out there and will become increasingly embedded in our lives and devices. See [IPv6 settings](#) for more details.

Hand Out LAN Addresses

With the WAN configured, it's time to look at your own network—the LAN. The LAN can be configured to assign IP addresses to client computers in one of four ways:

- **Dynamic private addresses:** In this common mode, the Extreme N shares one incoming Internet address with all the machines on LAN. The base station assigns addresses to computers on the LAN from a private range; you can modify what that range is. The addresses are typically transient for any given computer. The Extreme N coordinates traffic between the LAN and the greater Internet so that all packets end up in the right place.
- **Dynamic public addresses:** With this setup, the Extreme N shares multiple, publicly routable Internet addresses with computers on the LAN.
- **Reserved addresses:** With this feature, you can assign specific private or public addresses to individual computers on the LAN.
- **Passthrough and bridging:** you can set up an Extreme N to let another device on a larger network dynamically assign addresses or allow static addresses. With this set up, the Extreme N doesn't manage addressing.

The first option is by far the most common, in which computers on the LAN receive addresses that can change from time to time, and which exist solely to give the computers access to the Internet. The other options are typically used when computers on the LAN side of

the network need to be reached by computers on the Internet or by computers on another LAN to which your Extreme N is connected.

Let's look through each of these in turn.

Warning! *In testing the Extreme N, I discovered performance issues in one particular configuration. A NAT-enabled Extreme N bogs down when you send data between devices on the base station's LAN (via Ethernet or Wi-Fi) and devices on a network connected to the base station's WAN. In this rare configuration, Ethernet tops out at 70 Mbps; Wi-Fi at 50 Mbps. Fortunately, you would almost never use NAT on a base station that connects its WAN port to an office or a larger LAN network—see [Passthrough and Bridging](#).*

Apple is aware of this problem (I reported it), and they improved the speed by 25 percent from the Extreme N (original) to Extreme N (gigabit) model.

NOTE DHCP works by having a computer or other device send out a message over a network asking for an address. A DHCP server hears this message and provides an address. The DHCP client pulls the address that the DHCP server provides.

Dynamic private addresses

As with the WAN side of the equation, if you set up your network using the straightforward assistant in AirPort Utility, you should have no changes to make, so you don't need to proceed further in this section to set up the base station; you can skip ahead to the next section, [Connect Your Computers](#).

However, should you want to control which addresses are assigned or manage other details of NAT and DHCP, read on.

Set up the base station

In AirPort Utility, click the Internet icon at the top of the window, click the Internet Connection button, and choose Share a Public IP Address from the Connection Sharing pop-up menu.

Set up client computers

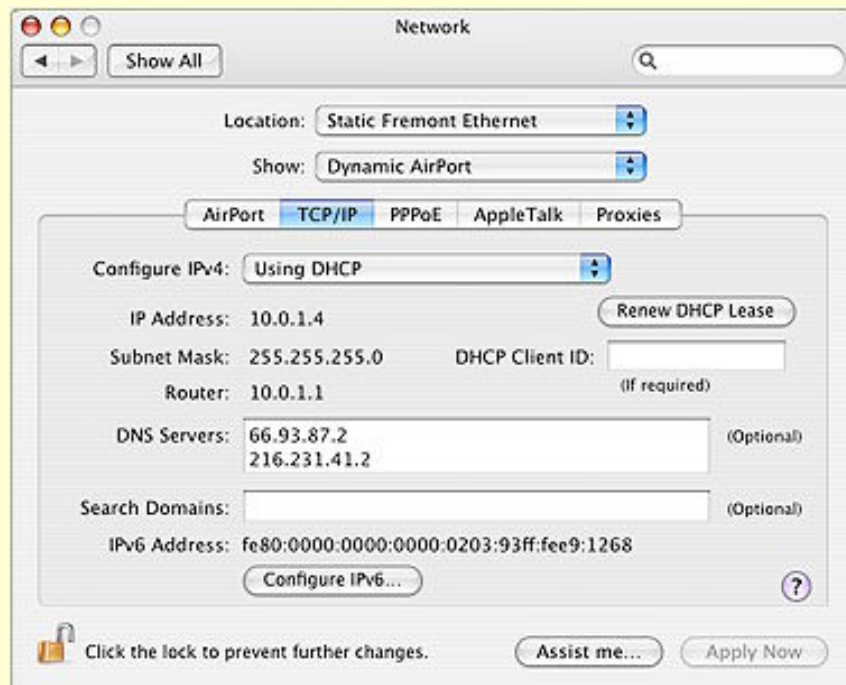


With an Extreme N set to use dynamic addressing, each of your computers needs to be set to receive an address via DHCP. This is the default setting for any network adapter.

In Mac OS X:

1. Open the Network preference pane.
2. Switch to the TCP/IP view for any adapter—Wi-Fi or Ethernet.
3. Choose Using DHCP from the Configure IPv4 pop-up menu (**Figure 20**).

FIGURE 20



With TCP/IP set to use DHCP, Mac OS X automatically obtains a dynamically assigned IP address, in this case from a private range.

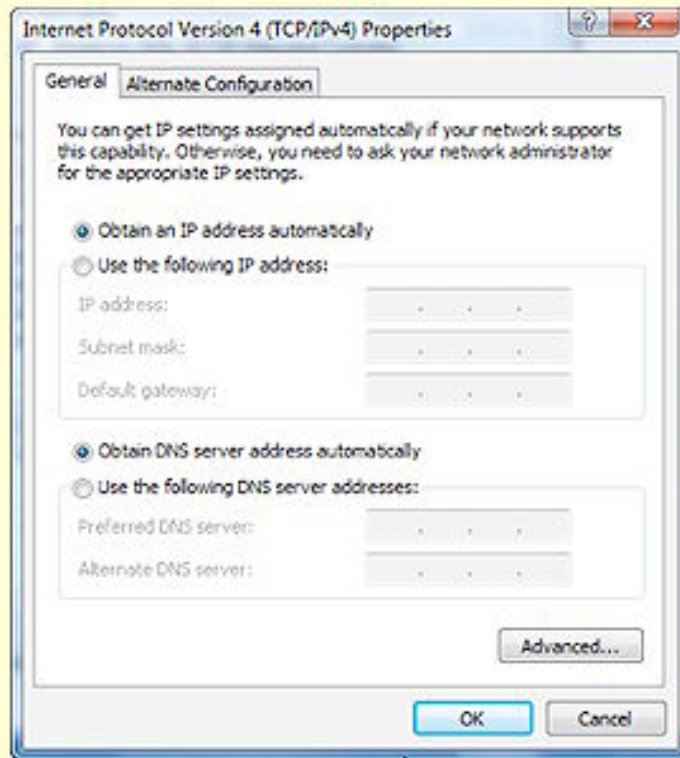
Your Mac should now be set up to receive an IP address via DHCP.

In Windows XP and Vista:

1. Choose Control Panel from the Windows menu.
2. Access network connections:
 - In XP, open Network Connections.
 - In Vista, open the Network and Sharing Center, and then in the left-hand Tasks list, click Manage Network Connections.

3. Right-click the adapter you want to view settings for, such as Wireless Network Connection, and select Properties. (In Vista, you should be prompted to approve that action; click Continue, if so.)
4. In the Networking tab that appears, select Internet Protocol (TCP/IP) in XP or Internet Protocol Version 4 (TCP/IPv4) in Vista, and click Properties. TCP/IP settings are configured in the General tab; the default settings are the correct ones (**Figure 21**).

FIGURE 21



In Windows Vista, selecting Obtain an IP Address Automatically—the default setting for an adapter—allows the operating system to get a dynamic address. (In Windows XP, the interface for making this selection looks quite similar.)

Your Windows system should now be configured to receive an IP address via DHCP.

Refining base station DHCP settings

You have two additional views in the Internet pane in AirPort Utility for configuring the LAN. These allow you to control how private addresses are generated.

The DHCP view offers a DHCP Range pop-up menu where you choose one of three reserved ranges of private addresses—10.0.*.*, 192.168.*.*, or 172.16.*.*—as the two-number prefix to your private network numbers. (The prefixes in the pop-up menu are reserved by the global numbering authority, and they are guaranteed to not be in use on any public Internet network.)

You enter the third number, any number from 1 to 254, in the field to the right of the pop-up menu. The fourth number is generated by DHCP in a range limited to the starting and ending values shown in the DHCP Beginning and Ending Address fields.

The only reason to change the range of numbers is if you want to create and assign static *private* addresses. These would be addresses that start with the first three numbers in the base station's private network range, but which you enter manually on each computer. This used to be the only way to create a fixed private address, but I now suggest you avoid this method by using reserved addresses; see [Reserved addresses](#), next page.

2⁸-2: *The lowest legitimate number in the fourth number position of an IP address is 1; the highest is 254; 0 and 255 have particular reserved network purposes.*

Limited addresses: *The range you assign must start with the same prefix you defined in the DHCP Range pop-up menu. AirPort Utility prevents you from modifying the first three numbers in the four-number IP address in the range fields. This is also true anywhere you can enter a LAN address in AirPort Utility.*

In the DHCP view, you can also set the length of a time of a *DHCP lease*, which is the association of a given computer with an address that's been handed out, and you can set the DHCP Message, which will pop up in a dialog box on a computer when the computer receives its DHCP address. (The LDAP Server field is relevant only for networks that use that directory protocol.)

The DHCP Reservations list is in [Reserved addresses](#) (next page).

Also on the Internet pane, the NAT (Network Address Translation) view has two settings relevant for remotely accessing programs running on one or more computers on the LAN. I discuss how NAT works and what these settings offer in [Reach Your Network Remotely](#).

Dynamic public addresses

Some people need to assign public addresses to their LAN computers so that each computer can be reachable from the Internet. In this case, you usually want to use a static public address, in which you must configure each computer manually, and DHCP isn't involved.

However, some networks use only public addresses for all connected devices, while also not requiring that each device have a static address over time. In that case, you configure an Extreme N to hand out public addresses from a defined range using DHCP.

To configure an Extreme N to assign dynamic public address, follow these steps:

1. In AirPort Utility, select the base station at the left, and then click the Internet icon at the top of the window.
2. Now, on the Internet Connection view, from the Connection Sharing pop-up menu, choose Distribute a Range of IP Addresses.

In this mode, the NAT button disappears because there's no translation going on.

3. In the DHCP view, enter values for DHCP Beginning and Ending Address. The range you specify is limited to the same IP network that the Extreme N uses for its Internet Connection IP address. For instance, if your Extreme N is 218.23.1.200, your range has to be within 218.23.1.1 and 218.23.1.255.

Warning! Using public routable addresses means your entire base station LAN is fully exposed to the higher-level network through its WAN port, which usually means that all the computers can be reached via the Internet.

Reserved addresses

Reserving an IP address using DHCP is a new feature in the Extreme N—new to Apple, as it's been available in other devices for years. Reservation allows a given computer on a network to obtain the same IP address, whether public or private, each time it joins the network. This works whether or not you share the Extreme's connection or distribute a range of addresses, but does require DHCP service to be turned on.

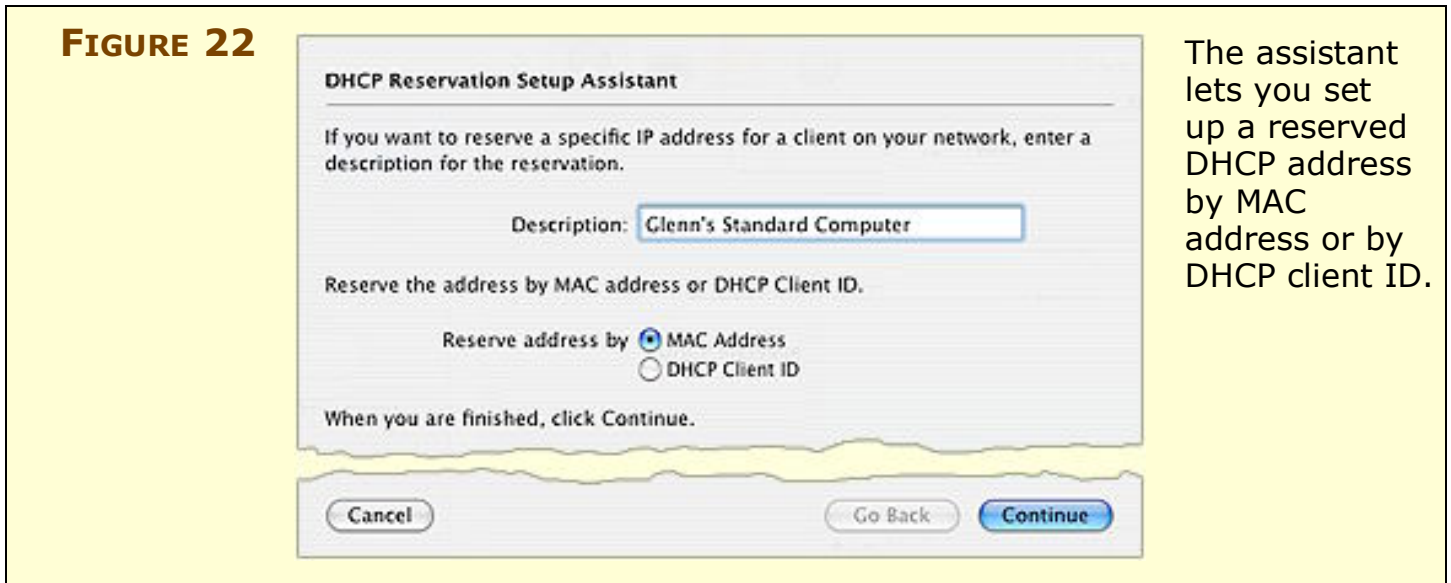
The reserved address is never assigned to another computer, and if the computer in question has to restart or is shut down, the next time the computer powers up and its network adapter is active, that computer still receives its reserved address.

Reserved addresses work well if you want to connect from the WAN side of a base station to computers, printers, and other devices that are connected via the LAN side.

Follow these steps to set up a reserved address:

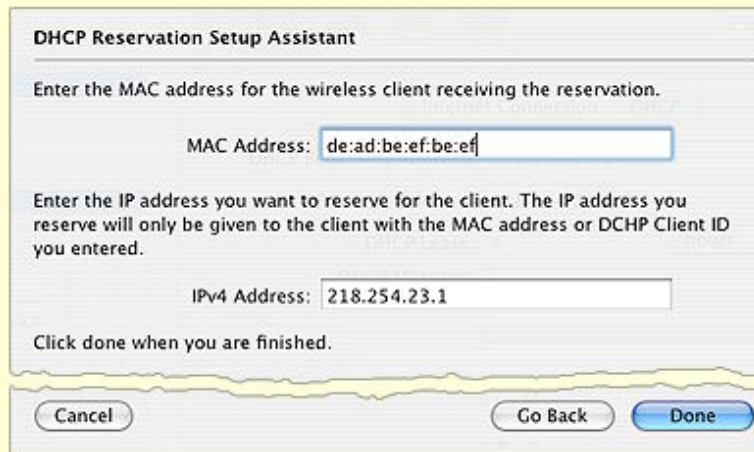
1. In AirPort Utility, in the DHCP view of the Internet pane, click the  button.

The DHCP Reservation Setup Assistant (**Figure 22**) appears.



2. Enter a description, which will later appear in the DHCP Reservations list.
3. Select whether to reserve an IP address by a Wi-Fi adapter's MAC address or by its DHCP Client ID, and click Continue. DHCP Client ID is easier to set up, but works only with Mac OS X (and earlier).
4. Now:
 - **If you reserved by MAC address:** enter the MAC address (AirPort Utility fills in the colons as you type two-digit hexadecimal numbers), choose the last number in the IP range that you want to reserve, and click Done (**Figure 23**). If you need help locating the MAC address, see [What and Where Is a MAC Address?](#) (p. 59).

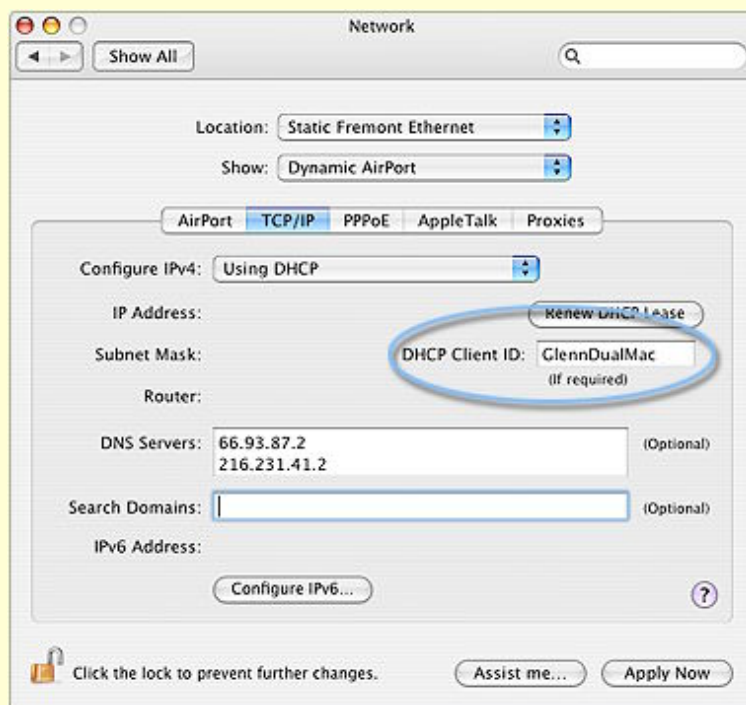
FIGURE 23



Enter the MAC address and your reserved IP address, and then click Done.

- **If you selected Reserve by DHCP Client ID:** The DHCP Client ID is a text tag that you assign when configuring a Wi-Fi or Ethernet adapter. This text is transmitted when an adapter requests a dynamic address (Windows XP and Vista don't support this), and the base station uses that tag to assign a reserved IP address:
 - a. First set the DHCP Client ID on a client computer running Mac OS X: Open the Network preference pane, click TCP/IP, choose Using DHCP from the Configure IPv4 pop-up menu, and enter the DHCP Client ID in the field at the right. **Figure 24** shows the DHCP Client ID set to GlennDualMac.

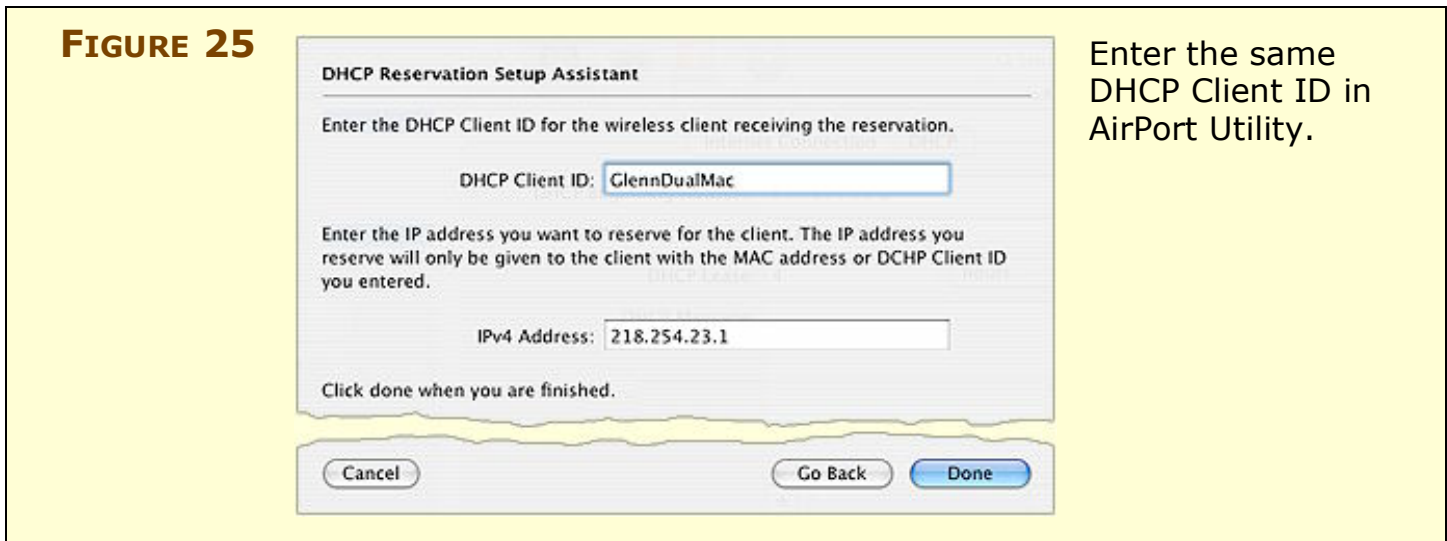
FIGURE 24



The DHCP Client ID field is found in the TCP/IP view when the Configure IPv4 pop-up menu is set to Using DHCP.

Warning! To avoid confusing the Extreme N, make sure that DHCP Client IDs are unique.

- b. In AirPort Utility, enter that DHCP Client ID in the DHCP Reservation Setup Assistant and click Done (**Figure 25**).



5. When you've entered all the reservations, click Update.

After restarting, the DHCP Reservations list shows the entries you made and any computers listed will have retrieved their new addresses.

Passthrough and bridging

For networks in which the Extreme N is connected to a larger LAN, you may already have a DHCP server running that handles address distribution. In that case, you need to turn off Connection Sharing:

1. In AirPort Utility, click the Internet icon at the top of the window.
2. In the Internet Connection view, choose Off (Bridge Mode) from the Connection Sharing menu. The DHCP and NAT buttons disappear in the Internet pane when that option is selected.
3. Click Update to restart the base station.

With bridge mode, the Extreme N simply passes through any DHCP messages or other traffic, and isn't involved in assigning addresses.

NOTE If you connect base stations wirelessly using Wireless Distribution System, all the base stations other than the "main" unit, which acts as the Internet or LAN conduit, are turned into bridges. See [Bridge Wirelessly](#) for details on setting up a WDS connection.

CONNECT YOUR COMPUTERS

Once you've set up your Wi-Fi network and connected it to the Internet, you'll want to configure your computers to connect to the network properly, whether you're working with a few desktop computers or helping customers use a public hotspot. Making a connection is quite simple, but configuring how your computers connect may take a little thought. You might choose to connect automatically to unknown networks, or need to connect to a network that doesn't advertise its name. You may also reconnect to networks that you've visited before.

Read this section to learn how to use Tiger (below), [Windows XP](#), and [Windows Vista](#) to connect to networks, modify stored profiles for networks, and choose when to connect to unknown networks.

NOTE Leopard hasn't shipped as the book goes into production. To learn about the Leopard update to this book, click Check for Updates on the [cover](#) and sign up for the update mailing list. If you have only the printed version of the book, [send us an email message](#).

Warning! Remember that if you set up your network as 802.11n-only in the 2.4 GHz band, or if you set the base station to use the 5 GHz band, neither an 802.11b nor a 802.11g adapter found in an older computer will be able to connect. If you can't see your network on a given computer or can't connect to a network that shows up in a list of available networks, check your base station setup (see [Consider your spectrum choices](#) for more details).

Connection problems: Just because a network is visible doesn't mean you can connect to it. MAC address access control and other restrictions could keep you from joining. See [Secure Your Network](#).

Connect in Tiger

Connecting to a Wi-Fi network with Mac OS X involves two phases: *discovering*, or finding, a network, and connecting to it. Separately, you can create stored profiles for Wi-Fi networks that you wish to connect with automatically in the future.

Warning! If the AirPort status menu on your menu bar displays an icon like an open fan (shown at left), your network adapter is turned off. To turn it on, choose Turn AirPort On from the menu. If the AirPort icon still looks like a fan or you get an error saying that there's no card or it can't be turned on, you may have a hardware problem. If you have a model with a removable Wi-Fi card, check that the card is seated properly: power the computer down, open the case, and check the card; start up the machine and see if AirPort is now available. If you don't have a serviceable card or this doesn't help, bring the computer in for service.



Discovery

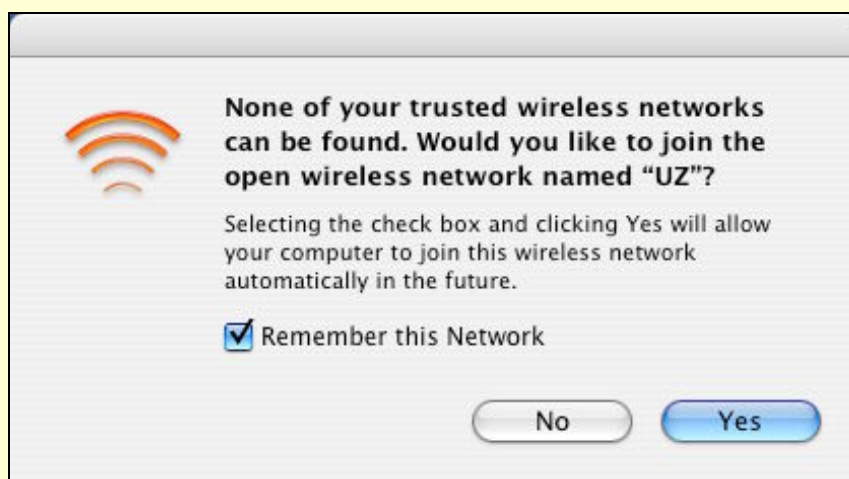


Mac OS X constantly looks for networks when the Wi-Fi adapter is turned on, and a list of them appears in the AirPort status menu at the right of the menu bar (If you don't see the menu, you can turn it on by opening Internet Connect from **/Applications**. A checkbox for the menu is on the AirPort pane.)

You can also use software like iStumbler to get more information about your own and other networks in the vicinity (see [Testing from client to base station](#)).

If a Wi-Fi network appears in your vicinity and you aren't already connected to one (for instance, if a neighbor turns on a new network or if you open your laptop in a coffee shop), Mac OS X alerts you (**Figure 26**). From that alert, you can then choose whether you wish to connect to the network, and if you want Mac OS X to remember the network so that you always connect to it again in the future.

FIGURE 26



Mac OS X alerts you to a new network and lets you choose to always join it in the future.

You can configure a Mac running Tiger so that it automatically picks which network it connects to: Mac OS X can recognize a new connection when you wake up or turn on the Mac, when you turn AirPort off and back on, when a network is turned on near you, or even when a Wi-Fi network disappears and reappears while you're actively using your computer.

Warning! *The fact that Mac OS X and other operating systems constantly scan for networks is a security problem. Many patches were released in 2006 that dealt with flaws in Wi-Fi drivers that could be exploited with maliciously crafted data designed to crash an operating system when it is scanning for networks. This is one reason why it's critical to keep your software up to date, especially if you use Wi-Fi networks that aren't in your home or office.*

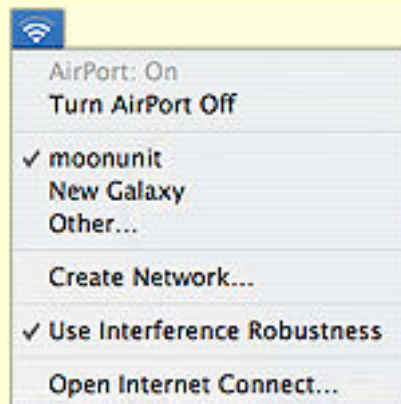
Connecting

To connect to a network, you typically select its name from a list, and then enter an encryption key if it is secured. In some cases, you might have set up your network to be “closed” (invisible to casual passers-by). Let's walk through these options for connecting.

Connect to a named network

To connect to an AirPort network in Tiger when the network broadcasts its name—as most do—choose the network name from the AirPort status menu (**Figure 27**). The AirPort menu's icon should go from gray to black, with the number of black waves indicating signal strength by their quantity.

FIGURE 27



Choose a network from the list or choose Other to join a closed network by name.

At hotspot networks and other open networks, before you can do anything else on your connection, you may need to open a Web

browser window and try to visit any site. Instead of going to that site, the network will redirect you to a gateway page at which you may be asked to agree to terms of service, or enter account information or a credit card number to proceed. You typically have no Internet access until you've passed the gateway page.

If the network is secured with a key, see just below for the next steps, or look on the next page for WPS information.

Enter an encryption key (WEP, WPA/WPA2 Personal)

If encryption is active on the network, after you select the network name, you are prompted by a dialog to enter an encryption key. Typically, the AirPort software on a Mac automatically chooses the correct encryption type, and you simply enter the encryption key that you have been given or that you set yourself for the network.

Save the key, save time: You can choose to store the key in the Keychain to avoid having to retype it in the future.

If the encryption type is incorrect, you can choose the correct type from the pop-up menu. Click OK to join the network.

You enter an encryption key or passphrase differently depending on how the network was configured. Extreme N networks can always be joined with either a WPA or a WPA2 password, but WEP keys may be needed to join older networks:

- **Apple WEP Password:** If you created a WEP key on an original AirPort Base Station, the 2003 Extreme, or an AirPort Express, enter the password exactly as you entered it in setting up the base station or as it was provided to you.
- **WEP hexadecimal key:** If you are joining a non-AirPort network, you need to enter a \$ (the dollar sign character) followed by 10 to 26 hexadecimal digits. Whoever set up that network needs to provide those hex numbers to you.
- **WEP ASCII key:** If the network was set up with WEP using an ASCII (text) key, you must enter that password between quotation marks, like "**f i s h y**". WEP ASCII keys are 5 or 13 characters long.

Extract WEP key: *AirPort Utility lets you extract a WEP key when using WEP Transitional in case you have older Windows computers or other devices that need to join. Connect via the utility to your base station, choose Base Station > Manual Setup, and then choose Base Station > Equivalent Network Password. The ASCII and hex WEP keys are identical, just expressed in different forms.*

- **WPA/WPA2 passphrase:** Enter the passphrase exactly as it was entered on the Extreme N or other base station. All computers handle WPA/WPA2 passphrases the same way. Some networks may be configured to accept either a WPA or a WPA2 password; others may require only a WPA2 password.

Warning! *Macs with the original AirPort Card cannot connect to WPA2 Personal protected networks, but won't provide an error to explain that. If you are using an AirPort Card on an older machine, make sure via AirPort Utility that the network is configured with WPA/WPA2 Personal, not WPA2 Personal.*

- **WPA/WPA2 hex key:** In rare cases with WPA or WPA2, you may need to enter the 64-digit hexadecimal encryption key. To enter this in Tiger, hold down the Option key while selecting WPA Personal or WPA2 Personal from the Wireless Security pop-up menu, and an extra large field appears allowing entry. Yes, it's a pain to enter 64 hex digits.

Connect to a simplified secured network with WPS

Wi-Fi Protected Setup (WPS) lets you join a secured network without entering an encryption key. But this method requires access to the base station via AirPort Utility at the time you want a computer to join the network. To read the full procedure, skip ahead to [Use WPS](#).

Connect to a closed (hidden) network

For a closed network, choose Other from the AirPort status menu. In the resulting dialog, enter the network's precise name (close doesn't count), and choose the form of encryption and enter the password.

If there's no encryption, leave the option set to WEP Password and enter no password. Click OK to join. (For more on closed networks, see [Closed network](#).)

Saved locations

Tiger can automatically connect to networks that you've joined previously, including password-protected networks for which you've saved the password in your Keychain.

But you can also create custom settings for different locations where a computer might be used (perhaps at the office, at a relative's house, and at a local coffee shop), and you can set up multiple profiles at each location.

To create a new location, in the Network preference pane, choose New Location from the Location pop-up menu, enter a name, and click OK.

Managing profiles





You can manage profiles for connected networks and create new profiles from scratch. To show those profiles, and to create and edit them:

1. In the Network preference pane, choose your AirPort adapter from the Show pop-up menu and click the AirPort button.
2. Choose Preferred Networks from the By Default, Join pop-up menu.

A list of networks appears, ordered from top to bottom by the most preferred to least preferred network to join.

Warning! *Even though you can create different profiles for your other network settings through the Location pop-up menu, Wi-Fi networks in this profiles list are shared in all locations.*

Warning! *I discovered a bug some time ago with location profiles created in Panther and used in Tiger. I was unable to get Preferred Networks to appear in the pop-up menu with a Panther-created location; instead an option that's not supposed to appear in Tiger shows up: A Specific Network! When I created a new location in Tiger, the correct menu commands appeared. This bug has never been fixed.*

3. To work with these profiles:
 - Add a profile manually by clicking the  button.
 - Delete a profile you no longer need by selecting the profile and clicking the  button.
 - To edit an existing profile, select it and click Edit; you can change the password or type of password, too.
 - To change the preferred order in which the Mac connects to networks if more than one is available, drag a network name to a new position in the list.
4. Click Apply Now when you're done.

Advanced connection options



For more control over how a Mac connects via AirPort at a particular location, in the Network preference pane, choose a location, click the AirPort button, and then click Options at the lower left. Now you can:

- Set whether you want to add profiles for new networks that you connect to by checking or unchecking the “Automatically add new networks to the...” box. (If, instead, you chose Automatic from the By Default, Join pop-up menu, that box is checked and cannot be disabled. In Automatic mode, you manage networks entirely via the AirPort status menu.)
- You can also choose one of three items from the If No Preferred Networks Are Found pop-up menu:
 - ◇ Ask Before Joining an Open Network lets you join any network that's within your Mac's range, but first prompts you.
 - ◇ Automatically Join an Open Network is ill advised: it's rare that every open network will be acceptable to you, or even intended for use by outsiders.
 - ◇ Keep Looking for Recent Networks prevents your Mac from joining, or asking to join, networks that you haven't agreed to connect to before.
- In Tiger, Apple added the checkbox Disconnect from Wireless Networks When I Log Out, which disconnects the Mac when no user is active. This makes sense for users who routinely log out of Mac OS X, or on computers with multiple users.

TIP If you can't get your AirPort interface to connect to a network, Tiger has a troubleshooting feature called Network Diagnostics that's available when you click Assist Me at the bottom of the Network preference pane.

TIP WHERE YOUR MAC STORES PASSWORDS

When you enter a WEP, WPA, or other encryption key in Mac OS X, it's stored in the Keychain. You can run Keychain Access (located in **/Applications/Utilities**) to delete entries you no longer wish to store or to retrieve passwords that you have forgotten.

Keychain passwords are secured with your Mac OS X user password, unless you specifically set a special Keychain password, which you can do in Keychain by choosing Edit > Change Password for Keychain "*keychain name*". For more advice on Keychain, see [Take Control of Passwords in Mac OS X](#).

Connect in Windows XP

In this subsection, I first look at how to make a basic connection. I then cover a few more advanced options, and look at how to create a preferred network profile. In all cases, my steps apply specifically to Windows XP Service Pack 2 (SP2).

Discovery and connecting

To start setting up a Windows computer to connect to a wireless network under Windows XP Service Pack 2, right-click the wireless network icon in the System Tray and choose View Available Wireless Networks.

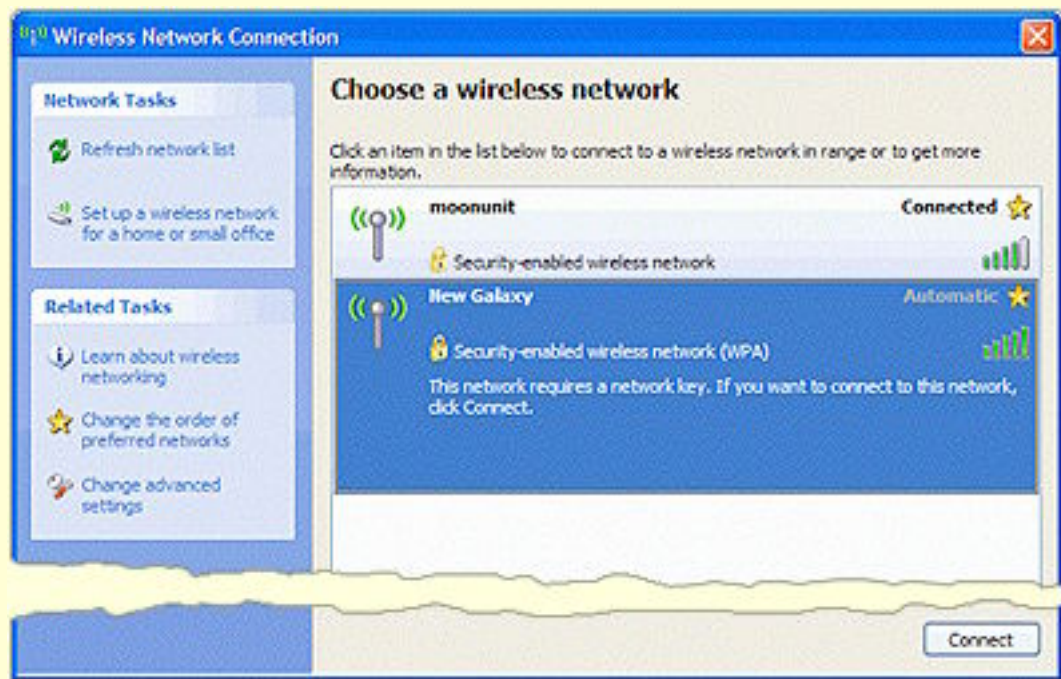
Windows responds by showing any networks that it can see, along with info about the status and nature of each one (**Figure 28**). This is an enormous improvement in SP2 over previous XP releases, which left you guessing.

TIP WATCH OUT FOR WIRELESS ZERO CONFIGURATION

If Windows XP says that another program is controlling wireless access or that it can't use the wireless adapter, Wireless Zero Configuration may be at fault. Despite its name, it needs hand-holding: Go to Control Panels, open Administrative Tools, then open Services, and finally select Wireless Zero Configuration. Click the square stop button at the top of the Services window; after you've been told that the service has stopped, click the triangular start button.

That typically takes care of the problem.

FIGURE 28



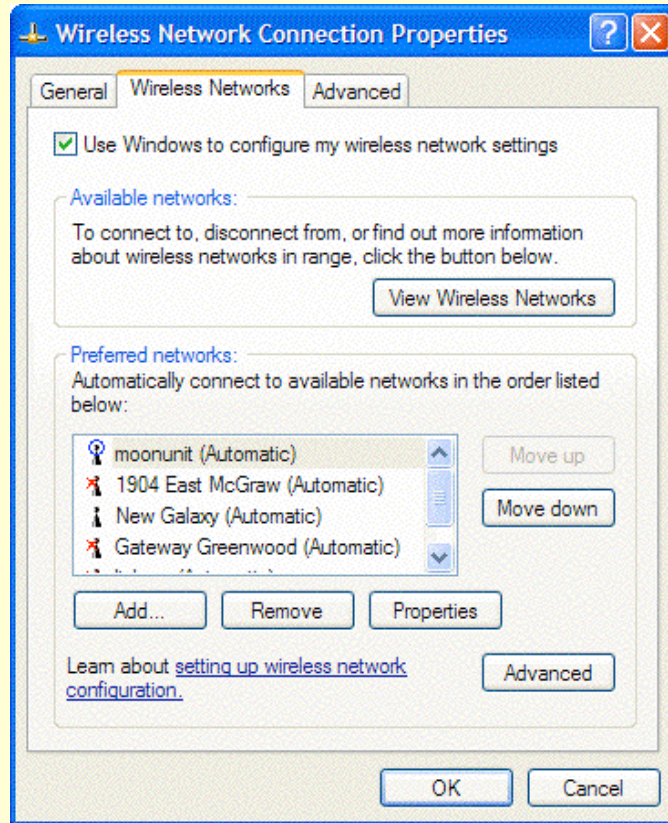
Windows shows you all the networks that it can see in the vicinity, as well as their security parameters and signal strength.

Now, select a desired network and click Connect, at which point you're prompted for any encryption keys needed to join.


Advanced connection options


Now that you've established a connection, you can tweak aspects of that connection. To see more options, at the left, in the Related Tasks list, click Change the Order of Preferred Networks. That brings up the Wireless Networks tab of the Wireless Network Connection Properties dialog (**Figure 29**).


FIGURE 29



You can use this tab for many tasks, such as setting which networks you prefer to connect to in which order when more than one is available (use the Move Up and Move Down buttons).

The  symbol at the top of the Preferred networks list marks the currently connected network.

A red x () marks any networks that are not visible.

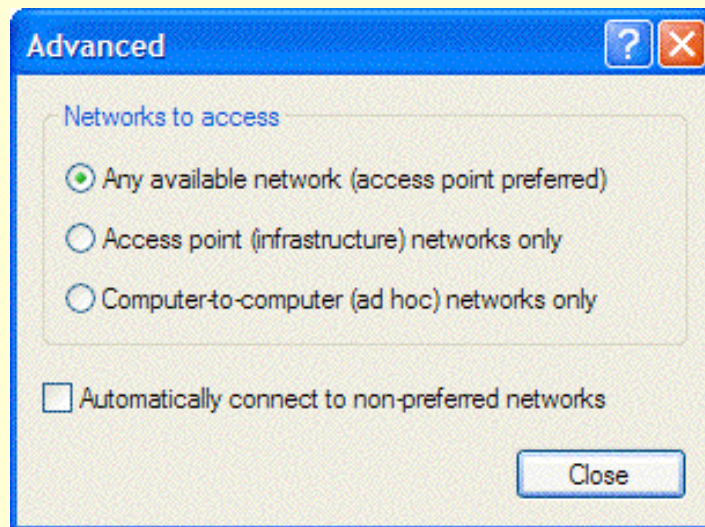
An icon by itself () means the network is available in the vicinity.

This dialog box is a bit of a powerhouse despite its demure appearance. Using it as a launching pad, you can:

- Re-order your preference for which network your machine automatically connects to. Select a network name and click the Move Up or Move Down button to rearrange it.
- Add new Wi-Fi connections. Click Add.
- Delete a preferred network. Select a network and click Remove. Your computer no longer automatically joins that network.
- Set advanced connection properties: Click the Advanced button and then choose whether to connect to any available network, only to base station Wi-Fi networks (access point or infrastructure

networks), or only to ad hoc (computer-to-computer) networks (**Figure 30**). You can also choose whether to connect automatically to non-preferred networks—ones that you haven't already set up profiles for. I recommend leaving that box unchecked.

FIGURE 30



The Advanced dialog box controls how your computer connects to available networks that it finds.

Creating a preferred network profile (WPA/WPA2)

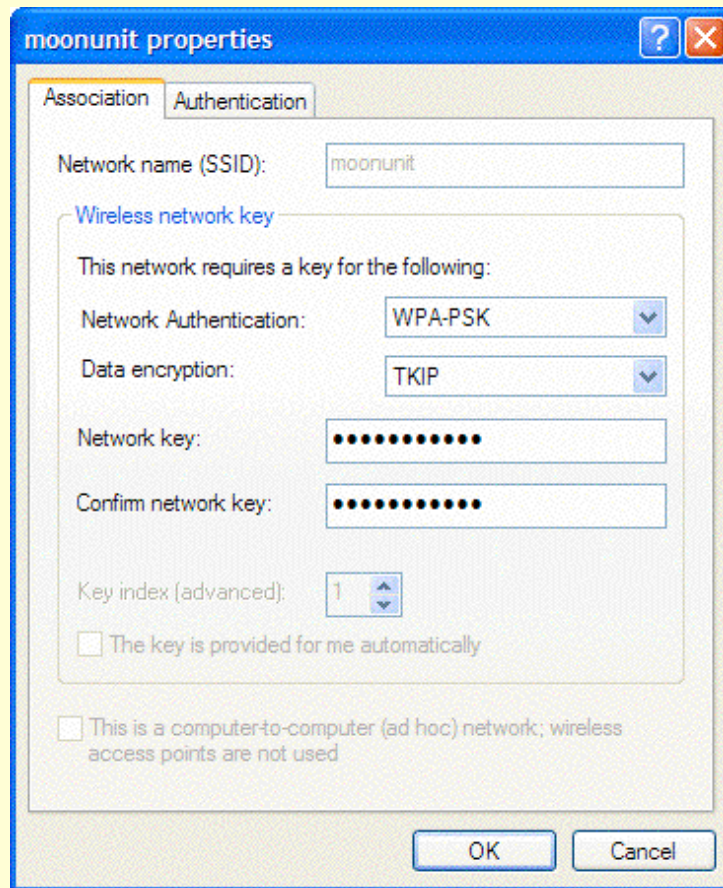
To set up a stored preferred network profile with WPA/WPA2, follow these steps:

(I don't describe how to use WEP encryption here because you are unlikely to be limited to WEP on a Windows XP SP2 system when connecting to an Extreme N!)

1. Navigate to the Wireless Networks tab for a Wi-Fi adapter as shown in **Figure 29** (previous page).
2. Now, either:
 - Add a new profile by clicking Add.
 - or
 - Select an existing profile, and click Properties.
3. If you don't already have one filled in, enter the network name (SSID).

4. Set network authentication to WPA-PSK, and set data encryption to TKIP for WPA, or to AES for WPA2 (**Figure 31**).

FIGURE 31



Choose WPA-PSK and TKIP in order to enter your WPA key; choose AES from the Data Encryption pop-up menu for WPA2.

5. Enter your WPA or WPA2 passphrase in Network Key and again in Confirm Network Key. Since you can't see the key as you type it, you can't verify visually that you have typed it correctly. Retyping the key helps ensure that you've entered it correctly.
6. Click OK.

Windows stores the profile. You can then drag the profile to make it more or less preferred than other networks already listed.

Connect in Windows Vista

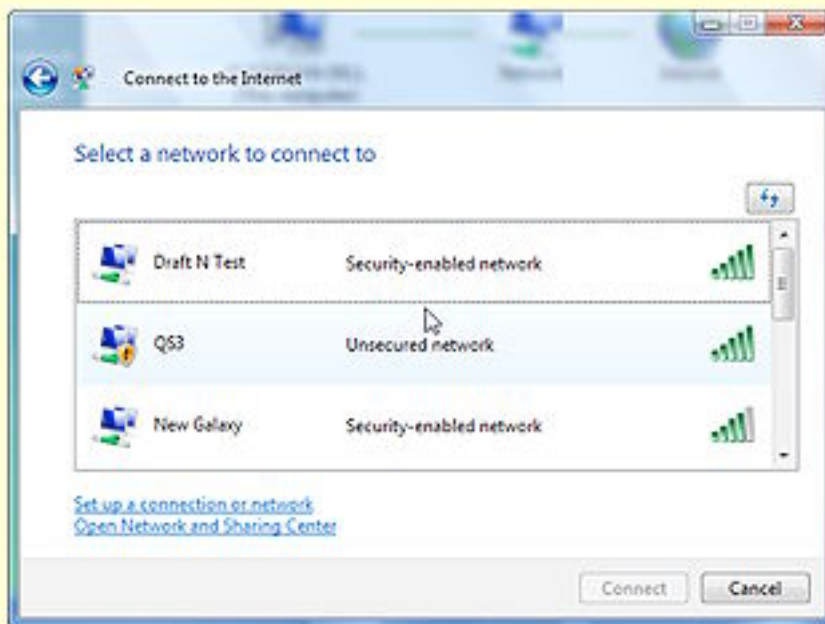
Windows Vista streamlines connecting to a Wi-Fi network by providing much clearer information than Windows XP's process along with a better designed interface for working with wireless networks.

Warning! Because Draft N is in flux, a Windows computer with an 802.11n adapter might have trouble making a connection to the Extreme N. In testing, I found I couldn't get the highest speed connection rates using an Intel Draft N card that had been released at the same time as Apple's N enabler and Extreme N (original). Firmware updates due in late 2007 should improve this situation enormously.

Discovery

To see what Wi-Fi networks are available in Vista, right-click the Network icon in the System Tray and select Network and Sharing Center. Click Connect to a Network from the left-hand Tasks list. This reveals a list of wireless networks (**Figure 32**). If you hover the pointer over a network, more detail is revealed, such as the type of network encryption.

FIGURE 32



View available networks.

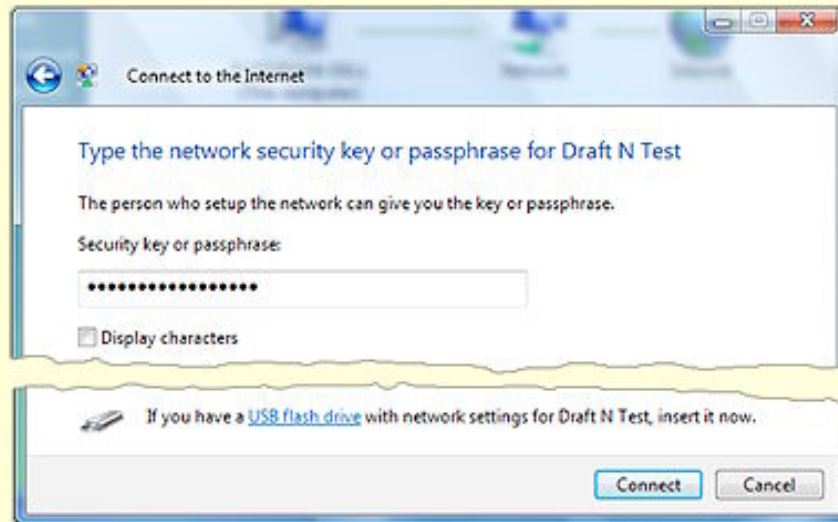
Connecting

Let's connect to a Wi-Fi network with Vista. You can double click a network in the browser shown above in **Figure 32**, or select a network and click the Connect button to start:

- **Open network:** If the network is open, Vista warns you that there's no protection with an exclamation point in a shield.

- **Secure network:** A secure network appears in the list as a “Security-enabled network,” and when you select it and click Connect, Vista prompts you for an encryption password (**Figure 33**). Unlike in XP, you need only enter the key once—I mean, if it’s wrong, it’s going to tell you, right? Vista, like Mac OS X, handles the password type automatically, but doesn’t tell you what kind of encryption is being used. You can also select the Display Characters checkbox to see what you’re typing.

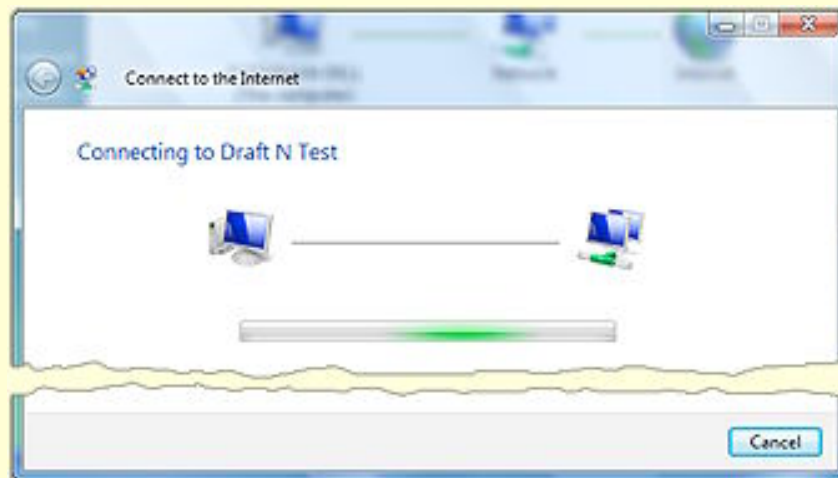
FIGURE 33



Enter the security key to connect to the network.

Next, Vista shows a dialog while it’s trying to connect, and even warns you if the connection is taking longer than usual to hook up (**Figure 34**).

FIGURE 34



The progress bar shows that something is happening while the connection is set up.

Managing profiles

Vista offers a new profile manager to help store information about networks you'll connect to on an ongoing basis. In the Networking and Sharing Center, click Manage Wireless Networks in the left-hand Tasks list. The resulting dialog is shown in **Figure 35**.

FIGURE 35



You can add and configure networks that you connect to regularly in Vista's profile manager.

To add a profile, follow these steps:

1. Click the Add button.
2. Make one of the following choices:
 - Choose Add a Network That is in Range of This Computer (scan for networks).

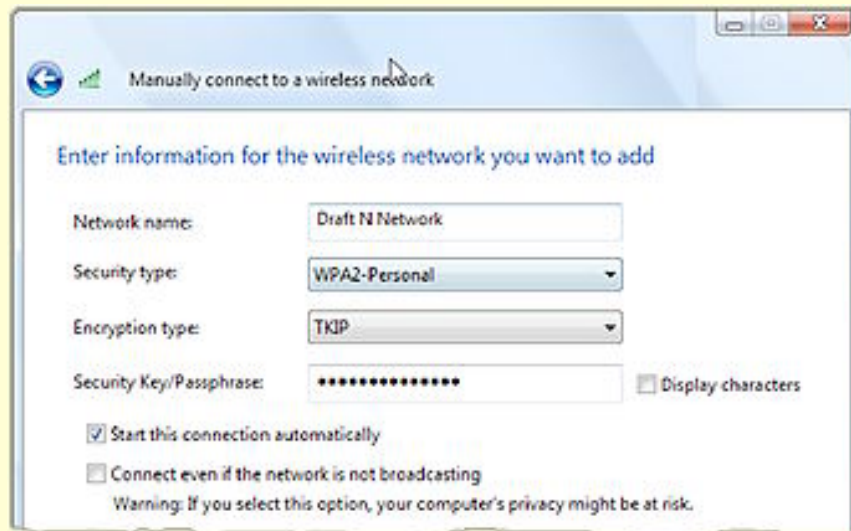
Now enter an encryption key when prompted. Vista will store the key along with your other network details.

- Choose Manually Create a Network Profile (enter the network name).

Now, you can enter your network's name, encryption type, and security key (**Figure 36**):

- ◇ For WPA, choose WPA-Personal from the Security Type pop-up menu, and TKIP from the Encryption Type pop-up menu.
- ◇ For WPA2, choose WPA2-Personal from the Security Type pop-up menu and either TKIP or AES from the Encryption Type pop-up menu.

FIGURE 36



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: Draft N Network

Security type: WPA2-Personal

Encryption type: TKIP

Security Key/Passphrase: ***** Display characters

Start this connection automatically

Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Set up a manual profile for a network you connect to more than once.

3. Click Next and then Close.

The profile appears in the networks list.

CONNECT MULTIPLE BASE STATIONS

Wi-Fi is described as reaching “only” about 150 feet, which is a very rough estimate of the radius of older 802.11b and g devices. With an Extreme N, the distance is much farther. But you can also extend the covered area by adding more base stations with overlapping signals.

As a Wi-Fi adapter in a laptop or handheld moves across overlapping areas, it can automatically switch base stations while maintaining a continuous network connection—as long as you’ve set the network up right.

While it’s always critical to follow instructions exactly when setting up any kind of network gear—or almost anything computer related—extending a network with more base stations is particularly rough because a failure to check one box or enter exactly the right text could result in a network problem that none of the base stations can accurately report.

If, in following the steps below, you find yourself stymied, retrace your steps from the start and see what went wrong.

When you extend a network, the additional base stations tend to be *dumb*; that is, they don’t assign out addresses or handle other features you think of as belonging to a base station’s set of options. Rather, one base station remains *smart*, offering DHCP and NAT (if needed), among other network choices. The rest pass through traffic from that main unit. Dumb base stations are typically called *access points* to distinguish them from *routers*.

Because dumb base stations (access points) simply pass traffic through, an adapter retains the same IP address as it switches from one base station to another, thus maintaining a continuous connection in most cases.

There are two mix-and-match methods of extending your network:

- Add base stations via Ethernet
- Add base stations wirelessly via Wireless Distribution System (WDS)

I write “mix and match,” because you can use any combination of Ethernet and WDS to build a network. Let’s start with the simpler case, which is extending a network via Ethernet.

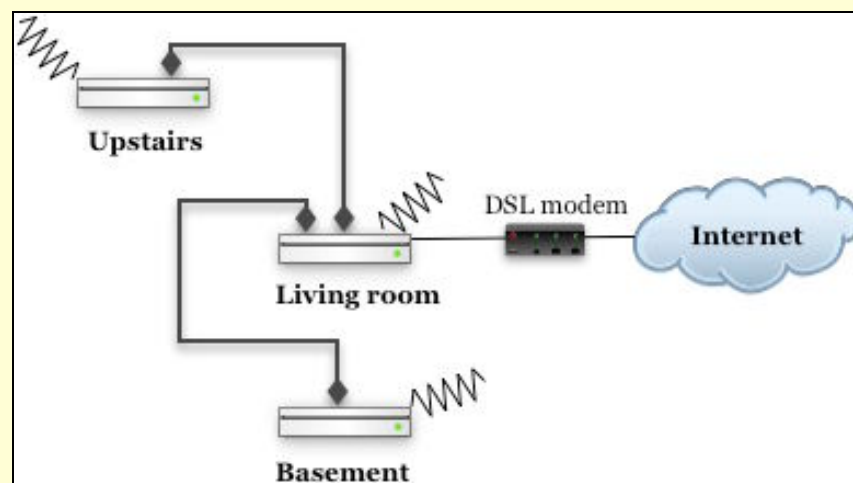
Add Access Points via Ethernet

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

Different names for seamless networks: In [Mix Legacy, New N Networks](#), I will advise you to set different network names for the old and new networks. That advice is designed to keep the networks separate. However, when adding access points to grow a single network, you keep the same name so that the connecting computers see the network as a single entity.

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 37**). However, you can also use wireless connections or electrical connections to form that network backbone, as I describe ahead in [Bridge Wirelessly](#) and [Extend with HomePlug](#).

FIGURE 37



A common Ethernet backbone connects one base station in the living room, another upstairs, and a third in the basement.

The most important part of adding access points is choosing the Wi-Fi channels for them wisely. Because each access point can communicate over a unique hunk of spectrum, you can avoid interference by making sure that no adjacent APs use the same frequencies. See [Configure the Spectrum and Channel](#) for more details on how to pick channels. Typically, all the base stations on an extended network will use either the 2.4 GHz or 5 GHz band for simplicity, but it's not strictly necessary (see [Mix Legacy, New N Networks](#)).

Set up a main wired base station

Your main base station should be plugged into your broadband connection, and configured as discussed in [Set Up Your Network](#) for setting up a base station to share addresses.

Where you deviate from those instructions is in choosing the channel for the base station to operate on. You need to select the 2.4 GHz or 5 GHz channel manually, rather than using the Automatic setting, so that you can set additional base stations that overlap to use different channels. Instead of following the procedure detailed in [Set a band and channel](#), follow these steps:

1. Launch AirPort Utility, connect to your base station, and choose Base Station > Manual Setup.
2. In the AirPort pane's Wireless view, choose a numbered channel from the Channel pop-up menu.
 - If you chose from the Radio Mode pop-up menu either "802.11n (802.11b/g compatible)" or "802.11n only (2.4 GHz)," select channel 1, 6, or 11. These are the "clearest" channels that can be used in overlapping areas.
 - If you chose from the Radio Mode pop-up menu either "802.11n (802.11a compatible)" or "802.11n only (5 GHz)," hold down the Option key to select a 5 GHz channel manually, such as 36.
3. Click Update to restart the base station with these changes.

Set up additional wired base stations

Adding additional access points is straightforward:

1. Launch AirPort Utility, connect to your base station, and choose Base Station > Manual Setup.
2. In the AirPort pane, choose the Wireless view.
3. Enter the same Network Name as your main base station (this enables seamless roaming).
4. Choose a channel that won't interfere with your main base station or other base station's choices:
 - In 2.4 GHz (B, G, or N), any three base stations can uniquely use channels 1, 6, and 11 with the least interference. If you set your main to 1, set an additional one to 6, for instance.
 - In 5 GHz (A or N), all channels are nonoverlapping. But if you use the "wide" channel mode, an Extreme N uses the equivalent of channels 36 and 40 at the same time. Choosing channels eight numbers apart for base stations that have overlapping signals produces the best results; those would be 36, 44, 149, and 157.
5. Choose the same Wireless Security option and enter the same Wireless Password as on your main base station.
6. Click Update to restart your base station with the new settings.
7. Plug your additional access point into your main base station via Ethernet, connecting the cable from the WAN port on the additional access point either to a LAN port or to an Ethernet switch connected to a LAN port on the main base station.

EXTEND WITH HOMEPLUG

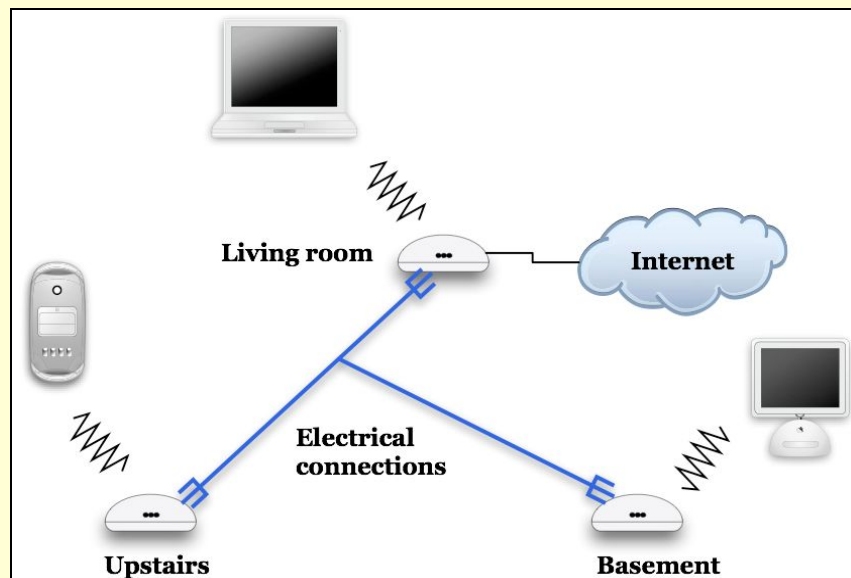
What's the most robust and ubiquitous wired network in your home? The electrical system! We don't think of data transmitting over power, but all wired networks use electricity to encode data. In the case of powerline networking, small adapters plugged into outlets modulate data over the 60-hertz (Hz) frequency used in U.S. power. At least three incompatible versions of powerline networking now exist, operating at speeds up to 200 Mbps.

Powerline networks have no central hub in most cases. Mac users should purchase Ethernet bridges, which offer a single Ethernet jack. You plug a cable from a Mac into this bridge, plug the bridge into a wall socket, and you're done. The powerline system handles communication among all the adapters on your electrical network.

When I say "wall socket," I do mean *wall socket*: powerline networking typically cannot work when an adapter is plugged into a power strip.

To extend a wireless network, simply place your access points in appropriate locations, configure them as described above for Ethernet network extension, and then plug them into HomePlug Ethernet bridges (**Figure 38**). And that's it.

FIGURE 38



A powerline network works like Ethernet over electrical outlets.

Bridge Wirelessly

Wireless Distribution Service (WDS) is a neat way to extend an AirPort network without running wires between locations. As I noted 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.

TIP You can mix and match WDS with Ethernet-extended networks, too. Each cluster of WDS machines can work together, and then the “main” base station in that group—see below—can hook into a larger network via Ethernet as an additional base station.

You can also set a main base station to be both a WDS base station and to handle serving DHCP to computers over Ethernet, which allows it to be the root of both kinds of networks without additional configuration.

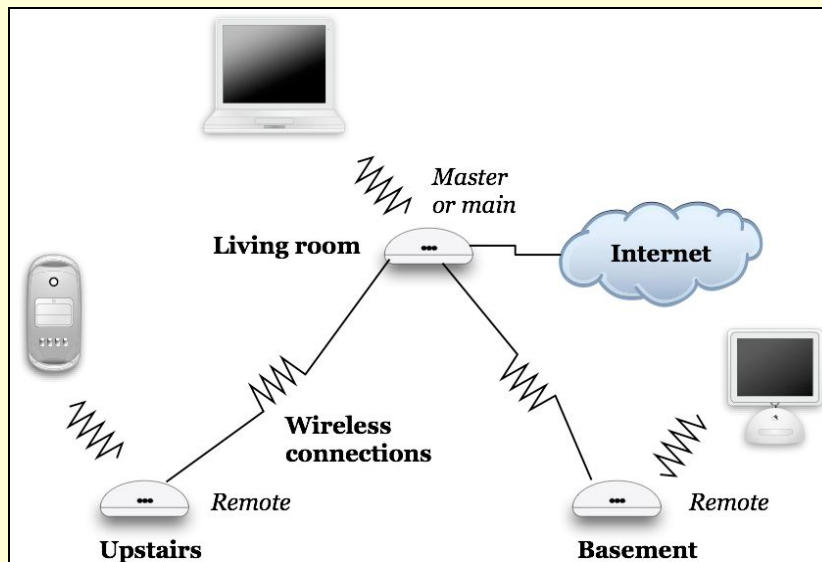
How it works

WDS works much like plugging an Ethernet hub into an Ethernet switch. An Ethernet hub interconnects 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 has information about which computers (by MAC address) are on other segments; this info allows the switch to transfer data across segments.

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 39**).

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 nearly 100 Mbps on an 802.11n network, even splitting that into pieces still provides plenty of usable bandwidth.

FIGURE 39



The same basic setup for an Ethernet-connected network can work with WDS.

Here, each base station is set to WDS and also to serve access to local computers wirelessly.

Distribute wirelessly

In general, to set up WDS you need to know the MAC address for each of the wireless gateways you want to connect (see [What and Where Is a MAC Address?](#), earlier, p. 59).

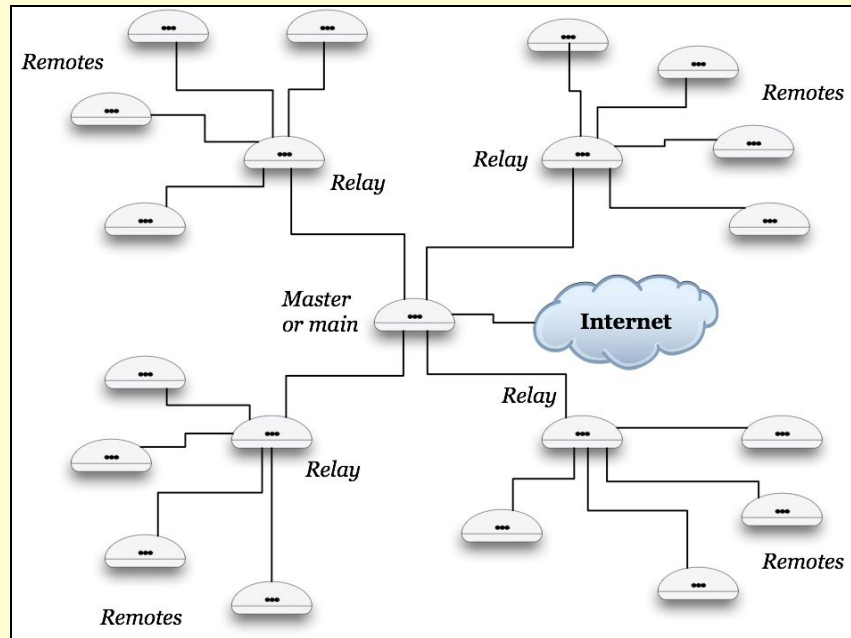
Mix and match: *You can mix and match an older or newer Extreme and the AirPort Express, as long as you recall that the 802.11g devices slow down overall network performance both by the general backward compatibility overhead hit (about 10 percent loss there), and when they're actively sending or receiving.*

Resolved bug—Extremes didn't mix: *In testing for this first edition of the book, I found WDS would not work between an Extreme N (original) and an Extreme 2003. When I tested the Extreme N (gigabit), I had no such troubles.*

Apple requires that you configure one device as the *main* base station; you should choose 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 the Internet. Finally, Apple defined a *relay*, which a remote can connect to and which is in turn connected to a main. Relays can't connect to relays; remotes can't connect to remotes. You could have 4 remotes on each relay

and 4 relays connected to a main for a total of 21 base stations (Figure 40), although bandwidth would be enormously reduced.

FIGURE 40



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

THE HIDDEN NODE PROBLEM

In a wireless network in which more than two access points connect among themselves in any manner, 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. Wi-Fi 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 other problems. When designing a network to use WDS with more than a few access points, you may have to give this issue some consideration, keeping all base stations within at least weak reception range of each other. In some cases, you’ll experience reduced performance if you ignore it; in others, the network might mysteriously vary in its quality and reliability.

To set up a WDS network, follow these steps, repeating for each base station you need to configure. There are two separate methods: one for all-Extreme-N networks (next page); another for a [Mix of Extreme N and older Extreme/Express units](#), ahead.

All Extreme N

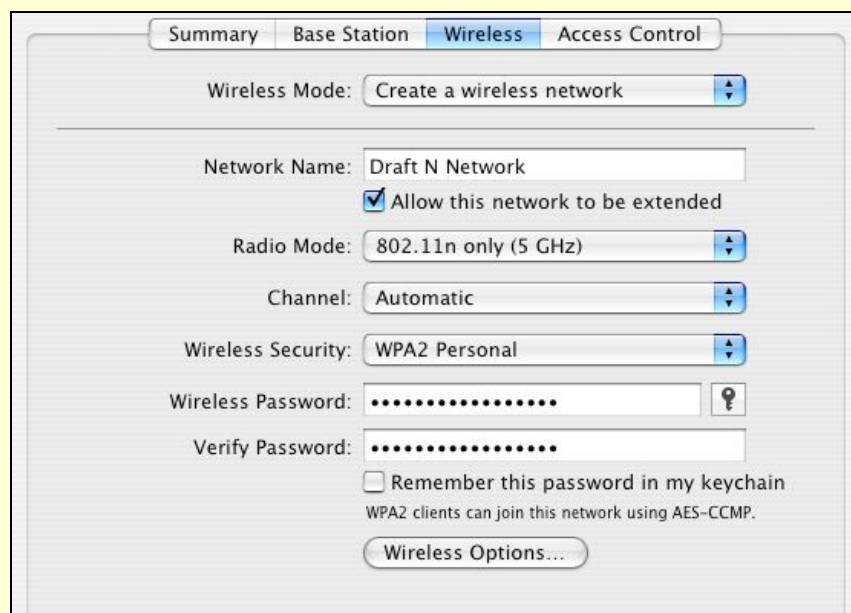
Apple rather oddly added a way for Extreme-N base stations to configure themselves via WDS without providing enough cues for most of us—myself included—to figure it out. You have to read page 46 of their ebook on designing 802.11n networks to find this out! And even then, it's a bit obscure. (See *Designing AirPort Networks Using AirPort Utility*, a free download from <http://www.apple.com/support/manuals/airport/>.)

Warning! *This option works only with Extreme-N base stations. If you set up an Extreme N as your main and try to connect with 802.11g Extreme or Express models, AirPort Utility doesn't list the necessary Wireless Mode option. If you set up an 802.11g AirPort as your main, and try to connect via Extreme N, AirPort Utility tells you after you restart that the base station you're trying to connect to lacks the proper checked option.*

Configure the main base station

1. In the AirPort Utility, in the toolbar, click AirPort.
2. In the Wireless view, choose Create a Wireless Network from the Wireless Mode pop-up menu (**Figure 41**).
3. In the same view, check Allow This Network To Be Extended.
4. Click Update to restart the base station with that setting.

FIGURE 41



Check Allow This Network To Be Extended to make an Extreme N the main base station in a WDS network.

Configure additional base stations

1. In AirPort Utility, in the toolbar, click AirPort.
2. In the Wireless View, select Extend a Wireless Network from the Wireless Mode pop-up menu.
3. Check Allow Wireless Clients if you want the remote base station to be available via Wi-Fi, not just to Ethernet-attached computers.
4. In the same view, set your Wireless Security choice and Wireless Password to be identical with your main base station.
5. Click Update, and you should be prompted after the base station restarts for the base station password of the main unit. (If the password is the same for the main and additional base station, you may not be prompted.)

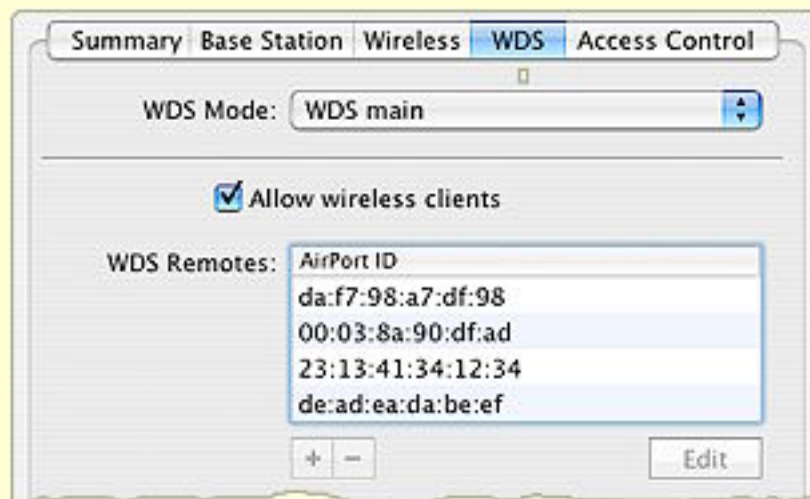
Mix of Extreme N and older Extreme/Express units

1. Launch AirPort Utility, select a base station to configure, and choose Base Station > Manual Setup (Command-L).
2. In the AirPort pane, click the Wireless button.
3. From the Wireless Mode pop-up menu, choose Participate in a WDS Network

A WDS button appears in the AirPort pane.
4. Click the WDS button.
5. If you want this unit to act just as an Ethernet extender or a bridge between a main and a remote, uncheck Allow Wireless Clients. In this mode, wireless clients can't connect to a base station, but the Ethernet port is active and a main, remote, or relay could connect to other base stations via WDS.
6. Set radio mode, channel, base station password, wireless security method, and wireless password identically:
 - In the AirPort pane, in Base Station view, set the Base Station Password.
 - In the AirPort pane, in the Wireless view, set the remaining items: Radio Mode, Channel, Wireless Security, and Wireless Password.

7. In the WDS view, enter the AirPort ID (Apple's name for the "air" interface's MAC address on a base station; see [What and Where Is a MAC Address?](#) (p. 59) as follows:
 - **Main base station:** Click the button at the bottom of the WDS Remotes list to enter the AirPort ID of the base station(s) that you want to add, up to four total (**Figure 42**).
 - **Remote base station:** Enter the AirPort ID of the main base station in the WDS Main field.
 - **Relay base station:** Enter the AirPort ID of the main base station in the WDS Main field and use the to enter WDS remote base stations.

FIGURE 42



When configuring a main base station, click the button to enter each base station in a WDS network in turn.

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

If WDS has failed to work, AirPort Utility will flash the light on the front of an Extreme N amber while displaying an amber icon next to the base station's icon.

Troubleshooting by double-checking or re-entering: *If you have problems after following these directions, remember that the frequency, channel, base-station password, wireless security method, and wireless password must all be identical on every WDS base station (Step 6). Failing that, ensure that the MAC addresses were entered correctly on each base station, (Step 7).*

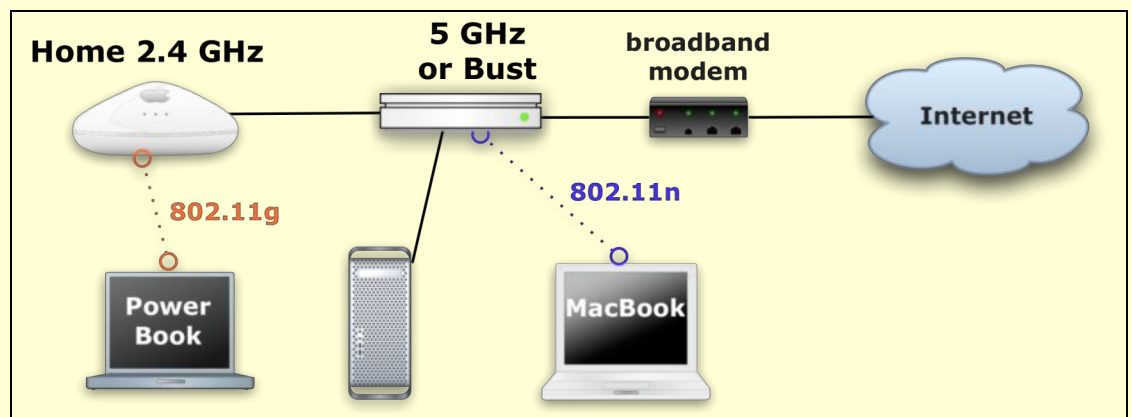
MIX LEGACY, NEW N NETWORKS

I expect that many readers of this book already have an AirPort Extreme from 2003 to 2006, or another 802.11g gateway. If that's the case for you, you may be thinking of shutting down that network in favor of a new one. But to achieve your greatest efficiency, I'd like to suggest that you run two networks: one operating in 2.4 GHz and handling computers and devices with 802.11b or 802.11g built in; the other, an Extreme N using 5 GHz and handling only newer adapters.

This is especially worthwhile if you expect to move lots of files across your network, or use Apple TV wirelessly, where you'll need a lot of unimpeded bandwidth to have video stream at its best quality.

Setting up a two-band network isn't hard, particularly because the Extreme N has an Ethernet switch built in. The goal state for the network is shown in **Figure 43**.

FIGURE 43



The finished mixed network: The Extreme G and desktop Mac are connected to the Extreme N's LAN Ethernet ports. A PowerBook connects via 802.11g to the older base station; a MacBook connects using 802.11n to the newer base station. The Extreme N's WAN port is connected to the broadband modem, which is in turn a conduit to the Internet.

Update Your Older Base Station

Your older base station needs to have three specific settings changed in order to work in this configuration:

- Its network name should make clear that it's a distinct network.
- Connection Sharing must be set to Off (Bridging), so that the existing base station doesn't create a nested set of private network addresses.
- The base station needs to obtain its address via DHCP from the new 5 GHz base station.

NOTE If you already have a DHCP server running on a LAN, you can skip connecting your existing base station to your new Extreme N base station. The existing base station can obtain an Internet address from your network's DHCP server instead by being plugged into any Ethernet switch on the network.

To configure and connect your old base station:

1. Launch AirPort Utility, select your existing base station, and choose Base Station > Manual Setup (Command-L).
2. At the top of the window, click the AirPort icon, and then click the Wireless button.
3. Change the Network Name to something descriptive, like **Home 2.4 GHz** or **Old Slow Network**.
4. Click the Internet icon.
5. From the Configure IPv4 pop-up menu, choose Using DHCP.
6. Select Off (Bridging) from the Connection Sharing pop-up menu.
7. Click Update to restart the base station with the new settings.
8. Now, plug an Ethernet cable from the WAN port of your 2.4 GHz base station into any of the three LAN ports of the Extreme N.

Wireless base station connections won't work: *While you can connect two or more Apple base stations together via Wi-Fi using Wireless Distribution System, that works only when the base stations are using the same frequency band, channel, base station password, and wireless security method and password. See [Bridge Wirelessly](#).*

Configure Your New Extreme N

Next, you need to set up your Extreme N to use the 5 GHz band:

1. Launch AirPort Utility, connect to your Extreme N, and switch to Manual Setup (Command-L).
2. Click the AirPort icon and then the Wireless button.
3. Enter a unique and descriptive name in the Network Name field, like **5 GHz** or **Bust** or **Fast New Network**.
4. From the Radio Mode pop-up menu, choose 802.11n only (5 GHz).
5. Click the Wireless Options button and check Use Wide Channels. (This option is available only in certain countries, including the United States.)
6. Click the Internet icon.
7. Make sure that Connection Sharing is set to Share a Public IP Address (bottom pop-up menu).
8. Click Update to restart the base station.

Now you have two independent Wi-Fi networks operating at peak performance without contention between them.

Put Printers in the Right Place

A number of readers of the first edition of this book wrote in after reconfiguring their networks as described above because their printers stopped working. After some troubleshooting, we collectively discovered that printers needed to be moved from the old 802.11g network to the new Extreme N network to work reliably.

A setting change was also needed. Follow these steps:

1. Unplug your USB printer from the old base station; you needn't power down the printer unless you also plan to move it.
2. Plug the USB printer either directly into the new Extreme N base station, or into a USB hub that's plugged into the base station.
3. Launch AirPort Utility, connect to your Extreme N, and switch to Manual Setup (Command-L).
4. Click Printers on the toolbar, and confirm that the printer appears in the list of printers shown.
5. If you are plugging the Extreme N into a larger LAN, check the Share Printers over Ethernet WAN Port box so that computers on that larger network can access the printer, too.

REACH YOUR NETWORK REMOTELY

When you share an Internet connection among one or more computers on a local network using private addresses, you give up an easy way to connect from the outside world to a service, like a Web server or fileserver, that's located on one of those local computers. Public IP addresses allow anyone on the Internet to connect directly to a computer, barring any firewalls or other blocks in place, but private IP addresses are specifically non-routable without a bit of extra work.

Extreme N and AirPort Utility mark a major breakthrough for Apple, finally adding features that have been found in other gateways for years, but adding the usual Apple twists: their products are later than similar ones from competitors, but they are easier to use. You can choose from three different methods of reaching your network from the outside world:

- **Basic port mapping and reserved addressing:** While earlier Apple base stations offered *port mapping*, a way to connect a public port on a routable address on the base station with a private port on a locally connected computer, the Extreme N also lets you assign addresses to local computers on a persistent basis—these *reserved* addresses don't change over time. When the base station is restarted, or when the computer is restarted, the same address is assigned to the computer once again.

This reservation system makes the whole mapping system work consistently with less effort. I cover these options beginning on the next page.

- **Punch through from certain programs:** A protocol from Apple just starting to become more widely used, called *NAT-PMP* (NAT plus Port Mapping Protocol), helps with port mapping without requiring any special configuration on a computer or a base station. You can find out more in [Punch Through from Certain Programs](#).
- **Use one computer as your default host:** There's a coarser way to make NAT work, too, allowing a single computer behind the NAT gateway to act as if it's directly connected to the Internet. I describe the *default host* option in [Set a Default Host for Full Access](#).

Map Ports for Remote Access

Port mapping relies on network address translation (NAT), which I've noted only in passing previously in this book. NAT acts as a gateway between a WAN IP address for a router reachable from a larger LAN or the public Internet, and the private addresses hidden behind NAT on the base station's LAN.

NAT maps private to public connections

When a computer within the LAN wants to connect to the Internet, the NAT software creates an association between that computer's outgoing connection and a public port on the WAN IP address of the base station. (I talk more about [Ports](#) in a sidebar on the next page.)

When, for instance, a LAN-connected computer wants to retrieve a Web page, that computer might send a request from its IP address (192.168.1.100) using port 5509. (Ports for outbound connections are arbitrarily numbered above 1024.) The NAT server receives that connection and creates a request over the Internet using the WAN IP address and typically a different port. So the NAT gateway's request might originate from a public address such as 36.44.0.6 with a port of 12087.

The Web server receiving the request doesn't know about the original computer behind the NAT. Rather, the Web server responds by sending HTML for the requested Web page to port 12087 on IP 36.44.0.6. The NAT server retains a list of associations between public and private ports and addresses, and hands that Web connection over to the machine that originally requested it. This process is ugly, but it works reliably, almost all the time.

Port mapping maps public to private connections

With port mapping, you create a persistent connection that allows computers outside the LAN to connect to computers inside the LAN. This port mapping lets you expose very limited services in a way that you fully control.

When you map a port, you make the gateway connect one of its Internet-accessible ports to the same (or a different) port on a computer on the otherwise-private inside network.

PORTS

Every kind of network server you might run, including a personal Web server and your side of a multi-player online game, uses a *port* to communicate with the rest of the machine, network, or world. A port number in Internet networking can be compared to an apartment number in a typical postal mail addressing system: a computer has an IP address just like an apartment building has a street address, and each kind of service used by a computer has a port number, just like each apartment has its own number within the building.

With ports, it's as if every apartment building had the manager in unit 1, the mailroom in unit 25, a lounge in unit 80, and so forth. Ports are consistent for the same services on whatever machines those services are running on.

Taking it one step further, if you have a static IP addresses, that's like having a street-front address. In contrast, NAT-provided private addresses are like buildings within a gated compound, where nobody on the outside knows the building numbers on the inside.

If you were inside the compound, you might carry a letter to be mailed to the outside world to the compound's mailroom, and the mail carrier would pick up your letter from there. Return mail, addressed to a mailbox number in the mailroom, is delivered only to that outer mailroom, where you can receive it without leaving the compound.

Warning! *Anything you do to punch through ports or computers from the private network to the outside world reduces your security. Be careful about what you leave open. You may want to provide better security on computers that you expose in this fashion by installing active firewall and intrusion-monitoring software.*

INSTANT MESSAGING WITH NAT

You might wonder how software like iChat and Skype works behind a NAT gateway, because it seems like they have two-way communication where it shouldn't be possible. Both systems hide the fact that central servers are involved in connecting chatters:

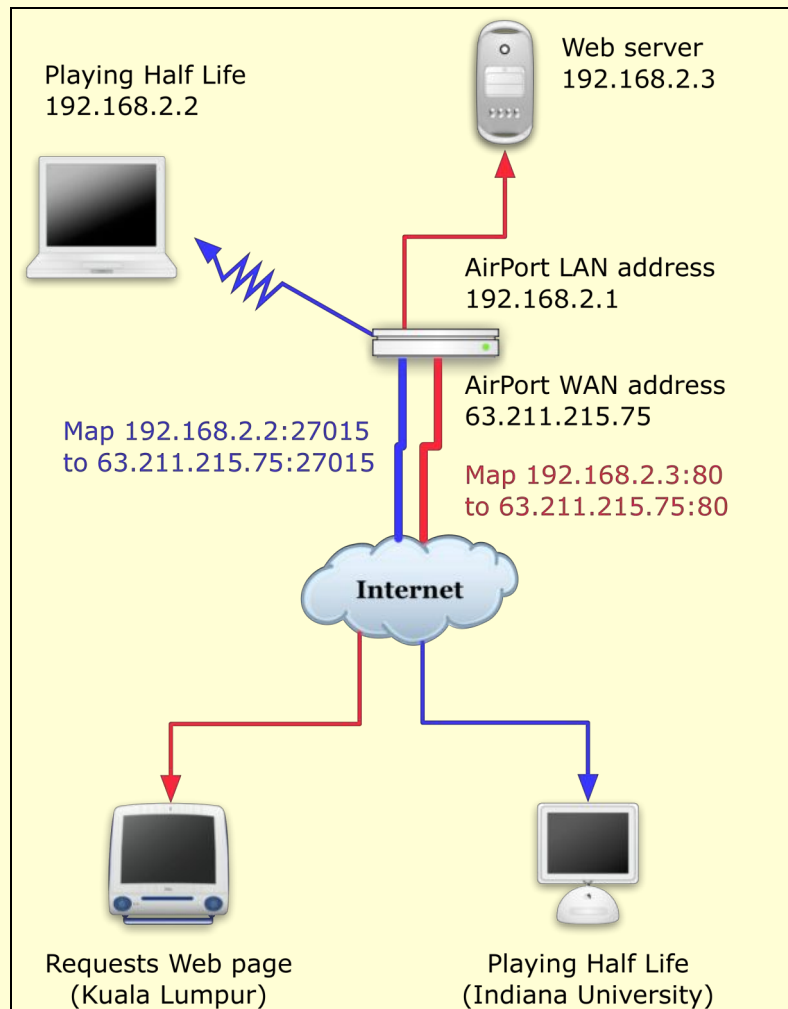
- **iChat:** In iChat, the central server is run by AOL, as iChat is part of the AOL Instant Messenger network. Each person using iChat connects to the AIM server, which maintains a persistent connection to iChat using the channel that iChat opened up. The server coordinates among everyone chatting to move messages among all those connections.
- **Skype:** Skype uses a different method, because it's decentralized. Instead of using one central server, Skype uses what it calls supernodes, or Skype clients on publicly reachable IP addresses that can coordinate connections among NAT-connected Skype users. Your computer can be picked as a supernode without you ever knowing it, but because the system is so distributed, that shouldn't affect any given user unduly.

This is also how services like GoToMyPC and LogMeIn work, where you can remotely connect to a Windows computer when on the road: the software on the computer maintains an open connection to the remote-control firm's servers.

Once you've created a mapping, the gateway listens for traffic on the specific port on its public, WAN interface. When traffic arrives and a connection needs to be opened, the gateway reroutes the traffic from that public interface port to the appropriate private address on its LAN interface, whether that's a Wi-Fi LAN or a wired LAN (**Figure 44**). In the figure, I show the example of operating a Web server and playing Half Life behind a NAT gateway.

Using port mapping reliably has two parts: set a persistent private IP address for a computer on the LAN, and then set a persistent port mapping between a port on the base station and a port on the LAN computer.

FIGURE 44



One user on a laptop is playing Half Life over the Internet; another computer on the network is running a Web server. When a user in Kuala Lumpur requests a Web page, the gateway maps the incoming request on port 80, the standard port for Web servers, from its public address to the Web server's private address. Likewise, when traffic needs to run over port 27015, the standard port for Half Life, the gateway connects traffic from a player at Indiana University with our network's laptop user.

Set a reserved address

Before the Extreme N, you had to use a variety of complicated work-arounds to maintain a private NAT-enabled address on an AirPort network. Now, you can create this with just a few keystrokes and clicks.

For each computer with which you want to use port mapping, you should create a DHCP reservation, which I describe fully in [Reserved addresses](#), earlier.

I recommend creating a text file or other simple list that contains a list of your computers in some descriptive way—the owner or its unique name—and the corresponding reserved addresses.

Once you've reserved addresses, you can set up effective port mapping.

Dynamic addresses don't cut it: *Port mapping ties a public port to a specific private IP address, so if you don't use a DHCP reservation, you can't easily keep port mapping working without constantly making changes to the Extreme N configuration and restarting—which changes the IP addresses assigned dynamically!*

Set base-station-to-computer port mapping

To use port mapping, you need to know which ports to map! This can be trivial. You could map port 80 on the public side to port 80 on a given computer on the private LAN, and establish a Web server connection, for instance. For games, streaming media, and other purposes, you might need to set up a bunch of ports.

Let's look first at the simple example of setting up that Web server, along with setting up ports for other services. First, we need to configure the firewall on the computer that's acting as a Web server. The firewall protects the computer from unwanted inbound connections, and must be set to allow the ones you do want. Second, we need to set up the base station to pass traffic to the newly configured port.

Running a Web server in non-server versions of Tiger:



1. Open the Sharing preference pane, and click the Firewall button.
2. Look at the upper left corner of the Firewall view. If you see Firewall Off, click the Start button.
3. To allow inbound Web server requests, make sure Personal Web Sharing is checked. (If you're using Apple's built-in Web server, the firewall On box for Personal Web Sharing is checked automatically.)
4. To allow requests for other ports or for a non-Apple Web server, click the New button, choose Other from the Port Name menu, and fill out the entries for ports as discussed a few pages ahead in [Configure the Extreme N for other ports](#).

Running a Web server in Windows XP and Vista:

Typically, you use third-party firewall software for added security, and these packages allow you to enter exceptions for particular ports, such as port 80; read their instructions for details. But Windows XP and Vista each come with a built-in firewall package that you can configure quite simply:

1. Open Control Panel from the Windows menu.
2. Open Windows Firewall.
3. In Windows Vista, click Change Settings to the right of the Windows Firewall text, and then click Continue when prompted.
4. In the General pane, make sure the firewall is set to On, and Don't Allow Exceptions should be unchecked.
5. In the Exceptions pane, click Add Port.
6. Enter Web Server in the Name field, and 80 in the Port field.
7. Click OK, and then OK again.

Configure the Extreme N to pass through to the Web server:

With the server set up to accept connections, we now can configure the Extreme N in this fashion:


1. Launch AirPort Utility, select your Extreme N, and choose Base Station > Manual Setup (Command-L).
2. Click the Advanced icon at the top of the window, and then click the Port Mapping button.
3. Click the  button to bring up the Port Mapping Setup Assistant (**Figure 45**).

FIGURE 45

Port Mapping Setup Assistant

Choose a service from the pop-up menu or enter the public and the private IP address and ports that you want to map between.

Service: Choose a service

Public UDP Port(s):

Public TCP Port(s): 80

Private IP Address: 10.0.1.201

Private UDP Port(s):

Private TCP Port(s): 80

Advertise globally using Bonjour

Service Type: _http_tcp

Cancel Go Back Continue

After you choose Personal Web Sharing from the Service pop-up menu, the correct ports are entered.

4. From the Service pop-up menu, choose Personal Web Sharing (really, this means any kind of Web server). (For a more advanced network setup, described on the next page, enter all the necessary ports in this step.)
5. Enter the reserved IP address in the Private IP Address field. (You can edit only the last number of the IP address, as the first three numbers are set in DHCP configuration.)
6. Click Continue.
7. In the next screen, enter a description for the entry so you can recall later what you meant by it.
8. Click Done.
9. Click Update to restart your base station with this setting.

After restarting the base station, you should attempt to make a connection from outside your network to the service you enabled, or have a friend or colleague initiate the connection. If the connection doesn't work, make sure the firewall on the computer running the service is configured correctly.

TIP ONE PER PORT

Here's the tricky part. If you want to run Web servers on different computers on your private LAN, you can't simply map public TCP port 80 to several computers. It won't fly. Instead, you can use different public ports; however, then visitors who type in a domain name as the Web address can't reach your alternate-port servers. You should reserve using alternate-port servers to special purposes or servers available only by clicking a link.

All Web browsers can specify a Web server not just by domain name, but also by port, in the form `http://serveraddress.com:0`, such as `http://tidbits.com:8001`.

Say you have two private Web servers, both receiving connections on port 80. Using port mapping, you would set one's public port to be port 80, and the other to be something like 8000 (a typical alternative Web server port). In port mapping, you would map port 80 to one private IP address's port 80, and port 8000 to the other Web server's private IP address at port 80. This avoids having to make any changes on the Web server, and renders the sites completely reachable.

Configure the Extreme N for other ports:

We won't all run Web servers on our private networks, however, so let's look at the options in the Port Mapping Setup Assistant more closely (**Figure 45**, previous page); these settings are nearly identical to those used when adding new ports to Tiger's firewall, too:

- **Service:** This pop-up menu is prefilled with the ports needed for many common services, like FTP for file transfer and SMB/CIFS (Windows File Sharing). If what you need isn't in that list, you have to look further.

For games and other more complex services, read the documentation for the game or program, which typically describes the port-mapping settings needed. You can also consult this extensive list: http://www.practicallynetworked.com/sharing/app_port_list.htm.

- **UDP and TCP:** These two different kinds of packets can be carried over an IP network. *UDP* (User Datagram Protocol) is often used for streaming media, while *TCP* (Transmission Control Protocol)

handles Web and other kinds of connections. Any service you might want to use could have a combination of UDP and TCP ports.

- **Port(s):** Each field for entering ports can handle a single number or a range as two numbers separated by a hyphen. You can have multiple numbers or ranges separated by commas. For instance **407, 1216-1300, 6000-7000** would be a legitimate entry.
- **Bonjour advertising and service type:** You can use Bonjour network discovery to allow access to various services by name via the WAN port. Typically, this means that in a program that supports Bonjour, like Safari, any Web site that you offered up via port mapping would appear in the browser's list of Bonjour-advertised Web sites. (In Safari, choose Bookmarks > Bonjour, and the program lists any Web sites available in this fashion.)

Punch Through from Certain Programs

Apple has developed a new protocol to help with port mapping without requiring special configuration on a computer or a base station: *NAT-PMP* (NAT plus Port Mapping Protocol) lets properly enabled programs on a computer on the LAN part of a base station's network ask the base station for the base station's public address. This new service can then be available remotely via Bonjour or through the WAN IP address.

NOTE Stuart Cheshire, an Apple employee, created both Bonjour (also known as *zeroconf* for zero configuration, in the wider Internet world) and NAT-PMP. I knew of him back when he was a grad student, writing about latency for *TidBITS*: <http://db.tidbits.com/series/1014>. You can read his Internet Engineering Task Force (IETF) draft of the NAT-PMP spec at <http://files.dns-sd.org/draft-cheshire-nat-pmp.txt>.

To enable this feature, select your base station in AirPort Utility, select the Internet pane, and, in the NAT view, check Enable NAT Port Mapping Protocol. Click Update.

The downside to the NAT-PMP protocol is that each program must have built-in support built in to work with the protocol. With regular port mapping, software can be entirely unaware that it's not exposed to the Internet.

Apple notes that for Macs behind NAT gateways, .Mac can sync its mountable iDisk more easily with NAT-PMP turned on, because that lets .Mac initiate remote connections to those Macs. With iChat AV, Apple told me that NAT-PMP enables more reliable initiation of file transfers when the feature is enabled on base stations on both ends.

There's not yet widespread use of NAT-PMP, because it's not found in routers outside Apple's. However, as Apple continues to sell its routers in great numbers, it's more likely that applications will enable the feature.

Set a Default Host for Full Access

The alternative to creating reserved addresses and port mapping for each service on each computer you want to expose from your private network is to appoint a single computer as your public machine. This exposed machine could serve any kind of service over any port without the necessity of adding port mapping rules. If one computer runs FTP, Web, and Samba servers, and no other computers on the LAN have any public services, this might be the right option.

Apple calls this machine the *default host*; other gateway makers call it the *DMZ host*. You must share an IP address over DHCP and NAT for this option to be available.

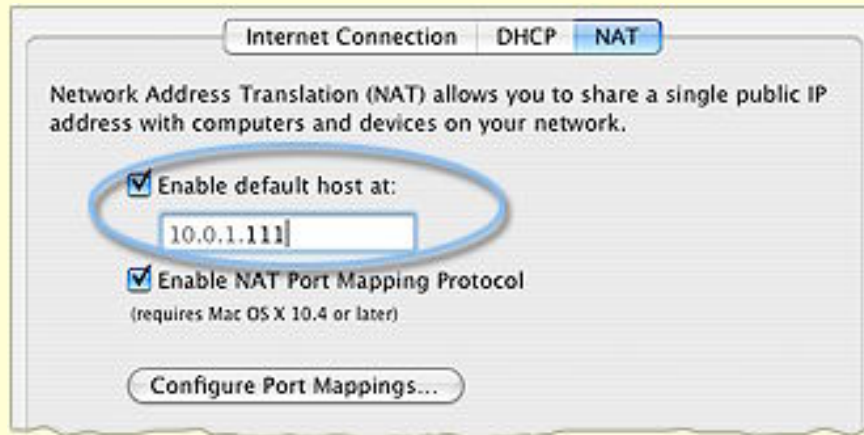
Warning! *If your Extreme N has a public IP address, your default host is as exposed as if it were on the public Internet.*

You should still use DHCP reservation to maintain the computer's private address over time; see [Reserved addresses](#).

To set up a default host, follow these steps:

1. Launch AirPort Utility, select your base station, and choose Base Station > Manual Setup (Command-L).
2. Click the Internet icon at the top of the window, and click the NAT button.
3. Check the Enable Default Host At box and enter the last number in the IP address for your default host (**Figure 46**).

FIGURE 46



To set up an exposed computer, check Enable Default Host At and enter the private IP address's last number.

4. Click Update to restart the base station with these settings.

SET UP A SHARED USB PRINTER

With a base station set up to handle local computers and hooked into the Internet, your next step may be to attach a USB printer to the base station so that it can be shared among all the local computers.

TIP ADDING TWO USB DEVICES

To attach more than one USB device to the base station, such as a USB printer and a hard disk, or more than one of either, you need to attach a USB hub to the base station, and then attach the devices to the hub. I recommend a Hi-Speed powered hub that uses external AC power; this ensures greater reliability.

Add a Printer

For each printer you want to attach to the Extreme N:

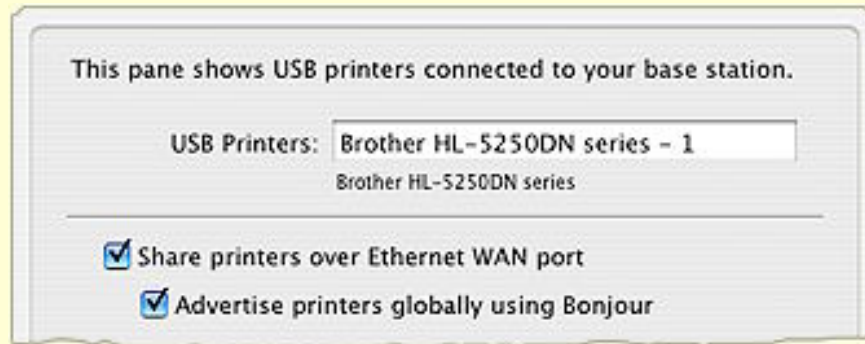
1. Plug the printer into the base station or USB hub. You should not need to reboot your base station for it to recognize the printer.
2. Give the printer a custom name and share it over a larger LAN or the Internet; see “Rename and Widely Share a USB Printer,” (below).
3. As needed, configure recent Macintoshes to connect to the printer; [Add a Shared Printer in Mac OS X](#) explains how.
4. As needed, configure Windows XP and Vista machines to connect to the printer; [Add a Shared Printer in Windows XP and Vista](#) has instructions.

Rename and Widely Share a USB Printer

Your first task in setting up a printer is to get it working with respect to your base station. You can assign the printer a custom name that appears on the network during set up. Follow these steps:

1. Launch AirPort Utility and connect to your base station, and choose Base Station > Manual Setup (Command-L).
2. At the top of the window, click the Printers icon to open the Printers pane (**Figure 47**).

FIGURE 47



You can change a printer's name as it appears on the network.

3. Enter a name for the printer in place of the default name, or leave the name that AirPort Utility prefilled in place. This name will appear in the Print dialog when you select a printer or print.
4. Check Share Printers over Ethernet WAN Port to make the printer available to other computers on a larger LAN (and even over the Internet if the Extreme N has a public IP address).
5. Check Advertise Printers Globally Using Bonjour to make the printer browsable over a larger LAN (outside the base station's private network) from all Mac OS X machines, and from Windows machines with Bonjour installed.
6. Click Update to save this change and restart the base station.

NOTE Apple briefly offered a list of supported USB printers when this shared capability first appeared, but they withdrew this list years ago when it became, in their words, “unwieldy” to maintain. If the steps above don't work, your printer may be unsupported—for more info, read the last suggestion in [Troubleshoot an Unavailable Shared USB Printer](#) (ahead about six pages).

You should also consult iFelix's unofficial list of USB printers that work with an AirPort Extreme or Express base station at <http://www.ifelix.co.uk/tech/1013.html> for the Extreme 2003 and at <http://www.ifelix.co.uk/tech/8013.html> for the Extreme N. It contains the original Apple list supplemented with details from readers of the page and tested by iFelix's maintainer.

Add a Shared Printer in Mac OS X



Follow these steps to set up printing from a Macintosh running Jaguar (you need at least Mac OS X 10.2.7), Mac OS X 10.3 Panther, or Mac OS X 10.4 Tiger to a shared USB printer:

1. Open your printer utility from the **/Applications/Utilities** folder. In Jaguar, it's called Print Center. In Panther and Tiger, it's called Printer Setup Utility.
2. Click the Add icon.
3. Now:
 - In Jaguar and Panther, choose Rendezvous from the top pop-up menu. Then, find your printer in the resulting list, select it, and click Add.
 - In Tiger, click the Default Browser icon at the top, if it's not selected already.

Your printer should appear in the list. However, if your printer doesn't show up, try the suggestions offered ahead in [Troubleshoot an Unavailable Shared USB Printer](#).

Now, your printer connection is set up. You can print from any application offering a Print command—just choose the printer from the Printer pop-up menu in the Print dialog.

NOTE You can also add a printer from the Print dialog. From the Printer pop-up menu choose the printer from the Shared Printers submenu, if it's there. If not, then choose Edit Printers or Add Printer (which command you see depends on the version of your operating system). After you add the printer, it shows up in the list of printers in the Print pop-up menu.

Warning! *Don't choose the printer from the Shared Printers submenu again, or you may create yet another instance of the printer!*

Add a Shared Printer in Windows XP and Vista

We can do it the hard way or the easy way. Let's try easy first: Bonjour for Windows! (I recommend Bonjour because it is easy to set up, but if you prefer to not install additional software, I also give directions for setting up a printer without Bonjour in Windows XP and Vista, ahead.)

Apple lets you add Bonjour network resource discovery in Windows XP and Vista with the free, downloadable Bonjour for Windows package from Apple at <http://www.apple.com/support/downloads/bonjourforwindows.html>.

Once you've installed the package, make sure your printer is turned on and follow these steps to add printers shared by the base station:

1. Launch the Bonjour Printer Wizard and click Next.
2. Select a printer and click Next.
3. Choose a printer driver if one hasn't been selected automatically for you, and click Next.
4. Click Finish to install the printer.

The printer is now available to all applications.

Add a shared printer in Windows XP

The following advice comes in general form from Mac OS X Hints (<http://www.macintoshhints.com/>), a great Web site for technical advice. I was initially stymied in my attempt to convince my Windows XP box to print to a shared USB printer, and the advice on Mac OS X Hints was of great help in getting started. Here are the steps, which you should follow after making sure your printer is on:

1. From the Control Panel, open Printers and Faxes.
2. From Printer Tasks in the list of tasks in the left navigation bar, click Add a Printer.
3. The Add Printer Wizard appears. Click Next.
4. Select Local Printer Attached to This Computer. Uncheck Automatically Detect and Install My Plug and Play Printer. Click Next.

5. Select Create a New Port (near the bottom of the screen). Choose Standard TCP/IP Port from the pop-up menu, and click Next to launch the Add Standard TCP/IP Printer Port Wizard.
6. Click Next again to show the Add Port screen.
7. For Printer Name or IP Address you have two choices, depending on whether the Windows machine is connected via Wi-Fi or Ethernet to the base station LAN, or is outside that LAN (either on a larger LAN or remotely printing over the Internet):
 - **Within the base station LAN:** Enter your base station's LAN network address—this is the first three numbers in your DHCP address range with a 1 in the fourth number's position, like 10.0.1.1.
 - **Outside the base station LAN:** Enter the base station's WAN IP address.

Leave Port Name alone; Windows will fill it in for you. Click Next.

8. On the next screen, choose Hewlett Packard Jet Direct from the pop-up menu next to the Standard radio button. I don't know why, but Mac OS X Hints found that it works. We obey. Click Next.
9. Click Finish to return to the first wizard. From the list of manufacturers and printers, select your precise model. Click Next.
10. The final screen has you name your printer. By default, it uses the name from the model type in the previous screen. You can enter a new name if you'd like, however. Select whether or not you want this printer to be your default by clicking the Yes or the No radio button. Click Next.
11. Leave the Do Not Share This Printer radio button selected unless you want this computer to share the printer to other computers, which makes no sense given that it's already a shared printer, right? (If you must be contrary, click the Share Name radio button and enter a name.) Click Next.
12. Choose to print a test page by leaving the Yes radio button selected, which is the default, and click Next.
13. Finally, click Finish.

14. Walk over to your printer, and see if a test page was printed.

If the page printed, you're ready to go. If not, check through the preceding steps to make sure you configured everything correctly or try the suggestions in [Troubleshoot an Unavailable Shared USB Printer](#), two pages ahead.

Add a shared printer in Windows Vista

Vista streamlines the process of adding a shared USB printer to a Windows setup, though not as much as Bonjour (covered a few pages earlier). Here are the steps, after making sure your printer is on:

1. From the Windows menu (the icon in the lower left of the screen), click Control Panels.
2. Double-click Printers.
3. From the menu bar at the top, click Add a Printer.
4. Click Add a Network, Wireless, or Bluetooth Printer.
5. After a moment, the printer should appear in the list of available printers. Select it and click Next.

(If the printer doesn't appear, skip ahead to "Additional Steps," next page.)

6. Vista now contacts the printer to obtain the printer's information, such as its name. If all is well, Vista will suggest you use a currently installed driver for the printer. Click Next.
7. If you want the printer to appear in Vista with a different name, enter that name. Click Next.
8. Click Print a Test Page. Then click Close in the test page window and Finish in the Add Printer wizard.

If the page printed, you're all set. If not, go through the preceding steps again to make sure you configured everything correctly or try the suggestions in [Troubleshoot an Unavailable Shared USB Printer](#), two pages ahead.

Additional Steps

If your printer didn't show up in Step 5, continue with these steps:

1. Click The Printer That I Want Isn't Listed.
2. Select Add a Printer Using a TCP/IP Address or Hostname, and click Next.
3. In the "Hostname or IP Address" field, enter an address based on your Vista computer's position in the network: connected via Wi-Fi or Ethernet to the base station LAN, or outside that LAN (either on a larger LAN or remotely printing over the Internet):
 - **Within the base station LAN:** Enter your base station's LAN network address—this is the first three numbers in your DHCP address range with a 1 in the fourth number's position, like 10.0.1.1.
 - **Outside the base station LAN:** Enter the base station's WAN IP address.

Leave Port Name alone, as Vista prefills it as you type. Click Next.

Vista tries to find the appropriate printer driver. In my testing, it fails at this stage, and requires manual selection. If Vista succeeds in finding the right driver, resume at Step 7 on the previous page.

4. Otherwise, in the screen that results—Additional Port Information Required—choose Hewlett Packard Jet Direct from the Standard pop-up menu. (Don't ask why; just do it!) Click Next.
5. Now:
 - If your printer maker and model show up in the list, first select the maker on the left and second the model on the right; then click Next. Leave Use the Driver That Is Currently Installed unchecked, and click Next.
 - If you don't see your printer maker and model listed, insert a disk that came with the printer and click Have Disk to install a driver that way. Click Next and follow the resulting directions.
6. Resume at [Step 7](#) on the previous page!

Troubleshoot an Unavailable Shared USB Printer

If you followed the directions earlier in this section and you can't print to your shared USB printer, one of the following suggestions should shed light on the problem:

- Make certain that the printer is powered up and not in an error condition (such as out of paper or out of ink).
- Make sure your computer is on the same network as the base station (on the computer, launch AirPort Utility and make sure the base station appears in AirPort Utility's left-hand list of base stations).
- Make certain the base station recognizes the printer: use the instructions in [Rename and Widely Share a USB Printer](#).
- Using AirPort Utility, restart the base station and try again.
- Consult the suggestions from Apple at <http://docs.info.apple.com/article.html?artnum=107418>. Note that the last suggestion, under "Still not working?" is to confirm that your printer is able to work with AirPort printer sharing. Apple has linked to Lexmark and HP's list of compatible printers.

SET UP A SHARED USB DISK

Extreme N adds an interesting option for sharing disks across a network without attaching them to a computer. The base station can share attached drives over a network both via the standard Apple Filing Protocol (AFP) format, the same format used with Personal File Sharing and Mac OS X Server share files, and via *Samba*, a network file-sharing service compatible with Mac OS X, Windows, and Linux.

Warning! *There's no way to share volumes via either only AFP or only Samba; you have to share through both.*

You can connect a single drive to the USB port on the Extreme N, or connect a USB hub and then a series of drives to the hub. The drives may be hard drives or USB thumb (flash) drives, but you cannot use CD/DVD drives with removable media.

You must format mountable disks before you attach them to the base station, using either the Mac HFS+ format, or the FAT16 or FAT32 (MS-DOS) formats. Each partition on a disk becomes a separately available shared volume. (FAT16 supports smaller maximum partition sizes than FAT32; you're unlikely to see FAT16 except on disks formatted by very old computers.)

Warning! *Before you format anything, read [Grant Access](#), ahead, to learn the quirks that can arise with different formats and different types of access.*

Warning! *Unix, Microsoft NTFS, and other partition formats are not supported.*

Once one or more drives are connected, you can access them and let others access them, too. You handle all the configuration in AirPort Utility in the Disks pane.

Slow Speeds Ahead! *The performance of base-station-connected drives is slow to creeping, when compared to network throughput and to the speed of reading and writing to a drive connected to a computer.*

In my tests of the Extreme N (gigabit), I saw speeds about one-third that of directly connected USB drives when transferring larger files. When I copied 8,000 tiny HTML files—documentation for a program, the transfer speed dropped to below 10 percent of directly connected USB. This is partly due to inefficiencies in copying many small files in AppleShare File Protocol (AFP), and partly due to the low-power, but adequate, processor in the Extreme N (both models). For networks in which speed is an issue, use a computer-based fileserver or dedicated network-attached storage (NAS) device.

DISKS, PARTITIONS, VOLUMES, FILES & FOLDERS

Here's a guide to file-sharing concepts that you need to understand in order to make sense of this section:

- **Hard disk:** A *hard disk* is a physical piece of hardware that contains data.
- **Partition:** A *partition* is a division of a disk's available storage into a separate logical compartment—part of the physical disk is written with certain kinds of data, and a disk-wide partition map is updated to reflect that partition information. Many disks have a single partition that spans the entire disk's storage capacity.

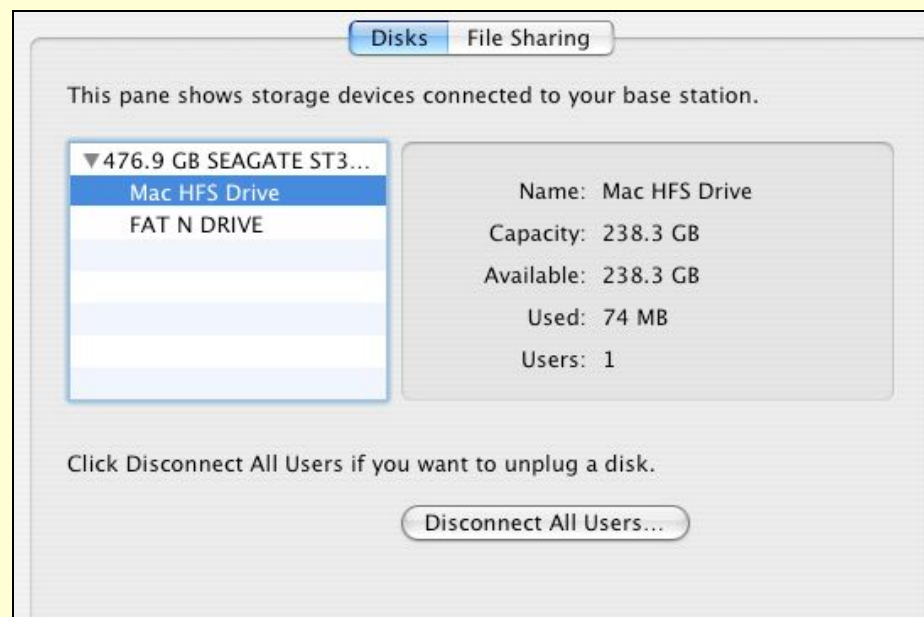
The partition's format—like HFS+, FAT16/32, or NTFS—determines how data is written to the disk; each operating system supports a different set of formats.

- **Volume:** While *volume* is a synonym for any partition on a disk, I like to use *shared volume* to mean a shared partition that can be mounted over a network in the context of file sharing. A *fileserver* is a device that has one or more volumes available to share.
- **Files and folders:** Any format you deal with stores files inside folders, the latter also known as *directories*. With some systems, you can share folders as volumes. In some cases, Extreme N makes folders into volumes, so that you can control access more finely, as described ahead.

Viewing Connected Volumes

In AirPort Utility, the Disks view in the Disks pane offers a little information and one option. Each disk connected to the base station is noted in a list on the left, and each partition on that disk is found by clicking the triangle next to the disk name (**Figure 48**). Selecting a partition reveals the capacity of that partition, the used and remaining storage, and how many users have mounted the partition.

FIGURE 48

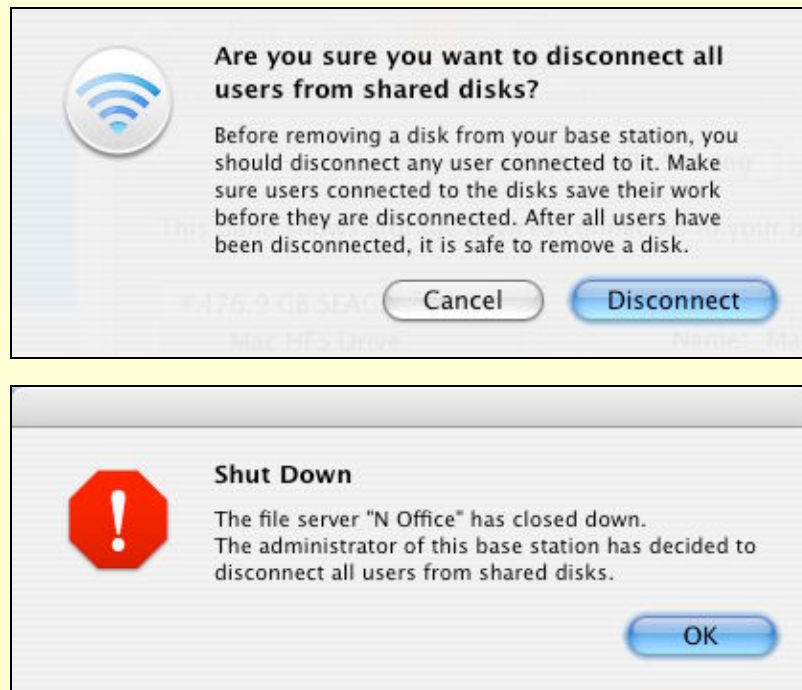


In this example, AirPort Utility shows two partitions for the drive attached to the base station. Selecting the partition shows storage information and connected users.

Clicking Disconnect All Users shuts down all file service, forcing connected users' computers to lose a connection with mounted volumes no matter whether they have open files or transfers in progress, so click it with care. It's better to have each user (or you) unmount each connected volume first. If you do disconnect users by clicking the button, Mac OS X warns you in AirPort Utility and informs each user with an alert message (**Figure 49**). This button appears even if no users are connected.

When no users are connected, the drive is in a standby state that lets you unplug it from the Extreme N without harm.

FIGURE 49



Clicking Disconnect All Users brings up the warning (top) about the consequences to users still working on data stored on those drives.

If you want to bump working users off, however, AirPort Utility obliges and Mac OS X complains (bottom).

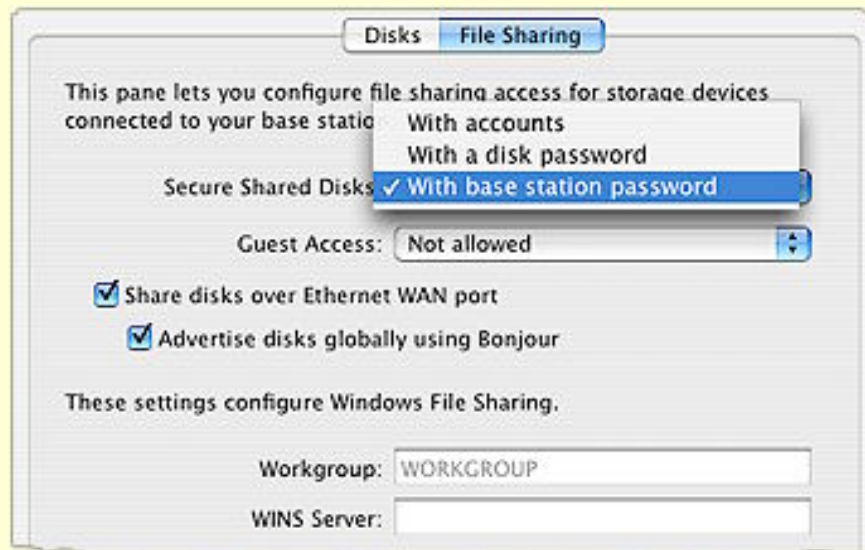
Grant Access

Apple offers relatively little granularity in setting up security and access for hard disks you connect to an Extreme N. You can choose only one of three methods for setting passwords, and you can't set permissions individually for folders or files on each hard disk, nor set permissions differently for different partitions or different hard disks.

Kinds of access

AirPort Utility has three ways to grant access, found in the Disks pane, in the File Sharing view, in the Secure Shared Disks pop-up menu (**Figure 50**).

FIGURE 50



AirPort Utility offers three options for securing a shared disk by controlling the level of security.

The three ways to grant access are:

- **With Base Station Password (default):** This self-explanatory option is the default method, and means that only a single password is used to secure the base station's settings *and* any attached hard disks. This option is good for home and small networks in which you're not concerned about someone changing the settings on a base station.
- **With a Disk Password:** This sets a password that controls access to all disks; this password is distinct from the base-station password. All users accessing the disk have access to all files. This works for a small network where you want to make sure those with fileserver access can't modify the base station, even unintentionally.
- **With Accounts:** On partitions formatted with HFS+, you can set up individual user names and passwords, each with different levels of access; these accounts are distinct from any Mac OS X or Windows user accounts set up on the computer that's configuring the base station. An Accounts button appears, and you can click it to add and edit users. User access options can be set to Read and Write, Read Only, and Not Allowed. (That last option lets you disable an account without removing it.)

Accounts are useful for larger networks, but they are a new feature and still have some quirks that I hope Apple will work out soon:

- ◇ **No directory services:** You can't yet tie in network directory services with this option, so accounts must be entered one at a time and manually updated.
- ◇ **Inconsistent partition-to-account matching:** With partitions formatted using HFS and named accounts, you can't choose which HFS+ partition winds up containing the user-specific account folder. In my testing, it seemed arbitrary, and even moved from partition to partition after changing seemingly unrelated settings and restarting the base station. All other partitions formatted with HFS+ are served as single, whole-partition volumes, which is a related bug or missing option.

This could result in the strange circumstance in which you attach a 1 terabyte (TB) disk drive and a 1 GB flash drive to your Extreme N, and the unit puts user accounts on the smaller drive. I expect Apple will add an option to select the volume on which user accounts are created to solve this.

Single drive, no worries: *With a single hard disk that's formatted in HFS+, you won't see this problem.*

Paired with each of the three ways to grant access is the Guest Access pop-up menu. You can set those without a password to have full access, read only, or no access.

Other network settings for file sharing

You can limit access to what network or part of a network is available through two related checkboxes beneath Guest Access:

- If you check Share Disks over Ethernet WAN Port, other computers on a larger network or the Internet can access your base-station fileserver.

With the Share Disks box checked, you can also check Advertise Disk Globally Using Bonjour. This option has risks, too, as it ties in your fileserver access with a globally registered domain name that could expose you more broadly than you intend.

Warning! *If you enable WAN access and the Extreme N has a public IP address, you are exposing your files to a larger potential audience of crackers and ne'er-do-wells, so it becomes critical to set guest access appropriately. Or, you can use a firewall between the Extreme N and the larger world to provide additional access control, such as limited fileserver access to particular IP ranges that represent other locations you work for or remote offices.*

- The other option in this section lets you configure Windows File Sharing—more frequently called *Samba*—by naming the Workgroup and choosing a WINS Server. The Workgroup name allows other Samba-capable computers to organize file servers into a group for display. The WINS server, if there's one on your network, provides a separate name-based association for Windows computers to the IP address on your base station.

Gain Access



You or users on your network can access disks connected to an Extreme N in two ways:

- With the new AirPort Disk Utility, which can identify drives as they appear using Bonjour
- With normal file-sharing connection options, such as Connect to Server in the Mac OS X Finder

Before we look at methods of accessing shared disks, though, we need to figure out precisely which volumes are mounted based on the settings on a given base station, the disk's format, and what kind of access you're attempting to gain. I lay out the options in **Table 4**, because they're too baroque to explain conversationally.

Table 4: Comparing Methods of Serving Shared Disks

Access Control	Access Method	How Partitions Are Served
Base station or disk password	Password	The entire volume is served. Users mount it as a volume having the partition name.
	Guest*	A folder named <i>Shared**</i> is served as a volume. Users mount it as a volume having the partition name.
Accounts	Account	<p><i>HFS+-formatted partition:</i></p> <ul style="list-style-type: none"> • A folder named with the account is created on only one partition, no matter how many HFS+ partitions are attached; users mount this folder as a volume having the account name. • A folder named <i>Shared</i> is also created on one partition, and users mount it as a volume named with the partition name. • Any other partitions are served as volumes named with the partition name. <p><i>FAT 16/32-formatted partition:</i></p> <ul style="list-style-type: none"> • A folder named <i>Shared</i> is served. Users mount it as a volume having the partition name.
	Guest*	A folder named <i>Shared**</i> is created on each partition, and users mount it as a volume named with the partition name.
<p>* If Guest Access is set either to Read and Write, or to Read Only.</p> <p>** The shared folder appears on the disk, viewable as a folder only by users with a password, only after the first guest accesses the volume.</p>		

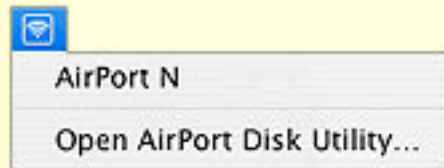
AirPort Disk Utility



The AirPort Disk Utility program makes it convenient to identify base stations that are sharing hard disks. That sounds great at first, but the utility has few advantages over other ways of accessing shared volumes. (Versions are available for both Mac and Windows; I cover the interface for Mac OS X here.)

When you install the utility (see [Install new software](#), earlier), you can turn on a status menu that lists each base-station fileserver (**Figure 51**). You can also remove this menu, and turn off automatic notification when new shared volumes are added to any base station on the network (**Figure 52**).

FIGURE 51



The AirPort Disk menu shows all base station filesystems.

FIGURE 52



AirPort Disk Utility lets you set notification and menu preferences, as well as allowing you to change the way you connect to base station filesystems.

If you don't change the utility's default, when a new volume is added, you're prompted to act on it; the same is true if you choose the base-station filesystem name from the AirPort Disk menu. A dialog appears (**Figure 53**) that wants to know your action:

- **Ignore:** Don't notice if this volume appears in the future.
- **Connect as Guest:** No password required, but you can view only shared files. (This option doesn't display if Guest Access is set to Not Allowed in AirPort Utility.)
- **Connect with Password:** This option shows up with a Username field if, on the base station, Secure Shared Disks is set to With Accounts; or as just a Password field otherwise.

FIGURE 53



AirPort Disk Utility displays these options for mounting all volumes connected to a base station.

There's no way to tell AirPort Disk Utility to mount a single volume, which makes the tool less than ideal if you need only a single volume. If you want to mount all volumes at once or have only a single partition, then the utility is fine. Otherwise, I recommend using normal volume mounting, described next.

Normal volume mounting

Fortunately for us, the file sharing in the Extreme N uses standard methods: AFP, commonly known as AppleShare, and Samba, Windows's default method.

Stick to their own kind: *The Extreme N fileserver shares only HFS+ volumes as AFP volumes, while Samba can share either HFS+ or FAT32 (MS-DOS) formatted partitions as SMB/CIFS volumes.*

Mount in Mac OS X

You can mount volumes in Mac OS X by following these steps:

1. In a Finder window, click Network in the sidebar, or choose Go > Network (Command-Shift-K).

A list of connected servers appears in the Finder window, and the fileserver should appear in the list twice: first as an AppleShare fileserver and second as a Samba fileserver.

2. Double-click the base station's fileserver name to open an authentication dialog.

3. In the Name field:

- If you don't have a user account because the base station is using base-station or disk passwords enter any short bit of text or leave the field blank.
- If you have a user account name, enter it.

4. In the Password field, enter the base station, disk, or account password.

5. Select the volume or volumes you want to mount and click OK.

If you are mounting a volume remotely or it doesn't appear in Step 1, choose Go > Connect to Server and enter the IP address of the base station or an associated domain name (for FAT16/32 volumes, enter **smb://** followed by the IP address.) Then, follow Steps 3 to 5 above.

Mount in Windows

With Windows XP and Vista, open the network browser by double-clicking Network on the Desktop. The base station name should appear in the Network browser. When you connect, enter the name and password as in Steps 3 to 5 above.

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 traffic passing over your network. This could be a neighbor, someone in a parked car, or a nearby business. Many free, easy-to-use programs 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 on security.

Likelihood, Liability, and Lost Opportunity

When Adam Engst and I were writing *The Wireless Networking Starter Kit, Second Edition*, back in 2003, we disagreed over how concerned the average home Wi-Fi networker should be about security. 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 for your network.

NOTE If you'd like to know more about the topics in this section, read *Take Control of Your Wi-Fi Security*, a companion book we wrote.

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, raising the question of whether you want to allow others to share your Internet connection or not.

TIP Because Wi-Fi and public hotspots (free and fee) go together like coffee and cream, it's very likely that you'll use a laptop on a network outside your home, too. There are a whole different set of concerns about the likelihood of someone snarfing your data and passwords on hotspot networks as opposed to networks you set up yourself. We address those concerns and how to solve them in *Take Control of Your Wi-Fi Security*.

The likelihood of attack increases significantly if you're running a business, since it's plausible that your network would carry desirable 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 a 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 an ecommerce Web site that unusually doesn't use *SSL/TLS* (Secure Sockets Layer/Transport Layer Security, a security standard for Web servers), maybe 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. A few scary stories have surfaced of police obtaining a warrant, knocking down a door, and finding an innocent person or family who had an open access point. (For one such example, see <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/10/AR2007021001457.html>.)

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. For instance, rules protecting patient information could lead to significant fines if a medical office or hospital had its network compromised. 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 software to promote overall security.

Your spot in the security spectrum

It's up to you to determine the likelihood of someone breaking in to 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 could 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 for setting up basic security that advise you to hide your network's name and make it hard to connect to, such as employing a *closed network* or using *MAC address filtering*.

Closed network

In a closed network, your base station stops broadcasting its network name, or SSID (Service Set Identifier), as part of its *beacon*, an “I’m here” message that access points regularly transmit in order to help clients connect to them. However, the beacon continues to be sent because it still includes information that is used for network data synchronization.

An open network appears by name in the AirPort menu or in other places in the Mac OS and Windows that show the names of networks you can connect to. But closing the network makes it only slightly obscure. A cracker can easily find out that the network exists, and by monitoring for a connection or using a tool to create a *disassociation* for a computer on the network—which forces that computer to reconnect—the cracker can grab the network’s name. So you cannot rely on closing your network for any real security.

Although I discourage bothering with a closed network, here’s how to set one up:

1. Launch AirPort Utility, connect to your base station, and choose Base Station > Manual Setup (Command-L).
2. At the top of the window, click the AirPort icon. Then, click the Wireless button.
3. Click the Wireless Options button.
4. Check Create a Closed Network.
5. Click Done, and then click Update to restart the base station.

MAC address filtering

MAC address filtering initially sounds more promising than a closed network. 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 that computer can’t connect.

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, 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. You can use AirPort Utility to save one base station's configuration, and then import just the MAC address controls, to your other base stations. See [Export and import configuration profiles](#).

If you don't want to build a security fortress against crackers, but you do want to mediate the access for kids in your house or you want to clarify to outsiders that you've restricted access, MAC address restriction works quite well. You can also combine encryption and MAC address filtering for a pretty good overall solution.


The Extreme N adds another element to the mix: controlling access by time of day and day of week for particular MAC addresses.

To restrict access, first note the MAC addresses for devices you want to limit; see [What and Where is a MAC Address?](#) (p. 59). You can also use AirPort Utility to extract the MAC address of a computer you're using to configure setup.

Warning! *Don't store the base station's password in the Keychain on a computer that you're restricting via AirPort Utility. Otherwise, later, someone on that computer could quite easily reconfigure the base station to remove those restrictions!*

NOTE If you use Wi-Fi Protected Setup (WPS) to allow computers to join the network, but limit their access to 24 hours, an entry appears in the access control client list with a special tag. See [Use WPS](#) for more details.

To restrict access by MAC address on an Extreme N, follow these steps:

1. Launch AirPort Utility, select your base station, and choose Base Station > Manual Setup (Command-L).
2. Click the AirPort icon; then click Access Control and select Timed Access.
3. Click the  button at the bottom of the access control client list.

4. In the Timed Access Control Setup Assistant, repeat these steps for each Wi-Fi device you want to restrict:
 - a. Enter the MAC address of the computer you want to add, or click This Computer to fill the field with the MAC address of the computer on which you are running AirPort Utility
 - b. Enter a description of the computer you are adding.
 - c. If you want to control access time, choose restrictions: Click the button to add an entry, or select an entry and click the to delete it.

You can choose a day of the week, weekdays (Monday through Friday), weekends (Saturday and Sunday), or Everyday. The time of access is either All Day or a range in the current day. You can't set a range of time that spans two days; that requires two separate entries. (The combination of Everday and All Day would be an ineffective barrier to access!)
 - d. Click Done.
5. You should also edit the "(default)" entry in the access control client list. It's set at the factory to Unlimited. If you want to exclude all computers that aren't listed here from having any access, select it, click Edit, and then choose No Access from the Day pop-up menu. Click Done.
6. Click Update after you have added all the computers that you want to restrict.

Now, only those computers on your network whose MAC addresses you've entered may connect to the network. If one can't connect, check that you've set the access time restrictions correctly.

Use Built-In Encryption

Although MAC address filtering and a closed network will deter casual passers-by, they don't constitute a defense. If you want a better defense, you need to step up to encryption and password protection.

Wi-Fi has always offered some form of built-in encryption to secure the connection between a client computer or device and the base station; this connection is the most vulnerable part of a wireless network.

Unsecured out to the Internet: The connection from the base station to the rest of the network or the Internet has to be secured separately from the Wi-Fi segment. Some people use virtual private network (VPN) connections to secure a larger chunk of their traffic.

Encryption always requires a key. With Wi-Fi encryption, you don't enter the key directly, but instead enter a password that is used by the system to generate or retrieve a key. Sharing the password reduces security by allowing others to see the same network traffic.

Three different encryption methods have been offered since 802.11b started appearing in hardware in 1999, each of which supersedes the previous one. See **Table 5** for side-by-side comparisons. I look at each option in more detail next.

Table 5: Wi-Fi Security Compared		
Name	What Can Use It?	Difficulties
WEP	Any Wi-Fi adapter using 802.11a, b, or g, including the earliest made	Encryption easily broken; deprecated since 2003
WPA Personal	Works with original AirPort Card (10.3 or later), and with many early adapters with new firmware	Requires slightly newer computers and operating systems; no Mac OS 9 or earlier support
WPA2 Personal	Works only with gear shipped starting in late 2002, including AirPort Extreme, but requires 10.3 or later, or Windows XP SP2 or Vista	Older machines can't connect, including those with original AirPort Card
WEP Transitional	Allows mix of WEP and WPA/WPA2 Personal	Doesn't seem to work consistently; doesn't allow robust security
WPA/WPA2 Enterprise	Supported in Mac OS X 10.2 or later, Windows XP SP2, and Vista	Requires back-end server to handle account management

WEP

WEP (Wired Equivalent Privacy) allows the use of a 40-bit or 104-bit password, the equivalent of 10 or 26 hexadecimal digits, or 5 or 13 text characters, respectively. WEP was never designed to be very strong, and *cracks*, or ways to retrieve the encryption key by watching network data, started to appear in 2001. It's acceptable for home use, but I wouldn't rely on it as a business.

You could use WEP to signal that your network is off limits. In some U.S. states and in some countries that “no trespassing” intent could result in an interloper between charged with a computer crime and even convicted, as recent cases in Florida, Alaska, and Singapore indicate.

WPA & WPA2 background

WPA (Wi-Fi Protected Access) was introduced by the Wi-Fi Alliance as an interim measure when work by an IEEE committee—802.11i—was taking too long. Released in 2003, WPA is considered to be quite strong and was designed to allow even the earliest Wi-Fi gear to be upgraded to support it. The original AirPort Card can use WPA with Mac OS X 10.3 or later; see <http://docs.info.apple.com/article.html?artnum=107795> for Apple's requirements and software links. (The original 802.11b AirPort Base Station cannot be upgraded.)

WPA2 was the final version of WPA security that includes all the work done in the 802.11i committee. WPA2 can use the weaker, but still relatively secure form of encryption offered in WPA. But WPA2 significantly adds a government-grade method favored by corporations. Any equipment released in 2003 or later can handle WPA2. The Extreme 2003 and 2007 and AirPort Express all handle WPA2, but Mac OS X 10.3 or later is required to use it. The original AirPort Card cannot access WPA2-protected networks.

NOTE THE KEY TO KEYS

The difference between WPA and WPA2 is that the former offers an encryption method that's a repaired version of WEP, known as *TKIP* (Temporal Key Integrity Protocol). WPA2 adds *AES-CCMP* (Advanced Encryption System, Counter-mode CBC-MAC Protocol, *whew*), which incorporates the U.S. government-backed AES method limited to 128 bits. WPA2-enabled Wi-Fi adapters may use either TKIP or AES-CCMP to connect.

The Extreme N can offer WPA/WPA2 protection, in which both older and newer devices can join with either form of key; or it can offer a WPA2-only network, in which only computers that support WPA2's advanced encryption key type can join.

NOTE On 802.11n networks that are set to use only 802.11n, WPA2 is the minimum level of security. This makes sense because all 802.11n devices must support WPA2.

Both WPA and WPA2 come in two versions: Personal and Enterprise. The Personal versions allow the use of *passphrases*, long sequences of text—minimum 8 characters, maximum 63 characters—that are converted into the source material for generating an encryption key. This makes a WPA/WPA2 passphrase memorable, and the length adds *entropy*, the principle of adding greater disorder to make it harder to use brute force to uncover a key. A key could look like **my d000gs have lite_brite_hair!** I kid you not.

TIP Researchers believe that WPA and WPA2 keys are susceptible to cracking through brute force if you choose passphrases that are shorter than 20 characters and that contain only dictionary words. Choosing short passphrases that combine a random assortment of numbers, letters, and punctuation; or longer passphrases with a few punctuation marks defeats this problem, as in the example passphrase above.

The Enterprise flavor of WPA and WPA2 requires a server to manage accounts, but simplifies access by letting people enter a user name and password—one that might be shared for resources across a

network, including file servers—and receive a unique encryption key that they never need to know about.

TIP Even small offices might like to use WPA/WPA2 Enterprise, and a few companies offer affordable ways to add it to an Extreme N:

- You can buy server software from Periodik Labs (<http://www.periodiklabs.com/shop/>, \$750).
- You can use a hosted option in which the server is located outside your network and you use a Web site to add and delete users. I recommend WiTopia's SecureMyWiFi (<http://witopia.net/securemore.html>; \$20 setup and \$10 per month for up to five users, \$100 setup and \$100 per year for up to 100 users).

Turning on WPA/WPA2 with AirPort Extreme

Here's how to enable WPA/WPA2 or WPA2 only:

1. Run AirPort Utility and select your base station. Choose Base Station > Manual Setup (Command-L).
2. Click the AirPort icon. Then, click the Wireless button.
3. From the Wireless Security pop-up menu, choose WPA/WPA2 Personal or WPA2 Personal.

Warning! *Macs with the original AirPort Card can't connect to WPA2 Personal-configured networks.*

4. Enter a key of 8 to 63 characters in the Wireless Password field and the same key again in the Verify Password field.
5. Click Update and wait for the base station to reboot.

The next time someone tries to connect to the network, they'll have to enter a password to gain access; for details on entering a password, see [Connect Your Computers](#), earlier.

WEP Transitional

The Extreme N supports WEP Transitional, a rare and interesting security mode that I and colleagues have found to be problematic and buggy in actual usage. WEP Transitional lets you mix older WEP-only Wi-Fi connections with newer WPA/WPA2 connections.

The problematic part is conceptual: the network encryption is as weak as the weakest link. Using WEP Transitional leaves you vulnerable to the same cracks that affect plain WEP. The buggy part is that it's seemingly erratic whether computers can connect via WEP, WPA, or WPA2 in this mode. Apple will surely fix that—we hope.

If it's necessary for you to mix modes, or occasionally allow WEP clients on your network, here's how to set this up, but I warn you that it might not work at all:

1. Run AirPort Utility and select your base station. Choose Base Station > Manual Setup (Command-L).
2. Click the AirPort icon. Then, click Wireless.
3. From the Wireless Security pop-up menu, choose WEP (Transitional Security Network).
4. Your WEP password must be exactly 13 characters, although Apple doesn't note this until you try to update the configuration. Enter the WEP key in the Wireless Password and Verify Password fields.
5. Choose Base Station > Equivalent Network Password.

A dialog appears, showing the WEP key you just entered, which is also the key you use as a WPA passphrase to join the network (**Figure 54**). The dialog shows the 26-digit hexadecimal WEP key for older devices or those that can't handle ASCII WEP keys.

You can select and then copy—Edit > Copy—either key from the dialog. (This isn't an error in this book: You can really select and copy within this dialog.) Also, if you ever forget or misplace the keys, you can also later follow these steps again to retrieve the key.

FIGURE 54



The Equivalent Network Password dialog shows you the passwords needed to gain access using WEP or WPA.

6. Click OK, and then click Update and wait for the base station to reboot.

The next time you or another user tries to connect to the network, whatever operating system you're using will prompt you for a password to gain access. You can find details on connecting to a network in [Connect Your Computers](#), earlier.

Use WPS

WPS, Wi-Fi Protected Setup, lets a computer or other Wi-Fi device join a WPA/WPA2 Personal protected network without entering a key. Instead, in the two versions that Apple has implemented, you can join without a password or via a simpler PIN (personal identification number). Apple's use of WPS requires that you connect to the base station using AirPort Utility and, while connected, have the device that wants to join the network attempt to join.

Warning! *The only Macs that support WPS at the moment are those that have 802.11n adapters in them with the latest software installed. Windows XP SP2 and Vista don't seem to yet have built-in support. As an industry-wide standard, WPS will appear in more operating systems and more base stations during 2008.*

For either kind of WPS, follow these steps to get set up:

1. Connect to your base station via AirPort Utility and choose Base Station > Manual Setup.
2. Choose Base Station > Add Wireless Clients to open the Wireless Client Setup Assistant (**Figure 55**).

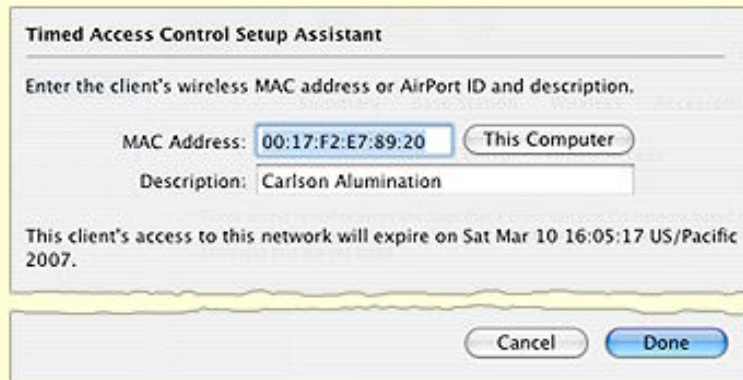
FIGURE 55



The assistant allows a client to join the network without a password.

3. If you like, you can check Limit Client's Access to 24 Hours, perhaps for a visitor. This will put a special restriction on the account in its access control settings after you finish the configuration (**Figure 56**). (See [MAC address filtering](#) for more detail.)

FIGURE 56



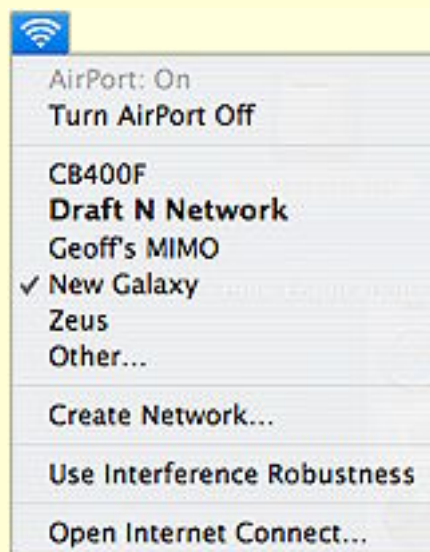
The special 24-hour limit entry for timed access can't be edited for time, only by name and MAC address.

4. Select PIN or First Attempt, and then click Done.

This puts AirPort Utility and the base station into a state of watchful awareness! AirPort Utility notes that it's waiting for a connection.

5. On the client machine, look in the AirPort status menu on the menu bar for the network name, which appears in bold. Choose that network name (**Figure 57**).

FIGURE 57



The network with WPS standing by appears in bold: Draft N Network.

6. Now:

- If you've selected the First Attempt option, the first computer that tries to connect to the network after this point is presented with an encryption key automatically.
 - If you've selected a PIN, the Mac OS X system that's trying to connect generates a code onscreen that you must enter in AirPort Utility. A key is then exchanged between that computer and the base station, and that computer joins the network.
7. AirPort Utility's watchful-waiting dialog disappears, and AirPort Utility confirms that the device has been added. This lone operation, out of all others on the base station, requires no Update to complete.

The client is now connected.

OVERCOME INTERFERENCE

Interference from other Wi-Fi and non-Wi-Fi devices using the same spectrum is one of the most frustrating problems to deal with in making your AirPort network work well. Let's first look at eliminating sources of conflict, and then at a mysterious option Apple offers that seems to help as well.

Eliminate Conflicting Signals

A frustrating part of Wi-Fi networking is that you can't control your "air space." All too often, neighboring Wi-Fi networks and other emitters cause reception problems in areas that otherwise would have good reception. If your network's performance varies by time of day or even by the minute, these ideas may help you identify the problem.

Do some basic testing

What you test for varies by band. Keep reading after the tests for some suggestions for how to fix found problems.

For 2.4 GHz:

- Run iStumbler (<http://www.istumbler.com/>) to determine whether other networks are running in the vicinity. iStumbler scans for networks and can display their characteristics, such as signal strength and whether security is enabled. It can't tell you more general info about signals being generated in the spectrum range, however.
- Investigate your cordless phones and microwave oven as culprits—they can both create static on the Wi-Fi line; see [Set Interference Robustness](#) (ahead). Do you have problems only when talking on the phone or making popcorn? There you go.
- Also check if you have problems while Bluetooth devices are in use. Older Bluetooth equipment can interfere with Wi-Fi networks.
- Do you live in an area near a hospital, or light or heavy industry? Some medical and industrial devices use the 2.4 GHz band, including microwave sealers that close bags of potato chips. You might need to switch to 5 GHz to overcome that problem.

- If you're desperate for a solution, check out Wi-Spy, a relatively inexpensive spectrum analyzer. It can show whether there's interference beyond Wi-Fi. (See [Testing from client to base station.](#))

For 5 GHz:

- Check whether you have 5.8 GHz cordless phones.
- See whether a wireless ISP might be broadcasting over 5 GHz in your area. Most wISPs are using the 5.8 GHz section of the 5 GHz band. (If that's the case note the second bullet item in the solutions for cordless phones, below)

Try a solution

Here are ideas for solving some of the problems noted just previously.

If cordless phones are the culprit:

- Buy new cordless phones using an unused band (swapping 2.4 GHz for 5.8 GHz or vice versa). Or swap your Wi-Fi from 2.4 GHz to 5 GHz, a potentially expensive proposition, but one guaranteed to produce better results.
- In 5 GHz, use lower-numbered channels; 5.8 GHz is in the highest range of channels supported by the Extreme N. (This also works for wISP interference.)
- Try T-Mobile's HotSpot@Home, which offers cordless calling from a cell phone that also includes a Wi-Fi radio. You make and receive unlimited U.S. calls for \$20 per month (one line) or \$30 per month (2–5 lines) over your own Wi-Fi network or any T-Mobile HotSpot.

If a neighboring network is causing the problem:

- Propose an informal channel usage agreement: if your neighbor and you are both using 2.4 GHz's channel 6, switch to 1 and 11 to increase the distance between signals. In 5 GHz, you have a number of additional channels to choose from.
- You (and your neighbor) could move your access points farther away from one another to reduce the signal conflict in the middle.


TIP Another way to reduce network overlap is to engage in unilateral or multilateral curtailment (you know, like the former Soviet Union and the United States). You can cut the amount of transmit power on many Wi-Fi gateways, which reduces the interference you cause. If your neighbor backs off a little, too, both sets of network improve. You know: the Prisoner's Dilemma.

To reduce transmit power from an Extreme N, run AirPort Utility, connect to the base station, and click Wireless Options in the AirPort pane's Wireless view. Set Transmitter Power to a level below 100 percent, click OK, click Update, and then re-test.

If Bluetooth is causing the problem:

- A Bluetooth headset from 2002 or earlier could cause terrible interference. The standard was updated to version 1.2 in 2003, but not all devices are upgradable. Check your equipment to see.

Set Interference Robustness

 Why not use a setting labeled Interference Robustness to more robustly resist interference and thus improve range? In short, the setting won't help with range but it might provide a more reliable connection over short distances.

Apple offers Interference Robustness for 2.4 GHz use of the Extreme N, but not for 5 GHz, which doesn't need the additional "robustness," as there's much less interference. Apple has offered the option for years with little explanation. They describe it sketchily on their Web site, saying that it provides better performance in the presence of 2.4 GHz cordless phones and near working microwave ovens. A writer at Macinstruct says he figured it out: Interference Robustness instructs the base station and Mac OS X to send packets of smaller and smaller length to ensure that data gets through if interference otherwise disrupts the transmission of longer sequences. Read <http://macinstruct.com/node/213> for more details.

Interference Robustness doesn't seem to make much difference in normal networks. One Web site documents testing that indicated that the setting increases power while reducing reception sensitivity, thus blasting through interference when sending data, while listening less carefully (ignoring more noise) when receiving it.

Turning Interference Robustness on is helpful only if you use Wi-Fi at a short distance from a base station and if you believe that interference is causing problems. Interference Robustness reduces the range, but can improve performance within that smaller area.

Better than using Interference Robustness, if you operate 2.4 GHz cordless phones, you might consider switching to older 900 MHz phones (lower quality but often better range) or newer 5.8 GHz phones (higher price, and range is an issue); or using 5 GHz with 802.11n to avoid 2.4 GHz altogether.

You can turn on Interference Robustness in Mac OS X through the AirPort menu in the menu bar: choose Use Interference Robustness. Windows has no similar option in any version. For an Extreme N, connect to your base station in AirPort Utility; click the AirPort icon, and click Wireless; then click Wireless Options to see the checkbox.

Interference robustness can be a unilateral decision: If a single computer or the base station has the option enabled, there could be a performance improvement.

APPENDIX A: STREAM MEDIA WITH AIRPORT

Apple continues to extend itself into the media world, and the AirPort system hasn't been left out of the mix. When Apple introduced the AirPort Express, they made a big deal about *AirTunes*, Apple's name for streaming music over a wired or Wi-Fi network to an AirPort Express, which could then dump that music out as analog or optical digital audio via a standard stereo mini-jack. Strangely, AirTunes never appeared in any other devices.

In late 2006, Apple revealed plans to offer the Apple TV, initially codenamed the iTV, which would stream high-definition video and digital audio over a wired or Wi-Fi network for output via HDMI (the high-definition digital video standard), composite analog, and both digital and analog audio. The Apple TV was unveiled in early 2007 and shipped in March 2007.

In this section, I cover how to best configure your Apple TV to stream video, and how to work with an AirPort Express. The big difference between the two devices, beyond video, is that Apple TV *pulls* content from connected computers, while the AirPort Express allows audio to be *pushed* to it from a copy of iTunes running on a computer on the same network.

Cheap music: *The AirPort Express is still being sold as I write this, and at \$99, it's not a bad deal for transferring audio over your network. You can connect an Express wirelessly or via Ethernet on an Extreme N network with no problems, except the previously mentioned network performance hit.*

Apple TV

The Apple TV can receive content from a single computer via synchronization and store it on an internal hard disk. It can also stream content live from up to five computers on the network. The Apple TV has 802.11n built in and can use 2.4 GHz and 5 GHz bands just like the Extreme N. It also has just 10/100 Mbps Ethernet, not gigabit Ethernet, which is peculiar for a device intended to move a lot of data.

TIP If you're using Apple TV with an 802.11g network or in the 2.4 GHz band, connecting via Ethernet lets you sync to that one enabled computer at the fastest possible rate. You can then disconnect from Ethernet and use Wi-Fi thereafter. Apple has a technical note about this: <http://docs.info.apple.com/article.html?artnum=305254>.

TIP Reports from Apple TV users indicate that placing an object on top of the Apple TV can dramatically decrease the range of its Wi-Fi radio, if you're using Wi-Fi as your connection method.

Choose a Band

The big consideration in adding an Apple TV to your network is ensuring that you have enough bandwidth to stream video while performing other tasks on the network. Also, if you sync content regularly to the Apple TV, you'll likely want a lot of speed in order to move your movies and audio files quickly.

MPEG4-compressed video used for top-resolution (1,080p or 1,080 by 1,920 pixels) requires about 10 Mbps of throughput. Apple says the maximum resolution for the Apple TV is 720p, and the iTunes Store doesn't yet sell video at even that resolution. Thus, you need to have somewhere between 2 and 5 Mbps of solid throughput available for each Apple TV on a network that's streaming video.

An ideally configured 802.11g network should top 20 Mbps in throughput, but it's likely to actually work at much lower speeds due to nearby networks, interference, and other factors described earlier. In contrast, an Extreme N network with only N devices connected can hit 90 Mbps.

You might choose, therefore, to set up an Extreme N in the 5 GHz band. You can read [Mix Legacy, New N Networks](#) for how to best set this up. But, keep in mind that the speeds demanded for good video streaming by the Apple TV might be achievable on your network at 2.4 GHz. It depends on your particular environment—and it's worth testing before getting rid of an older base station.

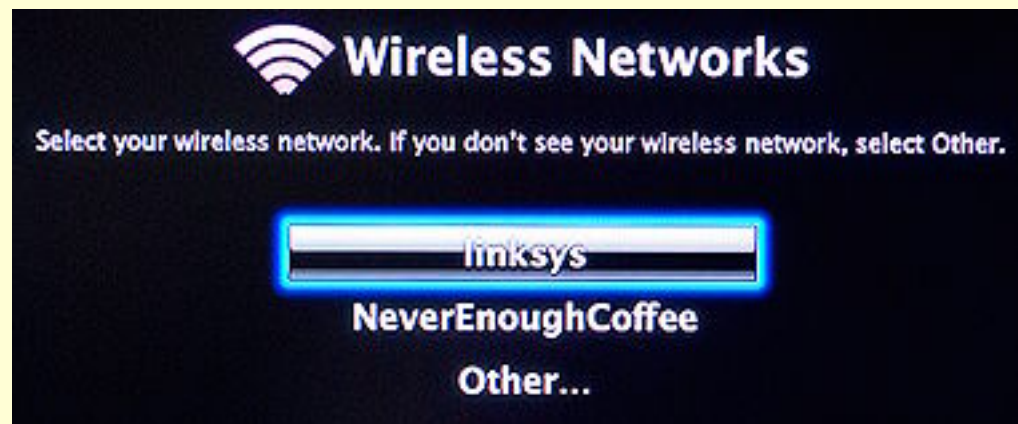
Connect an Apple TV

The Apple TV uses a straightforward way to connect to a network. If you plug the Apple TV into an Ethernet network with DHCP

enabled, the device automatically obtains an address. If you don't have an Ethernet network, or are just using Ethernet for an initial sync, connect your Apple TV to your TV, power up both devices, grab your Apple Remote, and follow these steps:

1. On the TV, from the Apple TV main menu, choose Setup > Network.
2. Select Configure Wireless.
3. From the Wireless Networks screen, select your network (**Figure 58**), or if your network is closed (see [Closed network](#)), choose Other and enter a network name

FIGURE 58



Choose your network from the list.

4. If your network has an encryption key or passphrase, use the Wireless Password screen's visual keyboard to enter that text (**Figure 59**). The Apple Remote lets you select each letter one at a time. Select Done when finished. (The password is displayed on the TV screen as you type it.)
5. If your network uses static addresses or has other particular network requirements, choose Configure TCP/IP from the Network screen to enter an IP address, set DNS servers, or control other details (**Figure 60**).

With the network connected, you now can proceed to use your Apple TV by following the instructions to pair one computer's iTunes library. A code appears on the Apple TV, you enter that code in that computer's iTunes link to the Apple TV, and then syncing begins!

Synchronization can take some time, as noted, over a slower network. After or instead of synchronization, you can follow instructions to set up streaming with up to five computers on the network, similarly using the Apple TV code paired with iTunes entry.

FIGURE 59



Use the Apple Remote to navigate the visual keyboard and select the letters in your network passphrase.

FIGURE 60



You can set TCP/IP details manually via the Network > Configure TCP/IP command.

AirPort Express and AirTunes

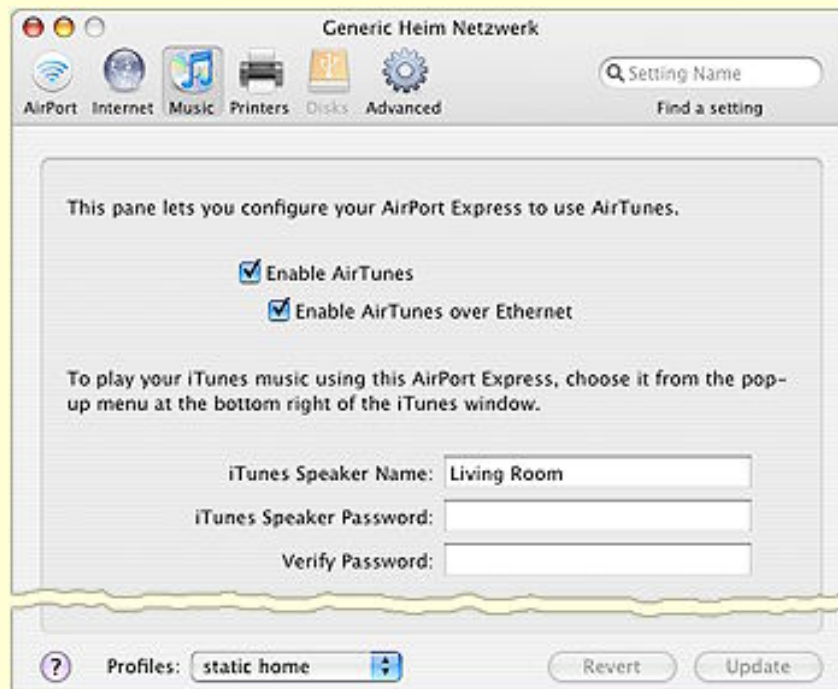
The AirPort Express features AirTunes, a method of streaming music from iTunes (versions 4.6 and later) through the audio output port on the base station. You control the settings in AirPort Utility and then play the music via iTunes.

TIP The fine folks at Rogue Amoeba offer AirFoil, a program that lets you take the sound output from any program—not just iTunes—and play it over AirTunes (<http://rogueamoeba.com/airfoil/>; \$25, downloadable demo version).

Set up music features in Airport Utility

After connecting to your base station, use the Music pane in AirPort Utility to control music streaming and speaker settings (**Figure 61**).

FIGURE 61



The Music pane lets you set AirTunes options.

Here's how the controls work:

- **Enable AirTunes:** Click this box to turn streaming on and off, on the base station.
- **Enable AirTunes over Ethernet:** Check this box to let both wired and wireless computers stream music. I can't think of why you might want to restrict this, but if you're concerned about

restricting streaming, don't uncheck this box; instead, password-protect the remote speakers (see the last item in this list).

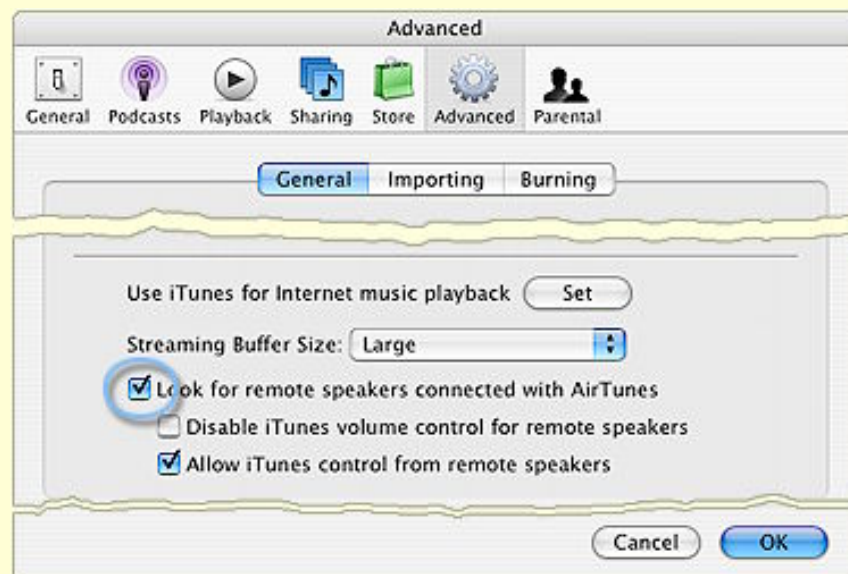
- **iTunes Speaker Name:** This name shows in the iTunes remote speaker list.
- **iTunes Speaker Password:** Set a password to limit use of this speaker set to people who have the password. The Verify Password field requires you to enter the password a second time to make sure you didn't mistype it.

Play music with iTunes

Here are the steps for playing music via iTunes and AirPort Express:

1. In iTunes, choose File > Preferences, and then click the Advanced icon (**Figure 62**).

FIGURE 62



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

2. In the General view, verify that Look for Remote Speakers Connected with AirTunes is checked (look near the middle of the view). This option causes iTunes to be aware of AirPort Express Base Stations that are plugged into stereos or powered speakers.
3. If you want to control volume only from your stereo (and not also from iTunes), select Disable iTunes Volume Control for Remote Speakers.

4. A very limited number of devices can control iTunes volume remotely, including the Apple HiFi when connected via the AirTunes jack on the AirPort Express. If you care about this behavior, you can check or uncheck Allow iTunes Control from Remote Speakers.
5. Click OK.

Now that you have a configured AirPort Express on the network and the Look for Remote Speakers Connected with AirTunes checkbox is selected, iTunes should display a new pop-up menu with a speaker icon next to it in the lower right of its main window (**Figure 63**).

FIGURE 63



Choose the AirPort Express to stream through from the pop-up menu at the lower right. A lock appears next to those that are password protected.

6. In iTunes, select a base station from the new pop-up menu. The menu lists all the AirPort Express base stations connected to stereos; Computer means the audio output option you chose on your own computer in the Sound preference pane. You can select only one item from the menu, but you can choose Multiple Speakers to play music through both your computer and other AirPort Express base stations as well (**Figure 64**).

FIGURE 64



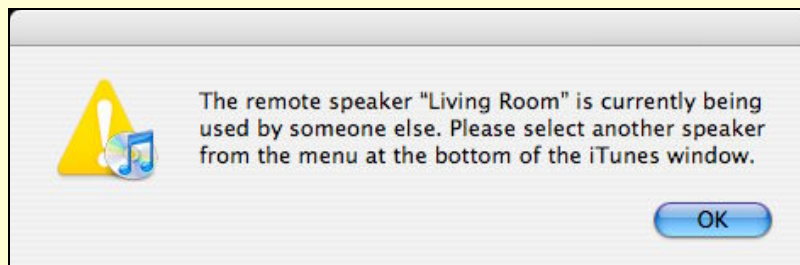
The Remote Speakers window lets you choose one or more speaker sets to stream through.

Quiet! The AirPort Express knows if there are no speakers attached and warns you.

Here are a few more things you might like to know about AirTunes:

- **Two people playing music at once:** If you try to play music through an AirPort Express that someone else is actively playing music through, iTunes notifies you when you press the Play button (**Figure 65**). If that person clicks Pause, iTunes releases that person's control of the speakers, and within 2–3 seconds, another iTunes user can start playing music through that AirPort Express.

FIGURE 65



This message appears when someone else is already playing music through a particular AirPort Express.

- **Password protection:** You can password-protect AirPort Express music streaming (as noted a few pages earlier). For instance, if you live in a dorm, you might want to prevent pranksters from blasting through your speakers. When you try to connect to protected base stations to play music, you must enter the password (**Figure 66**).

FIGURE 66



Connect to password-protected AirPort Express speakers by entering the correct password and clicking OK.

APPENDIX B: SETTING UP A 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. This appendix explains how to set up a software base station under Mac OS X.

Apple's software base station has two distinct problems:

- **Security:** You can use only WEP encryption, which I describe back in [Use Built-in Encryption](#) as a last-resort method of security. It's definitely better than nothing, however.
- **Frequency:** Even though 802.11n allows the use of the uncrowded 5 GHz band for less interference and better throughput, Internet sharing over AirPort works just with the busy 2.4 GHz band.

SOFTWARE BASE STATION VS. AD HOC NETWORKS

You needn't create an ad hoc network (also known as a computer-to-computer network, an informal network that you set up quickly, perhaps to transfer a file or to chat during a keynote speech) before setting up a software base station, and in fact, the two are mutually exclusive. Use an ad hoc network for connecting with another computer when you have no Internet connection to share.

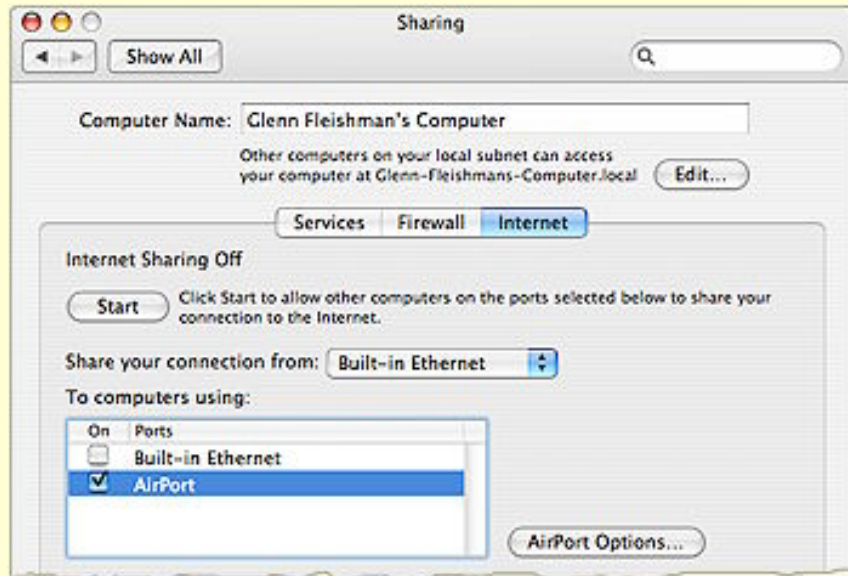
When you set up an ad hoc network by choosing Create Network from the AirPort menu, your Mac assigns itself an IP address in the 169.254.x.x range; Macs that connect to your network pick up addresses in that range so they can communicate. Bonjour services in iChat should work fine over ad hoc networks.

The Software Base Station feature is found in the Sharing preference pane. Before starting, make sure you have either an Ethernet or an Internal Modem connection set up in the Network preference pane, because 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. Here's what to do:

1. In System Preferences, open the Sharing pane and click the Internet button (**Figure 67**).

FIGURE 67



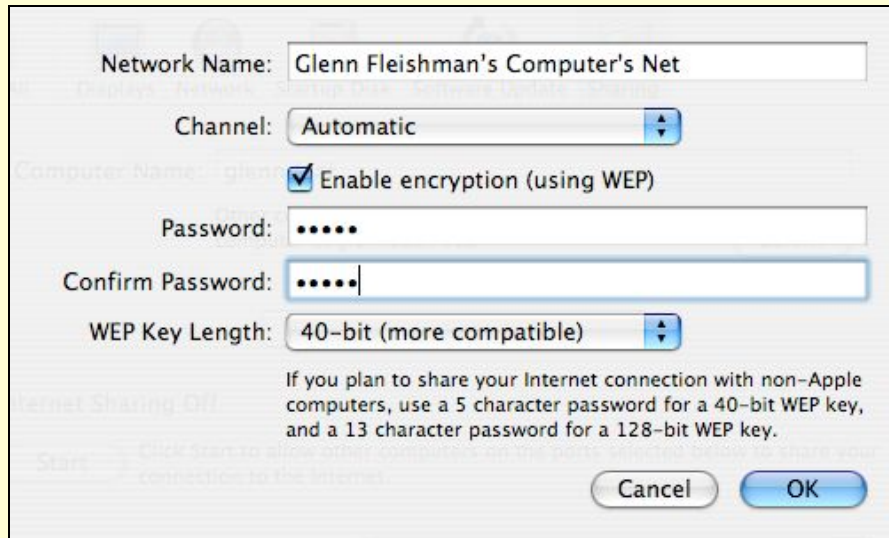
In the Internet view of the Sharing preference pane in Tiger, you can share your wired Internet connection as a software base station by choosing Built-In Ethernet and checking AirPort.

2. From the Share Your Connection From pop-up menu, pick either Built-In Ethernet or Internal Modem (whichever matches how you access the Internet), and then select AirPort in the To Computers Using list.
3. If you want to also share a connection to wired computers connected directly to your computer, select Built-In Ethernet from the To Computers Using list.

Warning! Because most Macs have a single Ethernet port, if you select Built-In Ethernet, you wind up pushing out DHCP messages over the same network connection that you're retrieving your Internet feed from. This is generally not a good idea, but might be required in some limited circumstances.

4. Click AirPort Options to set the network name, channel, and, optionally, a WEP key (**Figure 68**).

FIGURE 68



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

TIP If you turn on WEP 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. When you type a dollar sign in a password field, the WEP Key Length menu dims and the OK button won't light up until you type the correct number of matching digits in both password fields.

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

APPENDIX C: ADVANCED EXTREME FEATURES

I tucked the kitchen sink here at the end, because only a few of you may be interested in the advanced features found here and there across the AirPort Utility.

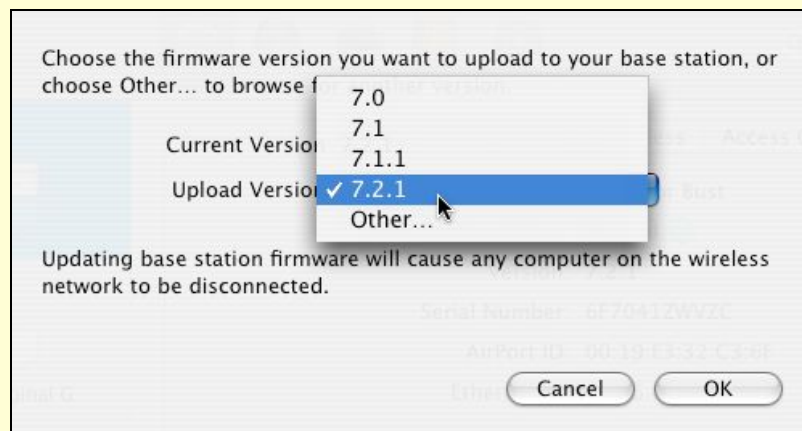
Revert to Older Firmware

Apple isn't perfect, although many Apple fans like to pretend they're close to it when compared to the rest of the computer industry. Sometimes, they release software that causes their products to work more poorly than they previously performed.

This has often happened with AirPort base station firmware, the software code that runs on the base station itself. Many firmware releases have turned out to have minor defects, often quickly fixed, that disable or render erratic critical features.

Apple has neatly provided a way to go backward in AirPort Utility: choose Base Station > Upload Firmware (**Figure 69**). As long as the base station is responsive, you should be able to use this command to restore a previous firmware release.

FIGURE 69



You can choose firmware that's stored in AirPort Utility, or choose a separate firmware file.

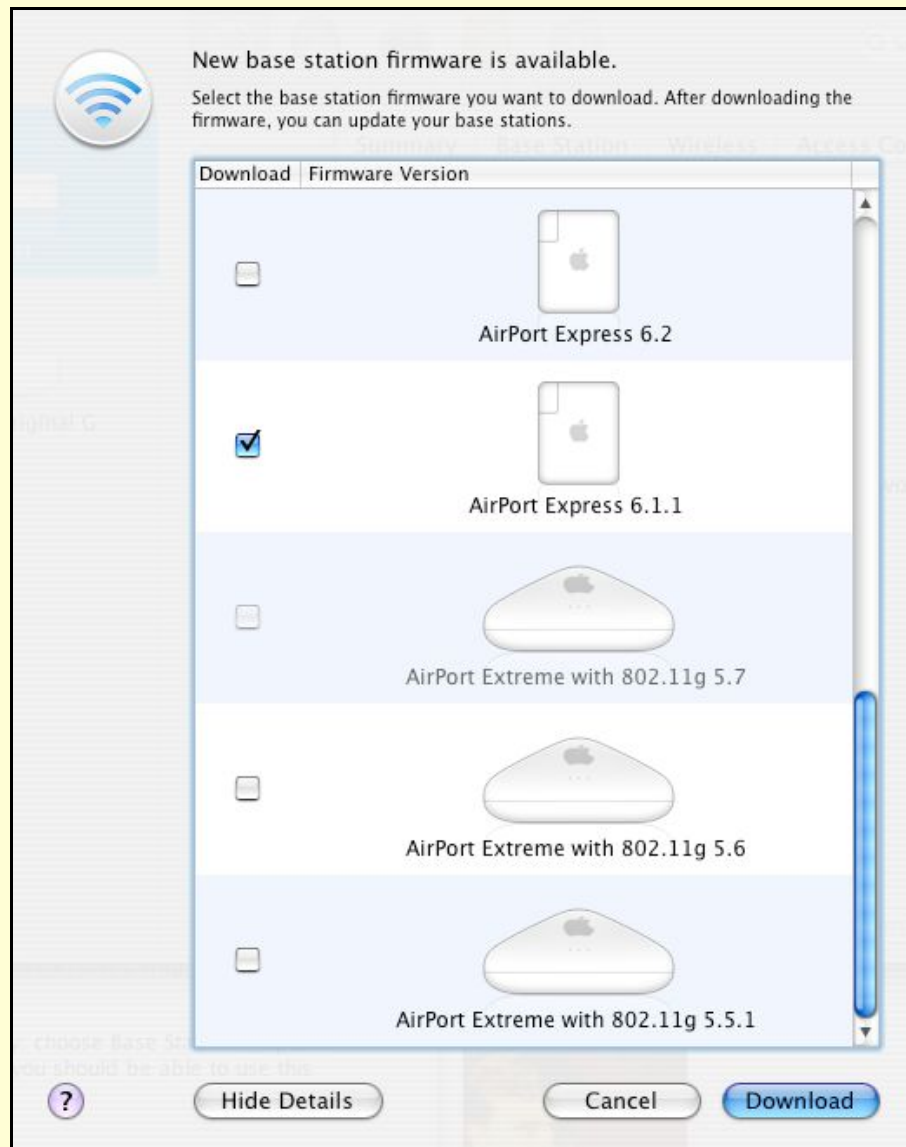
If you already have previous versions of firmware downloaded, they appear in the Upload Version pop-up menu. Otherwise, you can retrieve older firmware via the AirPort Utility:

- On a Mac, hold down the Option key and choose AirPort Utility > Check for Updates.

- Under Windows, hold down the Control key and choose File > Check for Updates. Windows also requires that you click Show Details to proceed.

A list of all firmware releases appears with each entry comprising a graphic of the model type and a description of that type along with the firmware release number (**Figure 70**). Select the checkbox next to each firmware release you'd like to retrieve, and click Download. Entries that are already stored locally are grayed out.

FIGURE 70



AirPort Utility lets you retrieve any older versions of base station firmware.

You can also download these older firmware releases from Apple's Web archives at <http://docs.info.apple.com/article.html?artnum=75422>.

AirPort Pane

A handful of options in this view beg for additional explanation.

Base Station settings

The Set Time Automatically checkbox and field allow you to set the time on your Extreme N (and previous models) via time servers operated by Apple or that you specify yourself. You must choose your time zone manually. Setting your time in this fashion can ensure that any timed access rules you set function; see [MAC address filtering](#). Hardware tends to lose track of time without external correction.

Click the Base Station Options button to set blinking options. The Status Light pop-up menu controls whether the amber/green light on the front of the Extreme N is green when everything is situation normal—Always On (Default)—or if it blinks with activity—Flash On Activity.

Wireless settings

The Wireless view's Wireless Option dialog hides several useful controls for the built-in radio.

- **Region:** Choose the country in which you are operating your Extreme N. With the Americas model, the menu lists only countries that have approved the device. You could violate a number of laws by setting the region to a regulatory domain in which you are not using the base station!
- **Multicast Rate:** This option concerns a subset of networking traffic that all connected computers can receive. It's seldom used without a particular purpose in mind, so you almost certainly won't need to change the value.
- **WPA Group Key Timeout:** On WPA-protected networks, each connected device creates its own particular key material—based on the WPA passphrase—in concert with an access point. Each device also receives from the access point a group key that's used for broadcast traffic sent to all devices. The timeout value increases

the entropy in encryption by ensuring that a group key doesn't persist for very long. It does not require that any computer log in to the network again.

Access Control settings

The MAC Address Access Control pop-up menu lists RADIUS as one option. If you use 802.1X or WPA/WPA2 Enterprise, here is where you fill in server details provided by a network administrator or a service provider you contract with.

Advanced Pane

The Advanced pane has, as you can imagine, less frequently used options.

Logging & SNMP settings

The Extreme N can *log*, or note information about, many kinds of events, from users logging in, to updates of its internal clock, to specific encryption information. This view controls all those aspects.

The Syslog Destination Address and Syslog Level allow an existing system logger (a server called **syslog**) on a Unix or Linux—or really *any*—system to receive messages from the base station, and place them in a text file that's updated constantly as new messages come in. (The syslog monitor is part of Mac OS X and every Unix and Linux flavor I'm aware of; configuring it to accept these messages requires system administrator experience.)

The SNMP options let the base station leverage a standard method of receiving information with a bit more sophistication than syslog. Many network management packages use SNMP for figuring out the status of network components and the traffic passing over them; and determining bad behavior by users or interlopers.

If you click the Logs and Statistics button, you see additional options:

- Click Logs to see a short list of the logging messages that can be sent to a syslog or SNMP server.
- Wireless Clients and DHCP Clients show connections and their quality.

Bonjour settings

Apple likes to look to the future, and the advanced Bonjour settings are part of that forward-looking detail. In these settings, Apple lets you set up *wide-area Bonjour*, a way of pushing information about services and hardware on your *local* network out to the *global* Internet by using the domain name system (DNS). In this scenario, a domain name's DNS information, which normally contains IP addresses and mail server records, would also keep an updated list of file servers, printers, and other Bonjour-broadcasting information that could be accessed by people outside your local network

The problem with that? Internet service providers and DNS hosts must support wide-area Bonjour for that to happen.

Within a large local network, such as at a college, wide-area Bonjour can be supported internally, allowing networks of all scales to share resources across the campus's wide-area network. Bonjour services on the network served by the Extreme N get shared to the next network level. Any service that uses NAT-PMP publishes information about itself via wide-area Bonjour, if that's enabled.

For practical purposes, and Apple has confirmed this, presently, home users don't need wide-area Bonjour, and most corporations don't have it in place. However, settings for wide-area Bonjour appear throughout AirPort Utility.

IPv6 settings

An explanation of IPv6 could fill pages and pages, and perhaps it will in a future edition of this book. *IPv6* is the next-generation Internet protocol that will replace the current version, *IPv4*, which has been in use for decades. IPv6 was designed in the 1990s, but because it requires a reworking of the entire infrastructure of the Internet, it's been slow to catch on.

IPv6 has a much larger address space, allowing trillions of addresses compared to billions in IPv4. And, it allows address mobility: an address in IPv4 is usually fixed to a particular router or gateway on the Internet. With IPv6, that router or gateway can provide forwarding info so that a mobile device can be reached elsewhere, if desired, with no special effort.

Some corporate networks and some ISPs in Japan now use IPv6, which explains Apple's support. But there's an additional interesting option. In IPv6, you don't need NAT, because IPv6 addresses and ports can be used directly. And many organizations have set up IPv6 tunnels on the Internet that allow IPv6 traffic to pass over the current IPv4 network. The Extreme N supports this tunneling.

By default, the Extreme N is set up to allow incoming IPv6 connections and to route IPv6 traffic through these public Internet tunnels. Because Mac OS X also, by default, enables IPv6 traffic, you do face some exposure, and may wish to set IPv6 Mode to Link-Local Only, which restricts traffic to the local network, and check Block Incoming IPv6 Connections to further restrict behavior.

For the Extreme N (gigabit) Apple enhanced security options, adding a checkbox for blocking incoming connections to the IPv6 view, and a new view called IPv6 Firewall with configuration choices for what IPv6 tunnels and networks can pass through.

APPENDIX D: WHAT'S NEW IN LEOPARD

Leopard didn't change the face of AirPort networking, but it did rework how AirPort and network settings appear throughout the system, consolidating those settings and making them more accessible. (Some long-time irritations weren't fixed, unfortunately.)

In this special appendix, I cover three primary areas:

- The new Network preference pane, which reorganizes how you find and configure TCP/IP and other network settings for AirPort.
- The revised AirPort menu in the system menu bar, which now offers live information about the networks around you.
- Miscellaneous changes, ranging from Web server and printer setup changes, to updates in mounting shared AFP and Samba volumes in the Finder.

Watch for spots! *The occasional leopard spots (🐆) in the margin of this ebook can be clicked to quickly jump to corresponding Leopard-related material in this appendix.*

Meet the New Network Preference Pane

Leopard reorganized the Network preference pane to consolidate separate activities and information into one dashboard. The Internet Connect program is gone, replaced by features now built into the Network preference pane. A list at the left of the pane now shows all adapters and their respective status, replacing the previous interface where you used different menus from the top of the pane to access active adapters and change overall adapter settings.

Set DHCP and DHCP Client ID for AirPort

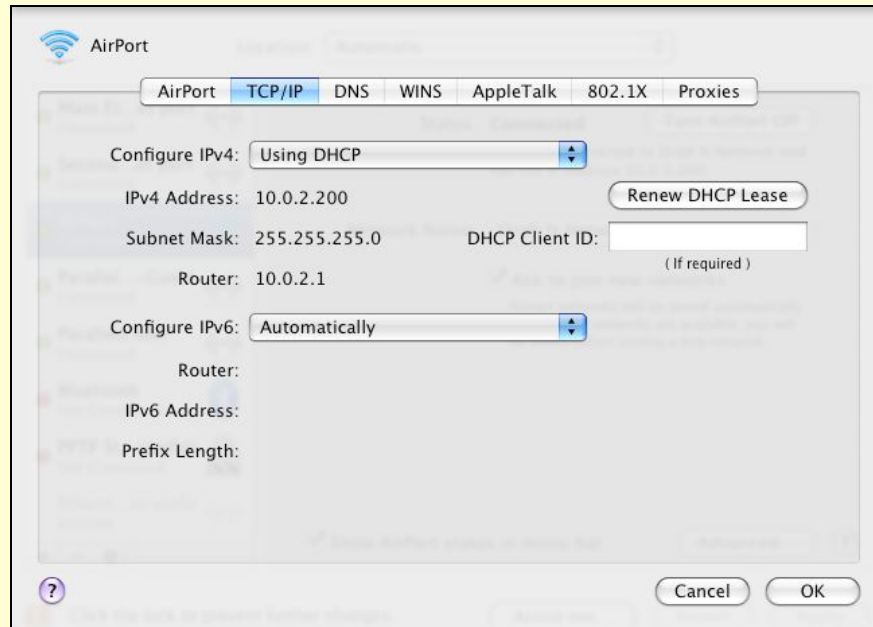
(p. 63 and p. 68)

Here are the steps to set an AirPort adapter to use DHCP to obtain an address:

1. Open the Network preference pane.
2. Select your AirPort adapter in the list at left.
3. Click the Advanced button.

4. Click the TCP/IP button to open the TCP/IP view (**Figure 71**).

FIGURE 71



DHCP settings are now found nested in the Advanced options for the AirPort adapter, in the TCP/IP view.

5. Now, do either or both:
 - Choose Using DHCP from the Configure IPv4 pop-up menu.
 - Enter a name into the DHCP Client ID field to use with DHCP reservation in AirPort Utility.

Managing Profiles

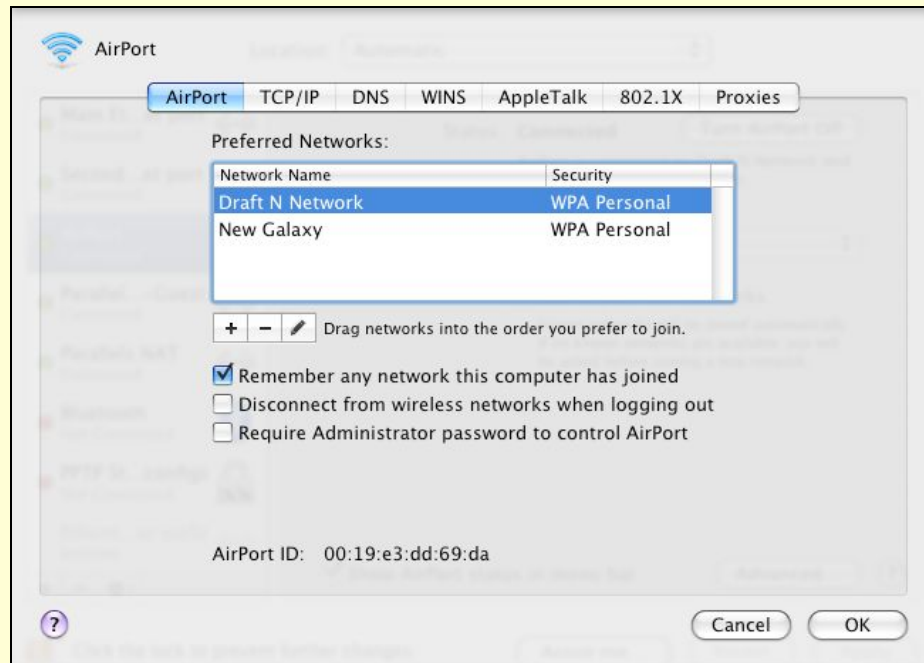
(p. 75)

To create, edit, and delete profiles in Leopard, in the Network preference pane, select the AirPort adapter and then click the Advanced button to see the advanced options (**Figure 72**).

Profiles are managed much the same as in Tiger:

- Add a profile manually by clicking the button.
- Delete a profile you no longer need by selecting the profile and clicking the button.
- To change the preferred order in which the Mac connects to networks if more than one is available, drag a network name to a new position in the list.

FIGURE 72



In the Advanced options for an AirPort adapter, you can easily add, delete, edit, and rearrange networks with which you want to connect.


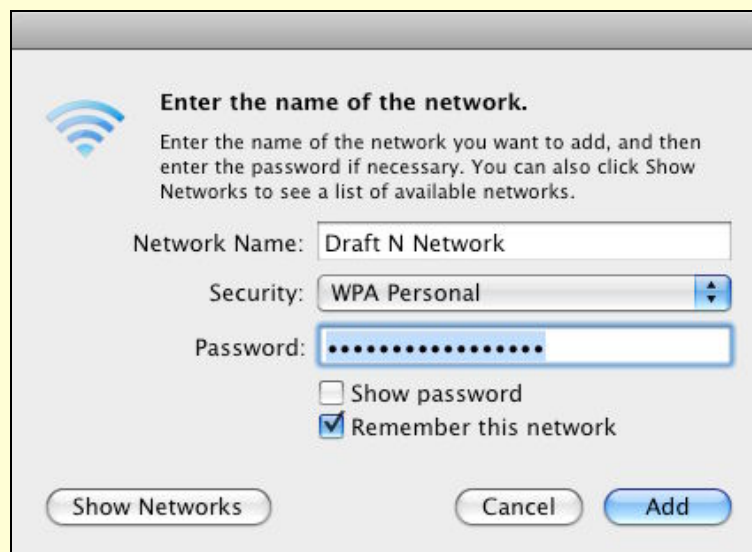
- To edit an existing profile, select it and click the  button; you can change the password or type of password, too (**Figure 73**).

FIGURE 73



With the edit option, you can change the network name, security type, and password without needing to re-select the network.


If you click the  button to reach the dialog shown in **Figure 73**, above, you're presented with a new option in Leopard: the Show Networks button. This somewhat recursive seeming choice lets you connect to a network within the edit feature, so you can change details without exiting the nested dialog (**Figure 74**).

FIGURE 74



Choose the network from this list, or click Other to enter a network from scratch.

Advanced connection options

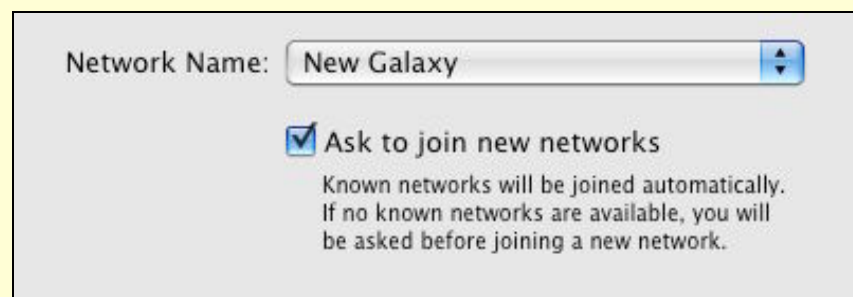
(p. 76)

To control some aspects of how AirPort connects to networks, select the AirPort adapter in the Network preference pane, and choose any of the following options:

- Check Ask to Join New Networks if you want Mac OS X to alert you when there's no network you've stored a profile for in the vicinity (**Figure 75**).

Warning! *This feature seems to work erratically. I have never been able to get it to work correctly and on request, but then, out of nowhere, I'll be prompted to join a network.*

FIGURE 75



The checkbox would seem to indicate that Leopard would ask you join networks; it rarely asks, though.

- Click the Advanced button to reach three additional methods of control:
 - ◇ Remember Any Network This Computer Has Joined. Checked by default, this option adds a profile for any network you join, whether a password is required or not.
 - ◇ Disconnect from Any Wireless Network When Logging Out does just that.
 - ◇ Require Administrator Password to Control AirPort allow you to override someone's attempt to switch networks or turn AirPort off.

NOTE Apple has eliminated the set of three weird options that never seemed to make much sense in Tiger, and that were hidden in an Options dialog: Ask Before Joining an Open Network; Automatically Join an Open Network; and Keep Looking for Recent Networks. Now, the behavior is, by default, to join any network for which a profile is stored; otherwise, Leopard asks to join a network if the Ask To Join New Networks box is checked, which it is by default. Joining any open network without asking is always a bad idea.

AirPort Menu

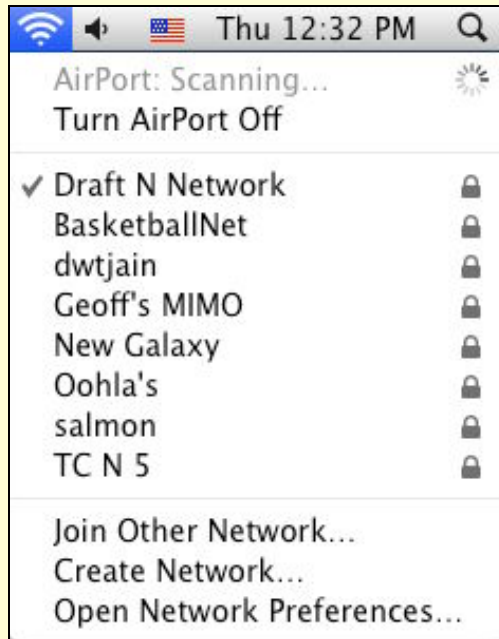
(p. 71)

The AirPort menu, a drop-down menu in the system menu bar, has been refurbished slightly to improve how you find and connect to Wi-Fi networks.

Dynamic network scanning

The AirPort menu is now dynamic, scanning for networks after you hold down the mouse button to select a network (**Figure 76**). Networks appear in alphabetical order, with the network that you're connected to coming first, if you're connected. A lock icon appears to the right of protected networks—ones using WEP or WPA/WPA2.

FIGURE 76



The AirPort status line at the top of the menu says it's scanning (and shows a progress spinner) while it's still looking for networks after you initially hold down the mouse button.

Network details via the Option key

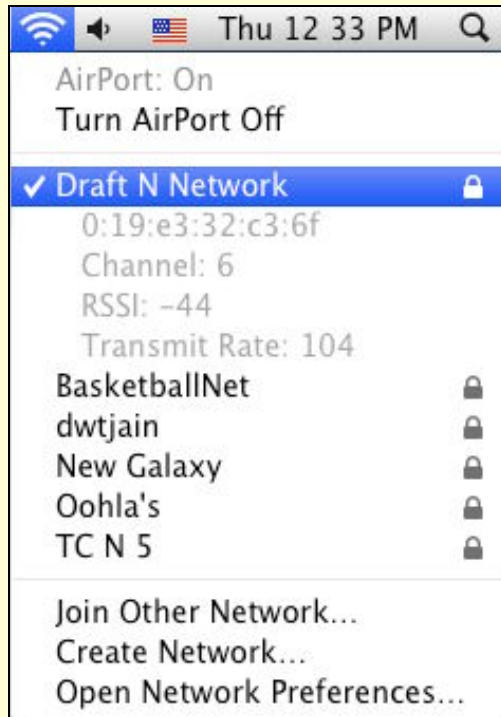
In Tiger, you could hold down the Option key while clicking the AirPort menu icon, and Mac OS X would sort the networks in order of signal strength, from strongest to weakest.

In Leopard, however, Option-clicking the AirPort menu icon provides details about the network (**Figure 77**) to which you are connected:

- The MAC address or AirPort ID of the network
- The channel the base station is using
- The signal strength measured as *RSSI* (Received Signal Strength Indication), which is a relative measure of how good a signal is
- The transmit rate, which shows how fast the network link is, not just how fast the base station *can* go

TIP RSSI is measured in decibels in such a fashion that a negative number is used; -44 (minus 44), as in **Figure 77** is typical. A higher number for the RSSI therefore means less signal strength: -75 is less power than -45.

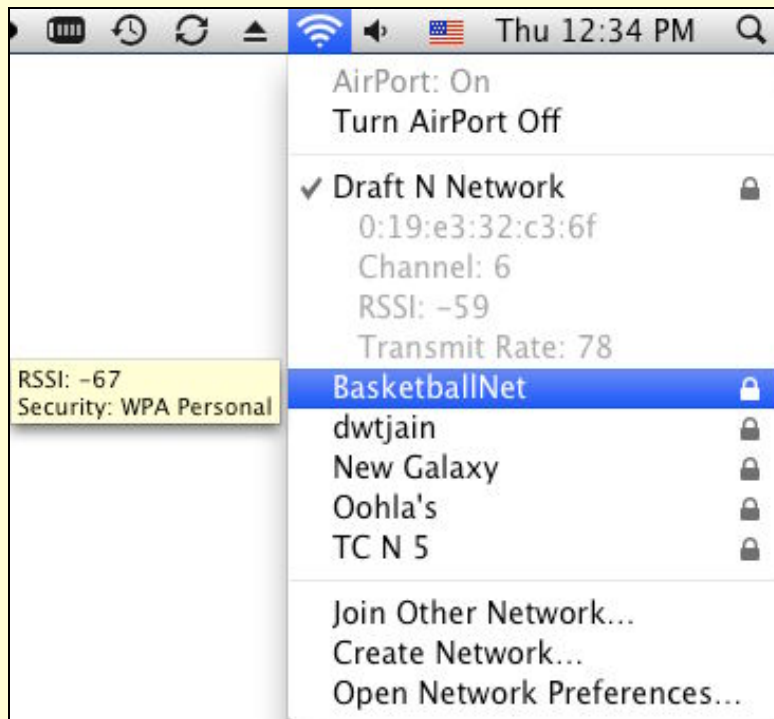
FIGURE 77



Option-click the Airport menu bar icon to see network details revealed right in the menu.

You can also reveal information about networks to which you aren't connected: Option-click to open the AirPort menu, and then hover over any network in the list that you're not connected to, in order to see the RSSI and type of encryption, if any (**Figure 78**).

FIGURE 78



Option-click to open the menu, and then you can hover to reveal information about Wi-Fi networks to which you aren't connected.

Miscellaneous

Leopard has a variety of other changes, which affect scattered sections of the book noted below.

Finding the MAC address

(p. 59)

In Leopard, you find the MAC address of your Wi-Fi adapter by following these steps:

1. Launch System Preferences and select the Network preference pane.
2. Select your AirPort adapter in the list of adapters on the left side of the pane.
3. Click the Advanced button.

The AirPort ID is found at the bottom of the AirPort view.

AirPort Utility

(p. 27)

AirPort Utility shipped as part of the Leopard set of utilities, so it no longer needs to be installed separately from an installer disc. (Apple also separately released a download for Tiger and for Windows XP/Vista.)

Running a Web server in Leopard

(p. 106)

Leopard no longer includes a port-based firewall that would be a problem for running a local Web server that's port mapped to be reached outside the network.

The Leopard firewall, configured in the Security preference pane in the Firewall view, automatically opens the right connections if you enable services, such as a Web server, through the Sharing preference pane (**Figure 79**).

FIGURE 79



The Leopard firewall automatically opens ports as needed for services enabled through the Sharing preference pane.

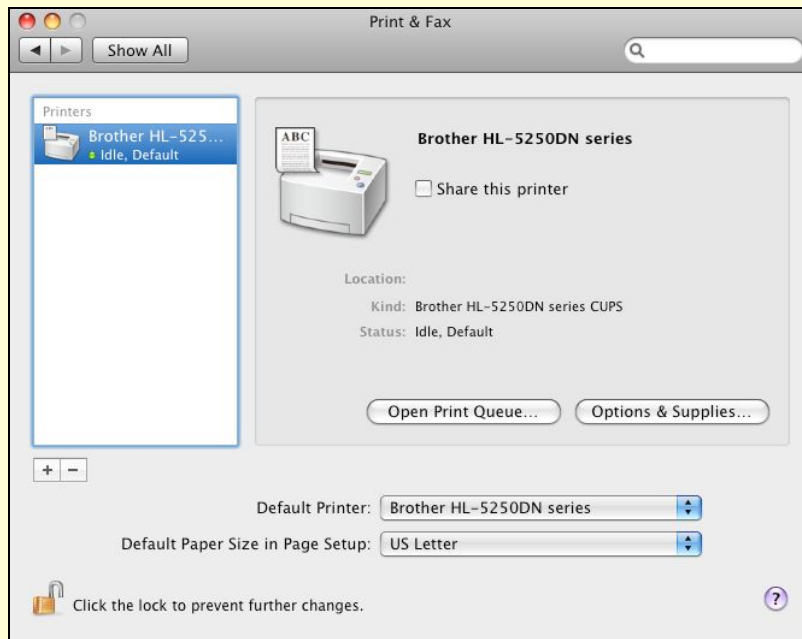
Add a printer in Leopard

(p. 115)

To let Leopard see a shared printer attached to an AirPort Extreme Base Station, an AirPort Express, or a Time Capsule, follow these steps:

1. Launch System Preferences, and select the Print & Fax preference pane (**Figure 80**).

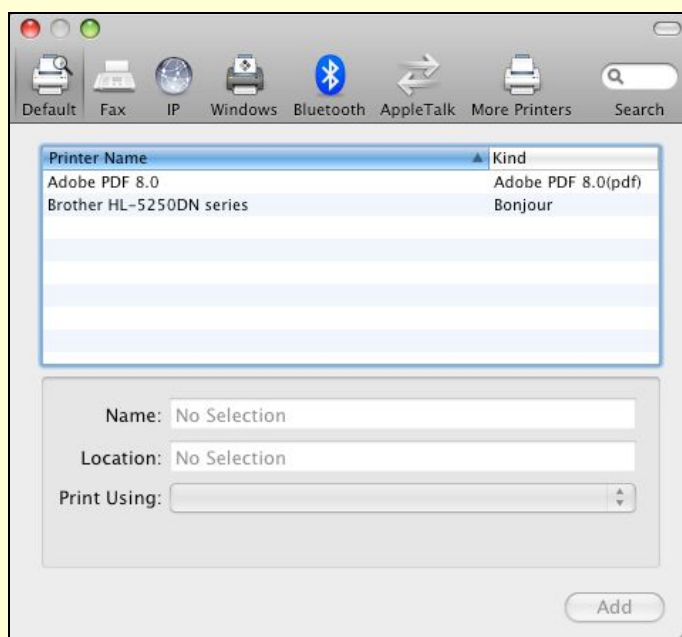
FIGURE 80



The Print & Fax preference pane lets you add and manage printers.

2. Click the **+** button.
3. Select the printer from the list that appears in the Default view (**Figure 81**).

FIGURE 81



A new utility to add printers is launched from within the Print & Fax preference pane. Shared printers show up in the Default view.

4. Click Add.
5. Optionally, choose that printer from the Default Printer list to make it appear as the choice whenever you print.

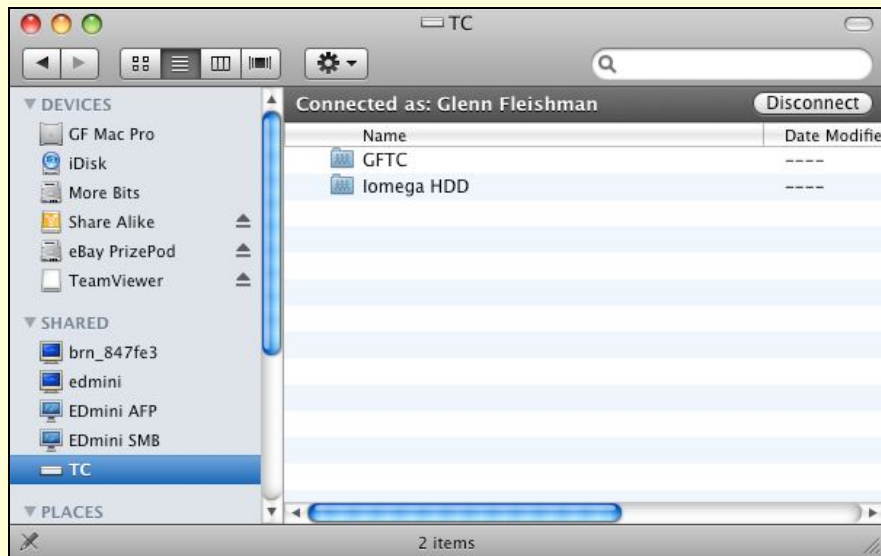
Accessing Shared Disks

(p. 127)

Apple seems to have abandoned the AirPort Disk Utility (p. 128–130), part of the initial package of software that was installed with AirPort Utility, for managing disks mounted via an AirPort Extreme Base Station. Instead, Leopard manages the base station server and disks through the Finder, just like any other network volume.

In any Finder window, you now see a list of servers in the new Shared category in the sidebar (**Figure 82**). This list shows any servers on the local network with AFP or Samba volumes available for mounting, as well as FTP servers that use Bonjour to advertise their availability.

FIGURE 82



The Shared section of the sidebar shows available servers. If you select a server and enter its password, volumes appear at the right. The “Connected as” banner at the top shows the user name you’re connected as. Click Disconnect to unmount all volumes for the selected server.

To mount a volume from one of these servers, follow these steps:

1. Select the server name under Shared in the sidebar.
2. Now:
 - To connect as a Guest user, you needn’t do anything for this step. Leopard automatically tries to connect using the Guest login, and it then shows any volumes that can be mounted in that fashion.

- To use a named account, click the Connect As button in the upper right and enter your credentials. Leopard is clever enough that for AirPort Extreme and Time Capsule shared drives that use just a password for access—no user accounts being defined—to prompt you just for that password.
3. Double click a volume that's shown in the mounted server window to mount it on your system.

By default, Leopard doesn't show a mounted server on the actual Desktop as an icon. This can be confusing! To fix this oversight, follow these steps:

1. Choose Finder > Preferences
2. Click General.
3. Under "Show these items on the Desktop," check Connected Servers.

Interference robust enough

(p. 148)

The setting for Interference Robustness, a way to improve reception for a wonky AirPort connection, is no longer available in Leopard. This setting can still be set for 2.4 GHz networks via AirPort Utility for AirPort Extreme, AirPort Express, and Time Capsule, but it's gone from Mac OS X. We were never sure if it helped much, anyway!

Software Base Station

(p. 158–160)

Much to everyone's chagrin, Apple just moved the location of its software base station controls; they didn't improve those controls at all.

Instead of being found in the Sharing preference pane's Internet view, which no longer exists, network sharing is a service listed in the Sharing preference pane. Open the pane and click Internet Sharing to see the option. If you choose AirPort from the Share Connect from pop-up menu, you can then click the AirPort Options button to set the same choices as the last two releases of Mac OS X: 2.4 GHz only (despite 5 GHz networks being available, faster, and less in use), and WEP encryption only (despite WPA's far superior quality).

ABOUT THIS BOOK

In contrast to traditional print books, Take Control books offer clickable links, full-text searching, and free minor updates. We hope you find them both useful and enjoyable to read.

About the Author

Glenn Fleishman contributes regularly to *Macworld*, the *New York Times*, the *Economist*, *Popular Science*, and the *Seattle Times*. He's the Macintosh columnist for the *Seattle Times*, and a contributing editor at *TidBITS*.

Glenn spends much of his time writing about wireless networking.

He co-wrote *Take Control of Your Wi-Fi Security* with Adam Engst,

and he edits the daily Web log *Wi-Fi Networking News*

(<http://www.wifinetnews.com/>) and five related wireless blogs.

Glenn also appears weekly on KUOW-FM in Seattle to talk about technology (<http://kuow.org/>).

He lives in Seattle in a bungalow with his wife and two sons. His oldest's first word was "book," not "Mac."

Acknowledgements

The new edition of this book happened fast—Apple shipped the Extreme N, and I and the Take Control team was determined to get out a fully revised edition of the previous book—fast!

I must thank Tonya Engst for her tireless and rapid work in editing; Adam Engst, a long-time friend, colleague, and collaborator, also deserves thanks for his role in fostering and perpetuating my work on Wi-Fi and AirPort. More thanks to Dan Frakes for his feedback and insight into early Extreme N troubles and fixes; the Take Control authors who have been fantastically supportive; and to a host of Take



Control pre-release technical reviewers, notably Criss Hyde, Chris Pepper, and Rich Wolfson. Thanks to Jeff Carlson for the use of his Apple TV screen photos.

Thanks are also due to Apple Computer's Teresa Brewer for her help in sorting out some early Extreme N quirks, and relaying my technical quibbles and bug reports to the AirPort team, notably Jai Chulani and John Richey.

Great thanks go to my wife, Lynn, who accepted a few weeks of me sitting on a couch every night tapping away, while our second child gestated. Sure, I'm working, honey, sure!

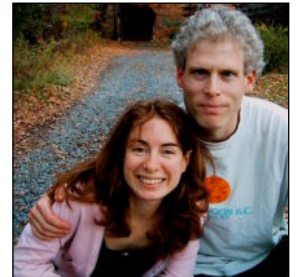
Thanks to Robert F. Unger for pointing us to the great tip on downloading older firmware releases for base stations.

About the Publisher

Publishers Adam and Tonya Engst have been creating Mac-related content since they started the online newsletter *TidBITS*, in 1990. In *TidBITS*, you can find the latest Macintosh news, plus read reviews, opinions, and more (<http://www.tidbits.com/>).



Adam and Tonya are known in the Mac world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.



Production Credits

Link-making AppleScript: Matt Neuburg

List macros and leopard spots (🐆): Sharon Zardetto

Take Control logo: Jeff Tolbert

Editor in Chief: Tonya Engst

Publisher: Adam Engst

Special thanks this time go to Amelia and Oliver Habicht, for helping with bicycles, and to Andrew and Monique Nielsen, for being fun and relaxing guests.

*Take Control of Your
802.11n AirPort Extreme Network*

ISBN 1-933671-28-9

April 2008. Version 1.2

Copyright © 2008 Glenn Fleishman. All rights reserved.

TidBITS Publishing Inc.

50 Hickory Road

Ithaca, NY 14850 USA

<http://www.takecontrolbooks.com/>

TAKE CONTROL books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control books also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

The electronic version of this book 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. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same info in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Although the author and TidBITS Publishing Inc. 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 book is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. 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.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are trademarks or registered trademarks of Apple Inc.; to view a complete list of trademarks and registered trademarks of Apple Inc., visit <http://www.apple.com/legal/trademark/appletm.html>.

FEATURED TITLES

Now that you've seen this book, you know the Take Control books have an easy-to-read layout, clickable links if you read online, and real-world info that puts you in control. Click any book below or visit our [Web catalog](#) to add to your Take Control collection!

Take Control of Your Wi-Fi Security

by Engst & Fleishman



Learn how to keep intruders out of your wireless network and protect your sensitive communications!

\$10

Take Control of Your Domain Names

by Glenn Fleishman

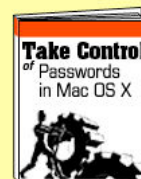


Get expert help with registering, configuring, and managing your Internet domain names like a pro!

\$10

Take Control of Passwords in Mac OS X

by Joe Kissell

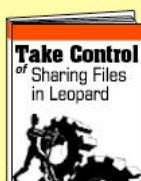


Create and manage strong passwords that keep your data safe without taxing your memory!

\$10

Take Control of Sharing Files in Leopard

by Glenn Fleishman

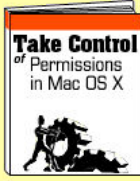


Share files the smart way! Select the right hardware and software, configure your set up, and start sharing files.

\$10

Take Control of Permissions in Leopard

by Brian Tanaka



Solve quirky problems, increase privacy, and share files better by managing Leopard permissions.

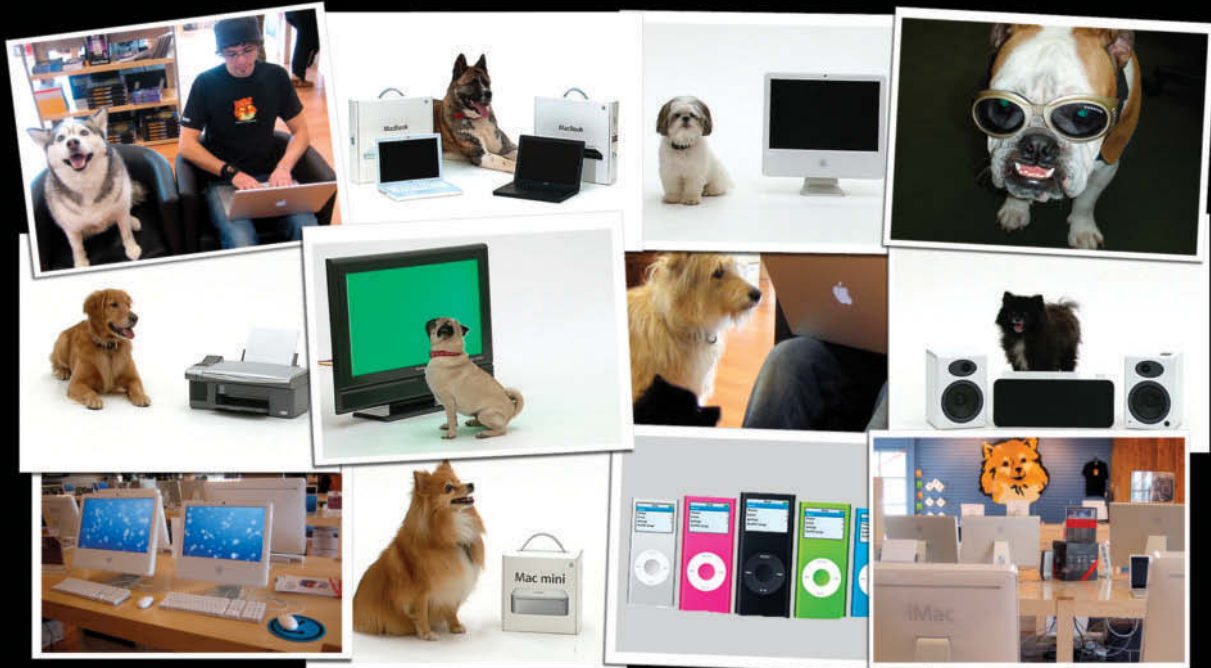
\$10

More Titles!

Delve into even more topics, including:

- Running your Mac—upgrading the OS, understanding accounts, syncing, backups, maintenance, fonts, and more.
- Buying gear—Macs and cameras.
- More topics—.Mac, Mail, iWeb, spam, podcasting, GarageBand, iPhone, and more.

Exclusive coupon for Take Control readers!



\$5 off any Web order from Small Dog Electronics!

Small Dog Electronics offers over **4000 Mac-compatible products**, great prices, and famously superior customer service. We're also a 100% Mac-based company. Every employee is a certified Apple Product Professional, who uses Macs at home as well as on the job. Small Dog Electronics has been part of the Mac community for more than 12 years. We've grown into one of the top Apple Specialists in the United States - and had great time doing it.

Visit **Smalldog.com** and save \$5 on any web order with this coupon!



**Small Dog
Electronics**

Always by your side.

Redeem your coupon on-line at **www.smalldog.com**. Limited to one use per customer. Enter coupon # **bone80317339** at check out.

www.smalldog.com 800-511-MACS

 **Apple Specialist**