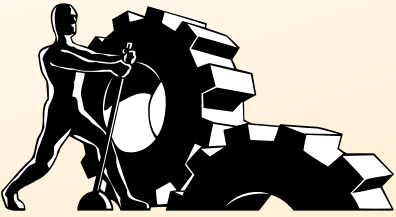


**Check for Updates**

Make sure you have the latest information!



TidBITS Publishing Inc.

**Take Control of Your**

**v1.6**

# 802.11n

# AirPort

# Network

**Glenn Fleishman**

**\$15**

[Help](#)

[Catalog](#)

[Feedback](#)

[Order Print Copy](#)

# Table of Contents

Skip to next section.

## **READ ME FIRST 5**

Updates .....	5
Who Needs This Book.....	5
What's New in Version 1.6 .....	6
What's New in Version 1.5 .....	6
Earlier Editions .....	6
Basics .....	7

## **INTRODUCTION 9**

## **QUICK START TO AIRPORT NETWORKING 10**

## **QUICK TROUBLESHOOTING GUIDE 13**

Reset a Locked-up Base Station.....	13
Printer Problems.....	14
Other Troubleshooting.....	15

## **AIRPORT ICONOGRAPHY 17**

## **LIGHT READING 18**

## **KEY GLOSSARY TERMS 19**

## **LEARN WIRELESS BASICS 23**

Access Points and Adapters.....	23
The Spectrum Part of Wi-Fi .....	24
Wi-Fi and AirPort Flavors .....	25

## **APPLE AND MAC WI-FI GEAR 31**

802.11n and Apple's Choices.....	31
AirPort Base Station Models .....	32
Adapters in Macs .....	39

## **PLUG IN YOUR BASE STATION AND GET STARTED 44**

Unpack and Power Up .....	44
Know Your AirPort Software .....	46
Launch AirPort Utility and Keep Up to Date.....	48
Decide on Your Next Step .....	50
Connect to Your Base Station .....	51
First Steps in Setup .....	53

## **SET UP A NETWORK 56**

Get Started.....	56
New Network, Single Base Station .....	57
Extend a Network via Ethernet .....	64

Replace an Existing Base Station .....	68
Extend a Network via Wi-Fi .....	71
Create Separately Named 2.4 and 5 GHz Networks .....	74
<b>DETERMINE THE BAND, CHANNEL, AND LOCATION 76</b>	
Spectrum Trade-offs .....	77
Pick Compatibility and Optionally Set a Channel.....	82
Pick the Right Place .....	85
<b>ADVANCED NETWORKING 92</b>	
Get a WAN Address.....	92
Hand Out LAN Addresses .....	100
<b>CONNECT YOUR COMPUTERS 111</b>	
Connect in Both @opards .....	111
Connect in Tiger .....	124
Connect in Windows XP .....	126
Connect in Windows Vista .....	130
<b>AIRPORT EXPRESS EXTRAS 134</b>	
AirPort Express and AirTunes .....	134
Share with Airfoil.....	138
Connect to Any Base Station .....	140
<b>CONNECT MULTIPLE BASE STATIONS 143</b>	
Know the Basics .....	143
Add Access Points via Ethernet .....	146
Bridge Wirelessly .....	150
<b>MIX 2.4 GHZ AND 5 GHZ 802.11N NETWORKS 159</b>	
Know the Goal .....	159
Set Up Your 2.4 GHz Base Station.....	160
Configure Your 5 GHz Base Station .....	162
Put Printers in the Right Place .....	162
<b>REACH YOUR NETWORK REMOTELY 164</b>	
Know Your Options .....	164
Map Ports for Remote Access .....	166
Punch Through with NAT-PMP.....	174
Set a Default Host for Full Access .....	176
Access a Base Station via MobileMe.....	177
<b>SET UP A SHARED USB PRINTER 180</b>	
Add a Printer .....	180
Rename and Widely Share a USB Printer.....	181
Add a Shared Printer in 10.5–10.6 .....	182
Add a Shared Printer in 10.2–10.4 .....	183
Add a Shared Printer in Windows .....	184
Troubleshoot an Unavailable Shared USB Printer.....	188

<b>SET UP A SHARED USB DISK</b>	<b>189</b>
Prepare Your Drive .....	190
View Connected Volumes.....	191
Work with Time Capsule .....	193
Grant Access.....	199
Gain Access .....	202
<b>SECURE YOUR NETWORK</b>	<b>207</b>
Likelihood, Liability, and Lost Opportunity .....	207
Simple Tricks That Don't Work .....	210
Use Built-In Encryption.....	213
Set Up Guest Networking.....	222
<b>OVERCOME INTERFERENCE</b>	<b>224</b>
Eliminate Conflicting Signals .....	224
Set Interference Robustness .....	226
<b>EXPLORE THE INTERNET'S FUTURE WITH IPv6</b>	<b>228</b>
IPv6 Background .....	228
IPv4 and IPv6 Tunneling.....	230
Configure IPv6 in N Routers .....	231
IPv6 Advances .....	234
<b>APPENDIX A: APPLE TV AND WI-FI</b>	<b>235</b>
<b>APPENDIX B: AIRPORT UTILITY EXTRAS</b>	<b>238</b>
Create and Manage Profiles.....	238
Export and Import Configuration Profiles.....	240
Connect Remotely .....	242
Revert to Older Firmware.....	243
AirPort Pane.....	245
Advanced Pane.....	246
<b>APPENDIX C: SETTING UP A SOFTWARE BASE STATION</b>	<b>248</b>
Software Base Station.....	248
Ad Hoc Networking .....	252
<b>APPENDIX D: CHANNELS EXPLAINED</b>	<b>254</b>
2.4 GHz Channels .....	255
5 GHz Channels.....	256
<b>APPENDIX E: AIRPORT COMMAND-LINE UTILITY</b>	<b>259</b>
Scan .....	260
Getinfo.....	261
<b>ABOUT THIS BOOK</b>	<b>262</b>
<b>COPYRIGHT AND FINE PRINT</b>	<b>264</b>

# Read Me First

Welcome to *Take Control of Your 802.11n AirPort Network*, version 1.6, published in September 2009 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and edited by Tonya Engst.

This book helps you install and get the most out of your network using Apple's AirPort and Time Capsule gear with the 802.11n Wi-Fi networking standard in Leopard and Snow Leopard.

Copyright © 2008, 2009, Glenn Fleishman. All rights reserved.

If you have the PDF version of this title, please note that if you want to share it with a friend, we ask that you do so as you would a physical book: "lend" it for a quick look, but ask your friend to buy a new copy to read it more carefully or to keep it for reference. You can click [here](#) to give your friend a discount coupon. Discounted [classroom and Mac user group copies](#) are also available.

---

## UPDATES

---

We may offer free minor updates to this book. To read any available new information, click the Check for Updates link on the [cover](#), or click [here](#). On the resulting Web page, you can also sign up to be notified of major updates via email. If you own only the print version of the book or have some other version where the Check for Updates link doesn't work, contact us at [tc-comments@tidbits.com](mailto:tc-comments@tidbits.com) to obtain the PDF.

---

## WHO NEEDS THIS BOOK

---

If you're setting up, extending, or retooling a Wi-Fi network with one or more 802.11n base stations from Apple—including the AirPort Extreme, AirPort Express, or Time Capsule—with either Mac OS X 10.5 Leopard, 10.6 Snow Leopard, or Windows XP or Vista, this book will help you get the fastest network with the least equipment and fewest roadblocks.

---

## WHAT'S NEW IN VERSION 1.6

---

Most changes in this version are for Mac OS X 10.6 Snow Leopard:

- The Network system preference pane looks slightly different in Snow Leopard.
- The AirPort status menu on the menu bar in Snow Leopard has some new features; see [Learn from the AirPort Menu](#) (p. 121).

Nearly everything else about using AirPort in Leopard and Snow Leopard is identical.

---

***Printing only the important changed pages from 1.5: Print these pages: 1–6, 34, 38, 46–48, 89–91, 101, 111–123, 170, 178–182, 193–195, 204–206, 219, 249–250, and 259–260.***

---

---

## WHAT'S NEW IN VERSION 1.5

---

Here's a summary of the most important changes between 1.0 and 1.5:

- Added coverage of the March 2009 models of the AirPort Extreme Base Station and Time Capsule. To learn more about the new base station models, consult [AirPort Base Station Models](#) (p. 32).
- [Extend a Network via Wi-Fi](#) (p. 71) is reworked for enhanced clarity and to explain how the Wireless Distribution System (WDS) differs in 802.11n base stations from previous generations of gear.
- A new section, [Light Reading](#) (p. 18), decodes what the light on your base station is trying to tell you.
- The section about setting a base station's spectrum is now called [Determine the Band, Channel, and Location](#) (p. 76), and it has been revised: advanced background information was expanded and moved to the new [Appendix D: Channels Explained](#) (p. 254).

---

## EARLIER EDITIONS

---

This book is based largely on two previous books: *Take Control of Your AirPort Network* (2005) and *Take Control of Your 802.11n AirPort Extreme Network* (2007). The former book covered 802.11g AirPort

networking; the latter, the newer 802.11n networks. Both books focused on using Mac OS X 10.4 Tiger. This new book covers much of the same material, but in slightly to extremely different ways.

Apple thoroughly revised the new AirPort Utility base station configuration program between the release of the second version of the AirPort Extreme Base Station with Draft N (August 2007) and the release of Time Capsule (February 2008). These changes meant reworking much of the earlier part of the book explaining how to use the Assist Me mode in AirPort Utility; in the process, I split my advice into scenarios that cover the different kinds of networks you might be building or updating. This should make basic configuration easier, as well as help you easily find help if you return to the book to configure or add base stations in the future, or to set up multiple networks in different places.

I've also overhauled the manuscript to focus on Mac OS X 10.5 Leopard (and in version 1.6 I added 10.6 Snow Leopard details) along with network troubleshooting help. I've also updated the text for all the latest models of 802.11n base stations, including the simultaneous dual-band models that appeared in 2009. Further, I've added more information about IPv6, the next-generation Internet numbering standard, which is starting to have practical applications, and which can be used quite easily with all of Apple's current Wi-Fi gear, and Mac OS X since version 10.3 Panther.

---


## 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. For example, AirPort Utility gets installed into the Utility folder, which is in 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, such as those in the Network preference pane. To reach a preference pane, open System Preferences by clicking its icon in the Dock or by choosing  > System Preferences. Then, to open a preference pane, click its icon or choose it from the View menu. For example, to see “the Network preference pane,” launch System Preferences and then click the Network icon or choose View > Network. To find the AirPort view in the Network preference pane, you would use the same steps and then click the AirPort item in the adapter list at the left of the Network preference pane.
- **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, and then choose Base Station > Manual Setup (Command-L) to proceed. You can alternately click the Manual Setup button in the lower-left corner of the setup screen after selecting the base station.
- **AirPort menu:** The AirPort menu is a status menu near the right side of the system menu bar on a Macintosh. If yours isn’t showing, you can turn it on via a checkbox in the Network system preference pane. To learn more about the icons that may mark the top of this menu, see [AirPort Iconography](#) (p. 17).
- **Know your AirPort model:** AirPort models change capabilities more often than they change names. You can use AirPort Utility to figure out which model you have, and [AirPort Base Station Models](#) (p. 32) will help you identify your model and its features. When I refer to “802.11n base stations from 2007 or later,” I mean those models *released* in 2007 or later, all of which include 802.11n networking. If you purchased an AirPort Express in 2007, but its model year is 2004, it doesn’t count as being “from 2007 or later.”



# 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 large campuses, 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 widely 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*, at one time more commonly called *Draft N*). Today, Wi-Fi is built into nearly every Mac.

Despite Apple's 10-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 this book focuses on 802.11n AirPort networks, I also cover compatibility and connections with older hardware, and connecting to 802.11n via 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 using an AirPort Express's unique features, and finish with how-to information on security for those who want their AirPort networks safe from freeloaders and intruders.

# Quick Start to AirPort Networking

You can read this book from start to finish, and you'll find that it covers topics like learning about Wi-Fi, unpacking a base station, starting configuration, figuring out the network you want to build, and then configuring that network. More specific cases follow, such as how to add a printer, separating older and newer flavors of Wi-Fi into two separate networks, and securing a network. Use this Quick Start to get an idea of how you might jump into the book if you are at a particular stage in working with your network, and to find more than one path through the material.

---

***Need a quick solution?** Flip ahead three pages to the [Quick Troubleshooting Guide](#) or see [Light Reading](#) (p. 18) to learn what the light on your AirPort base station is trying to tell you. Also, you may especially wish to consult [Overcome Interference](#) (p. 224).*

---

## **Learn wireless basics:**

- Get a quick grounding in wireless terminology and technology. See [Key Glossary Terms](#) (p. 19) and [Learn Wireless Basics](#) (p. 23).
- Familiarize yourself with [Apple & Mac Wi-Fi Gear](#) (p. 31).

## **Plan your network:**

- For common configurations, see [Set Up a Network](#) (p. 56), and focus on the diagrams and descriptions at the beginning of: [New Network](#), [Single Base Station](#), [Extend a Network via Ethernet](#), [Replace an Existing Base Station](#), and [Extend a Network via Wi-Fi](#).
- For ideas on using the AirPort Express, skim [AirPort Express Extras](#) (p. 134) to learn about the features and networking arrangements.
- For more advanced possibilities, consult [Connect Multiple Base Stations](#) (p. 143), and pay special attention to the descriptions and diagrams at the start of [Add Access Points via Ethernet](#) and [Bridge Wirelessly](#). Also, note that Appendix C (p. 248) covers creating a [Software Base Station](#) and [Ad Hoc Networking](#).

- To build a network that uses two base stations to separate 2.4 and 5 GHz devices for best performance, read [Mix 2.4 GHz and 5 GHz 802.11n Networks](#) (p. 159).

### **Set up your base station(s):**

- Unpack your base station and start down the path of configuring it in [Plug In Your Base Station and Get Started](#) (p. 44). You'll likely continue in one of these sections:
  - ◇ Learn how to configure a new network with a single base station. See [New Network, Single Base Station](#) (p. 57).
  - ◇ For existing networks, find what you need to [Extend a Network via Ethernet](#) (p. 64) or [Replace an Existing Base Station](#) (p. 68).
  - ◇ Separate networks for best performance into different spectrum slices. See [Mix 2.4 GHz and 5 GHz 802.11n Networks](#) (p. 159).
  - ◇ When wireless is the way to go, learn what you need to extend a network using only Wi-Fi. See [Extend a Network via Wi-Fi](#) (p. 71) and [Bridge Wirelessly](#) (p. 150).
  - ◇ Hook up a larger network with many base stations. See [Connect Multiple Base Stations](#) (p. 143) to build a network that spans a house or office connected wirelessly, or via electrical outlets or Ethernet.
- Further configure your network's LAN settings for fixed addresses or special cases. See [Advanced Networking](#) (p. 92).
- [Determine the Band, Channel, and Location](#) (p. 76) for your base station, thus making sure your network reaches as far as you want with the bandwidth you need. For help with concepts used in that section, consult [The Spectrum Part of Wi-Fi](#) (p. 24).
- Share a printer or a hard drive. See [Set Up a Shared USB Printer](#) (p. 180) or [Set Up a Shared USB Disk](#) (p. 189).
- Set up Time Machine backups with a Time Capsule base station. Read [Work with Time Capsule](#) (p. 193).

### **Connect to your base station:**

- Find out how to connect Macs and systems running Windows to a base station in [Connect Your Computers](#) (p. 111).

- Access your network when you're not physically on it. See [Reach Your Network Remotely](#) (p. 164).
- Access hard drives in and connected to your base station via Back to My Mac. See [Access a Base Station via MobileMe](#) (p. 177).

### **Add music and video:**

- Use the AirPort Express to stream music. See [AirPort Express and AirTunes](#) (p. 134) and [Share with Airfoil](#) (p. 138).
- Get jiggy with a video- and audio-streaming set-top box, the Apple TV. See [Appendix A: Apple TV and Wi-Fi](#) (p. 235).

### **Secure your network:**

- Decide if you need encryption. Read [Likelihood, Liability, and Lost Opportunity](#) (p. 207).
- Avoid security tricks that don't work. Consult [Simple Tricks That Don't Work](#) (p. 210).
- Apply encryption using the best—and often simplest—method. See [Use Built-In Encryption](#) (p. 213).
- If you have a 2009 AirPort Extreme or Time Capsule, you can [Set Up Guest Networking](#) (p. 222).

### **Learn still more advanced topics:**

- Find out what the future will bring for end-to-end connections with intermediaries in [Explore the Internet's Future with IPv6](#) (p. 228).
- Stop pulling your hair out over a problem with new firmware you install that doesn't work. See [Revert to Older Firmware](#) (p. 243).
- Get a few details about special configuration options for AirPort Utility that I don't cover elsewhere by reading the [AirPort Pane](#) (p. 245) topic in Appendix B.
- Act wonky and fire up Terminal to learn more about your AirPort adapter. Read [Appendix E: AirPort Command-Line Utility](#) (p. 259).

# Quick Troubleshooting Guide

If you need quick help, here's the starting point. I first look at handling a locked-up base station and then give tips for solving a variety of common problems.

**Note:** [Light Reading](#), a few pages ahead, helps you learn information about a problem by decoding the appearance of a base station's LED status light.

---

## RESET A LOCKED-UP BASE STATION

---

If an AirPort Extreme Base Station, AirPort Express, or Time Capsule neither appears in the AirPort menu as an available network, nor in AirPort Utility as an available base station, 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:**

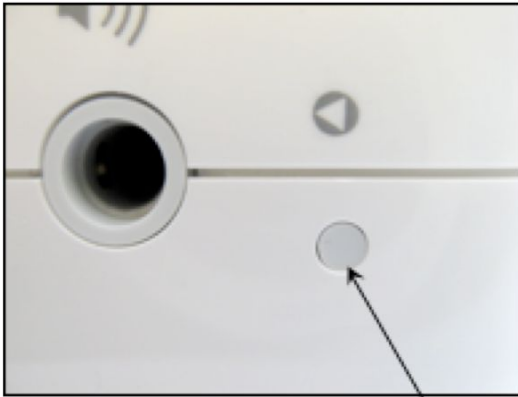
---

***Warning!*** You might damage the data on the internal drive by pulling the plug on a Time Capsule. Make sure Time Machine backups or other transfers aren't in progress when you power cycle a Time Capsule: in the Time Machine menu, choose Stop Backup and wait for it finish; or open the Time Machine preference pane and flip the On switch to Off, and wait until Time Machine is inactive.

---

Remove the power adapter's plug from 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 custom settings you've made (I recommend backing up these settings; see [Create and Manage Profiles](#)). To reset any of Apple's three base station models, 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 AirPort Extreme and Time Capsule and next to the audio jack on the AirPort Express; with all three models, the button is beneath the *reset symbol*, a white arrow reversed out of a gray circle (**Figure 1**).



**Figure 1:** The reset button is located below the reversed-out white arrow; here, it's next to the audio port of an AirPort Express.

4. **Failing a factory reset, try another method to reset the base station:** 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 all the above:** Call Apple for return instructions.

---

## PRINTER PROBLEMS

---

### **Printer on 802.11g part of a mixed legacy/new network won't print**

You'll need to connect it to your Extreme N or Time Capsule base station. [Put Printers in the Right Place](#) explains how (p. 162).

### **Can't print to a USB-connected printer**

See [Troubleshoot an Unavailable Shared USB Printer](#) (p. 188).

---

## OTHER TROUBLESHOOTING

---

### **Can't see base station's network from all Macs**

Did you set the base station to use just the 5 gigahertz (GHz) band? Only Mac models released starting in 2005 with 802.11a or 802.11n built in can connect. Or did you set the base station to allow 802.11n-only connections in 2.4 GHz? Only late 2006 and later Macs have 802.11n built in. For more help, read [Determine the Band, Channel, and Location](#) (p. 76).

Further, computers can sometimes temporarily lose their capability to find Wi-Fi networks. Try turning the adapter off and back on—on a Mac, choose Turn AirPort Off from the AirPort menu, and then choose Turn AirPort On. Another common fix is to restart the computer.

---

***Flaky adapter:** In some cases, the AirPort adapter may have gone flaky—“flaky” isn’t a technical term, but an apt description. The original AirPort Card and its AirPort Extreme replacement are known to behave erratically the older and more used they become. All Macs sold in the last few years include AirPort Extreme built in, which has turned out to be much more reliable.*

---

### **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](#) (look for the Warning on p. 111).
- Access control may be preventing access. See [MAC Address Filtering](#) (p. 211).
- Interference from other networks may be the problem. Consult [Eliminate Conflicting Signals](#) (p. 224).

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

You might be using a Mac with the older AirPort Card with a base station set up with WPA2 encryption. See [Turning on WPA/WPA2 Personal](#) (p. 216).

**Can't connect to a base station after selecting it and seeing the summary screen**

Are you using Jumbo (9000-byte) frames on your Ethernet adapter? See [Jumbo Ethernet Frames Disable AirPort Utility Access](#) (p. 54).

**Firmware update makes base station act erratically**

Try to [Revert to Older Firmware](#) (p. 243).

**Network works erratically**

Another network might be interfering with yours. See [Eliminate Conflicting Signals](#) (p. 224).

**Conflicting signals seem to cause network problems**

Read [Eliminate Conflicting Signals](#) (p. 224).



# AirPort Iconography

The AirPort menu—located on the system menu bar—reveals what kind of connection is in progress on your computer. There are four icons you'll commonly see, each of which has a particular meaning. Knowing what the icons mean can help you troubleshoot problems. This icon is always at the top of the AirPort menu.



A gray fan indicates an active Wi-Fi network adapter that isn't currently connected to any network. See [Connect Your Computers](#) (p. 111) to get started.



A full fan with one or more black bars—the bars represent current strength—indicates a current Wi-Fi connection to either a base station or a network created through the Sharing preference pane's Internet Sharing service. For more information, consult [Connect Your Computers](#) (p. 111) and [Appendix C: Setting up a Software Base Station](#) (p. 248).



A fan showing an up arrow indicates the Internet Sharing service is active on this computer. See [Software Base Station](#) (p. 248), in Appendix C.



A fan containing a computer shows that the computer is using *ad hoc networking*, a method of creating Wi-Fi communication among multiple computers without using a base station, not even the "software" base station that's created by Internet Sharing. See [Ad Hoc Networking](#) (p. 252), in Appendix C.



An empty fan outline indicates that either there's no Wi-Fi adapter in the computer, or the Wi-Fi adapter has been turned off. To turn it on, choose Turn AirPort On from the menu.

If the AirPort icon still looks like an empty fan or an error says 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.

# Light Reading

The light on the front of any Apple Wi-Fi base station indicates what the base station is up to: handling data correctly, hitting an error, or in a special mode. The guide below helps you decipher the meaning.

- **Off:** There's no power! Plug in the base station. If it is plugged in, check the outlet or power strip, and the places where the cord plugs into other cords or into the base station. If juice is flowing and the cord looks correct, you have a defunct base station.
- **Blinking green:** The base station light blinks or flashes green in three cases:
  - Startup: The light flashes green on and off for 1 second.
  - Reset: This happens after you press the recessed reset button for long enough to trigger a reset.
  - Network activity: You can set the light to show network activity, with green flashes that approximate the amount of activity. In AirPort Utility, on the AirPort pane, in the Base Station view, click Options and then change the Status Light pop-up menu. (See [Base Station Settings](#), p. 245.)
- **Solid green:** The base station is configured correctly, has no updates available, and is connected to the Internet.
- **Solid amber:** The base station is still powering up and hasn't loaded all its settings and connected to the network.
- **Blinking amber:** The a base station has a configuration problem, has lost its network connection, or is suffering from another problem. Use AirPort Utility to troubleshoot.
- **Solid blue:** If you've used AirPort Utility to allow a client to connect via Wi-Fi Protected Setup (WPS), the light remains blue until a client connects or you cancel the mode in AirPort Utility. (See [Use WPS](#), p. 219.)

# 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've presented the concepts in the order you need to understand them, building one on top of the other.

**Wi-Fi:** *Wi-Fi* refers to the set of wireless networking standards that encompasses all of Apple's AirPort products, and thousands of wireless networking products made by other firms. Wi-Fi provides a test-based way of ensuring that devices work in a consistent way using four IEEE 802.11 Working Group standards: 802.11b, 802.11g, 802.11a, and 802.11n (B, G, A, and N, respectively)

**802.11n and Draft N:** The most recent Wi-Fi addition is *802.11n*, which is currently in the final stages of development at the IEEE group. *Draft N* is the name used by the Wi-Fi testing group to indicate that a device conforms to the latest interoperable set of guidelines for 802.11n. Almost everyone now simply calls this standard 802.11n, even though the final steps for approval haven't been voted on. There's no chance of any change.

**Spectrum bands:** Wi-Fi operates in unique slices of radio-frequency spectrum: the 2.4 gigahertz (GHz) and 5 GHz bands. 802.11b and 802.11g operate exclusively in 2.4 GHz; 802.11a exclusively in 5 GHz; 802.11n may operate in either band.

**Ethernet:** Ethernet refers to 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:** An *access point* is 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*.

**Dual band:** A *dual-band* Wi-Fi router can use either 2.4 or 5 GHz to create a network. All Apple 802.11n Wi-Fi gear is dual band.

**Simultaneous dual band:** This kind of Wi-Fi router has two radios, allowing the creation of two networks at once, one each in the 2.4 GHz and 5 GHz bands. Apple Wi-Fi base stations released in 2007 and 2008 have a single radio that can use either band; the AirPort Extreme Base Station and Time Capsule models released in 2009 have two radios and can create two networks simultaneously.

**Ad hoc network:** An *ad hoc network* is a Wi-Fi network created from the Create Network item in the AirPort menu that comprises only computers, no base stations. Ad hoc networks don't require a connection to the Internet, and are used in the absence of other Wi-Fi infrastructure, just like plugging Macs together using FireWire.

**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. 97).

**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 offers 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 it 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 require an intermediary to reach private IP addresses directly (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](#) (p. 166). 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.

Apple's base station models include a DHCP server to provide this function. Each 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 a 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 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.

**Dynamic address:** DHCP can set an address that remains the same over time, or it can provide a new address to a computer or device every 5 minutes (although that's very unlikely; hours, days, or weeks is more common). With *dynamic addressing*, a computer requests an address and uses what it's given. The DHCP server controls the lifetime of the address and when it's refreshed or changed. Unlike a static address, a dynamic address is assigned; it may be public or private.

**Static address:** A *static address* is a fixed address for a computer or device that does not change over time. It can be assigned via DHCP, but is assigned and not changed by the DHCP server. More typically, a user enters a static address manually in a TCP/IP manual configuration area for a given network adapter. A static address is often public, but can also be private on a network in which fixed addresses are used to maintain consistent network access to a resource over time by number instead of by Bonjour or other local network name.

**Guest network:** A guest network is a new feature offered in the 2009 models of the AirPort Extreme and Time Capsule. It makes it possible to set up a secondary wireless network that guests can use to access only the Internet (with or without a password). Guests can access neither other machines on the primary local network nor printers or other devices. For details, see [Set Up Guest Networking](#) (p. 222).

# Learn Wireless 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* connects both to wireless adapters and to a broader network, such as the Internet via a broadband modem. 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, certain forms of hard-drive file sharing, and base-station-to-base-station connections.

The wireless adapter uses client software on the computer or handheld device to connect to a specific base station (or set of affiliated 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, and the AirPort adapter in the Network system 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. The key, which consists of a series of characters, may need to be entered exactly as it was entered on the base station, although a stored key can be sent without a person having to re-enter it.

---

***Avoid entering an encryption key manually:*** All Apple base stations now support a simple method that avoids key entry altogether. See [Use WPS](#), p. 219.

---

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 typically require users to obtain a license to use those airwaves, and everyone may use them. In contrast, cellular telephone companies pay huge amounts for the exclusive geographic rights to certain frequencies.

---

***Licenses in a few places:*** In some developing nations, inexpensive or free licenses are required for outdoor use but not indoor use, or by businesses but not individuals. In the United States, Australia, Japan, South Korea, and most of Europe, no licenses are required.

---

Unlicensed *bands*—specified ranges of frequencies—are divided into smaller portions 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.

In the United States and in most countries, two bands are available for use, the 2.4 GHz (gigahertz) band and the 5 GHz band. (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. When it comes to the way AirPort gear handles bands, there are three approaches:

- **One band only:** Older AirPort equipment works only in the 2.4 GHz band.
- **Dual band:** All 2007 and 2008 Apple base stations can use either the 2.4 or the 5 GHz band.
- **Simultaneous dual band:** The models introduced so far in 2009 can use both bands at once.

For more on the differences between 2.4 and 5 GHz, see [Spectrum Trade-offs](#).

---

***Warning!*** Apple and other manufacturers sell specific hardware for each country or regulatory domain in which they do business. Because laws vary so much by country or regulatory body, it's crucial that you don't take a base station from, say, the United States to France and turn it on. You could wind up facing fines and jail time.

---

---

## **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.” The current fastest generation is known as 802.11n or “N.”

**Note:** N isn’t technically a standard; See [Not Yet Finished](#) (p. 29), for more detail.

The Wi-Fi Alliance, a trade group, 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 the AirPort hardware, which correspond to three major revisions of the IEEE 802.11 standards—802.11b, 802.11g, and 802.11n (**Table 1**). Every older version can be used with even the newest models, so long as the newer base station has a legacy or compatibility mode enabled.

### **What about 802.11a?**

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 B and later G protocols, which were 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 first generation of Intel-based Macs without advertising the fact because the Intel chips that 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.

A colleague recently couldn’t understand how an older computer of his was connecting to a 5 GHz network; it turned out that the Mac was one of these Intel boxes with 802.11a. You may want to disable 802.11a in the 5 GHz band to avoid having it slow down your 802.11n devices; see [Eliminate 802.11a](#) (p. 83).

**Table 1: Wi-Fi Standards in Apple AirPort Hardware**

<b>Standard/ Band</b>	<b>Device (introduced, discontinued)</b>	<b>Raw Speed</b>	<b>Maximum Throughput</b>
802.11b (B)/ 2.4 GHz	<ul style="list-style-type: none"> <li>• AirPort (1999, discontinued 2003)</li> <li>• AirPort Card (1999, discontinued 2004)</li> </ul>	11 Mbps	5.5 Mbps
802.11g (G)/ 2.4 GHz	<ul style="list-style-type: none"> <li>• AirPort Extreme (2003, discontinued 2007)</li> <li>• AirPort Extreme Card (2003, superseded by built-in adapters, but still available)</li> <li>• AirPort Express (2004)</li> <li>• Built-in 802.11g adapter in Macs (2005)</li> <li>• iPhone (June 2007)</li> <li>• iPod touch (Sept. 2007)</li> </ul>	54 Mbps	25 Mbps
802.11a (A)/ 5 GHz	<ul style="list-style-type: none"> <li>• Never separately and officially supported by AirPort, but silently included in the Wi-Fi adapter in early Intel Macs</li> </ul>	54 Mbps	30 Mbps
802.11n* (Draft N)/ 2.4 GHz and/or 5 GHz	<ul style="list-style-type: none"> <li>• AirPort Extreme (Feb. 2007)</li> <li>• Apple TV (Feb. 2007)</li> <li>• AirPort Extreme with gigabit Ethernet (Aug. 2007)</li> <li>• Time Capsule (Feb. 2008)</li> <li>• AirPort Express (Mar. 2008)</li> <li>• AirPort Extreme Simultaneous Dual Band (Mar. 2009)</li> <li>• Time Capsule Simultaneous Dual Band (Mar. 2009)</li> <li>• Built-in 802.11n adapter in all current model desktop, laptop Macs (late 2006)**</li> </ul>	300 Mbps	140 Mbps (with gigabit Ethernet)

\* Current draft became a tested part of Wi-Fi in June 2007; the final version is due in 2010 in nearly the same form.

\*\* Intel Core 2 Duo Macs except discontinued 1.83 GHz 17-inch iMac and all Mac mini models before March 2009 update; optional adapter for the Mac Pro; not available for Xserve.

---

**Card or built-in?** Apple moved years ago from offering Macs with an AirPort Extreme card slot to including Wi-Fi onboard—but they still call the technology AirPort Extreme. Apple stopped selling the standalone card for older Macs in 2009, but you can find it on eBay, or use third-party adapters. (See [Third-Party Adapters](#).)

---

## 802.11n Details

Let's learn more about 802.11n and how it relates to Mac OS X and the three Draft N base stations Apple offers.

### 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 typically 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 it 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, Time Capsule, Express, and other consumer gateways so far all use the 300 Mbps speed, which can pass as much as 150 Mbps in real data, although rates from 50 to 80 Mbps are more common.

### Single Stream Radios

A form of 802.11n called *single stream* uses one or two antennas and a single data stream. While this seems contrary to the advantages of 802.11n, it's still a huge boost over 802.11g—as much as double the speed. A new technology called *space-time block coding* will also let an access point send data simultaneously and separately to as many single-stream devices as the base station has radios, further improving downstream (Internet to device) throughput.

The speed drops when other Wi-Fi networks used 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 (see [Compatibility among 802.11 Flavors](#), next page).

### **Not Yet Finished**

An important proviso when discussing 802.11n is that the standard isn't ratified. That means that the IEEE as an overarching group hasn't voted to approve a final form of the standard. But, in the case of 802.11n, what's left to do is all process and hand waving. The real work was finished in early 2007, when a second draft was issued that contained a grand compromise between firms with opposing views. Everything since then has been sanding the floorboards and straightening pictures. To extend the metaphor, even though the current plan is to ratify 802.11n officially in January 2010, the house was built long ago and families have been raised in it.

You'll still see the name Draft N attached to 802.11n devices, which equipment makers do partly so that they won't be sued for failing to disclose that the device doesn't formally conform to a completed standard. The only real concern with a Draft N device should be whether anything serious will change that can't be updated in firmware (the answer appears to be clearly, "no"), and whether 802.11n gear will all work with other 802.11n gear. The Wi-Fi Alliance tests and certifies 802.11n equipment (using the "Draft N" name), and all of Apple's 802.11n device's have this certification.

### **Outdated? Not until 2012 or Later**

You always worry whether you're buying last year's technology at this year's prices. Faster flavors of N with more simultaneous data streams and other improvements, but full backward compatibility, will slowly become available and more affordable by the end of 2010.

The IEEE has newer standards on the horizon for wireless LANs: 802.11ac, which updates the current standards for 1 Gbps or faster networking, and 802.11ad, which will use new spectrum up at 60 GHz for the same purpose. Still, it's likely 2 to 3 years before we see the first, expensive versions of these new technologies, and another 2 years beyond that before it trickles down into consumer and professional hardware that's affordable.

## Compatibility among 802.11 Flavors

Each 802.11 evolution is backward compatible with all earlier protocols in the same spectrum band, although backward compatibility can be turned off. With Apple gear, for instance, the original AirPort handled just 802.11b, and AirPort Extreme 2003 added 802.11g, which incorporates B with full support. Likewise, Apple's N base stations handle the older A, B, and G standards.

In fact, devices using 802.11n are *required* to support older A, B, and G devices. All equipment I've tested calls this a *mixed* mode, and Apple's 802.11n hardware sports controls that let you choose in 2.4 GHz whether to allow B, G, and N; G and N; or just N. In 5 GHz, you can choose A and N or just N.

**Tip:** The first-generation Intel-based Macs that Apple slipped 802.11a into handle A, B, and G (flip back a few pages for more info in [What about 802.11a?](#)); Macs with 802.11n handle A, B, G, and N.)

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. Any B device connecting to a 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 a network's maximum throughput. This overhead comes from the fact that each packet of data begins with a special message—a *preamble*—that's encoded at the slowest backward compatible speed so that the slowest devices can understand it.

You can increase the speed of networks by setting minimum levels of backward compatibility, as described in [Compatibility](#). By eliminating slower speeds or B adapters, you can speed up a network. Apple's simultaneous dual-band base stations avoid this problem largely by allowing N devices to work mostly in the 5 GHz band, leaving 2.4 GHz for slower B and G adapters. I discuss how to set this up with older equipment in [Mix 2.4 GHz and 5 GHz 802.11n Networks](#).

# Apple and Mac Wi-Fi Gear

A long history with Wi-Fi has led to three devices in Apple's current line up of base stations: each one includes 802.11n but has a distinct set of features. Let's look first at how Apple has chosen to work with 802.11n, and then at Apple's current base stations and the options for Apple and third-party adapters.

---

## 802.11N AND APPLE'S CHOICES

---

Although Apple has made distinct choices when implementing 802.11n, all three of Apple's 802.11n base stations can handle both the 2.4 band and the 5 GHz band.

When Apple first shipped the AirPort Extreme Base Station with 802.11n, most other N gateways lacked 5 GHz support. Apple made sure that all Macs it shipped with N could also use both bands, as can the Apple TV. The original dual-band 802.11n models of the AirPort Extreme and the Time Capsule could handle only one band at a time, whereas the revised 2009 models of the AirPort Extreme and Time Capsule can handle two bands simultaneously.

For the 5 GHz band, Apple enables just 8 of the 23 possible channels in the United States. The reasons for this have to do with a compromise among the radio equipment industry, the military, and the FCC. Equipment like a Wi-Fi gateway has to engage special mechanisms for the 15 channels Apple has chosen not to support. The compromise to protect limited military radar use in those frequencies makes those 15 channels frustrating to use for home networks.

Apple also chose to limit to the 5 GHz band the 802.11n feature of using two channels at once—*wide* channels—which doubles the raw bandwidth. This was an option under the Wi-Fi Alliance's certification rules. Some vendors offer wide channels in 2.4 GHz as an option.

In practice, 2.4 GHz wide channels don't work well, because N devices tread lightly to avoid interfering with other networks. In a real-world situation, you would likely see an improvement in throughput with 2.4 GHz wide channels only if no other Wi-Fi networks are nearby.

---

## AIRPORT BASE STATION MODELS

---

Apple current line-up of base stations that offer Wi-Fi comprise the AirPort Extreme, the latest standard small office and corporate model; Time Capsule, a backup system coupled with Extreme features; and AirPort Express, a refreshed version of the compact router (**Table 2**, next page). (You can also take a walk through memory lane, looking at all the discontinued models in **Table 3**, two pages ahead.)

### Field Guide to Base Stations

Because the names AirPort Extreme, AirPort Express, and Time Capsule have been used regardless of changes to features and internal options, unless you've just purchased a base station it's not always clear which model you have. In **Table 2** and **Table 3**, for models made in 2003 and later, I include the same identification information that you can see in AirPort Utility and imprinted on the bottom or back of the device.

The model number used by Apple on the gear itself unfortunately doesn't appear anywhere else online—Apple uses an entirely different stockkeeping unit for referring to its models.

To see what AirPort Utility (noted as AU in the table) says about the base station, launch the program, select your base station, and look at the first line in the main pane that starts, "AirPort Utility found..." Following that phrase is the model line of base station and characteristics about it, such as Fast Ethernet or Simultaneous Dual-Band.



**Table 2: Current Apple Wi-Fi Hardware (August 2009)**

<b>Name</b>	<b>Features</b>	<b>Price</b>
AirPort Extreme Base Station (Mar. 2009)	<ul style="list-style-type: none"><li>• Four gigabit Ethernet ports (three LAN, one WAN).</li><li>• USB disk and printer sharing (any number of each).</li><li>• Simultaneous dual-band networking using two radios.</li><li>• Guest networking option.</li><li>• 802.11n.</li><li>• AU shows "AirPort Extreme (Simultaneous Dual-Band)."</li><li>• Device bottom: two AirPort IDs listed, model A1301.</li></ul>	\$179
Time Capsule (June 2009)	<ul style="list-style-type: none"><li>• All AirPort Extreme features.</li><li>• Built-in 1 TB or 2 TB hard drive for network-attached storage or Time Machine networked backup.</li><li>• AU shows "Time Capsule (Simultaneous Dual-Band)."</li><li>• Device bottom: two AirPort IDs listed, model A1302.</li></ul>	\$299 (1 TB), \$499 (2 TB)
AirPort Express Base Station (Mar. 2008)	<ul style="list-style-type: none"><li>• One 10/100 Mbps Ethernet port (LAN or WAN).</li><li>• Audio streaming.</li><li>• USB printer sharing (one printer).</li><li>• 802.11n.</li><li>• AU shows "AirPort Express with 802.11n."</li><li>• Device back: model A1264.</li></ul>	\$99; \$39 for audio/power extension kit

AU: AirPort Utility description; see [Field Guide to Base Stations](#), previous page, for details.

**Table 3: Discontinued AirPort Base Station Models**

<b>Name</b>	<b>Basic Hardware</b>	<b>Distinguishing Features</b>
AirPort (graphite) (1999)	The original, spaceship-shaped AirPort had a single Ethernet jack and supported 802.11b.	<ul style="list-style-type: none"> <li>• Spaceship shape.</li> <li>• Can hang off existing network, much like later AirPort Express.</li> <li>• Modem jack.</li> </ul>
AirPort (snow) (2001)	Same shape, new white color, has two Ethernet ports.	<ul style="list-style-type: none"> <li>• Can dial up AOL for downloads.</li> <li>• Supports Ethernet-connected computers.</li> </ul>
AirPort Extreme (2003)	Still a spaceship shape, but with 802.11g; has a USB jack for printer sharing.	<ul style="list-style-type: none"> <li>• Optional antenna jack for extending network.</li> <li>• Added WDS for wireless network extension.</li> <li>• Some models had 56K modem.</li> <li>• AU shows "AirPort Extreme."</li> <li>• Models A1075, A1034.</li> </ul>
AirPort Express (2004)	A compact, portable base station with 802.11g, audio streaming, and printer sharing.	<ul style="list-style-type: none"> <li>• Single Ethernet jack allows network extension only.</li> <li>• AU shows "AirPort Express."</li> <li>• Models: A1084, A1088.</li> </ul>
AirPort Extreme (Jan. 2007)	This first 802.11n model had just 10/100 Mbps Ethernet, but added hard disk sharing, and multiple disk/printer sharing.	<ul style="list-style-type: none"> <li>• USB support for shared multiple printers and drives.</li> <li>• Ethernet switch for three 10/100 Mbps devices.</li> <li>• AU shows "AirPort Extreme with 802.11n (Fast Ethernet)."</li> <li>• Model: A1143.</li> </ul>
AirPort Extreme (Aug. 2007)	This second 802.11n model added gigabit Ethernet.	<ul style="list-style-type: none"> <li>• Gigabit Ethernet on all four ports.</li> <li>• AU shows "AirPort Extreme with 802.11n (Gigabit Ethernet)."</li> <li>• Model: Unknown.</li> </ul>
Time Capsule (2008)	The first hard drive/backup combination base station.	<ul style="list-style-type: none"> <li>• Internal hard drive.</li> <li>• Supports Time Machine backups.</li> <li>• AU shows "Time Capsule."</li> <li>• Model: Unknown.</li> </ul>

AU: AirPort Utility description; see [Field Guide to Base Stations](#), two pages earlier.

Let's take a quick tour through Apple's three 802.11n base stations.

## **AirPort Extreme Base Station**

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

In August 2007, Apple replaced the 10/100 Mbps AirPort Extreme model with a same-named unit that was upgraded to gigabit Ethernet and that improved nearly all performance measures over the early 2007 model. Then in March 2009, Apple did another overhaul, adding a second radio that allows two simultaneous networks be broadcast, one in each Wi-Fi spectrum band. That 2009 model of the AirPort Extreme is the only one currently on the market.

---

***Hardware, not software:** Before you ask, the earlier Extreme Ns can't be upgraded to support gigabit Ethernet, and single-radio base station models can't sprout a second radio to offer simultaneous dual-band networks. Okay, these are reasonable questions, 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; to add simultaneous dual-band networking, the company added a second radio to the Extreme N and Time Capsule.*

---

Here's a look at the 802.11n AirPort Extreme's features:

- **Simultaneous dual-band networking:** With two internal radios, the 2009 model of the Extreme N can operate a 2.4 GHz and a 5 GHz network simultaneously and independently, allowing the fastest devices to connect to the best network.
- **Guest networking:** The 2009 model of the Extreme N includes the Guest Network feature, which lets you turn on a separately named *virtual* network that shares the same networking hardware, but appears as a unique name in the AirPort menu. You can set separate security options, too. Guests who connect have no access to local network traffic or peripherals, like printers or file sharing.
- **Ethernet:** The Extreme N base station has four Ethernet ports, three of which are for the LAN, leaving one for the WAN. The N

standard can outstrip 100 Mbps Ethernet, which is the reason Apple upgraded the Extreme to gigabit Ethernet in August 2007.

---

***Fastest method:*** *If you 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.*

---

**Note:** All four ports on an Extreme N (or Time Capsule) can be used as switched LAN ports if the base station is set to bridging mode. In this mode, the Extreme N just passes through traffic from the network to which it's connected. See [Passthrough and Bridging](#) for more details.

- **USB:** All Extreme N models have a single USB port, which can be used to share a printer or hard drive across a network or the Internet; by attaching a powered USB hub, you can attach one or more printers or hard drives.
- **Physical size:** The Extreme N (**Figure 2**) 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 2:** 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.

- **Power:** AC power is supplied through a nearly 17-foot/5.2 m-long cable that's split into a 10 foot/3 m connection to the modest DC power brick, which itself has a 6.5 foot/2 m cord.

## Time Capsule

The Time Capsule (**Figure 3**) is a backup appliance that has all the functionality found in an Extreme N. Apple refreshed it in March 2009 to add simultaneous dual-band networking, just like the Extreme N. (The 2009 model is the only one available.)



**Figure 3:** The Time Capsule combines an internal hard drive for backup with all the features found in an Extreme N base station.

Apple designed the Time Capsule to pair with Mac OS X's Time Machine feature for network backup. Any computer with Leopard or later installed can back files up over Wi-Fi or Ethernet to a Time Machine's internal drive or an externally connected drive.

The Time Capsule is identical to the Extreme N in all its technical characteristics and external ports except the Time Capsule has an internal hard drive—with a capacity of either 500 GB (gigabytes) or 1 TB (terabyte), and it is slightly larger in order to accommodate the drive (in June 2009, Apple discontinued the 500 GB model and added a 2 TB option). Also, Apple did a little engineering to put the power supply entirely inside the Time Capsule: a 6.5 ft/2 m external AC power cord connects the Time Capsule to a power socket.

---

***Extra options for internal drive:*** Two options for erasing and archiving the internal drive in a Time Capsule are available in *AirPort Utility*.

---

The Time Capsule measures 7.7 inches/19.7 cm square and 1.4 inches/3.6 cm tall; this is the same footprint as the Apple TV, and a smidge taller than the Extreme N.

## AirPort Express

In 2008, Apple refreshed the 2004 AirPort Express by upgrading it to 802.11n. The faster unit remains the same price, while offering a choice of either the 2.4 GHz or the 5 GHz band; it can network over a single band at a time. It measures 3.7 inches/9.4cm by 3 inches/7.5 cm by 1.1 inches/2.9 cm (**Figure 4**).



**Figure 4:** The Express N streams audio, shares a USB printer, and connects to a LAN network via Ethernet or Wi-Fi.

For clarity's sake, I call the revised unit *Express N*.

The Express N has a single 10/100 Mbps Ethernet port, which is a bit of a shame, because that puts a top end on the speed of N traffic that can pass between it and Ethernet. The Express N also has a USB port for sharing a single printer, but it can't share multiple printers or a hard drive.

The Express N has a unique feature unique that makes it a must-have network add-on for some people: audio output. The unit has a special mini-stereo port that allows both analog output and digital optical (Toslink) output, depending on the jack and cord you use to route audio from the Express to a stereo. (See [AirPort Express and AirTunes](#).)

Due to its integral power plug, the Express N can just hang from a power outlet. A \$39 audio kit for the Express N has a special extension cord that can be used in place of the integral plug; that cord can't be purchased separately from the audio kit. However, for a few dollars, you could buy a simple extension cord instead.

Common ways to use an Express N include:

- To connect an Express N to a LAN network, creating a Wi-Fi extension of that network
- To connect to a WAN network, if you only want to share the network over Wi-Fi

- To connect to an existing Wi-Fi network, via Wireless Distribution System (see [Bridge Wirelessly](#)) for an Apple network, or one of two other methods explained in depth later.
- To stream music from a computer to stereo speakers located elsewhere.

---

## 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.)

All current Apple computers that include Wi-Fi have 802.11n built in. The Xserve lacks an option, and the Mac Pro—which is meant for performance networking—offers Wi-Fi and Bluetooth as a \$50 built-to-order extra.

See **Table 4**, next page, for the full rundown by Mac model over AirPort's history.

### Is 802.11n Enabled on Your Mac?

If you own a Mac model that was released in 2006, and you never ran the 802.11n enabler software that Apple includes with its Wi-Fi gear and sells on the Apple Store, check that you have 802.11n turned on. From [/Applications/Utilities](#), launch Network Utility, click the Info button, and choose the network interface item labeled Airport (enx), where x is an internal number describing for that adapter. In the Model text you should see "(802.11 a/b/g/n)". If the "n" is missing, obtain and run the updater. (In Leopard, choose an item from the network interface pop-up menu that causes "Wireless Network Adapter" to appear in the Model listing.)

If you use a simultaneous dual-band base station to offer two Wi-Fi networks each with same name, then an Apple adapter in a Mac running Leopard or later automatically chooses the fastest and best con-

nection. This ensures that without any extra effort on your part the connection will always be the best one for the circumstances.

<b>Table 4: Wi-Fi Flavor by Model</b>	
<b>Model(s)</b>	<b>Fastest Supported Wi-Fi Type</b>
iBook G3, iMac (2000–2003), G4 Cube, Power Mac G4 (1999–2002), PowerBook G3 (2000–2002), PowerBook G4 (2001–2002), eMac (2002)	802.11b
iBook G4, iMac (2003–2006), eMac (2003–2004), Mac mini (Core Solo/Duo, 2006–2007), PowerBook G4 (2003–2005), Power Mac G5 (all)	802.11g
MacBook and MacBook Pro (Core Duo, 2006), 1.83 GHz 17-inch iMac (Core 2 Duo, 2006), Mac Pro (2006)	802.11a/g
iPhone, iPod touch (2007–2008)	802.11g
MacBook and MacBook Pro (Core 2 Duo, 2006–), Mac Pro (2008–), and Mac mini (2009–), iMac (Core 2 Duo, 2006–, except 1.83 GHz 17-inch)	802.11n

### **Third-Party Adapters**

At one time, Apple made Wi-Fi an installable option on many Macs. The company gradually transitioned from including AirPort Extreme on higher-end laptop and desktop computers to building it in to all systems. (The Xserve and the Mac Pro are exceptions.) All Macs with Intel chips have built-in Wi-Fi, and Apple stopped selling the AirPort Extreme Card for PowerPC systems in late 2008.

Anyone with a Mac released before the third quarter of 2006 who would like to participate in the 802.11n speed and distance revolution, has to go third party, installing gear from a company other than Apple to get N mojo. See **Table 5**, next page, for which adapters work with which Macs, and keep reading for details on some adapters.



**Tip:** If you have an old Mac that only “talks” 802.11b, you could spend less and move up to 802.11g with one of several USB cards, including Newer Technology and Asus models (\$25 to \$30).

**Tip:** Most of the 802.11n upgrade gear works only in the 2.4 GHz band, limiting the maximum speed 802.11n can achieve, but also keeping the price low. Even without getting the highest speeds—which requires an all-5 GHz network—you can still improve range.

**Table 5: Matching the Adapter to the Mac**

Type	Models	Mac OS X	Compatible Macs
PC Card	<ul style="list-style-type: none"> <li>• MaxPower (Newer)</li> <li>• nMax (Edimax)</li> <li>• nQuicky (QuickerTek)</li> </ul>	10.3.9+	PowerPC: PowerBook models dating back to as early as 1999
PCI Card	<ul style="list-style-type: none"> <li>• MaxPower (Newer)</li> <li>• nMax (Edimax)</li> <li>• nQuicky (QuickerTek)</li> </ul>	10.3.9+	PowerPC: Any PowerMac G3, G4, or G5 with PCI slots
USB 2.0 stick	<ul style="list-style-type: none"> <li>• MaxPower (Newer)</li> <li>• Dually (QuickerTek)</li> <li>• nQuicky (QuickerTek)</li> <li>• nNano (QuickerTek)</li> <li>• nMax (Edimax)</li> </ul>	10.3.9+	PowerPC or Intel: Any Mac with USB dating back to about 1999*
ExpressCard	<ul style="list-style-type: none"> <li>• nMax (QuickerTek)</li> </ul>	10.4+	Intel: MacBook Pro
Mini-PCIe	<ul style="list-style-type: none"> <li>• aCard (QuickerTek)</li> <li>• Aria (Sonnet)</li> </ul>	10.4+	All Intel Macs without N (requires extensive skills or pro installation)

\* Apple upgraded Macs to include the 480 Mbps USB 2.0 in 2003 and 2004. Older Macs had USB 1.1, which maxes out at 14 Mbps. You won’t get a speed advantage from 802.11n USB adapter on a USB 1.1 Mac, but you can get range improvements; usually, a cheaper 802.11g USB adapter makes more sense.

## Sonnet Technologies

Sonnet offers the Aria Extreme N, a \$129.95 circuit board for Intel-based Macs that shipped without 802.11n support or for the pre-2009 Mac mini. The upgrade comes with several tools for what could be an involved process of disassembling the computer, inserting the card, and putting it back together properly.

<http://www.sonnettech.com/product/ariaextremen.html>

The adapter supports both 2.4 GHz and 5 GHz networks, and it requires no special software. It works with either Mac OS X 10.4.9 or later (Tiger), or any later version of Mac OS X. It's compatible with Windows XP Service Pack 2 and Vista on laptops that have a mini-PCIe slot.

## Newer Technology

Newer's line-up of 2.4 GHz-only 802.11n adapters includes the MaxPower PC Card, MaxPower USB 2.0 stick, and MaxPower PCI adapter. Each has a suggested retail price of \$49.99, and works with Mac OS X 10.3.9 or later, as well as Windows 2000, XP, and Vista.

<http://www.newertech.com/products/wireless.php>

The unique details of their Newer's models include a stand to hold the USB adapter for better positioning if you don't want to simply stick it in a computer and a three-antenna external base for the PCI adapter.

## QuickerTek

QuickerTek has released several adapters in the nQuicky series and under other names (<http://www.quickertek.com/>). Only their aCard line for Intel Macs without 802.11n supports 5 GHz; all their adapters handle 2.4 GHz networking.

The company has a range of USB adapters that vary by antenna performance and signal strength:

- **The low-end nNano:** At \$89.95, the nNano was priced reasonably at its introduction, but it now has no advantages over products costing as much as \$40 less from other makers. (The nNano was \$30 less at its introduction.)
- **nQuicky:** The \$149.95 nQuicky has a much stronger radio (100 milliwatts) and two external antennas

- **Dualy:** The Dualy produces 500 mW of signal strength, which could let the adapter reach networks some distance away, but it costs a staggering \$325.95.
- **PC and PCI card adapters:** QuickerTek also offers PC Card and PCI card adapters (\$89.95 and \$99.95), also seemingly overpriced.
- **ExpressCard:** This \$149.95 adapter is for early MacBook Pro models without 802.11n included.
- **Update for Intel Macs issued without 802.11n hardware:** QuickerTek offers hardware updates that require opening a case and messing about. Prices range from \$89.95 for a MacBook or MacBook Pro self-install up to \$229.95 for a Mac mini upgrade by the company.

### **Edimax via Other World Computing**

Other World Computing, a reseller, offers 802.11n gear from a variety of makers, but appears to be the only firm selling the Edimax line-up with Mac OS X drivers. The nMax line sold by Other World includes a USB stick (\$48.99), PCI Card (\$49.99), and PC Card (\$49.99).

<http://eshop.macsales.com/shop/wireless/>

# Plug In Your Base Station and Get Started

Let's get unpacking! This section focuses on getting your base station plugged in and on launching AirPort Utility, the program that modifies a base station's settings.

(The next section, [Set Up a Network](#), helps you determine which network type you want to use your base station with, and provides the specific instructions for streamlined setup. Also, [Connect Your Computers](#), later, explains how to connect via Wi-Fi from any computer in the vicinity to the newly set up base station.)

---

## UNPACK AND POWER UP

---

Unpack the base station to determine what you have and if you need any additional hardware:

### 1. Remove the base station from its box and check the parts:

- **Extreme N and Time Capsule:** The Extreme N box and the Time Capsule box includes just a few necessary parts: the square base station, a CD that you shouldn't need, and an AC power cord, and, in the Extreme N box, a power adapter. These base stations don't include a wall-mounting bracket; they're designed to work horizontally.
- **Express N:** The Express N includes just itself with its integral AC plug snapped away for storage and the CD noted above.

### 2. Is the power cord long enough?

- **Extreme N:** The power cord's length—17 feet/5.2 m—should aid in placement; in the U.S. 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.

- **Time Capsule:** Plan to buy an extension cord if the included 6.5 ft/2 m cord is too short for your purposes.
- **Express N:** If you need to locate the Express N where you can't directly hang it from a power outlet, you can buy the AirPort Express Stereo Connection Kit, which includes analog and optical digital audio cables, and an extension cord that replaces the fold-up plug adapter that comes with the Express. The \$39 cost is a bit annoying if you don't want the audio cables, which can be purchased for less at the same quality elsewhere. For a few dollars, you could buy a simple extension cord instead.

The Extreme N and Time Capsule work 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](#) before you continue.)

3. **Get an Ethernet cable:** Apple stopped including Ethernet cables with Wi-Fi gear in 2007. But configuring an AirPort Extreme or Time Capsule may be simpler if you hook it to your computer or existing LAN with an Ethernet cable. AirPort Express is best configured via Wi-Fi, because its sole Ethernet port is used to connect to a wide area network.

In the likely case that you plan to connect the base station to a broadband router or other network, you also need at least one Ethernet cable. All Apple Wi-Fi devices have auto-sensing, auto-switching Ethernet, so regardless of the particulars of your cable, the base station will make it work. I recommend Cyberguys.com as a good online source for cables (<http://www.cyberguys.com/>).

---

**Warning!** *Make sure you're using a newer Ethernet cable that's rated appropriately for your network:*

- *100 Mbps Ethernet: Use Category 5 (Cat5) or Category 5E (Cat5E).*
  - *Gigabit Ethernet: Use Category 5E (Cat5E).*
  - *Long Ethernet runs: Use Category 6 (Cat6).*
- 

**Note:** *TidBITS* publisher Adam Engst hit some problems when he used older Ethernet cables in his network. See "Switch Your Network to Gigabit Ethernet," <http://db.tidbits.com/article/9518>.

---

**Configuration computer:** You'll be using *AirPort Utility* to set up your base station, and the steps I give shortly show screenshots taken on a Macintosh running Mac OS X 10.5 Leopard (the screenshots would be the same had I used 10.6 Snow Leopard). *AirPort Utility* can also be installed under Tiger or 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 on the Time Capsule or Extreme N; connect via Wi-Fi for an Express. If you'd rather have mobility while configuring, you can also set up an Extreme N or Time Capsule via Wi-Fi, but you must reconnect after each configuration change if you change password or naming options.

---

**Flashy:** In a neat addition, all the Ethernet ports on an Extreme N and a Time Capsule have a tiny green LED that lights up when an Ethernet cable is connected to the port and a live connection is on the other end of the cable; the LED flashes to indicate activity. Also, a green/amber/blue LED on the front of the base station shows the status of the base station. Consult [Light Reading](#), earlier, for more information about the front LED.

---

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.

---

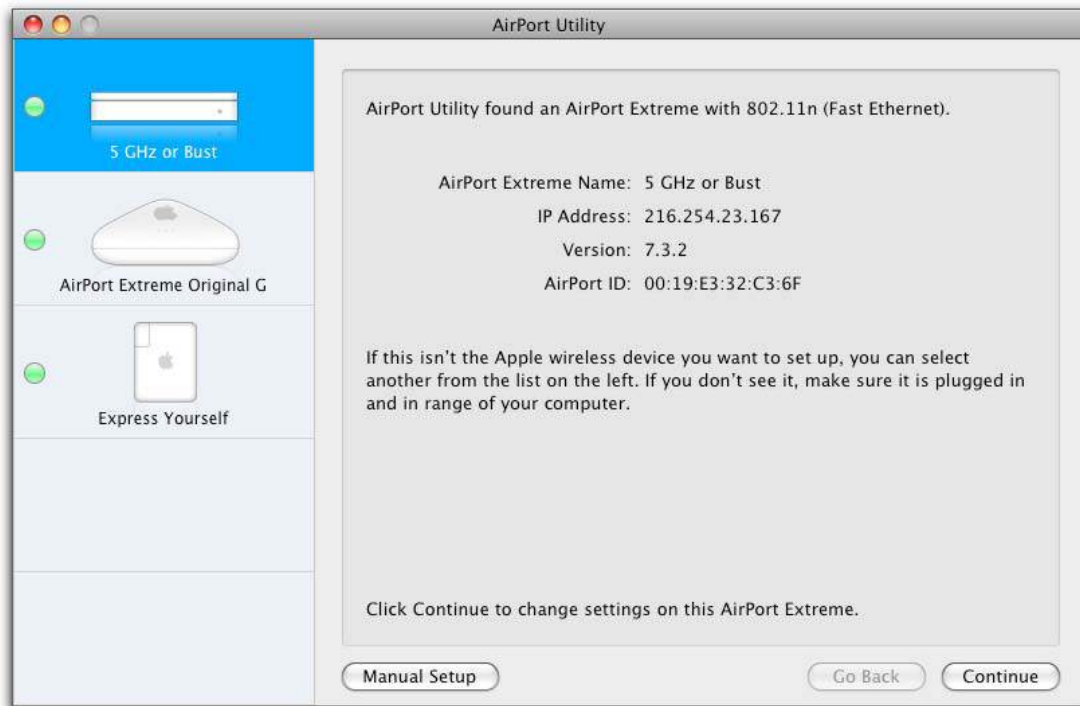
## KNOW YOUR AIRPORT SOFTWARE

---

If you just want to get going with your installation, skip ahead two pages to [Launch AirPort Utility and Keep Up to Date](#). Alternately, keep reading to learn background information and special details.

The AirPort software included with Leopard and Snow Leopard has two components:

- **AirPort Utility:** In 2007, AirPort Utility replaced the hoary AirPort Admin Utility, which dates back to 1999; the new AirPort Utility combines a set of assistants with advanced configuration options (**Figure 5**).



**Figure 5:** The main screen of AirPort Utility.

AirPort Utility can configure any of Apple's Wi-Fi hardware dating back to 2003; you must use it to configure devices released starting in 2007. AirPort Utility is included in Leopard and Snow Leopard, and you can download it for Tiger as well for Windows XP and Vista.

- **AirPort Base Station Agent:** This monitoring program, installed under Tiger and Leopard, can alert you to a problem with any modern base station on the local network. In Snow Leopard, it's a system-level component that you don't need to manage separately.

---

***Tiger and Windows:*** When you install AirPort software on Tiger or Windows, both components listed above are installed. However, the Tiger and Windows packages for AirPort Utility include a third component:

- *In Tiger, it's a separate application called AirPort Disk Utility.*
- *Under Windows, it's a system control panel called AirPort Disks.*

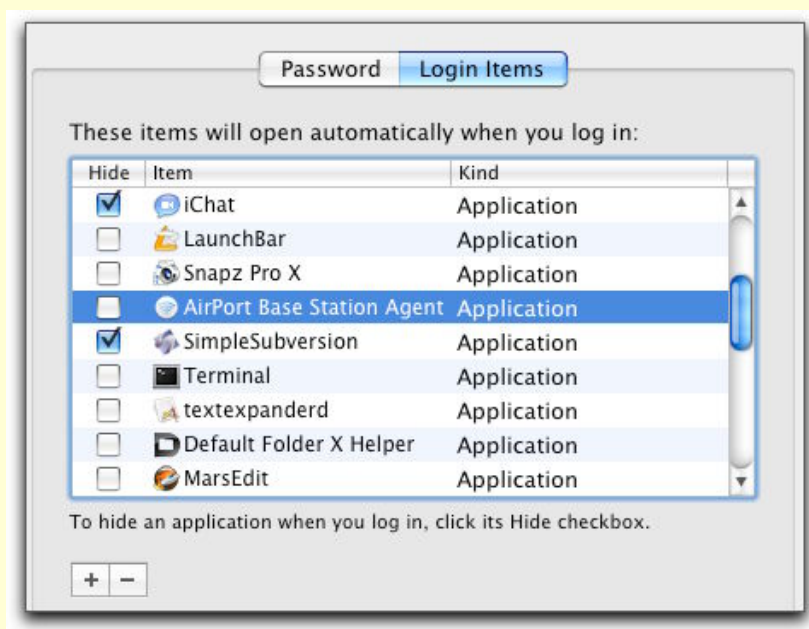
*In both cases, the software is designed to make it easier to control the mounting behavior of drives attached to or inside an Extreme N or Time Capsule. It's not needed in Leopard or Snow Leopard.*

---

## Disabling AirPort Base Station Agent

In Tiger and (as far as I can tell) in Leopard, Apple installs the AirPort Base Station Agent as a program that launches when you log in. In Snow Leopard, Mac OS X treats the agent just like a lot of other invisible background monitors.

To disable the agent in Snow Leopard, simply turn off Monitor Apple Wireless Devices for Problems (**Figure 7**, next page). In Tiger and Leopard, you may also need to go to the Accounts system preference pane, select your account, click the Lock icon and enter the password, and view Login Items (**Figure 6**). Select AirPort Base Station Agent and click the  button.



**Figure 6:** The agent hides in your account's login items.

---

## LAUNCH AIRPORT UTILITY AND KEEP UP TO DATE

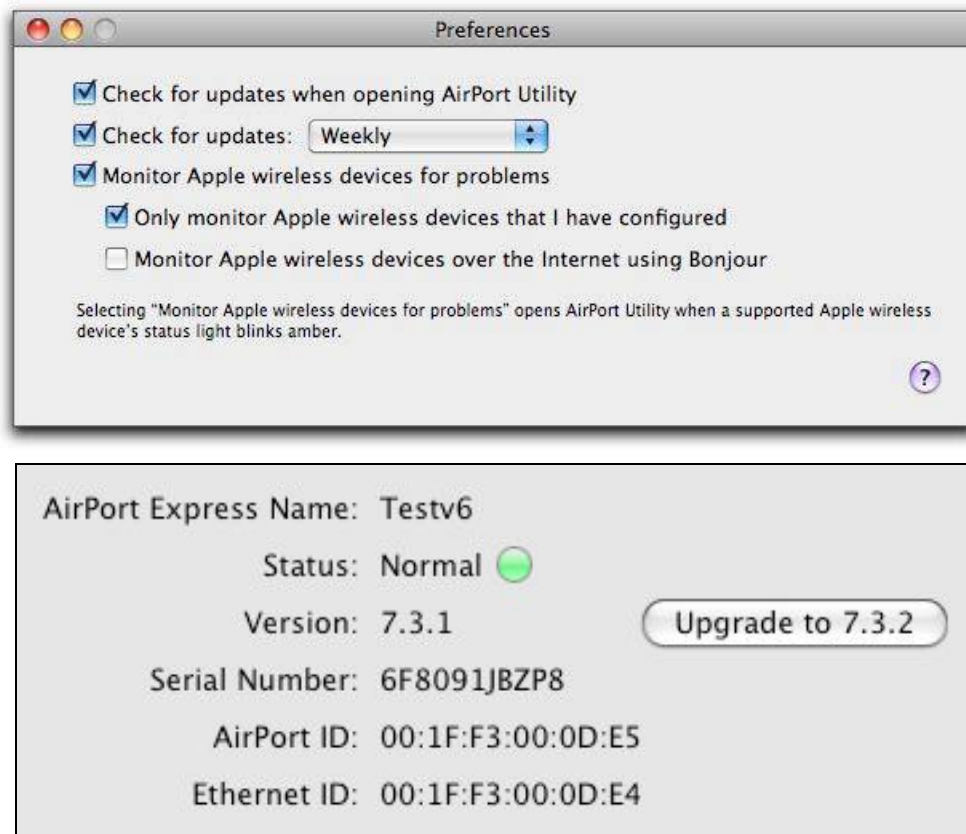
---

Now let's launch AirPort Utility (from [/Applications/Utilities](#)) and check its update settings. The first time you run AirPort Utility, it asks you if it should check for updates automatically. Although Mac OS X's Software Update feature (Apple > Software Update) will also alert you to 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.

AirPort Utility's update notification works whether or not you have AirPort Utility launched. The AirPort Base Station Agent monitors at the interval you specify for updates, and then launches AirPort Utility if an update is available. You can adjust the how often updates are checked in AirPort Utility's Preferences window (**Figure 7**).



**Figure 7:** The Preferences window lets you choose to check for updates regularly—or not (top). The Summary view for a base station alerts you when an upgrade is available (bottom).

**Tip:** A base station can also track updates for itself, which is an interesting option. See [Base Station Settings](#), in Appendix B, for how to control that setting.

If your copy of AirPort Utility isn't up to date, you should update it before proceeding.

---

## DECIDE ON YOUR NEXT STEP

---

Most people installing a base station have a broadband connection that they want to share via Wi-Fi. If that's the case for you, check if you meet these three tests:

- You're installing an Apple base station connected to your broadband modem for the first time, not replacing an existing Apple base station in that position.
- 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 via the broadband connection among devices that connect either to an Extreme N or Time Capsule with Wi-Fi or Ethernet, or to an Express N with Wi-Fi.

### **If all three bullet items describe you:**

If that's you, then plug an Ethernet cable from the Local Area Network (LAN) port of your broadband modem (labeled *LAN* or sometimes *Network*) into the Wide Area Network (WAN) port of the Extreme N or Time Capsule, or into the single Ethernet port of an Express N.

---

***Warning!*** *An Express N can't offer addresses over its Ethernet port when that Ethernet port is connected to your broadband modem. You need a base station with both a WAN port and a LAN Ethernet port.*

---

This simplified setup relies on the factory settings that Apple provides for base stations when they first power up. If this simplified setup appears to be working, and you have no reason to think that it shouldn't do the job, proceed by following the directions *in the pages immediately ahead* and continuing to the start of "Set Up a Network." Then, work through the appropriate material in that section.

### **If the above setup describes you, but doesn't work:**

If this simplified setup doesn't turn out to work, continue by following the directions *in the pages immediately following*, configure your base station in "Set Up a Network," and then proceed to "Advanced Networking."

### If any of the bullet items don't describe you:

- If they don't apply because you're replacing an existing base station, skip ahead to [Replace an Existing Base Station](#) (p. 68). Your steps are different from everyone else's because you need to leave your current base station set up until you've configured the new base station to take its place.
- Otherwise, proceed with the steps *immediately ahead*—you'll be connecting the Mac that's running AirPort Utility to the new base station, and then you'll be going through the first set up steps. After that, the steps branch for different types of configurations.

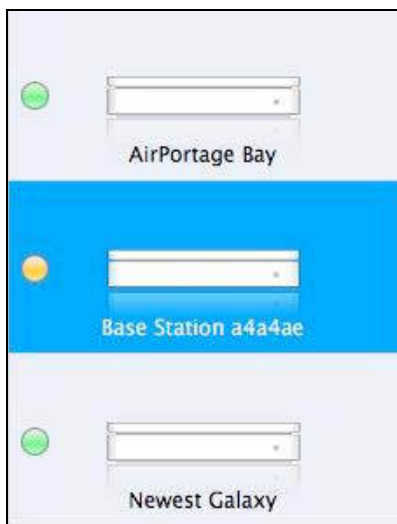
---

## CONNECT TO YOUR BASE STATION

---

AirPort Utility is your one-stop shop for setting up a base station. To begin, with AirPort Utility launched, use one of these methods to make a network connection to the base station; the methods are listed in order of simplicity:

- **Connect via LAN:** Use an Ethernet cable to connect the computer to one of the three LAN Ethernet ports on the Extreme N or Time Capsule, or the single Ethernet port on the Express N. Once connected, the base station should appear at the left of AirPort Utility (**Figure 8**). I don't recommend this method for an AirPort Express, because its Ethernet port is used to connect it to a larger network.



**Figure 8:** The selected (in blue) base station above isn't configured, so the last six digits of its AirPort ID appears in its name (see [Default Network Names](#), next page). (Dig the subtle reflection!)

- **Connect via a larger network:** For larger LANs, in which the base station is just a piece of the network, 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 see the unconfigured base station in AirPort Utility.
- **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. I recommend this method for an AirPort Express.

From the factory, all Apple base stations can be reached via a 2.4 GHz connection, so you can initially configure one via Wi-Fi from any computer; simultaneous dual-band models have networks active in both bands. An unconfigured base station shows with a default Wi-Fi network name in the AirPort menu (see "Default Network Names," below).

### Default Network Names

When you first power up any Apple base station, new or old, the gateway creates a Wi-Fi network named *Apple Network 0033FF* where *0033FF* is replaced with the last six digits of the AirPort ID of the base station's 2.4 GHz band wireless adapter. In AirPort Utility, the base station appears in the left list named *Base Station 0033FF* with the same substitution.

The *AirPort ID* is a unique address assigned by the manufacturer. Each Ethernet port and Wi-Fi radio has a unique address. The one (dual band, single radio) or two (simultaneous dual band) AirPort IDs along with the WAN port Ethernet ID are printed on the underside of an Extreme N or Time Capsule, and on the side with a power plug of an Express N.

The AirPort ID is a MAC (Media Access Control) address. See [What and Where Is a MAC Address?](#) (p. 97) for more information about MAC addresses.

---

## FIRST STEPS IN SETUP

---

Now that you've connected to the base station, the simplest way to configure the 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.

---

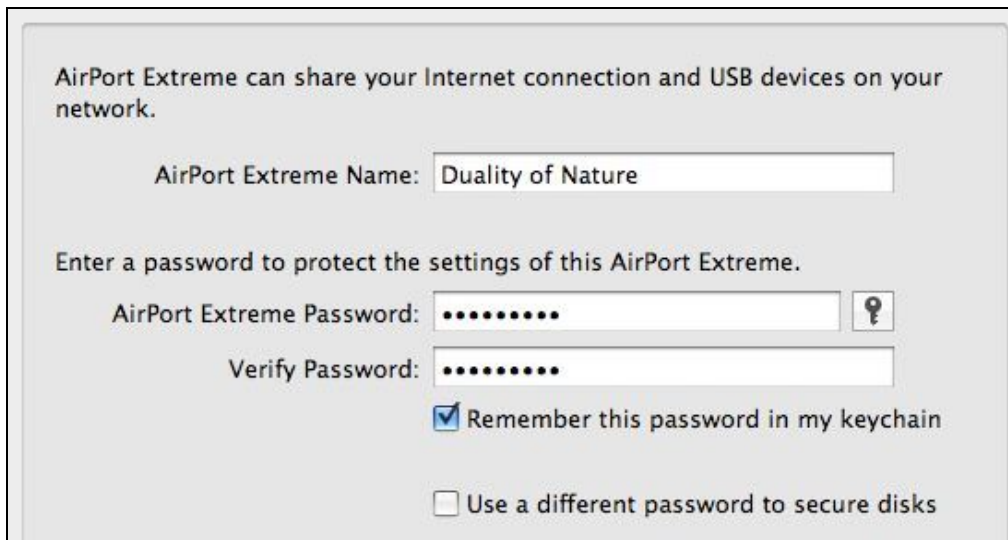
***Skip ahead for Manual Setup:*** You can skip the assistant and configure a base station using Manual Setup if you'd rather make all your choices at once. Manual Setup is described throughout the rest of the book.

---

**Tip:** These following steps are the same regardless of what kind of network you're building.

Follow these steps to start configuring your base station:


1. In AirPort Utility, select the base station from the list of base stations at the left and then click Continue.
2. The first screen, labeled with your base station's name, prompts you to name the base station and then choose a password to protect the base station's configuration (**Figure 9**).



AirPort Extreme can share your Internet connection and USB devices on your network.

AirPort Extreme Name:

Enter a password to protect the settings of this AirPort Extreme.

AirPort Extreme Password:  

Verify Password:

Remember this password in my keychain

Use a different password to secure disks

**Figure 9:** Enter a base station name and password, choose whether to store the password, and set a unique disk access 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.

**Tip:** Click the key icon to have AirPort Utility make up a password for you.

I recommend checking the Remember This Password in My Keychain option so that the Mac will store the password.

---

***Time Capsule, Extreme N:** If you check Use a Different Password to Secure Disks, the base station password won't automatically be used for the network access password for hard drives attached via USB or the internal drive in a Time Capsule.*

---

### **Jumbo Ethernet Frames Disable AirPort Utility Access**

If you can't proceed and your Mac is connected via Ethernet to the LAN side of the base station, you might have hit a rare bug that I found. If you've changed the minimum transmission unit (MTU) for your Ethernet adapter to anything but the standard 1,500-byte setting, you need to change it back; or, you can turn off IPv6 networking.

This is rather obscure; Jumbo frames are used to speed network data transfers on gigabit Ethernet networks, but for it to work properly, all devices must support Jumbo frames automatically. Apple's base stations apparently do not support them. In the Network system preference pane, select your Ethernet adapter, then click Advanced. In the TCP/IP view, choose Off from the Configure IPv6 pop-up menu; or, in the Ethernet view, choose "Standard (1500)" from the MTU pop-up menu. In either case, click OK, then click Apply.

3. Click Continue.

Now we can move into network planning, in order to figure out what settings are needed, starting in the next section.

## How to Return to the Factory Defaults

You can reset any Apple base station to its factory settings at any time through software or hardware. Resetting the base station 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.

To return to the factory defaults via software, launch AirPort Utility, select your base station, and choose Base Station > Manual Setup (Command-L). Now, choose Base Station > 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. (See [Reset a Locked-up Base Station](#), Step 3, to find the reset button.)

# Set Up a Network

How you configure your base station depends on the type of network you're building. In this section, I look at *scenarios*: pairing the kind of network that you want to which settings to make in the Assist Me mode of AirPort Utility.

Each scenario is followed by an explanation of how to use AirPort Utility for a basic configuration of that scenario. For a more advanced setup, each scenario links to later topics on extending a network wirelessly and changing security options, for instance.

---

## GET STARTED

---

### Placing a Base Station

If you haven't figured out where best to put your new base station(s), you may wish to skip ahead and read [Pick the Right Place](#) (p. 85). Note that you can configure a base station first, and then relocate it, using advice in that section to find the optimal placement.

The first question that needs to be asked is: What kind of network are you trying to build? This section answers that with scenarios that cover common situations. Pick a scenario and proceed as directed, noting that the links below lead to topics that begin with a diagram and explanation of the type of network and then give configuration steps.

Are you:

- Setting up a new network with a single base station connected to a broadband modem? See [New Network, Single Base Station](#) (p. 57).
- Extending an existing network via Ethernet, or via Wi-Fi? See the two corresponding sets of instructions: [Extend a Network via Ethernet](#) (p. 64) and [Extend a Network via Wi-Fi](#) (p. 71).
- Replacing an existing base station with a new unit or model and want exactly the same settings? See [Replace an Existing Base Station](#) (p. 68).



- Adding a base station to an existing network? Start with [Extend a Network via Ethernet](#) (p. 64), which will start you on the right path and then shunt you off to the next step. (This is also addressed more fully in [Mix 2.4 GHz and 5 GHz 802.11n Networks](#), p. 159.)

---

***Other scenarios:** If your scenario isn't in the list just previously, consult later sections in the book, which examine advanced options.*

---

**Tip:** The More Info button at the lower left of many configuration screens provides a nice summary of the reasons for choices that need to be made on each screen.

---

***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.*

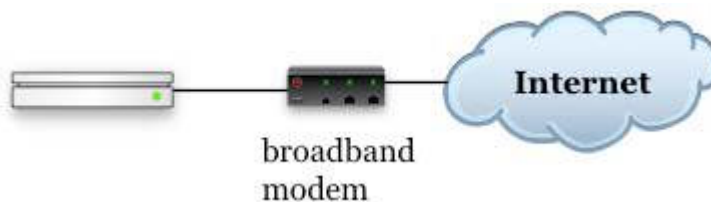
---

---

## **NEW NETWORK, SINGLE BASE STATION**

---

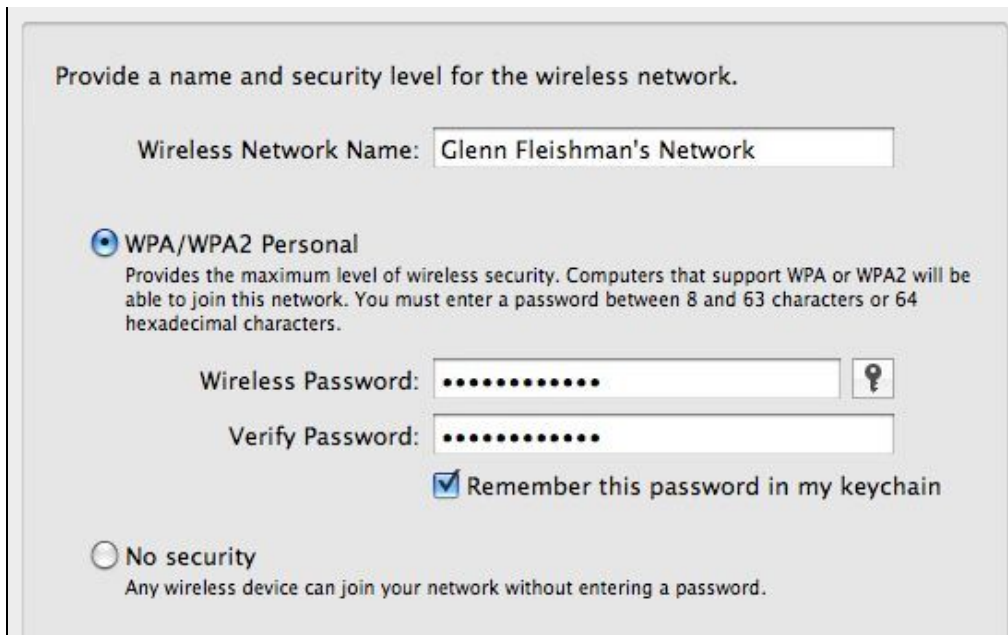
When you're starting from scratch, everything is a bit easier, because you get to make all your choices without regard for what's already on a network (**Figure 10**).



**Figure 10:** A simple network connects a base station via a broadband modem to the Internet.

Follow these steps to set up a new network:

1. Make sure your new base station is prepped as I described in [First Steps in Setup](#), a few pages earlier.
2. In AirPort Utility, on the first Network Setup screen, select the middle option, "I don't have a wireless network..." or "I want to create a new wireless network" (the text may vary depending on your current set of networks) and click Continue to reach the next Network Setup screen (**Figure 11**).



**Figure 11:** Set your network's name, and then enable security to prevent unwanted users.

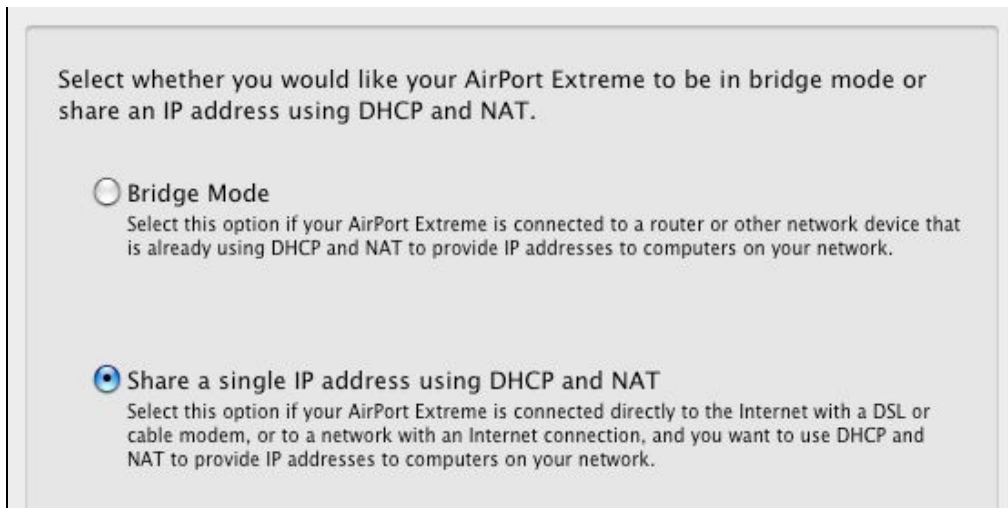
3. Enter a network name and select a security method:
  - **Network name:** The network name will be “advertised” to Wi-Fi adapters that scan for networks to connect to; for instance, on a Macintosh the network name will appear in the AirPort status menu in the menu bar. Multiple base stations may share the same network name to create a network with a larger area or more available bandwidth.
  - **Security method:**
    - ◇ WPA/WPA2 security allows Macs running Mac OS X 10.3 Panther or later and computers with Windows XP SP2 or later to connect.
    - ◇ No security allows all connections.

---

***Warning!*** Some older Macs and Windows systems may not be able to connect with WPA/WPA2 Personal. The [Use Built-In Encryption](#) section can help you check whether any of your computers fit that bill.

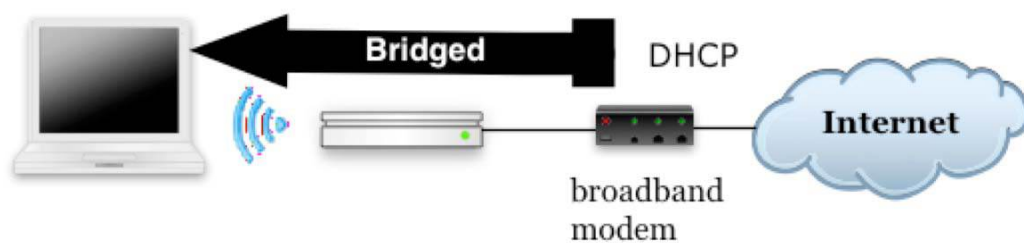
---

Click Continue to reach another Network Setup screen (**Figure 12**).



**Figure 12:** Select whether the base station passes through network addresses or assigns its own.

4. Select whether you want to use your computer in Bridge mode or share a single IP address using DHCP and NAT:
  - Select Bridge Mode if a computer or another base station on the network you’re connecting to hands out network addresses. For instance, select Bridge Mode if you have a broadband modem that has a DHCP server that assigns local addresses (**Figure 13**). The base station obtains its own address from the upstream DHCP server, too, except in highly unusual circumstances.



**Figure 13:** With Bridge mode, a device upstream of the base station—such as a broadband modem with a DHCP server built in—passes through an address to computers connected to the base station.

---

**Bridge mode limitations:** To offer a guest network or use Snow Leopard’s feature to wake on network access, your base station cannot be in Bridge mode.

---

- Select “Share a single IP address...” if your base station connects to a network or a broadband modem where it receives or you

assign a single IP address and then need to create addresses for computers that connect to the network.

Click Continue.

If you selected “Share a single IP address...”, AirPort Utility may prompt you with a warning, noting that the LED on your base station will flash unless you click Ignore; clicking Skip proceeds, but lets it flash.

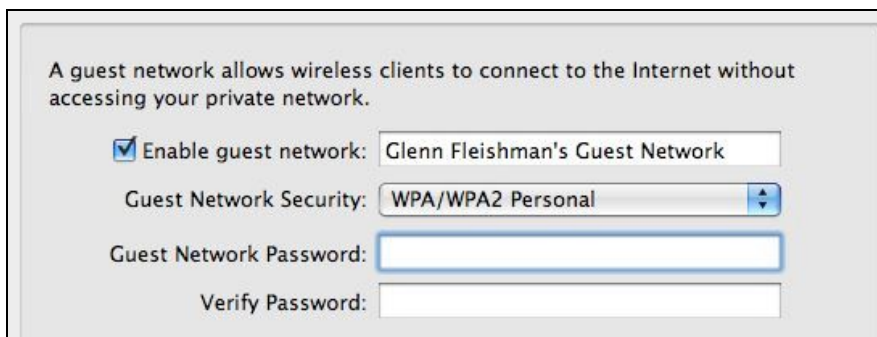
**Tip:** Apple omits an additional option here that’s available through Manual Setup that allows guests to see each other’s network traffic even though they can’t see the main network’s traffic. See [Set Up Guest Networking](#) (p. 222) for that tidbit.

**Tip:** For more details on how these two network types might be set up, see [Hand Out LAN Addresses](#) (p. 100).

5. Next (**Figure 14**), if you’re using a simultaneous dual-band base station and are sharing a single IP address, you’re prompted about setting up a guest network:

- You can set up a guest network with or without a password. A positive reason to not set a password is that all comers can easily gain access while you still protect your local network (set Guest Network Security to None). For more info, see [Set Up Guest Networking](#) (p. 222).
- Uncheck the Enable Guest Network box to bypass such a network.

Click Continue.

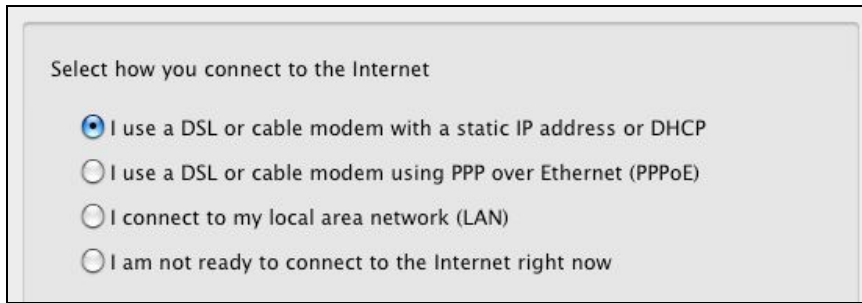


A screenshot of the 'Enable Guest Network' dialog box in AirPort Utility. The dialog has a light gray background and a title bar. At the top, it reads: 'A guest network allows wireless clients to connect to the Internet without accessing your private network.' Below this, there are four rows of controls:

- The first row has a checked checkbox labeled 'Enable guest network:' followed by a text field containing 'Glenn Fleishman's Guest Network'.
- The second row has a label 'Guest Network Security:' followed by a dropdown menu showing 'WPA/WPA2 Personal'.
- The third row has a label 'Guest Network Password:' followed by an empty text field.
- The fourth row has a label 'Verify Password:' followed by an empty text field.

**Figure 14:** Enable a guest network to allow visitors and colleagues Internet access without them joining your main network.

6. The first Internet Setup screen lets you choose how addresses are assigned on your network (**Figure 15**).

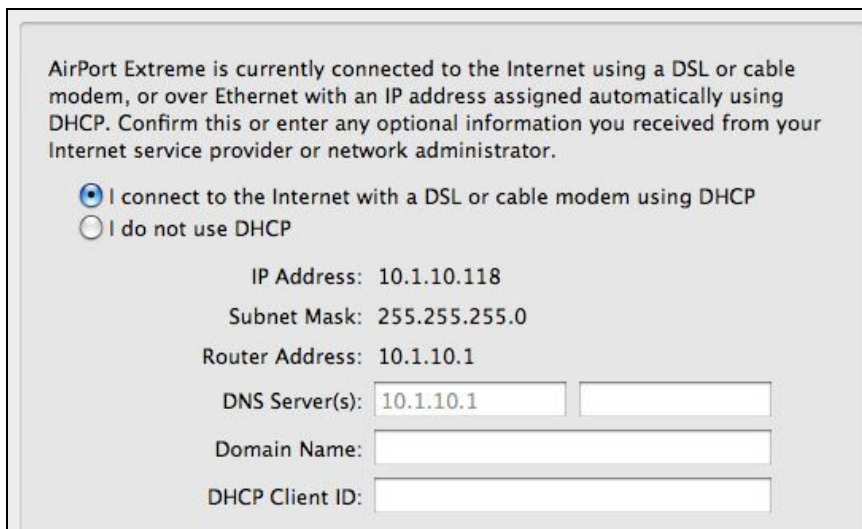


Select how you connect to the Internet

- I use a DSL or cable modem with a static IP address or DHCP
- I use a DSL or cable modem using PPP over Ethernet (PPPoE)
- I connect to my local area network (LAN)
- I am not ready to connect to the Internet right now

**Figure 15:** Select how your base station connects to the Internet.

***Different screen?** You might see the screen in **Figure 16** if your broadband modem is already plugged in and providing an address via DHCP. In this case, you can either proceed with the “I connect to the Internet with a DSL cable modem using DHCP” option that’s selected by default, or select “I Do Not Use DHCP,” and then click Continue to make a choice as shown in **Figure 15**.*



AirPort Extreme is currently connected to the Internet using a DSL or cable modem, or over Ethernet with an IP address assigned automatically using DHCP. Confirm this or enter any optional information you received from your Internet service provider or network administrator.

- I connect to the Internet with a DSL or cable modem using DHCP
- I do not use DHCP

IP Address: 10.1.10.118  
Subnet Mask: 255.255.255.0  
Router Address: 10.1.10.1  
DNS Server(s):    
Domain Name:   
DHCP Client ID:

***Figure 16:** You may see this screen if your broadband modem is connected and providing a DHCP address to the base station.*

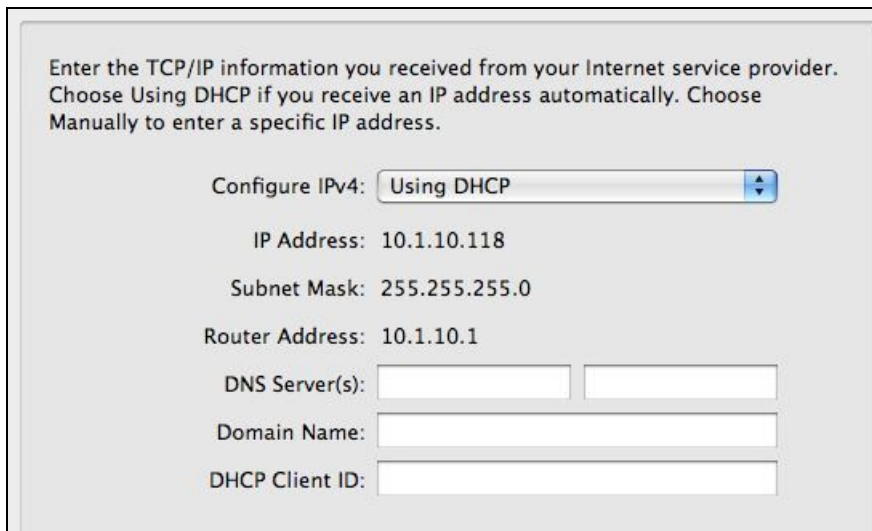
The four options in the first Internet Setup screen cover the major scenarios (which you then configure in the next step):

- **DSL or cable modem with a 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 using PPPoE:** This option works with ISPs that use a special login that the base station must handle. The login process lets an ISP server assign an address (static or dynamic) to your base station.
- **LAN:** For larger LANs, 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.

Confirm your selection, and then click Continue to reach the second Internet Setup screen (**Figure 17**).



The screenshot shows a window titled "Enter the TCP/IP information you received from your Internet service provider. Choose Using DHCP if you receive an IP address automatically. Choose Manually to enter a specific IP address." Below the title is a dropdown menu labeled "Configure IPv4:" with "Using DHCP" selected. Underneath are several fields: "IP Address: 10.1.10.118", "Subnet Mask: 255.255.255.0", "Router Address: 10.1.10.1", "DNS Server(s):" with two empty input boxes, "Domain Name:" with one empty input box, and "DHCP Client ID:" with one empty input box.

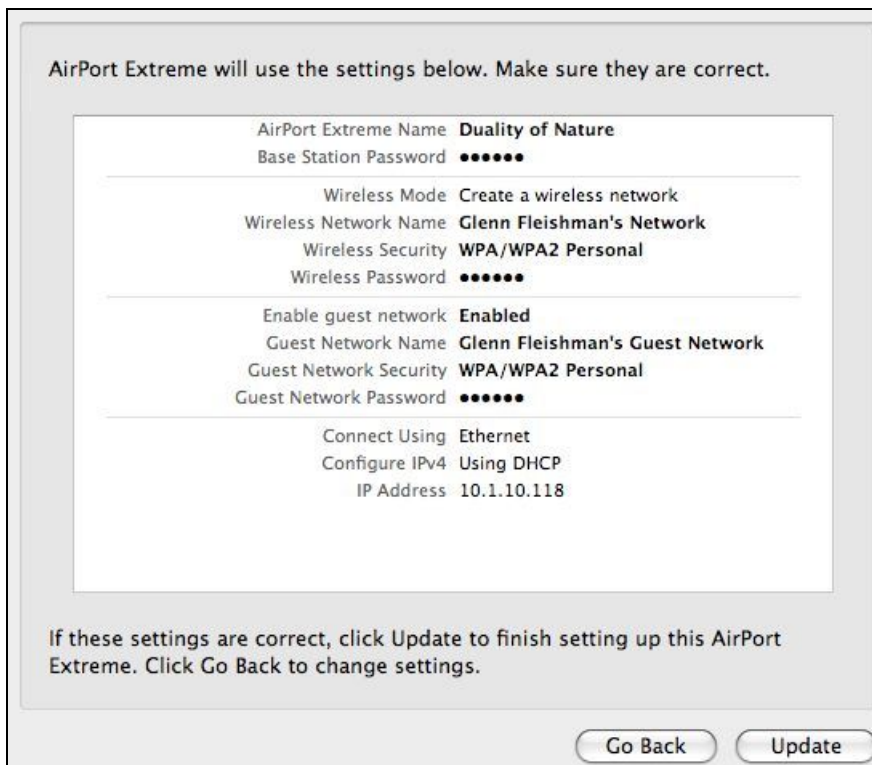
**Figure 17:** Choose to use a dynamic (DHCP) or static addressing.

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. Most people choose this option.

- ◊ 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).

Click Continue.

8. Review your choices in the Summary screen (**Figure 18**). You can click Go Back repeatedly to make changes, or click Update to store your settings and restart the base station with them.



**Figure 18:** The Summary screen shows the choices you've made.

**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.

Now that you've completed setting up your base station, you may want to add printers, configure special network settings, or add more base stations. To get a road map to other topics in this ebook, flip back to [Quick Start to AirPort Networking](#) (p. 10).

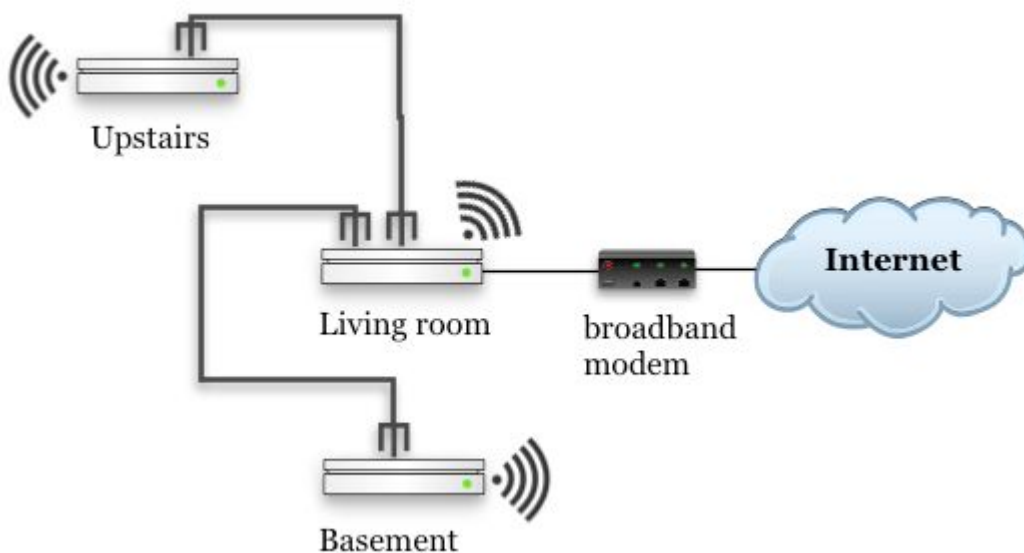
---

## EXTEND A NETWORK VIA ETHERNET

---

If you already have a network in your home or office, you may simply want to plug in another base station that extends its range. The easiest way to accomplish that is to use Ethernet to connect the first network with the second (**Figure 19**). One base station must be connected to the Internet, but the rest can connect via that base station for access. Every base station has a unique name, but the network name is the same for all of them.

This allows all base-station-to-base-station communication to happen over Ethernet, and any Wi-Fi user's adapter automatically picks up and switches to the strongest network signal it can spot among base stations you've set up with the same network name.



**Figure 19:** Ethernet lets you connect a number of base stations together to form one seamless network across a home or office.

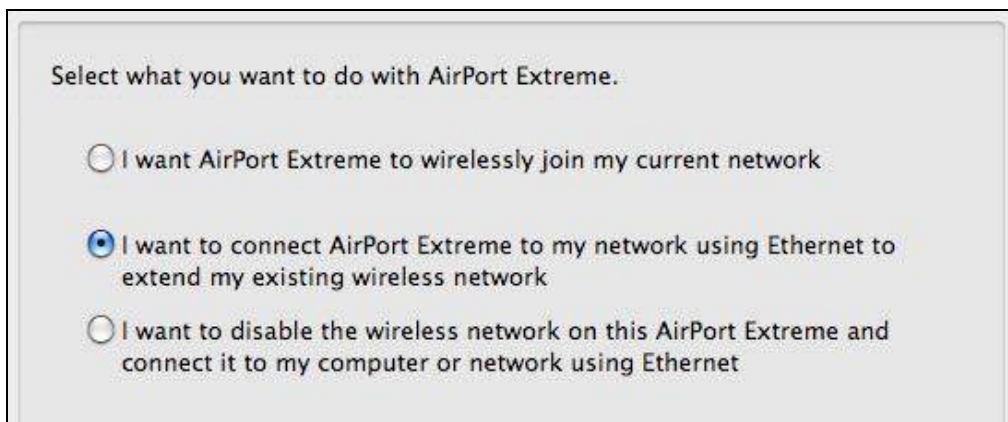
Because the Extreme N and Time Capsule both have four gigabit Ethernet jacks built in, you will likely plug a cable between the Wide Area Network (WAN) on the new base station you're adding to the network and any of the three Local Area Network (LAN) jacks on the main base station.



**Tip:** If the base station connected to your broadband modem is an older AirPort with a single LAN jack, you might swap in a 802.11n base station with multiple ports, or connect the single LAN port to an Ethernet switch to which you also connect additional base stations.

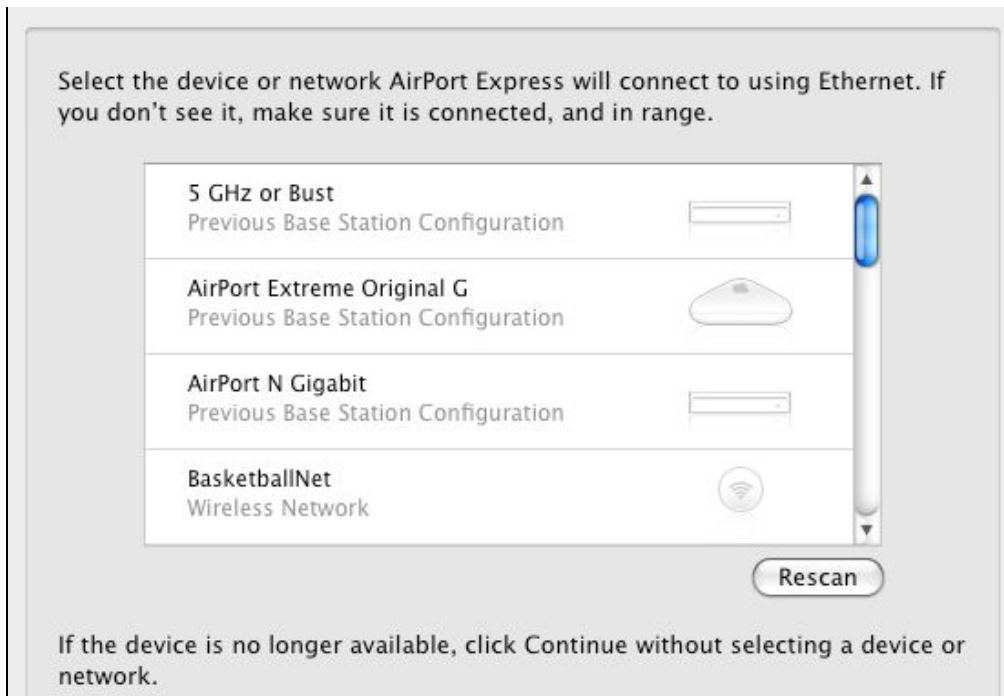
To proceed, follow these steps:

1. Make sure the new base station is prepared as described in [First Steps in Setup](#) (p. 53).
2. In AirPort Utility, on the first Network Setup screen, select the top option, "I want *AirPort model* to join my current network" (*AirPort model* will read "AirPort Extreme" or another model name depending on which base station model you're configuring.) Click Continue to reach the next Network Setup screen.
3. On the next Network Setup screen (**Figure 20**), select the second option, "I want to connect *AirPort model* to my network using Ethernet...", and then click Continue.



**Figure 20:** Choose the second option, extending via Ethernet.

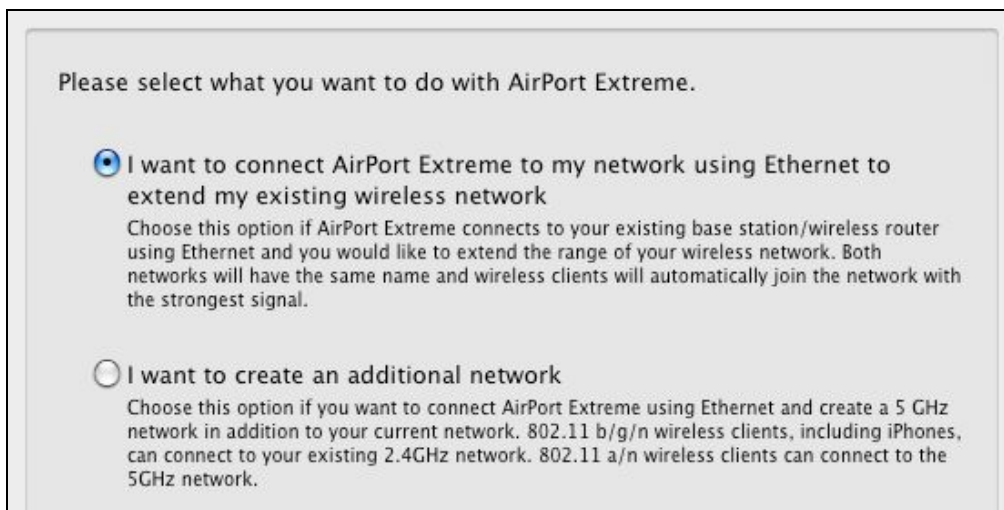
4. AirPort Utility offers another Network Setup screen that lets you select previously connected networks, stored configurations, or active networks (**Figure 21**). Choose an existing network from which to copy the configuration, and then click Continue. (You can also opt to click Continue, in order to proceed from scratch.)



**Figure 21:** You can choose a network or previous configuration from which to read setup details.

**Tip:** If you accidentally click a device in the list but meant to click Continue without a selection, hold down Command and click the selected item to remove the selection. Then click Continue.

5. On an 802.11n base station that can use just one band at a time—AirPort Express, 2007 or 2008 AirPort Extreme, or 2008 Time Capsule—you'll see the screen shown in **Figure 22**. If you're using a 2009 AirPort Extreme or Time Capsule, skip to Step 6.



**Figure 22:** Select the first option.

I discuss the radio buttons offered to one-band-at-a-time base stations on the Network setup screen in reverse order:

- You might set up a separate 5 GHz network to keep 802.11n computers and streaming video devices (like the Apple TV) apart from your existing network. Building a separate 5 GHz network ensures the fastest throughput for capable devices. (See [Mix 2.4 GHz and 5 GHz 802.11n Networks](#).) To set up the 5 GHz option, select the second radio button, “I want to create an additional network” and click Continue.
- Otherwise, select the first option, to extend an existing network, and then click Continue.

6. The next screen you see depends on what you chose in Step 4:

- If you chose to use an existing configuration that AirPort Utility has access to, either by using a stored password or other information, proceed to Step 7.
- If you chose a network that AirPort Utility doesn’t have stored details for, or you simply clicked Continue, then you need to enter the Network name and choose the network’s security (**Figure 23**). If you enter these details incorrectly, the network won’t allow seamless roaming among connected base stations.

This AirPort Extreme is set up with the following wireless settings, using WPA security settings.

Use this device's current settings

Change these settings

Provide a name and security level for the wireless network.

Wireless Network Name:

Wireless Security:

Wireless Password:

Verify Password:

Remember this password in my keychain

**Figure 23:** This screen lets you enter details from scratch or about a network that the AirPort Utility doesn’t have stored.

7. The summary screen appears. Confirm that your settings are correct, and then click Update to restart the base station.

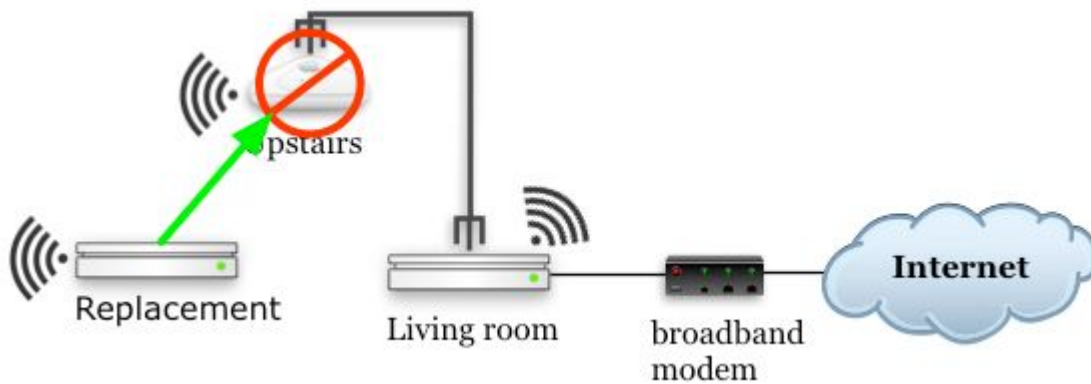
Now that you've extended your network via Ethernet, you may want to add printers, configure special network settings, or add more base stations. To get a road map to your options, flip back to [Quick Start to AirPort Networking](#) (p. 10).

---

## REPLACE AN EXISTING BASE STATION

---

This option lets you replace a base station that's already in use or that was in use on your network. For instance, you might be updating a network that had an 802.11g base station by replacing that older one with a new 802.11n unit that works over both frequency bands (**Figure 24**). You can copy the older base station's settings with a few clicks.

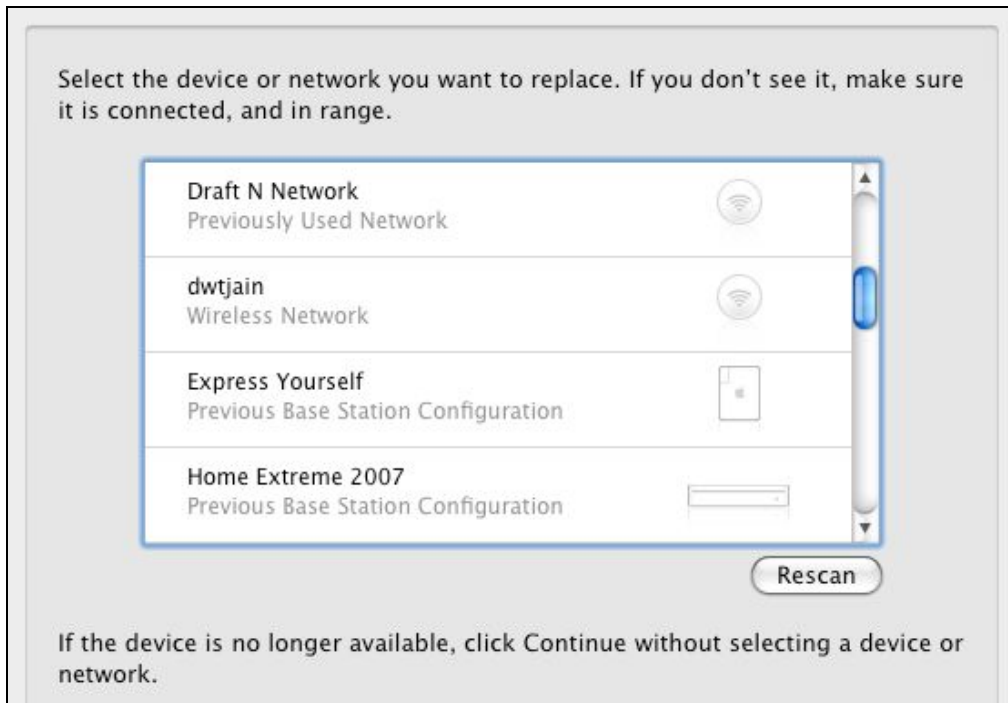


**Figure 24:** You might want to replace an existing base station with a newer, faster one, without having to re-enter all of the current base station's configuration details.

Put your new base station near your old base station for ease of swapping cables when you're ready, and follow these steps:

1. Connect your new base station to the existing network via a LAN port or a switch. This is necessary to be able to configure it while copying settings from your current base station.
2. From the Mac that you are using to configure the new base station, use Ethernet or Wi-Fi to connect to the network that's formed by the old base station so that both it and the new base station will be visible to AirPort Utility.

3. In AirPort Utility, select the new base station from the list at the left, and follow the steps to name the base station and choose a password to protect its configuration. Click Continue.
4. In the first Network Setup screen, select the first radio button, "I want to replace an existing base station..." and click Continue.
5. On the next screen, your old but still active base station network should be visible. Select the device or network that you want your new base station to replace (**Figure 25**).



**Figure 25:** You can choose a network or previous configuration from which to read setup details.

If you select a base station, AirPort Utility can copy its configuration details as long as you've connected to that base station previously from AirPort Utility and chosen to remember its password in the Keychain. Click Continue.

6. What you see next is either:
  - If you're using stored information, you'll see a summary of details to review, and an Update button at the bottom to click.
  - If you're connecting to a network with no stored details, you're taken to a Network Setup screen that lets you enter a network

name and its encryption key (if any). Fill that out, click Continue, and then you'll see the summary screen.

---

***If you can't access the existing base station's profile:*** you can abandon setup by clicking the existing base station in the list of devices at the left. AirPort Utility will ask if you want to switch; click Switch. Then click the Manual Setup button at the bottom of the AirPort Utility window, and enter and choose to remember the password for the existing base station. You should go back to Step 3, but this time automatically pick up the configuration.

---

7. Click Update to restart the base station with its new configuration.

If you receive a dialog asking you to unplug the older device and click OK, then follow the directions and click OK.

8. Depending on your AirPort model, you may now see an option to enable a guest network. (Flip to [Set Up Guest Networking](#), p. 222, to learn more about a guest network and note that you can set up a guest network later.) When you finish on this screen, click Continue.
9. You may now receive a "Select How You Connect to the Internet" screen. Select your best option and click Continue.
10. If you didn't already unplug your old base station from the broadband and modem and any LAN devices, do so now, and plug those cables into your new base station.

---

***If you're using cable broadband service:*** you may need to restart your cable modem after swapping in the new base station, even if the base station seems otherwise to be working fine. The cable modem has to register the new MAC address used by the Ethernet adapter in the new base station's WAN port.

---

## Replacing a Base Station and DHCP

When you start up a base station with an identical configuration as the one you replaced, computers that use DHCP to obtain an address from the base station might not know about the new base station and thus might not be able to communicate with it. If you find that a Mac can't access the Internet, open its Network preference pane, select the AirPort or Ethernet adapter (whichever is connected), click Advanced, and click the TCP/IP button. Click Renew DHCP Lease, and wait for the number to go away and reappear. Click OK and then Apply.

Also, note that the range of internal IP addresses that the base station's DHCP server assigns to your local computers may now be different; see [Refine Base Station DHCP Settings](#).

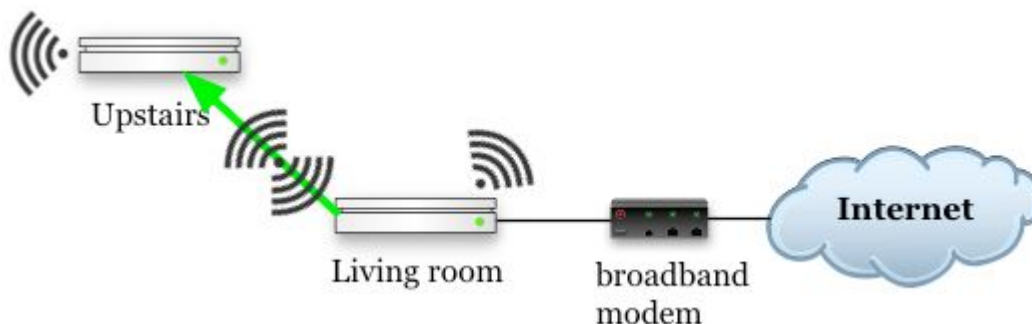
Now that you've completed setting up your base station, you may want to add printers, configure special network settings, or add more base stations. To get a road map to all the options, flip back to [Quick Start to AirPort Networking](#) (p. 10).

---

## EXTEND A NETWORK VIA WI-FI

---

If you have an existing Wi-Fi network and all 802.11n (2007 or later) Apple base stations (the AirPort Express switched to an 802.11n model in March 2008), you can use the AirPort Utility Assistant to extend that network over Wi-Fi to a new base station you're setting up (**Figure 26**). The following steps are covered with more technical background using the Manual Setup method in [Bridge Wirelessly](#); what you are setting up is called a dynamic Wireless Distribution System (WDS).



**Figure 26:** Extending via Wi-Fi lets you avoid running a cable.

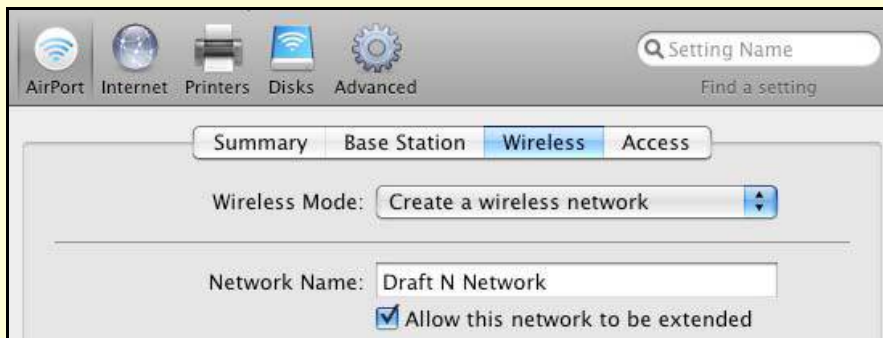
## Other Approaches to Wireless Extension

You can use a base station to extend an existing Wi-Fi network in two other ways, too:

- If you have one or more 802.11g Apple Extreme and/or AirPort Express base stations, you can use them together or with 802.11n Apple base stations via a static Wireless Distribution System (WDS) set up that requires a fair amount of configuration. See [Bridge Wirelessly](#).
- With an 802.11n AirPort Express (2008), you can extend any Wi-Fi network, using Apple equipment or otherwise, through a special, lightly documented mode called *ProxySTA*. This turns the Express into a regular Wi-Fi client, allowing you to connect other devices only through its Ethernet port. See [Connect to Any Base Station](#).

## Make Sure the Main Base Station Has the Correct Setting

The main base station to which you're connecting your new secondary base station must have a setting enabled to allow AirPort Utility to handle the following steps. Connect to the base station with AirPort Utility, click Manual Setup, and in the AirPort pane click the Wireless button. If Allow This Network to Be Extended *isn't* checked (**Figure 27**), check the box and then click Update. Now proceed.



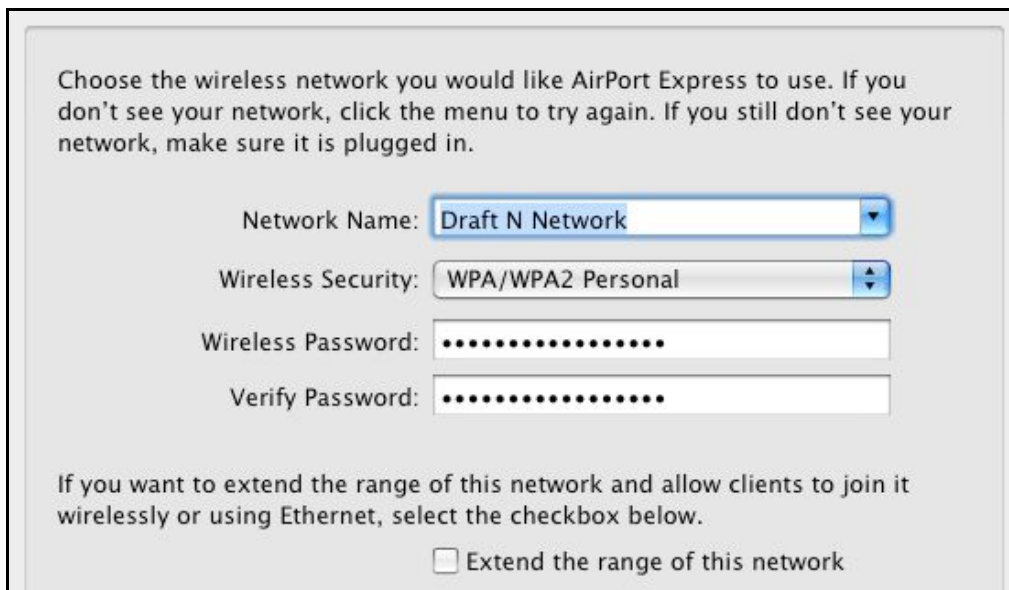
**Figure 27:** Make sure the network you want to extend is set to allow that.

To extend a network via Wi-Fi, follow these steps:

1. Make sure your new base station is prepped as explained in [First Steps in Setup](#) (p. 53) and that your main base station is configured as shown in **Figure 27** above.



2. In the Assistant, select “I want *AirPort model* to join my current network”. Click Continue.
3. Select the option “I want *AirPort model* to wirelessly join my current network.” Click Continue.
4. Choose your existing network from the Network Name pop-up menu, and then enter the security type and key; if you’re connected to this network from the computer you’re using, AirPort Utility should fill in the encryption type and its password for you (**Figure 28**).



Choose the wireless network you would like AirPort Express to use. If you don't see your network, click the menu to try again. If you still don't see your network, make sure it is plugged in.

Network Name:

Wireless Security:

Wireless Password:

Verify Password:

If you want to extend the range of this network and allow clients to join it wirelessly or using Ethernet, select the checkbox below.

Extend the range of this network

**Figure 28:** If you’re extending a network, choose the network you want to extend, and check the box at the bottom to allow Ethernet and Wi-Fi on the base station you’re configuring to be used.

5. Two choices emerge at this point.
  - a. If you leave Extend the Range of This Network unchecked, only Ethernet is active (despite the language of the message above the checkbox).
  - b. If you check that box on a 2007-or-later base station, then wireless clients and Ethernet-enabled devices can connect to the base station that’s being extended. On pre-2007 base stations, only Ethernet remains active.

A summary screen appears.

6. Click Update and wait for the new, secondary base station to restart. When it restarts, it should automatically connect to the main base station.

Now that you've extended your network, you may want to add printers, configure special network settings, or add more base stations. For a road map to the various options, see [Quick Start to AirPort Networking](#) (p. 10).

---

## CREATE SEPARATELY NAMED 2.4 AND 5 GHZ NETWORKS

---

Apple's simultaneous dual-band Time Capsule and AirPort Extreme base stations are designed to let a Wi-Fi client pick the best network at any given time, so by default both networks must use the same name. Mac OS X has been optimized to balance speed and range in choosing a given band's network, so it monitors a network connection for when the signal becomes marginal in 5 GHz, or for a 2.4 GHz connection, for when a 5 GHz signal is strong enough to swap over to. But in some cases, you might want your network to act as though it were two separate networks, locking some Wi-Fi devices to one network to avoid them flipping back and forth.

**Note:** Generally, the 5 GHz band provides faster networking than the 2.4 GHz band, but that's a generalization, not a rule. Also note that the 5 GHz band doesn't work with 802.11b or g devices, including all current models of the iPhone and iPod touch. Read [Spectrum Trade-offs](#) for details.

The limitation with a separately named 5 GHz network is that it must share all the settings of the 2.4 GHz network, such as encryption method, DHCP, and so forth.

Apple has buried this option only slightly; here's how you access it:

1. Make sure your new base station is prepped as explained in [First Steps in Setup](#) (p. 53).
2. Click Manual Setup.
3. In the AirPort pane, click the Wireless button.

4. Click Wireless Options.
5. Select the 5 GHz Network Name checkbox, enter a different name than the name shown in the main Wireless view, and click Done (**Figure 29**).

**Wireless Options**

5 GHz Network Name:

Country:

Multicast Rate:

Transmit Power:

WPA Group Key Timeout:

Use wide channels  
Wide channels provide higher throughput in your network, but might interfere with nearby networks.

Create a closed network  
The name of a "closed" network is hidden. To join the network, a user must know the name of the network.

Use interference robustness  
Interference robustness can solve interference problems caused by other devices, such as cordless phones or wireless video monitors. Using interference robustness may affect overall network performance.

**Figure 29:** Name the 5 GHz network separately.

6. Click Update.

# Determine the Band, Channel, and Location

The underpinning of Wi-Fi is radio technology, of course: wireless waves pass across the “ether” around us to communicate. Wi-Fi can communicate over either of two pieces of spectrum, contiguous series of frequencies grouped into *channels* (much like AM/FM radio channels) that are part of larger *bands* (much like the AM and FM bands). The 2.4 GHz and 5 GHz bands each have tradeoffs, and you may have to think carefully to pick the right band and to combine equipment to make it all work. The simultaneous dual-band base stations introduced in March 2009—base stations that have two radios and can transmit and receive over two bands at the same time—take most of the complexity out of the equation.

A default configuration may work well for your network. However, if it doesn't work perfectly, you can read this section to:

- Understand and set backward compatibility for pre-802.11n gear.
- Understand and set a base station's channel or channels.
- Find the ideal placement for your base station or base stations.
- Test those above choices to see how they work.

If you don't know the basics of spectrum bands and channels, read [The Spectrum Part of Wi-Fi](#), p. 24, before proceeding here.

**Note:** Before the 2009 models of the Extreme N and Time Capsule, all 802.11n Apple base stations could use only one band at a time. That's still true for the Express N. For details on mixing older and newer hardware, and on integrating an Express N, see [Mix 2.4 GHz and 5 GHz 802.11n Networks](#).

---

*If you have only simultaneous dual-band gear: You can keep reading to learn background information, but for practical purposes, you can skip to [Pick Compatibility and Optionally Set a Channel](#).*

---

---

## SPECTRUM TRADE-OFFS

---

Shortly, I explain how to use AirPort Utility to set the band (2.4 GHz and/or 5 GHz) and the channel for a base station. To make the best choice, you may need some background on spectrum and channel choices. Let's begin by comparing the two bands.

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 in order to avoid treading on older networks in 2.4 GHz. Wide channels use twice the amount of spectrum and thus can achieve twice the data throughput.

### 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 approved uses that can conflict at times. Industrial sealers, for instance, use heating processes that emit 2.4 GHz radiation. (There are many other junk bands, too, most not used for networking.)

Home microwave ovens use *dielectric heating*: water molecules are dipolar (have two oppositely charged ends), and a microwave oven switches the electromagnetic field in the oven 2.45 billion times a second. The water molecules continually try to realign, which releases heat, which heats the rest of the food. That's why dry rice can't be heated in a microwave, why microwave ovens heat from the outside in (the waves penetrate outer layers faster), and why frozen food tend to defrost poorly (the ice's crystalline structure dampens the twisting). If your friends think microwaves "leak" radiation, create ionizing radiation, resonate water molecules, or "irradiate" food, refer them to Wikipedia's concise explanation: [http://en.wikipedia.org/wiki/Microwave\\_oven](http://en.wikipedia.org/wiki/Microwave_oven).

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

## Throughput

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, 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 6**, next page, for specifics.

---

**Limits on N's top rates:** *While 802.11n is far speedier than 802.11g, you can still be slowed down by both the band and channel type, as well as the path a signal takes from or among Wi-Fi and Ethernet-connected computers, as you can see in **Table 6**.*

*The highest possible N rate happens when two adapters use the 5 GHz band with wide channels. However, the maximum potential throughput is reduced because the signal has to go from one adapter to the base station and then from the base station to the other adapter.*

*You will see the fastest possible speeds from an N adapter connected via a 5 GHz wide channel to a computer connected to the base station via gigabit Ethernet. The original Extreme N topped out below the maximum rate because it had just 10/100 Mbps Ethernet; the September 2007 models and all Time Capsules don't suffer from this Ethernet limit. The Express N has just 10/100 Mbps on its single Ethernet port, too, limiting its top network transfer speed to and from an Ethernet network to N devices.*

---

**Table 6: Throughput Based on Band Choice (Best Speeds) Using a Gigabit Extreme N**

Connection	2.4 GHz (regular channel)	5 GHz (wide channel)
N† to 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
N† to wired 100 Mbps Ethernet (LAN)	Up to 70 Mbps, but varies enormously	Over 90 Mbps
N† to gigabit Ethernet (LAN)		Over 140 Mbps
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	980 Mbps	
* With NAT turned off, speeds are the same as Ethernet LAN.		
† Tested with the gigabit Ethernet model of Extreme N.		

## Compatibility

You would think that the choice of using 5 GHz is obvious, right? Not so fast. If you have any B or G devices on your network—like Macs with the original AirPort Extreme built in—they can't connect. Or if a visitor with an older adapter would be out of luck. (Table 4, p. 40, summarizes which 802.11 standards are supported by various Macs and Apple handheld devices.)

To be compatible with all Intel Macs, you could use 5 GHz and mix A and N, which would provide better performance than mixing G and N in the 2.4 GHz band. See Table 7 for a comparison of the tradeoffs.

**Table 7: Comparing the 2.4 GHz and 5 GHz Bands**

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

## Channels

Now that you've figure out which band (or bands) you want your base station to broadcast on, it's time to consider which channel; even with simultaneous dual-band base stations, the channel can be critical. 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.

## **2.4 GHz**

For the 2.4 GHz band, Apple's base stations do a great job when set to Automatic in selecting a channel that's as free of competing uses as possible. In some cases, you may want to set a specific 2.4 GHz channel in order to interleave channel usage on multiple base stations that you're setting up, or because you know about particular problems in a given channel that you want to always avoid.

The 2.4 GHz channels are numbered 1 to 11, and 1, 6, and 11 are typically chosen because they lack any real overlap with each other. (The 2.4 GHz channels are staggered, meaning any two adjacent channels share about 75 percent of the same frequencies; 1, 6, and 11 are mostly clear of each other.)

## **5 GHz**

The 5 GHz band has a bigger tradeoff: Apple makes 8 out of 23 possible channels available (see [Appendix D: Channels Explained](#), for more details): 36, 40, 44, and 48 in the lower set, and 149, 153, 157, and 161 in the upper part. (The 5 GHz channel mapping doesn't overlap, with each channel having a full 20 MHz width; two channels used together for a wide channel have a full 40 MHz width.)

The lower set is limited by U.S. regulators to use 1/20th or 5 percent of the signal strength allowed in the upper band. More power usually means greater range. If you use Automatic to set the 5 GHz channel choice, Apple's firmware always tries to pick an upper-band channel. Sometimes it may sense interference and pick a lower-band channel.

You may want to set a specific channel in 5 GHz to ensure that you're always using the full available power for the best range. Or, you might want to set a low-numbered channel to avoid blasting your 5 GHz network.

---

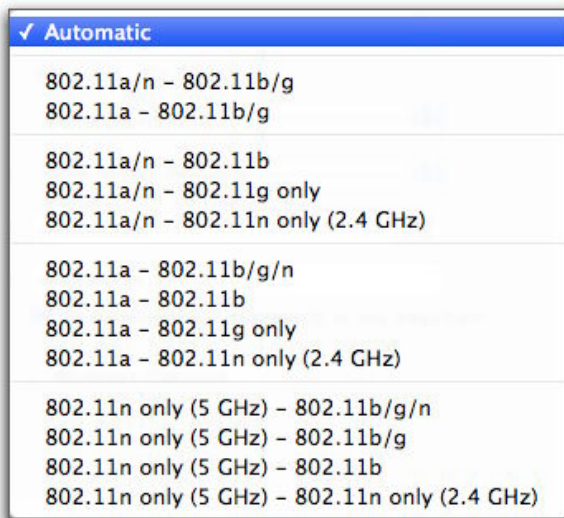
## PICK COMPATIBILITY AND OPTIONALLY SET A CHANNEL

---

To configure a base station's band, compatibility, and channel (or as many of those as you want), launch AirPort Utility, connect to your base station, and click the Manual Setup button. Click the AirPort icon to open the AirPort pane, and then click the Wireless button.

### Set the Radio Mode

The Radio Mode pop-up menu (**Figure 30**) offers a multitude of choices in every combination; notice that a label beneath the pop-up menu summarizes the type(s) of 802.11 supported by the chosen mode.

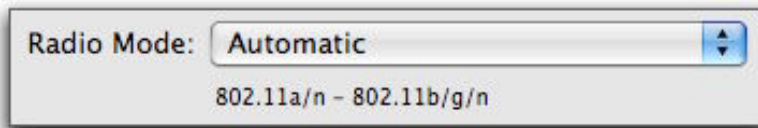


**Figure 30:** When you configure a simultaneous, dual-band base station, the Radio Mode pop-up menu offers Automatic along with two standard options (the top three of the many options shown here), but reveals eleven more options when the Option key is pressed before opening the menu (bottom eleven options).

You'll see fewer options for a one-band-at-a-time base station.

Let's look at the different radio mode options:

- **Automatic:** This default option for a simultaneous dual-band base station provides full compatibility with different types of 802.11 devices. As the label beneath the pop-up menu in **Figure 31** shows, it supports 802.11a/n in 5 GHz and 802.11b/g/n in 2.4 GHz.



**Figure 31:** Automatic sets the most compatibility.

- **802.11a/n:** This option gives full backward compatibility in 5 GHz, allowing older Intel devices without 802.11n to connect at better ranges and speeds.
- **802.11b/g/n:** This option is fully backward compatible in 2.4 GHz.
- **802.11a, 802.11b, 802.11g only, 802.11b/g:** These modes lock out various faster and slower modes, and are provided for compatibility only. I can't think of any good reason to use these options.
- **802.11n only (5 GHz), 802.11n only (2.4 GHz):** These modes disable the special backward-compatible *preamble* that's transmitted at the slowest speed, removing the overhead and disabling adapters that can't talk N from using either or both bands at all.

### Eliminate 802.11a

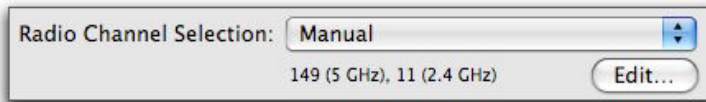
There's one strong reason to set the 5 GHz band to 802.11n only: The lurking specter of an 802.11a slowdown. Because Apple put 802.11a into nearly all first-generation Intel-based Macs (those with Intel Core chips), and because Mac OS X doesn't offer a band-selection or protocol selection option, one of your computers could be using 802.11a in 5 GHz.

I encountered this problem twice recently. As my colleague Ted Landau was troubleshooting Wireless Distribution System problems he discovered an errant 802.11a adapter in an iMac on his home network. And, when I installed a simultaneous dual-band base station in my home, I found out that my wife's MacBook was communicating over 802.11a.

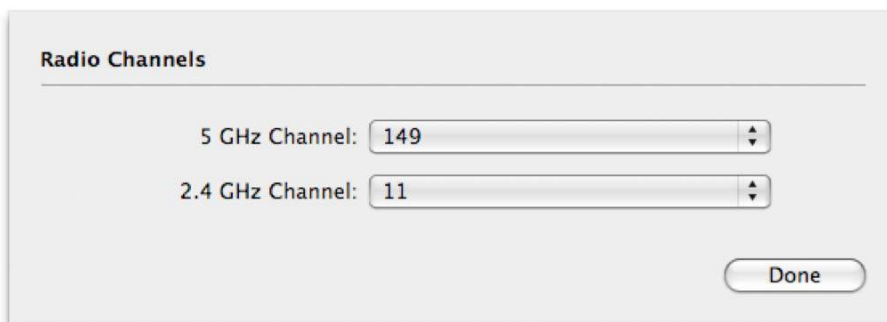
802.11a slows down the 100 to 150 Mbps potential of 802.11n in 5 GHz with wide channels to 802.11a's 25 to 30 Mbps throughput whenever it's in use. If you have active 802.11a devices, you're chewing up available bandwidth. The way around this is to choose 802.11n only (5 GHz) – 802.11 b/g/n from the Radio Mode menu. This allows b/g/n in 2.4 GHz, but 802.11n only in 5 GHz.

## Set the Channel

The Radio Channel Selection pop-up menu lets you choose a channel based on the band you selected. AirPort Utility defaults to Automatic, where the base station picks a channel based on which channel has the least amount of radio activity. If you choose Manual from the pop-up menu, the automatic channel choices are revealed in a label beneath the menu, along with an Edit button (**Figure 32**). Click Edit to see the full list of available channels (**Figure 33**).



**Figure 32:** The popup-menu shows the automatic choices when Manual is set, somewhat ironically.



**Figure 33:** The popup-menu shows the automatic choices when Manual is set, somewhat ironically.

---

***Which channel should you pick?*** 5 GHz channels 149 and higher can broadcast 20 times as much power as channels 48 and lower. Most people are totally unaware of this, and the base station always tries to pick one of these higher-power channels when it is set to Automatic for 5 GHz.

*To constrain a network as much as possible, force a lower channel to be used; for more power, force a higher channel. (If an upper-band channel wasn't automatically selected, this could mean there's interference in the area, however.) For 2.4 GHz, I recommend leaving the menu set to Automatic unless you have a specific overlapping network configuration you're building, or are aware of regular interference problems on a certain channel that you want to avoid.*

*Read [Channels](#), a few pages earlier, for more channel-setting advice.*

---

## Adjusting Power

What if you want to use more power than the least available but not as much as the maximum? That is, you want to control how far your network reaches—perhaps to keep the signal mostly workable inside your apartment or office. You’ve got an option, which Apple squirreled away.

When connected to your base station in AirPort Utility, click the AirPort pane and then the Wireless button. Now click the Wireless Options button. The Transmit Power pop-up menu lets you choose 10, 25, 50, or 100 percent.

---

## PICK THE RIGHT PLACE

---

Now that you’ve chosen a band and channel, it’s time to find the right spot to put the base station. I have a pile of advice for how to place your gateway in your home or office. In testing, you might need to change the band or channel, even!

When you walk around with a cell phone, the number of bars showing signal strength varies, depending on the strength of signals received from nearby cellular network transmitters. 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.

When you position your base station, consider these factors:

- Does your broadband modem hookup constrain where you locate your base station? Many of us have phone or cable connections in non-ideal locations for locating a Wi-Fi gateway. You might turn to powerline networking (see [Extend with HomePlug](#), p. 149) or even run an Ethernet cable through the walls in order to put your base station far from your broadband modem.
- Where do you want Wi-Fi connectivity? Do you want to work in your backyard? Upstairs and downstairs?
- What obstacles might block your signal? Walls, ceiling, floors, and even metal exercise bikes can all absorb and reflect Wi-Fi signals, reducing their range and quality.

- 2.4 and 5 GHz networks have different ranges at the same output power. Can you get the faster 5 GHz signals where you need them but have the coverage of the 2.4 GHz network for the rest of the area in which you want service?

While Apple's 802.11n base stations use *MIMO* technology—multiple sets of receiving and transmitting antennas—to cover a much greater area than their 802.11g predecessors, each base station still has limits, though N devices typically come much closer to covering the area of a typical home.

Pick a spot near the middle of where you want your signal to reach and test 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 a spot to see if the signal strength varies. (The next few pages explain how to check the signal strength.)
- Use sticky notes to mark signal strengths at the locations where you want to provide network access. 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.
- The Extreme N and Time Capsule are designed to be used flat; the AirPort Express can be used in any orientation. All three devices use *omnidirectional* antennas—ones that send and receive in all directions.

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

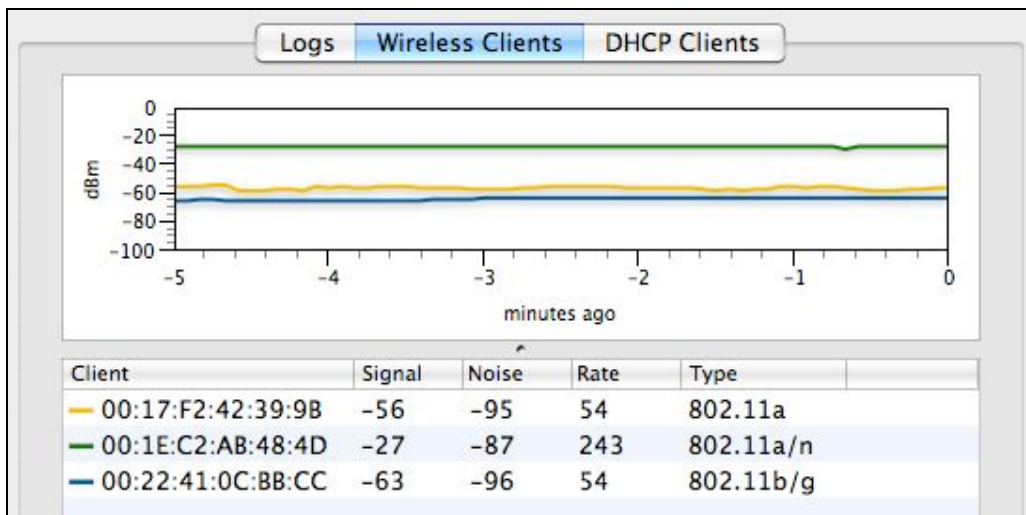
## Testing from Base Station to Client

AirPort Utility now incorporates what was a separate Apple utility to monitor the performance of wireless adapters connected to a base station. Base station monitoring can show you how several different adapters perform over time. You can use this in one of two ways: observing the connections live as you walk around with a laptop with AirPort Utility launched and set up as described below; or with AirPort Utility open on a still machine while you watch the numbers as someone else moves computers around, opens and closes doors, and adjusts other physical obstacles.

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 Statistics 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 34**).



**Figure 34:** 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, the raw data rate, and the protocol in use. The top device, using 802.11a, is a first-generation Intel Core Duo MacBook; the next, with 802.11a/n, an Intel Core 2 Duo MacBook; the last, connected via 802.11b/g, an iPhone.

This nifty readout provides ongoing monitoring of the transmit rate—the same number shown in the AirPort menu in [Figure 35](#)—for each connected device that was connected when you launched AirPort Utility, starting with when you first display the readout. 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.

Below the chart, you can learn more about each client's connection:

- **Client:** 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. 97.)
- **Signal and noise:** 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.

- **Rate:** The Rate column has the most useful information, because it shows the raw data transmit 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 that you need to tweak the base station's—or the computer's—position.
- **Type:** This column shows what protocols are active on the adapter that's connected to the base station. You might be surprised to see 802.11a listed when you're not aware it's available. 802.11a/b/g adapters were built into the first generation of Intel Macs, as well as certain Windows-oriented Intel Centrino models. Having an



802.11a adapter connect to your 5 GHz network can slow down 802.11n performance dramatically. See [Eliminate 802.11a](#) for how to fix this problem.

## 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. There are two ways you can go about this: Using Mac OS X's built-in but rough signal strength information in the AirPort menu, or using iStumbler, which works only in the 2.4 GHz band at present. You can also bring out the big guns and use a spectrum analyzer to troubleshoot why a network just won't work in a given channel or area.

### Use the AirPort Menu

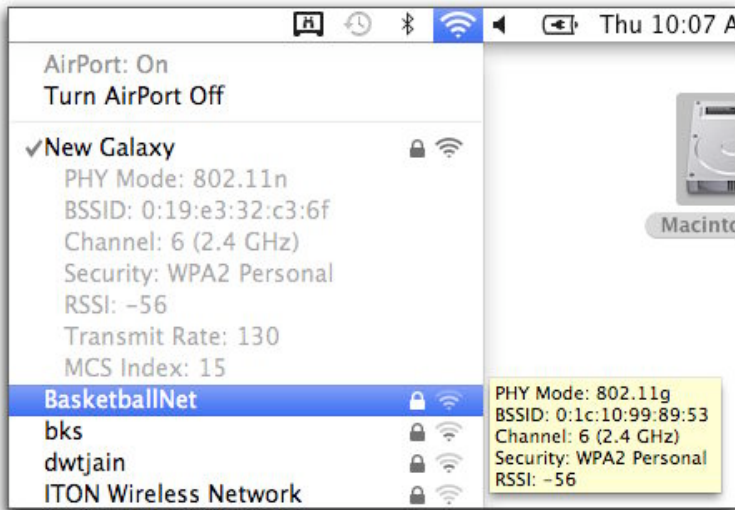
The AirPort menu in the menu bar offers connection information, and Snow Leopard's AirPort menu is more helpful than Leopard's. Hold down the Option key and select the menu (**Figure 45**), then hover over any network to get answers to several key questions:

---

***Snow Leopard additions:*** *The details in the AirPort menu were first added in Leopard and then further enhanced in Snow Leopard.*

---

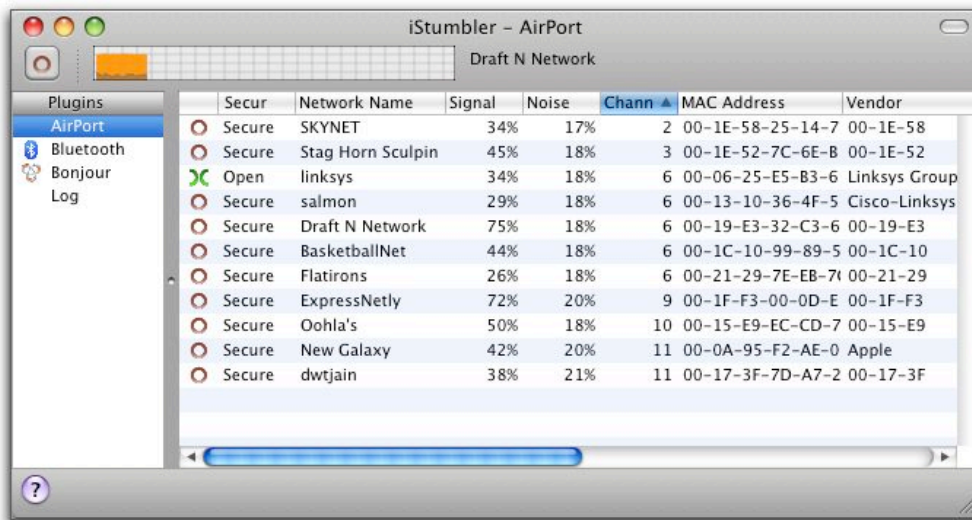
- **What standard is my connection using?** The *PHY Mode* shows the actual standard being used, which should be 802.11n if your base station is configured correctly (new in Snow Leopard).
- **How well can my computer receive the base station's signal?** The *RSSI* (Received Signal Strength Indication) measures in decibels how well a signal is being received. A higher number (closer to zero) means a stronger signal. New in Snow Leopard, you also can see a visual indication of signal strength by observing the number of black waves in the symbol at the far right of each network's name.
- **How fast is my network running?** For a network that you're currently connected to, you'll see the *transmit rate*, which indicates how "fast" the network is operating. Apple's 802.11n can operate at a raw rate of up to 270 Mbps (in 5 GHz) or 130 Mbps (in 2.4 GHz); in **Figure 35**, the rate is just 130 Mbps using 2.4 GHz channel 6. That can change constantly, as the adapter and base station negotiate for faster or slower connections as problems are encountered.



**Figure 35:** Snow Leopard's AirPort displays signal information.

### Monitor 2.4 GHz with iStumbler

iStumbler (<http://www.istumbler.com/>) provides a continuous scan with information about signal and noise for all the 2.4 GHz networks in your vicinity (**Figure 36**).



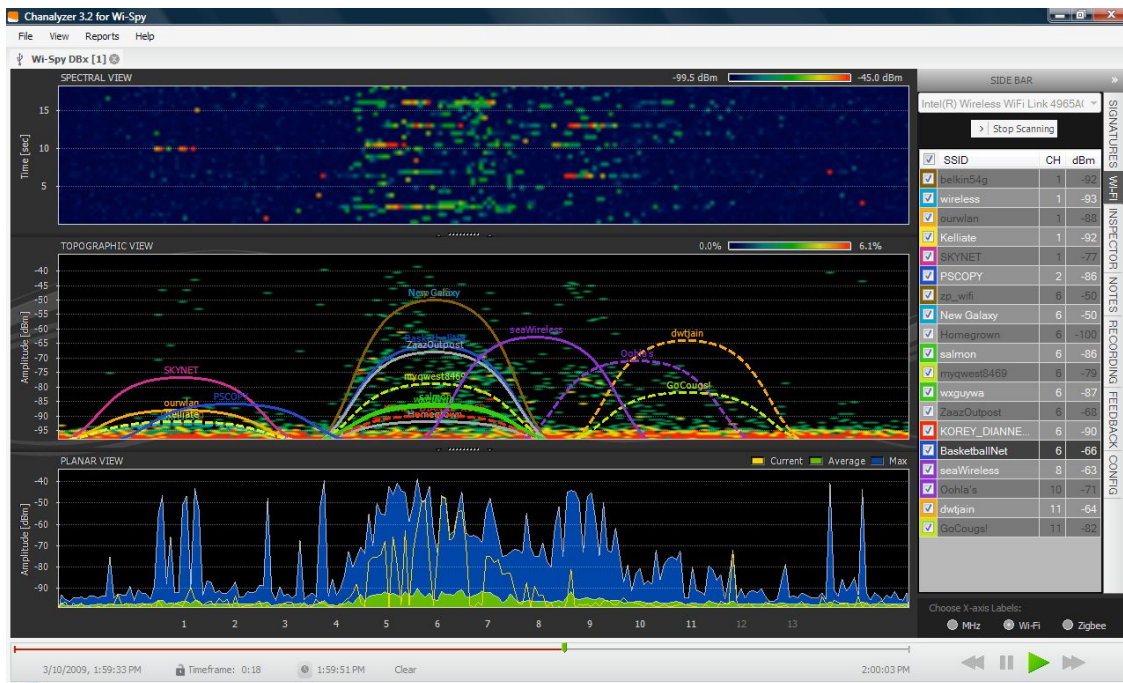
**Figure 36:** iStumbler shows nearby networks. I made this scan in my office, which is in the middle of a building in Seattle with a window off to one side. Imagine a scan made in Manhattan.

**Tip:** iStumbler can't scan for 5 GHz network channels, unfortunately, but in that band you're less likely to find other users and thus interference. The developer, who works for Apple but has independently released this free tool, said via email that he plans an update at some point to support modern Mac adapters.

## Run a Spectrum Analyzer

If you're truly frustrated with finding a good connection, you could buy a spectrum analyzer, an expensive piece of software. These analyzers might be a great group purchase among friends and colleagues who frequently set up and troubleshoot Wi-Fi networks.

A *spectrum analyzer* constantly measures the strength of signals in hunks of frequency, and it produces output that software can read (**Figure 37**). The more energy or more spikes in a given channel, the more likely that Wi-Fi won't work there.



**Figure 37:** Wi-Spy analyzers capture signal strength over time at frequencies in the 2.4 GHz or 5 GHz band and relay them to software, which displays the results. (Wi-Spy DBx data pictured.)

The \$99 Wi-Spy 2.4i and \$199 Wi-Spy 2.4x from MetaGeek analyze the 2.4 GHz band and provide a live analysis of the signals passing in the air around you. MetaGeek's 2.4/5 GHz analyzer, the Wi-Spy DBx costs a whopping \$599, but pulls a lot of interesting data out of bands that are hard to examine (<http://www.metageek.net/>).

# Advanced Networking

Did the simplified setups explained in [Set Up a Network](#) not cover everything you needed to get up and running? In this section, I spell out all the details for how to connect your base station to a WAN and how to further configure addressing on your LAN. Advanced options are needed for networks that use static or fixed addresses, and for anything the slightest bit unusual.

---

**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](#).*

---

**Stream music:** *If you want help getting AirTunes to work with your AirPort Express, see [AirPort Express Extras](#).*

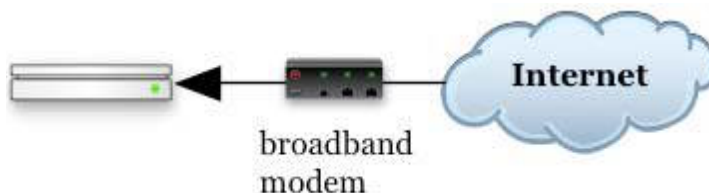
---

## GET A WAN ADDRESS

---

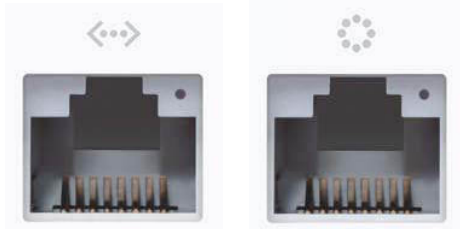
The more complicated scenarios start with getting a WAN address for your base station; you'll then move to LAN configuration.

To communicate with the rest of the world, you need to hook the wide area network (WAN) port of your base station either into a broadband modem or, if you have an existing Ethernet LAN to which you are connecting the base station, into that larger network (**Figure 38**).



**Figure 38:** Plug your broadband modem into the base station's WAN port.

For an Express N, that's the only port, and it's labeled as a standard Ethernet port (**Figure 39**, left); for an Extreme N or Time Capsule, it's a port labeled with a circle of dots (**Figure 39**, right).



**Figure 39:** The single Ethernet port on an Express N (left); the WAN port on the back of an Extreme N or Time Capsule (right).

In any case, start with an Ethernet cable and plug it into the appropriate 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:*** *N base stations all have auto-sensing, auto-switching Ethernet, which means you can use either type of standard Ethernet cable—straight-through or crossover—successfully. The cable should be at least Category 5 for 100 Mbps Ethernet or 5E for gigabit Ethernet; for long Ethernet runs, use Category 6. All recent Apple Ethernet ports (whether on a computer or base station) also automatically adjust the 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. For configuration details, consult [Dynamic Addressing](#), next page.
- A static address is more typical for small and large offices. For setup information, read [Static Addressing](#), a few pages ahead.

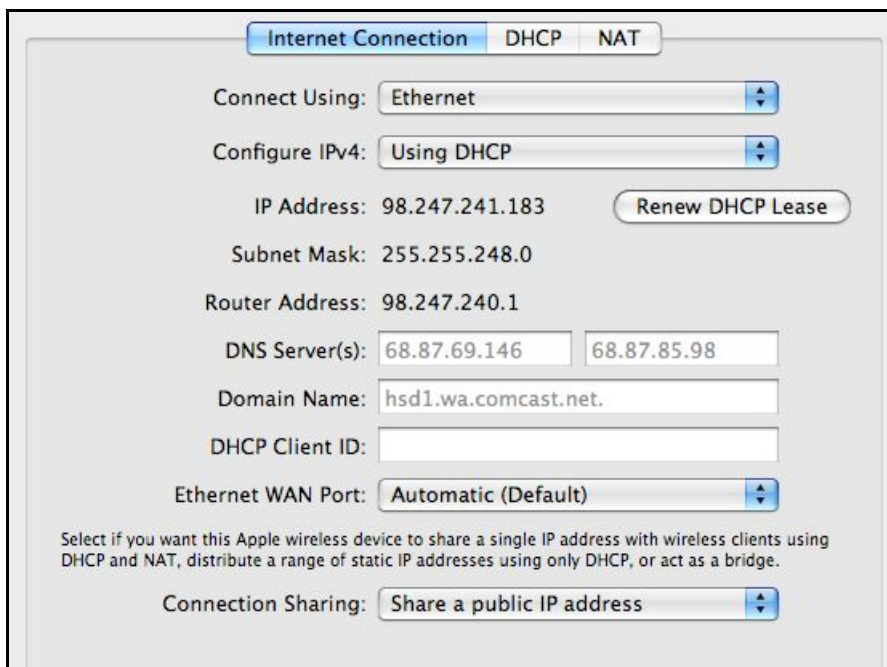
## Dynamic Addressing

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 base station 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. However, a dynamically assigned address could, instead, be a *publicly routable* address, which is part of the global numbering system for IP addresses.

To set up dynamic addressing for your base station, proceed as follows:

- Apple's base stations are set to obtain an IP address as a DHCP Client by default. In most cases, no additional steps should be needed (**Figure 40**).



**Figure 40:** The simplest way to get a base station on the Internet.

- In some limited cases, you might need to enter the DNS (Domain Name Service) IP addresses manually, or you may choose to override ISP-provided values. In **Figure 40**, you can see that the DNS

addresses provided by the DHCP server are shown in the DNS Server(s) fields in gray. You can type and replace them.

- If you need to use PPPoE or have MAC address issues with configuration, then [New Network, Single Base Station](#) may not have answered all your questions; keep reading ahead to find directions for how to “Log In via PPPoE over Broadband DSL,” below, and [Deal with MAC-Address-Restricted Cable Broadband](#).

### **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.

- OpenDNS is much faster than most ISPs. This makes Web pages load in a manner that seems noticeably snappier.
- The firm’s system automatically corrects common typos for non-existent addresses: [flickr.cmo](#) becomes [flickr.com](#).
- Anti-phishing features are standard, warning you about sites reported through a collaborative system.
- You can register an entire network and capture usage statistics.
- You can create custom shortcuts to control what domain name is looked up when you enter a keyword.

See <http://www.opendns.com/> for more details, including their two IP addresses to use in your DNS settings.

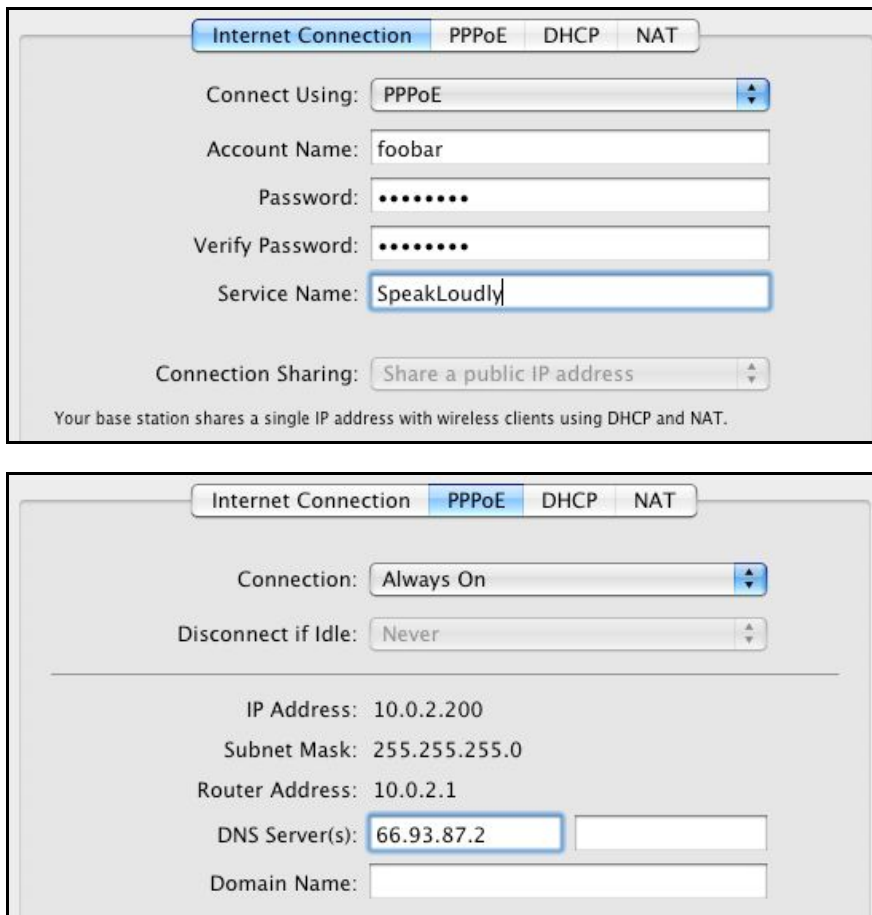
Some ISPs require you to jump through additional hoops to connect to their networks: a login process or a way to restrict access to a single computer. The former is used mostly by DSL providers; the latter, by cable firms.

### **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 41**). 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 41:** 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 base station.
- 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 base station's WAN port; see the next page for where to find that address.



## What and Where Is a MAC Address?

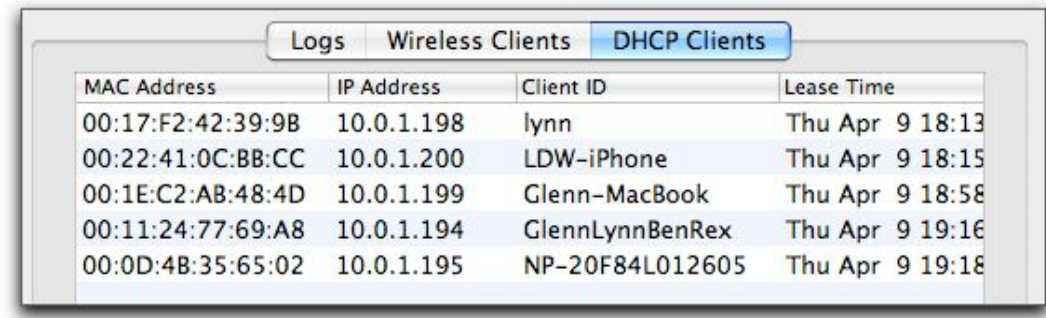
The MAC, or *Media Access Control*, address is a unique, factory-assigned address for every Ethernet and Wi-Fi adapter. A MAC address consists of six two-digit hexadecimal numbers separated by colons, such as 0C:F2:33:01:02:FC. (*Hexadecimal*, or *hex*, is the base 16 number system, with values running from 0 to 9, and then from A to F for 10 to 15.) The first three numbers are assigned to a manufacturer by a coordinating association; 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.

Some routers from other makers can have their MAC address changed in a process called *MAC cloning* or *spoofing*, which is sometimes useful when you have to register a computer's MAC address, but then want to use a router in its place. No Apple base station has ever offered this capability, although Mac OS X allows it for Macintoshes via a Terminal command.

Here's how to find MAC addresses:

- **Base station:** Look on the bottom of the base station (Extreme N, Time Capsule) or near the plug (Express N). Or, in AirPort Utility, select a base station at the left and click Manual Setup to see its MAC addresses on the right (you can copy a MAC address from AirPort Utility):
  - ◇ The *AirPort ID* is the device's wireless MAC address. The 2009 Extreme N and 2009 Time Capsule each have two AirPort IDs, one for each band's radio, and they are noted as such on the base station itself and in AirPort Utility.
  - ◇ The *Ethernet ID* is the WAN port's MAC address.
- **Computers connected to a base station via Wi-Fi:** In AirPort Utility, select the base station and choose Base Station > Manual Setup. Click the Advanced icon, and then—on the Statistics view—click the Logs and Statistics button. Click the DHCP Clients button and a list of MAC addresses appears for both Wi-Fi and Ethernet clients. The Client ID field shows either the value entered in the Network preference pane in Mac OS X or the Bonjour name of a computer or other device (**Figure 42**).

If no client ID is listed, you can turn your computer's Wi-Fi adapter off and on to see which MAC address corresponds to your computer.



MAC Address	IP Address	Client ID	Lease Time
00:17:F2:42:39:9B	10.0.1.198	lynn	Thu Apr 9 18:13
00:22:41:0C:BB:CC	10.0.1.200	LDW-iPhone	Thu Apr 9 18:15
00:1E:C2:AB:48:4D	10.0.1.199	Glenn-MacBook	Thu Apr 9 18:58
00:11:24:77:69:A8	10.0.1.194	GlennLynnBenRex	Thu Apr 9 19:16
00:0D:4B:35:65:02	10.0.1.195	NP-20F84L012605	Thu Apr 9 19:18

**Figure 42:** The DHCP Clients view can be a useful way to grab the MAC addresses for everything on the network.

- **Wi-Fi adapter in a Mac:** In Mac OS X, open the Network System Preferences pane. In Tiger, choose AirPort from the Show pop-up menu; in either Leopard or Snow Leopard, click AirPort in the adapter list and click the Advanced button. The MAC number is the *AirPort ID*.
- **Wi-Fi adapter under 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 that 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(s):** 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 43**).

The screenshot shows the 'Internet Connection' configuration window. At the top, there are three tabs: 'Internet Connection' (selected), 'DHCP', and 'NAT'. Below the tabs, there are several fields and dropdown menus. 'Connect Using' is set to 'Ethernet'. 'Configure IPv4' is set to 'Manually'. 'IP Address' is '98.247.241.183'. 'Subnet Mask' is '255.255.248.0'. 'Router Address' is '98.247.240.1'. 'DNS Server(s)' has two entries: '220.22.222.22' and '220.22.220.20'. 'Domain Name' is empty. 'Ethernet WAN Port' is 'Automatic (Default)'. 'Connection Sharing' is 'Share a public IP address'. A note at the bottom says: 'Select if you want this Apple wireless device 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.'

**Figure 43:** Configure the Internet connection manually by entering the static values provided by your ISP or network administrator.

### What's IPv4?

Another 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 the AirPort and Time Machine base stations, among other products. IPv6 isn't widely available, but it is out there and will become increasingly embedded in our lives and devices. See [Explore the Internet's Future with IPv6](#) for more details.

---

## HAND OUT LAN ADDRESSES

---

With the WAN link connected, 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 base station shares one incoming Internet address with all the machines on the LAN. The base station assigns addresses to computers on the LAN from a private range; you can modify that range. The addresses are typically transient for any given computer. The base station 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 base station 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 a base station to let another device on a larger network dynamically assign addresses or allow static addresses. With this set up, the base station 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 base station is connected.

Let's look through each of these in turn.

**Note:** DHCP works by having a computer or other device send 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.

---

**Warning!** *In testing the Extreme N and Time Capsule, I discovered that a NAT-enabled Extreme N or Time Capsule 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 configuration, you won't see speeds above about 70 to 100 Mbps, which is quite slow if you're using gigabit Ethernet. You wouldn't set up DHCP to work in this fashion on most networks, though you might in an office or with a larger LAN—see [Passthrough and Bridging](#).*

*You could also hit a blockage if you have a broadband connection faster than 70 Mbps—Cablevision just announced 101 Mbps service for \$100 per month—as the base station's LAN-to-WAN NAT would slow down your ability to download data from the Internet. Apple is aware of this, and has continually improved NAT conversion speed in each version of the AirPort hardware. This isn't an issue with the Express N because it can't send traffic to other devices via Ethernet using NAT and because it has just a 10/100 Mbps Ethernet port.*

---

## **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 needn't proceed further in this section to set up the base station; you can skip ahead to [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**

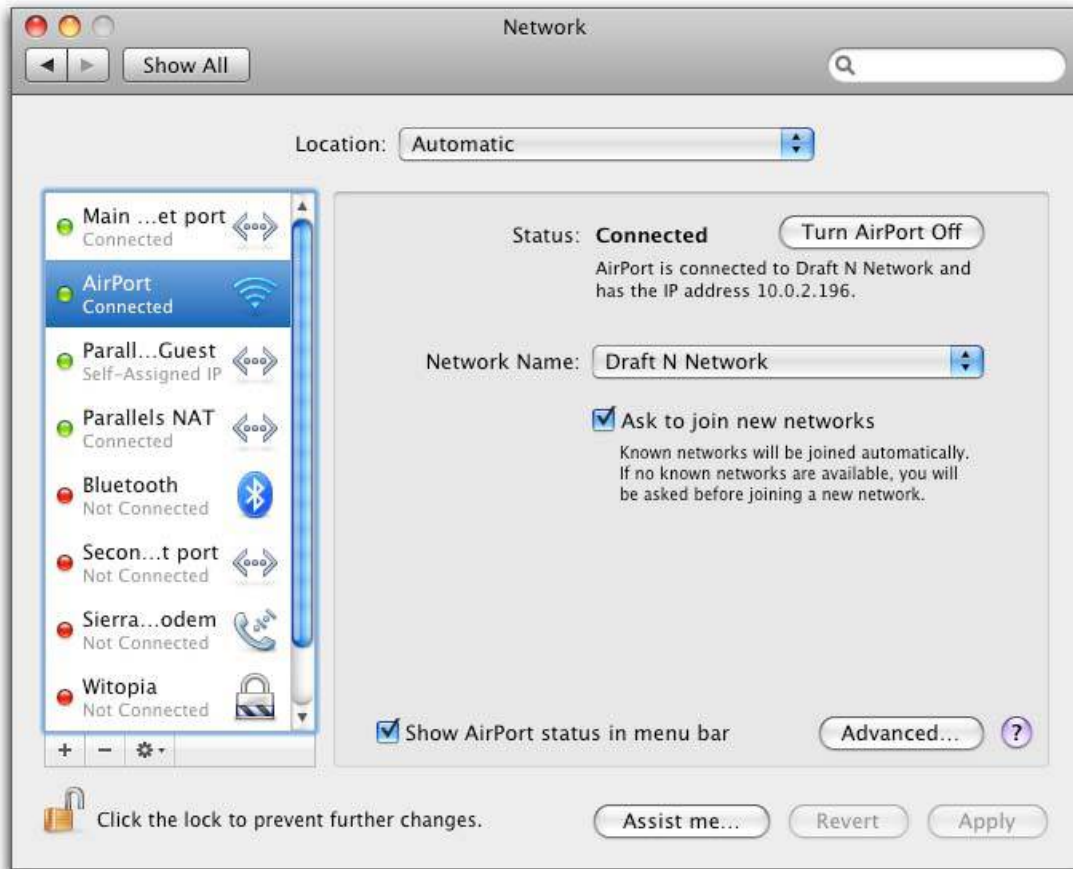
In AirPort Utility, click the Internet icon at the top of the window, click the Internet Connection button, and choose Share a Public IP Address from the Connection Sharing pop-up menu.

### **Set Up Client Computers**

With a base station set to use dynamic addressing, each of your computers must be set to receive an address via DHCP. This is the default setting for any network adapter.

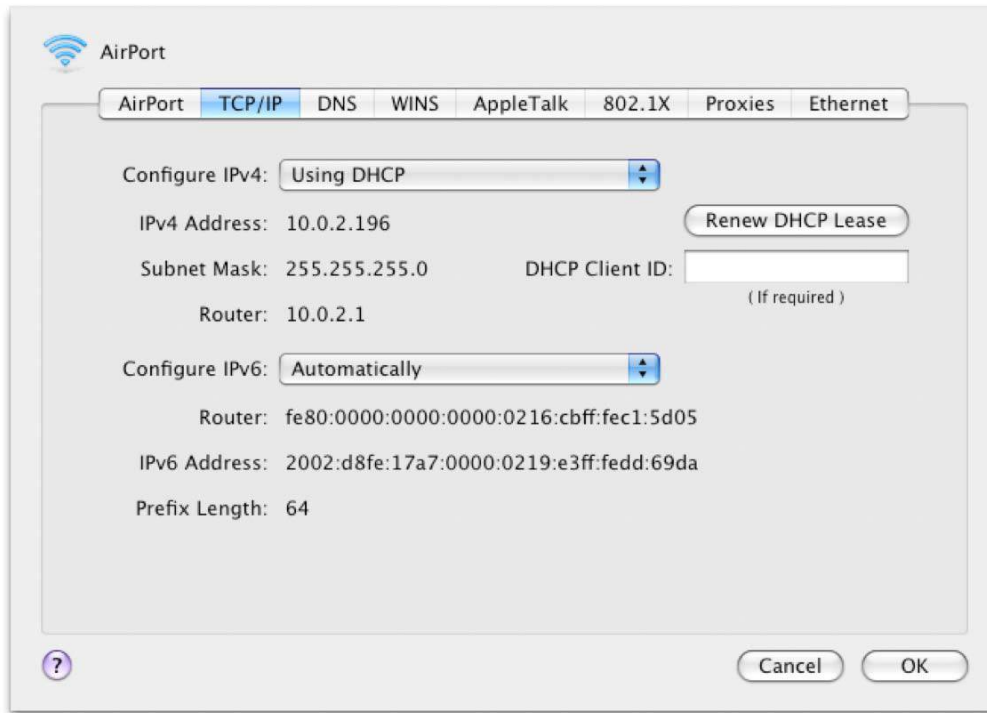
### **In Mac OS X Leopard or Snow Leopard:**

1. Open the Network system preference pane.
2. Switch to the TCP/IP view for any adapter—Wi-Fi or Ethernet (**Figure 44**).



**Figure 44:** Select the adapter from the list at left. For AirPort adapters, you must click the Advanced button to access the TCP/IP button that leads to the TCP/IP settings; for Ethernet, basic options are shown on the main screen.

3. Choose Using DHCP from the Configure IPv4 pop-up menu (Figure 45).

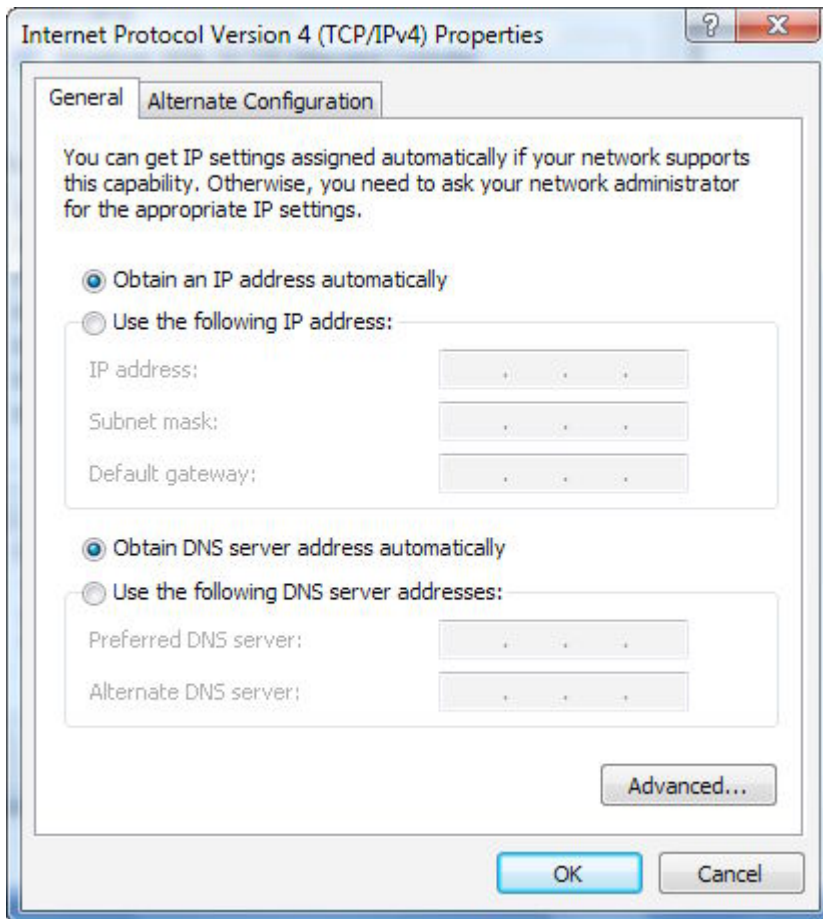


**Figure 45:** In the TCP/IP view for an AirPort adapter, set Configure IPv4 to Using DHCP; this pop-up menu is labeled just Configure on the Ethernet configuration main screen. Mac OS X automatically obtains a dynamically assigned IP address.

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 46**).



**Figure 46:** 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.

### **Refine 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. In most cases, you needn't change anything here, but I cover the options just in case, and for completeness.

#### ***DHCP View***

The DHCP view lets you set the numbers and range of addresses used for DHCP address assignment on your network, as well as a few other DHCP properties. The only reason to change the range of numbers is if you want to create and assign *private* addresses that remain static



instead of being allotted arbitrarily from a large pool when a computer or device requests an address via DHCP.

These statically assigned addresses would start with the first three numbers in the base station's private network range, but you would enter them 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](#), covered two pages ahead.

---

***Warning!*** *The DHCP view has suffered from a lot of surgery over the years, and might be confusing because of how the same information is handled in different ways.*

---

DHCP addresses are drawn from one of three reserved ranges of private addresses—10.0.\*.\*, 192.168.\*.\*, or 172.16.\*.\*. These prefixes are reserved by the global numbering authority, and they are guaranteed to not be in use on any public Internet network.

By default, Apple uses the 10.0 prefix in the DHCP Beginning Address pop-up menu; you can optionally choose either of the other prefixes as follows:

1. Type the third number in the IP address in the field to the right of the pop-up menu. You can enter any number from 1 to 254. The prefix combined with this third number defines your network. If you choose 192.168 and enter 1 for the third number, your network is [192.168.1.\\*](#), where the star represents numbers that can be set on the local network for individual computers and other devices.
2. The fourth number you enter, in the second field to the right of the pop-up menu, defines the starting address for a range of DHCP addresses. Typically, you enter [2](#) here because the router reserves the [\\*.\\*.\\*.1](#) address to itself.

---

***2<sup>8</sup>-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.*

---

The end of the DHCP range used to be a number you picked, but that's changed. Now the DHCP Ending Address field prefills the first three numbers you chose from DHCP Beginning Address. The final number is the only one you can enter, and it may be from any number larger

than the starting address number all the way to 254. Apple, by default, sets the ending address in the range to `*.*.*.200`.

---

***Limited addresses:*** *AirPort Utility prevents you from modifying the first three numbers in the four-number IP address in the DHCP Ending Address field, because those first three numbers must match the first three numbers in the DHCP beginning address. 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 on a computer when the computer receives its DHCP address. (The LDAP Server field is relevant only for networks that use that directory protocol.)

I explain the DHCP Reservations list in [Reserved Addresses](#) (next page).

### ***NAT View***

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 request public addresses from their ISP to use for their LAN computers; this allows each computer to be reachable from the public Internet without any intermediary address translation. In this case, you usually want to configure each computer manually with a static public address 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 a base station to hand out public addresses from a defined range using DHCP.

To configure a base station to assign dynamic public addresses, follow these steps:

1. In AirPort Utility, select the base station at the left, choose Base Station > Manual Setup, 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 the DHCP Beginning and the DHCP Ending Address. The range you specify is limited to the same IP network that the base station uses for its Internet Connection IP address. For instance, if your base station is 218.23.1.200, your range must be within 218.23.1.1 and 218.23.1.255.

---

***Warning!*** Using publicly 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. This makes computers susceptible to direct attacks by ne'er-do-wells—such as sending a bad message to a Web server, even to Apple's personal Web service in Mac OS X.

---

## Reserved Addresses


*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 base station's connection or distribute a range of addresses, but does require DHCP service to be turned on.

**Note:** Reserving an IP address using DHCP first became available with the January 2007 release of Extreme N. The feature was new to Apple, but it's been available in other devices for years. DHCP reservation isn't available for pre-2007 models.

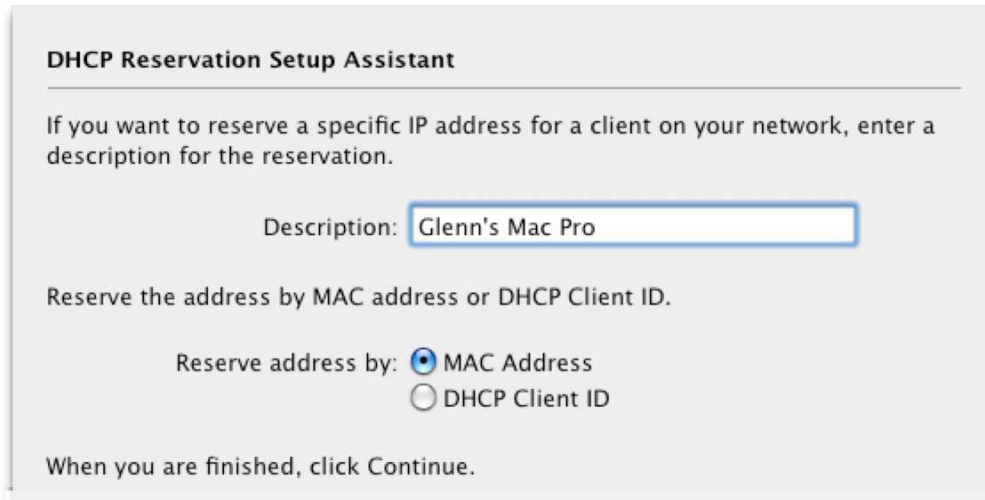
The reserved address is never assigned to another computer, and if the computer in question restarts or shuts down, the next time it powers up and its network adapter is active, it receives its reserved address.

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, select your base station and click Manual Setup. Then, in the DHCP view of the Internet pane, click the  button.

The DHCP Reservation Setup Assistant (**Figure 47**) appears.



**Figure 47:** The assistant lets you set up a reserved DHCP address by MAC address or by DHCP client ID.

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. If you need help locating the MAC address, see [What and Where Is a MAC Address?](#) (p. 97).
  - **If you selected Reserve by DHCP Client ID:** The DHCP Client ID is a text tag that you assign while configuring a Wi-Fi or Ethernet adapter. This text is transmitted when an adapter requests a dynamic address (Windows XP and Vista don't

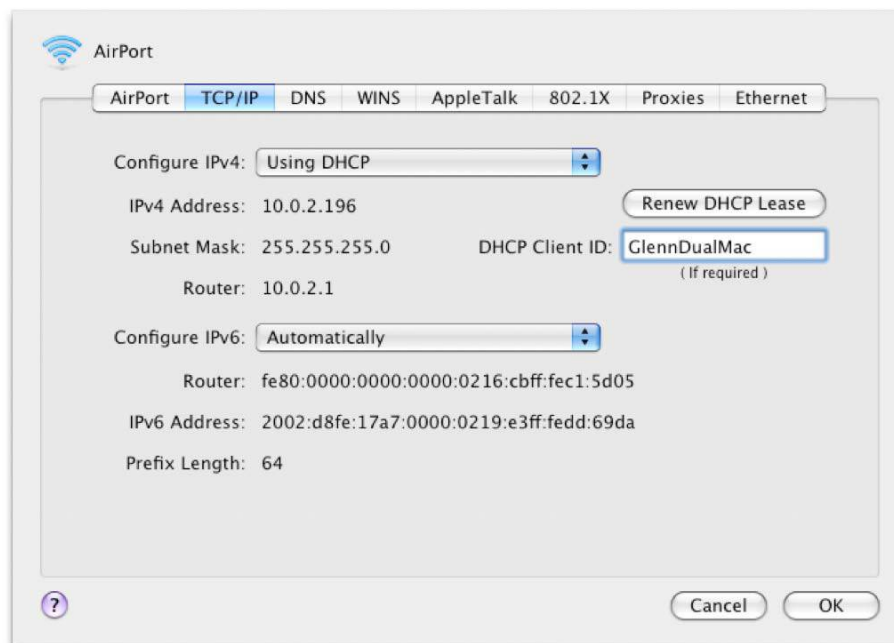
support this), and then the base station can use that tag to assign a reserved IP address:

- a. First set the DHCP Client ID on a client computer running Mac OS X: Open the Network system preference pane, select your adapter, click the Advanced button, and then click the TCP/IP button. Choose Using DHCP from the Configure IPv4 pop-up menu, and enter the DHCP Client ID in the field at the right. **Figure 48** shows the DHCP Client ID set to *GlennDualMac*.

---

**Warning!** To avoid confusing the base station, make sure that DHCP Client IDs are unique.

---



**Figure 48:** The DHCP Client ID field is found in the TCP/IP view when the Configure IPv4 pop-up menu is set to Using DHCP.

- b. In AirPort Utility, enter that DHCP Client ID in the DHCP Reservation Setup Assistant and click Done (**Figure 49**).
5. When you've entered all the reservations, click Update.

This is one of only two operations in AirPort Utility that doesn't require restarting the base station, so you needn't click the Update button after you click Done. The DHCP Reservations list shows the entries you made and any computers listed will have retrieved their new addresses.



**Figure 49:** Enter the same DHCP Client ID in AirPort Utility.

---

***If a Mac still shows its old address:** open the Network preferences pane, select the adapter, and click the Advanced button. Click TCP/IP and then click Renew DHCP Lease. That should blank the IPv4 Address field for a moment, and then the correct address should appear. Click OK and then click Apply if the Apply button is active.*

---

## **Passthrough and Bridging**

For networks in which the base station 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, select your base station at the left, click Manual Setup, and 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 base station 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, turn 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 Snow Leopard, Leopard, Tiger, Windows XP, and Windows Vista to connect to networks, modify stored profiles, and choose when to connect to unknown networks.

---

***Warning!*** Remember that if you set up your network as 802.11n-only in the 2.4 GHz band, neither an 802.11b nor an 802.11g adapter 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 [Compatibility](#) 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 BOTH LEOPARDS

---

You connect in Snow Leopard and Leopard, as with previous versions of Mac OS X, through either the AirPort menu, a status menu near the right of the menu bar, or via the Network system preference pane.

**Tip:** To learn what the different icons for the AirPort status menu mean, consult [AirPort Iconography](#) (p. 17).

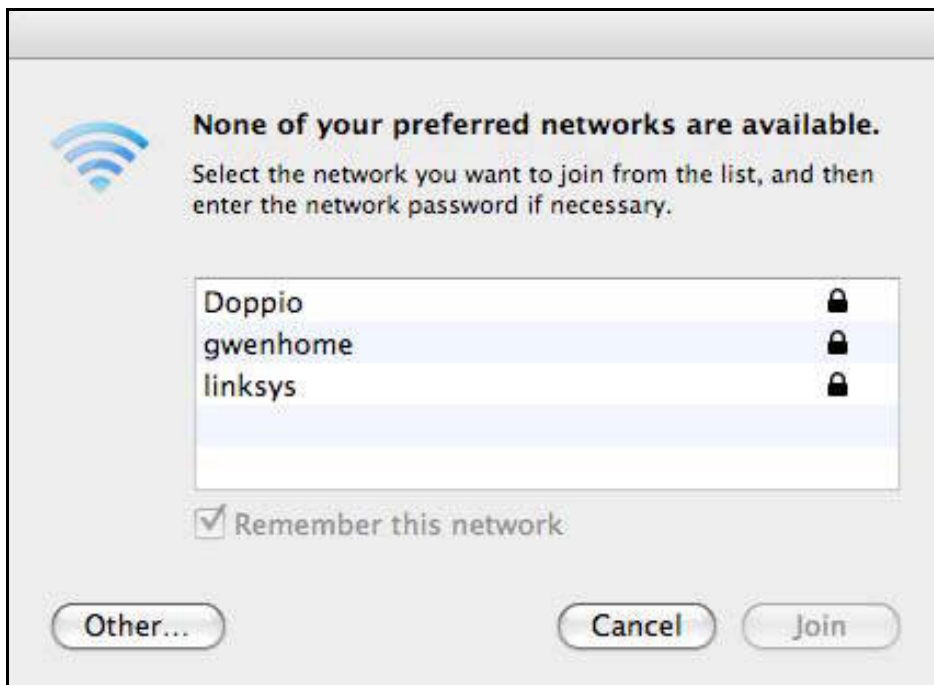
Let's start with how you find a network, proceed to connecting (including options for entering security and encryption information), and then discuss managing profiles.

## Discovery

Mac OS X constantly looks for networks when the Wi-Fi adapter is on, and a list of them appears in the AirPort menu.

**Tip:** If you don't see the menu, launch System Preferences and select the Network preference pane. Select the AirPort adapter at the left, and then check Show AirPort Status in Menu Bar.

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 50**). 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 50:** Mac OS X alerts you to a new network and lets you choose to remember (and thus join it) the next time it appears.

A Mac running Snow Leopard or Leopard automatically joins any network that you've told it to remember, and it optionally alerts you when new networks are available if you're not connected.



It can recognize a new connection when you wake it up or turn it on, 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 the 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 and 2007 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 crucial to keep your software up to date, especially if you use Wi-Fi networks that aren't in your home or office.*

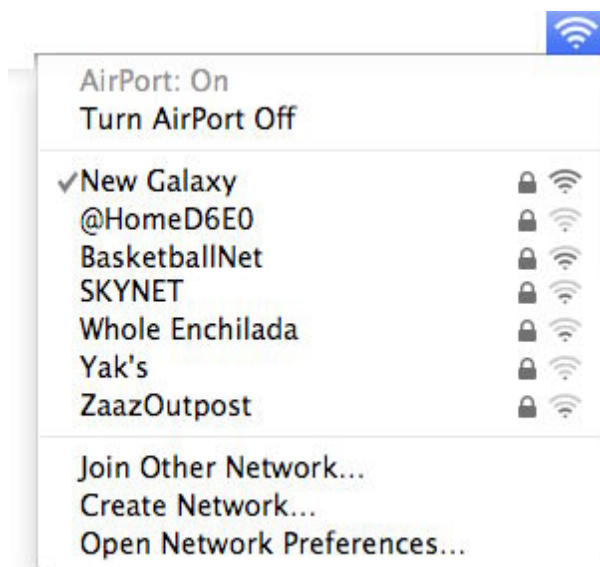
---

## Connect

To connect to a network, select its name from a list, and enter an encryption key if it is secured. Let's walk through connection options.

### Connect to a Named Network

To connect to an AirPort network when the network broadcasts its name—as most do—choose the network name from the AirPort status menu (**Figure 51**). In Snow Leopard, Mac OS X animates the bars in the AirPort icon, lighting them up one at a time in a back-and-forth pattern while the connection is in progress. After connecting, the AirPort menu's icon switches from gray to black, with the number of black waves indicating signal strength by their quantity.



**Figure 51:** Choose a network from the list or choose Join Other Network to join a closed network by entering its name.

I cover what to do next if the network is secured with a key on the next page, and I cover WPS ahead in [Use WPS](#), p. 219.

### Use Diagnostics to Solve Connection Problems

Leopard and Snow Leopard have a feature called Network Diagnostics; if you can't get your AirPort interface to connect to a network, you can get help by clicking Assist Me at the bottom of the Network preference pane, and then clicking Diagnostics.

### Gateway Pages Require Login; Boingo Bypasses for a Fee

At hotspot networks and other open networks, before you can use the 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.

You can avoid this if you use Boingo Wireless, a hotspot access reseller that aggregates access to thousands of networks. With Boingo's Go Boingo software installed, any network that's part of its footprint triggers a pop-up login dialog (**Figure 52**). You can have either a pay-as-you-go account or an unlimited North American \$9.95 monthly subscription. Global and mobile plans are also available (<http://www.boingo.com/>).



**Figure 52:** Boingo's software recognizes a network that's part of its plan and prompts a login.

## Better Band Selection in Leopard

A software update for Leopard in March 2009 (AirPort Client Update 2009-001) paired with a new simultaneous dual-band Extreme or Time Capsule allows your Mac to connect to the best band that's available. When the Mac is close to the base station, 5 GHz is often better due to better throughput. Further away, 5 GHz may work more poorly because signals in that frequency range drop off more rapidly than those in the 2.4 GHz band.

Your Leopard system will automatically and seamlessly switch to the 2.4 GHz radio on your base station if that becomes a better choice. This behavior changes only if you set separate network names for the two bands in your base station, as automatic roaming between bands doesn't occur. (This update is incorporated into Snow Leopard.)

## Enter an Encryption Key (WPA/WPA2 Personal, WEP)

If encryption is active on the network, after you select the network name, you are prompted by a dialog to enter an encryption key (your encryption key is your password) (**Figure 53**).



**Figure 53:** When you attempt to join a network that's protected by an encryption, you're prompted for its password.

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, and then click OK to join the network.

You may have questions about what format to enter the key in, or what to do if the key you have doesn't work. Read on for those details.

---

***Save the key, save time:*** You can choose to store the key in the Keychain by leaving Remember This Network checked; this avoids retyping the password in the future.

---

### **Encryption Key, Password, Passphrase**

In the text that follows, I use three terms that can be a little confusing to distinguish among:

- **Encryption key:** An *encryption key* is the raw material used by an encryption algorithm. The algorithm feeds the key into its set of procedures to turn normal text into scrambled bits, and it reverses the process with the same key (or a paired key in the cases of public key cryptography). A WEP encryption key might look like `AFD7FF88AF`.
- **Password:** A *password* is usually a short set of letters and numbers that are converted in a simple fashion to be used as an encryption key. A password might be `fisheggs`.
- **Passphrase:** A *passphrase*, as I describe it, can be a long stretch of text that passes through a more complex intermediate process to be turned into an encryption key. A WPA passphrase might be, `All G00d1 Men!! Eat St##akkk`; its encryption key equivalent is dozens of bytes long.

You enter an encryption key or passphrase differently depending on how network security was configured. Most networks set up in the last 4 years will use WPA or WPA2 Personal passphrases; older networks could still be using WEP.

WPA/WPA2 Personal has just two ways to enter a key, and you're virtually assured to only encounter only the first:

- **WPA/WPA2 Personal:** Enter the passphrase exactly as it was typed in to the base-station configuration software. 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.*

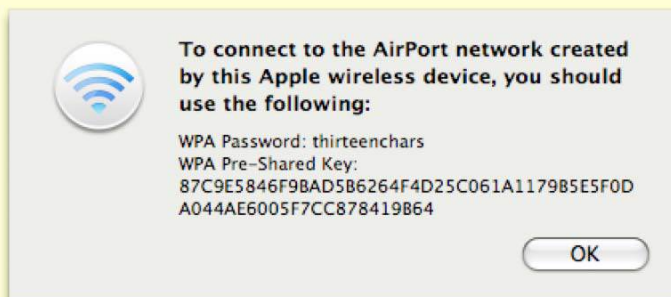
---

**Note:** WPA actually converts a text passphrase into a master encryption key that's then split into several pieces, one of which is used to secure the local network connection. The others are used for purposes like securing network messages that need to be broadcast to a group of computers. The hex key noted below is the whole megillah.

- **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 Leopard or Snow Leopard, hold down the Option key before you select the network from the AirPort menu. An extra large field appears allowing entry. Yes, it's a pain to enter 64 hex digits, and I've never had to. It's there for full compatibility's sake.

### Extracting the Long WPA Key

A vanishingly small number of devices might need you to enter the very long hex key instead of a WPA or WPA2 Personal passphrase. AirPort Utility can show the conversion of the passphrase into a 64-digit hex key. Connect via the utility to your base station, choose Base Station > Manual Setup, and then choose Base Station > Equivalent Network Password (**Figure 54**). You can copy and paste from the dialog, a violation of Apple's interface guidelines—but, hey, they wrote the program. (Pre-Shared Key is another name for WPA/WPA2 Personal.)



**Figure 54:** The horror that is the very long WPA Pre-Shared Key shown in hexadecimal.

WEP is much more finicky, so depending on the network, you may encounter any of three cases:

- **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 "fishy". WEP ASCII keys are 5 or 13 characters long.

---

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

---

### **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 (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 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 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](#), p. 219.

---

**WPS works only with current Apple gear!** In my testing, WPS works only with any of Apple's current Wi-Fi base stations and Leopard or later; base stations from other manufacturers don't seem to match with Apple's implementation of WPS.

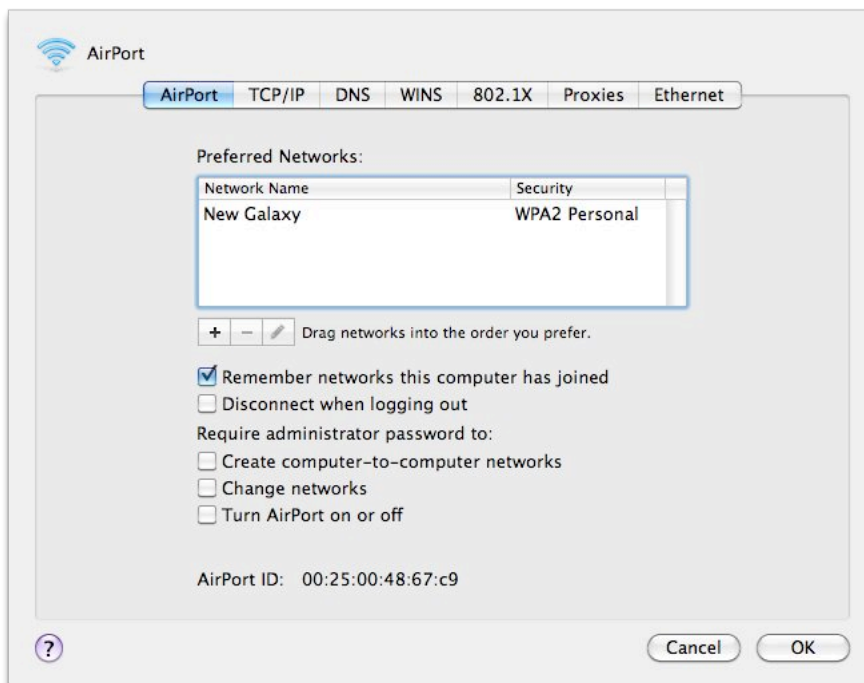
---

### Connect to a Closed (Hidden) Network

For a [Closed Network](#), choose Join Other Network 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.




### Manage Network Profiles

Wi-Fi network *profiles* let you enter and store any needed passphrase, key, or login details to access a network, and you can change those details for a network you've already stored a profile for. Profiles let Leopard and Snow Leopard rapidly reconnect to a network. You can manage Wi-Fi network profiles in the Network system preference pane. Open the pane and select the AirPort adapter; then click the Advanced button to see more configuration options in the AirPort view (**Figure 55**). (**Figure 55** and **Figure 56** were taken in Snow Leopard; in Leopard, the interface is slightly different.)



**Figure 55:** You can add, delete, edit, and rearrange networks with which you want to connect without re-entering details.

To manage your profiles, use the following options:

- Add a profile manually by clicking the  button.
- Delete a profile you no longer need by selecting it 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.
- To edit an existing profile, select it and click the  button; you can change the password or type of password, too (**Figure 56**).




**Figure 56:** With the edit option, you can change the network name, security type, and password without re-selecting the network.

---

**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.*

---

If you click the  button, you can click the Show Networks button. This recursive seeming choice lets you connect to a network within the Edit feature, so you can change details without exiting the nested preference pane that you're in.



## Connection Refinements

To control some of how an AirPort adapter connects to networks, select the AirPort adapter in the Network system preference pane, and choose any of the following options:

- Check Ask to Join New Networks to have Mac OS X alert you when it finds a network that’s not one you’ve stored a profile for (**Figure 57**). (See **Figure 50**, p. 112, for an example of what that alert looks like.)



**Figure 57:** If this checkbox is checked, when Snow Leopard or Leopard spots a new network, you’re asked if you want to join.

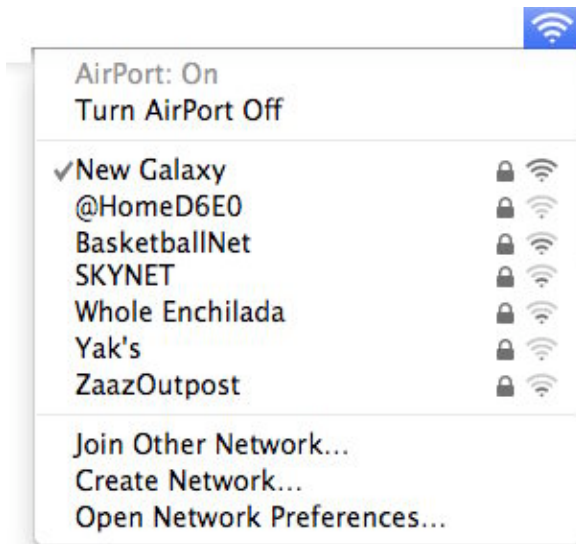
- Click the Advanced button to reach three additional options on the AirPort view:
  - ◇ Remember Networks This Computer Has Joined. Checked by default, this option adds a profile for any network you join, whether a password is required or not.
  - ◇ Disconnect when Logging Out does just that.
  - ◇ The “Require administrator password to” checkboxes allow you to override someone’s attempt to switch networks or turn the AirPort off.

**Note:** If you are using Leopard, your interface labels will be slightly different from those given above.

## Learn from the AirPort Menu

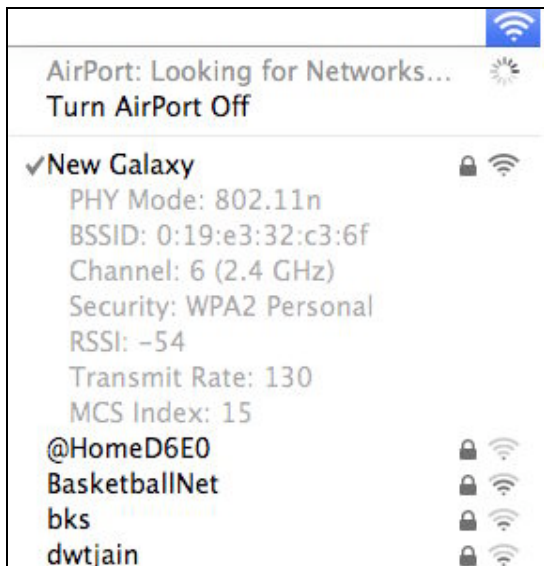
Leopard and Snow Leopard’s AirPort menu is dynamic: Mac OS X scans for networks after you open the menu, adding more to the list as it finds them (**Figure 58**). Networks appear in alphabetical order, with the network you’re connected to coming first. A lock icon appears to the right of *protected networks*—those using WEP or WPA/WPA2.

Snow Leopard added a signal strength indicator to the right of the network name.



**Figure 58:** When you first open it, the AirPort menu shows a progress spinner. It then shows the networks that your Mac has found.

To show more network details in the AirPort menu, hold down the Option key while opening the menu (**Figure 59**).



**Figure 59:** Hold down Option while opening the AirPort menu to see additional details about the network that you're connected to.

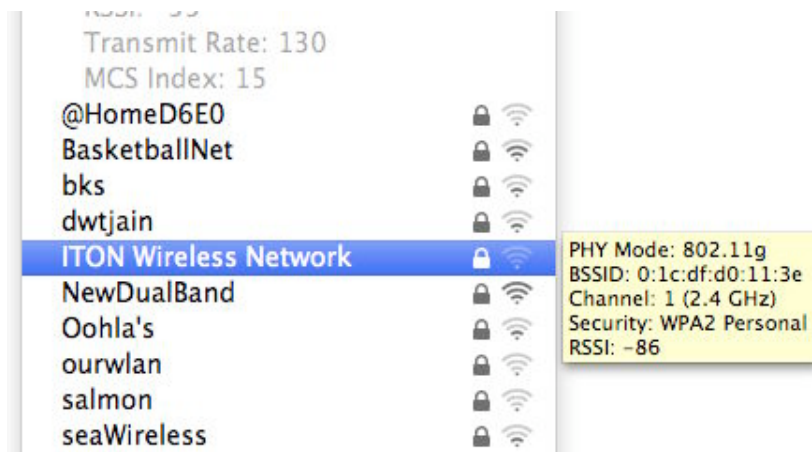
---

**Menu movie:** I demo the Snow Leopard AirPort menu in this YouTube video: <http://www.youtube.com/watch?v=vy3kOpL7tPw>

---

The menu now offers a plethora of data:

- You can see seven pieces of information about the network you've joined:
  - ◇ The *PHY Mode*, or protocol name in use (e.g., 802.11n)
  - ◇ The MAC address or AirPort ID of the network (BSSID), a unique address for each base station
  - ◇ The channel and band in use (e.g., channel 6, 2.4 GHz)
  - ◇ The security method in use, if any (e.g., WPA2 Personal)
  - ◇ The signal strength measured as *RSSI* (Received Signal Strength Indication), which is a relative measure of its quality
  - ◇ The *transmit rate*, which shows how fast the network link is, not just how fast the base station *can* go
  - ◇ The *MCS Index*, a technical item describing encoding method.
- Hover over any other network other than the one you're connected to in order to learn more about it (**Figure 60**). In this case, you see the PHY Mode, MAC address, channel and band, security method, and the RSSI (signal strength).



**Figure 60:** With the Option key held down, you can reveal information about Wi-Fi networks to which you aren't connected.

**Note:** To learn more about RSSI and transmit rate, see [Use the AirPort Menu](#) (p. 89).

---

## CONNECT IN TIGER

---

Mac OS X 10.4 Tiger works much the same as Leopard, but with some cosmetic differences.

### Discovery

Tiger shows available networks in three places:

- The AirPort menu
- The Internet Connect application ([Applications/Utilities/](#))
- The Network system preference pane with the AirPort adapter selected when you add a network profile

The AirPort menu doesn't show signal strength as in Leopard, but holding down the Option key before selecting the AirPort menu sorts the list of networks from strongest to weakest signal.

### Manage 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 system 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 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.

---

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. When you're done, click Apply Now.

## 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.
- Disconnect from Wireless Networks When I Log Out 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, try Tiger's Network Diagnostics troubleshooting feature; click Assist Me at the bottom of the Network preference pane to access the assistant.

---

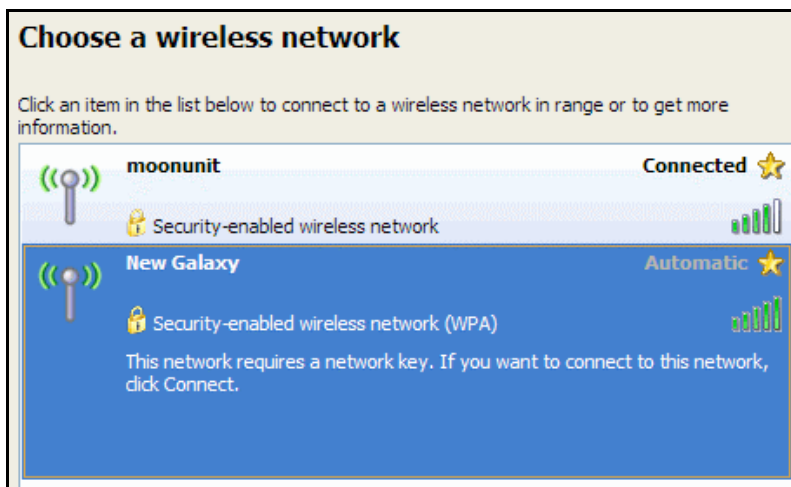
## CONNECT IN WINDOWS XP

---

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 connect a Windows computer 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 61**). This is a big improvement over previous XP releases, which left you guessing.



**Figure 61:** Choose a network from the list, or choose Other to join a closed network by name.

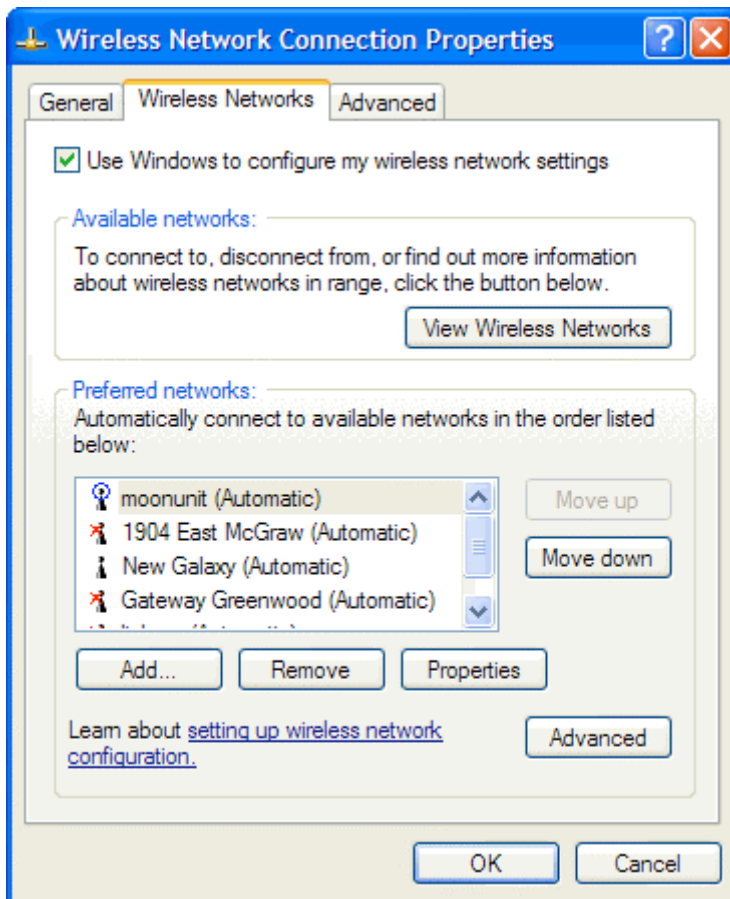
Now, select a desired network and click Connect, at which point you're prompted for any encryption keys needed to join.

### 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.

## 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 box (**Figure 62**).



**Figure 62:** 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.

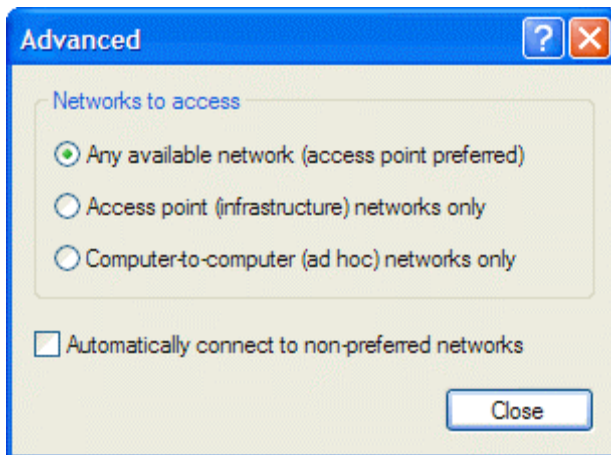
A red x () marks any networks that are not visible.

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 the 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 63**). 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 63:** The Advanced dialog box controls how your computer connects to available networks that it finds.

## Preferred Network Profiles (WPA/WPA2)

---

*WEP encryption? 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 base station!*

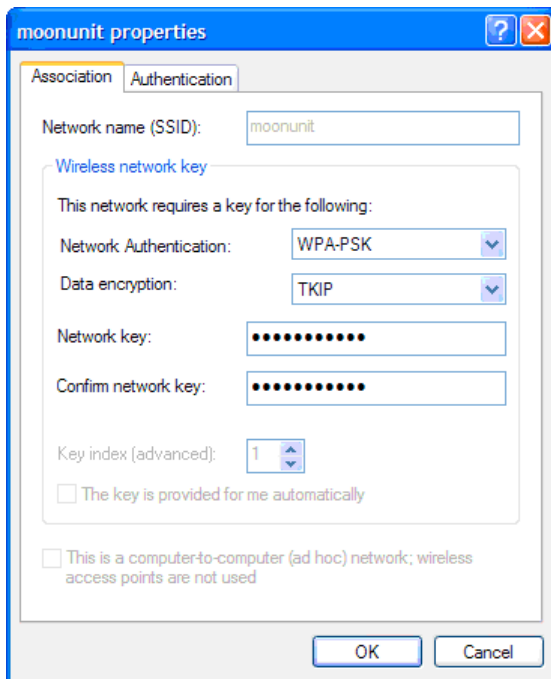
---

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

1. Navigate to the Wireless Networks tab for a Wi-Fi adapter as shown in **Figure 62** (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 (WPA/WPA2) or to AES (WPA2 only) (**Figure 64**).



**Figure 64:** From the Data Encryption pop-up menu, either choose TKIP to allow connections from systems that handle WPA or WPA2 (shown here) or choose AES to limit to WPA2 compatibility.

5. Enter your 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.

---

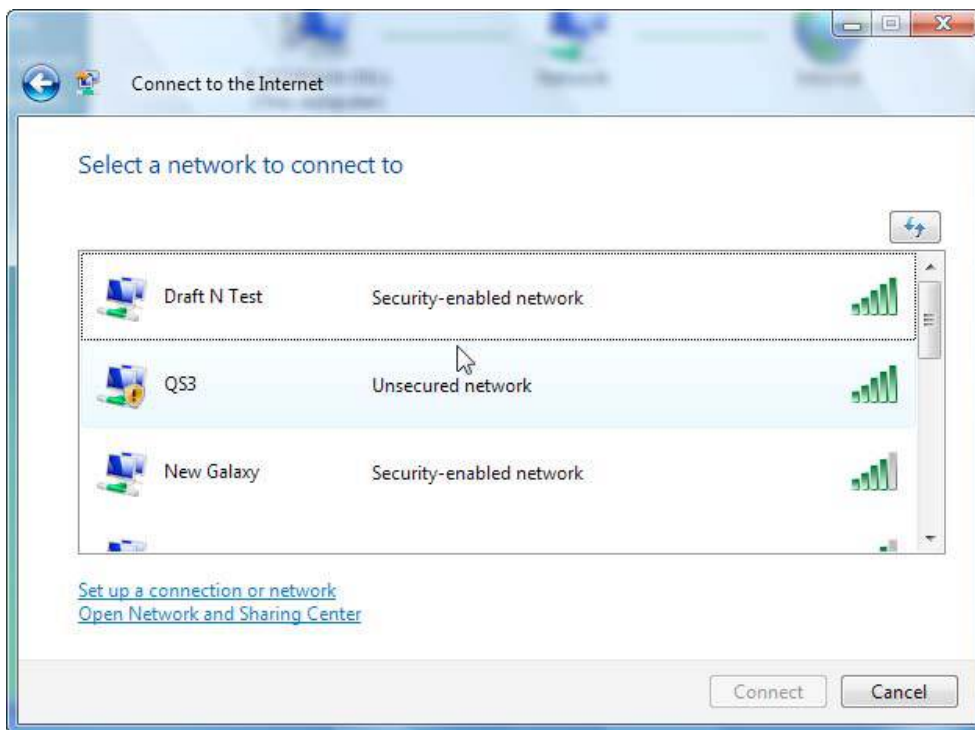
## CONNECT IN WINDOWS VISTA

---

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

### 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 65**). If you hover the pointer over a network, more detail is revealed, such as the type of network encryption.



**Figure 65:** View available networks.

### Connect

Let's connect to a Wi-Fi network with Vista. You can double click a network in the browser shown in **Figure 65** (previous page), 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. Unlike in XP, you need only enter the key once (**Figure 66**)—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.

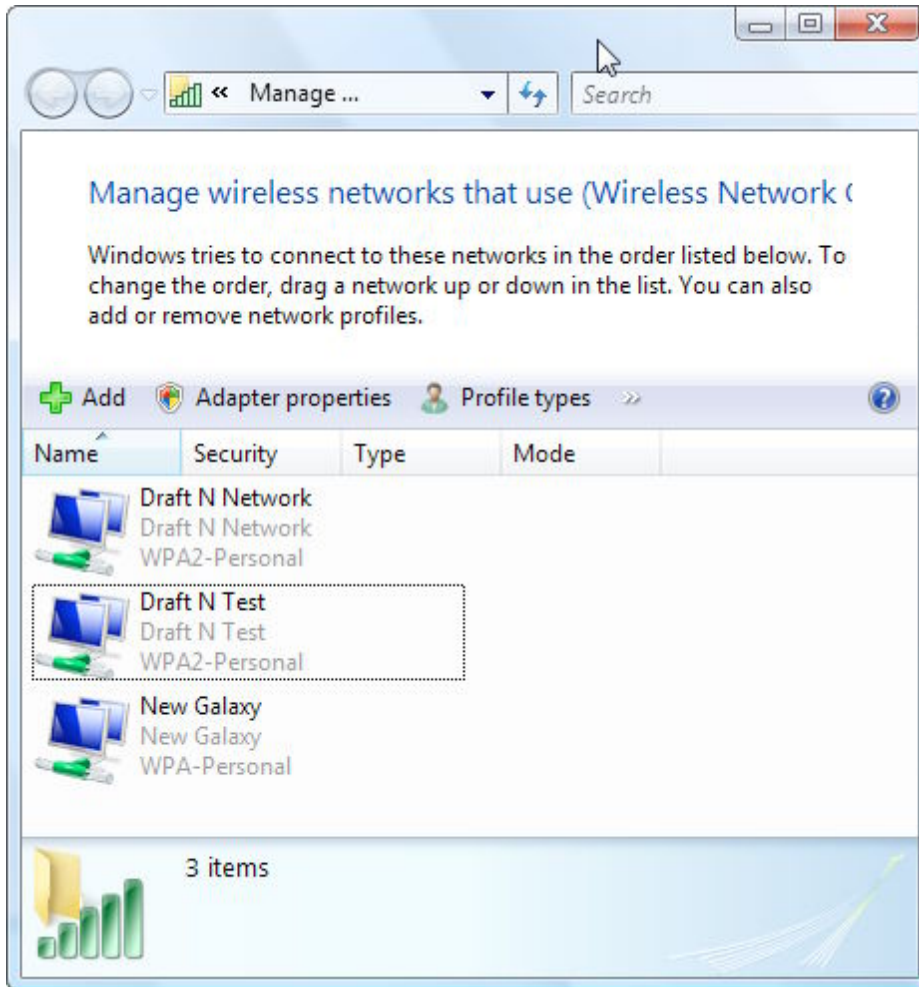


**Figure 66:** Enter the security key to connect to the network.

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

## Manage 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 box is shown in **Figure 67**.



**Figure 67:** 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 stores 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 68**):
    - ◊ 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.

The screenshot shows a window titled "Enter information for the wireless network you want to add". It contains the following fields and options:

- Network name:** A text box containing "Draft N Network".
- Security type:** A dropdown menu with "WPA2-Personal" selected.
- Encryption type:** A dropdown menu with "TKIP" selected.
- Security Key/Passphrase:** A text box with 12 black dots, and a checkbox labeled "Display characters" which is currently unchecked.
- Start this connection automatically
- Connect even if the network is not broadcasting

Below the checkboxes, there is a warning: "Warning: If you select this option, your computer's privacy might be at risk."

**Figure 68:** Set up a manual profile for a network you connect to more than once.

3. Click Next, and then click Close.

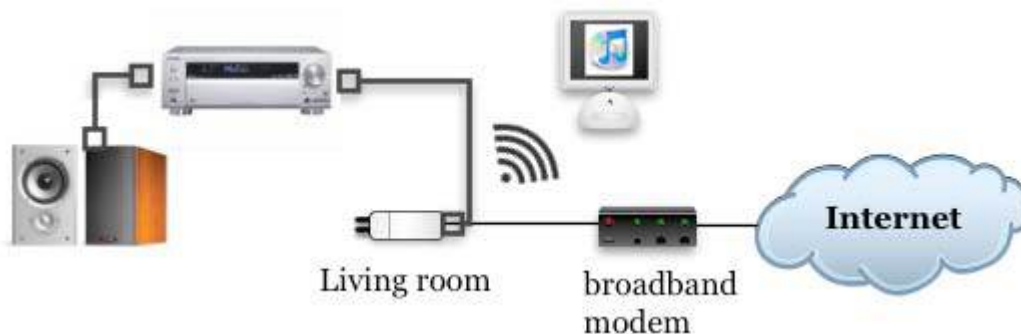
The profile appears in the networks list.

# AirPort Express Extras

The AirPort Express, for its modest size and price, includes several features found in neither a Time Capsule nor an AirPort Extreme Base Station, mostly around music. The Express also hides a nifty connection option for extending a network.

## AIRPORT EXPRESS AND AIRTUNES

AirPort Express includes *AirTunes*, a method of streaming music from iTunes through the audio output port on the base station (**Figure 69**). You control the settings in AirPort Utility and then play the music via iTunes. (AirTunes is also built into Apple TV; see [Appendix A: Apple TV and Wi-Fi](#).)



**Figure 69:** You can stream music from a computer on the network through AirPort Express to a stereo or powered speakers.

**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. See [Share with Airfoil](#), later in this section.

## 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 70**).



**Figure 70:** 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).

---

***No checkbox?** This checkbox is unavailable when you've set the AirPort Express to bridging mode, in which DHCP traffic passes through from the network to which it's connected. In that case, all traffic has to pass over Ethernet already.*

---

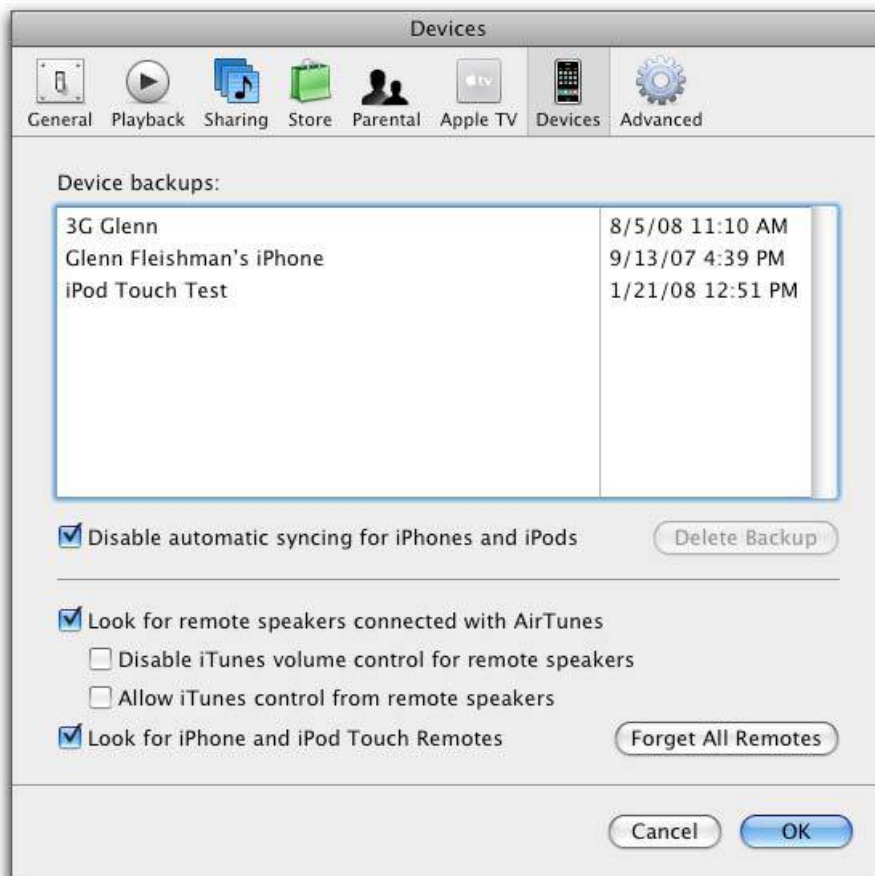
- **iTunes Speaker Name:** This name shows in the iTunes remote speaker list.

- **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 iTunes > Preferences and then click the Devices icon (**Figure 71**). Devices is where you manage backups for an iPhone or iPod touch as well as audio output for an Express.



**Figure 71:** Select Look for Remote Speakers Connected with AirTunes to automatically discover AirTunes-equipped base stations.

2. Verify that Look for Remote Speakers Connected with AirTunes is checked. 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), check Disable iTunes Volume Control for Remote Speakers.



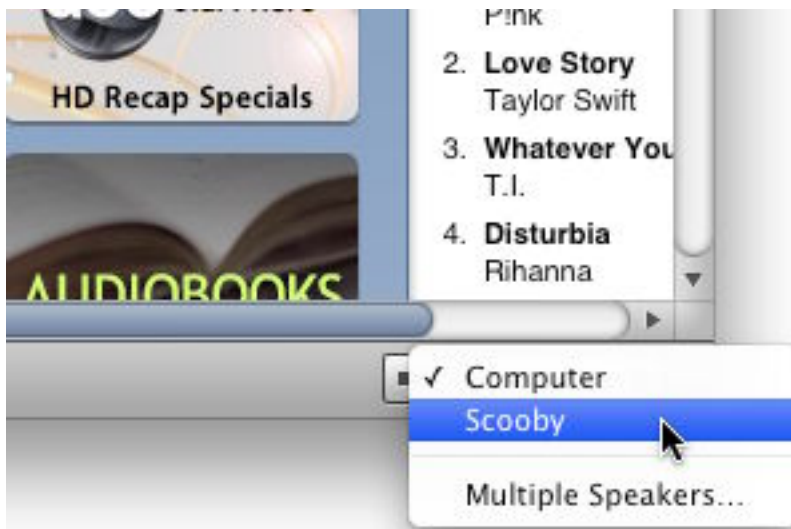
4. A few devices can control iTunes volume remotely, including the Apple HiFi when connected via the AirTunes jack on the AirPort Express. If you care about this behavior, you can check or uncheck Allow iTunes Control from Remote Speakers.

### Use the iPhone/iPod touch Remote App to Control Music

Even though few devices control AirPort Express's volume directly, there's a neat trick if you own an iPhone or iPod touch with 2.0 or later software installed: from the App Store, download Apple's free Remote app, which can connect over a local network to access any copies of iTunes running under Mac OS X or Windows. If a copy of iTunes is set to output its audio via an AirPort Express, then Remote and its volume control for iTunes can effectively handle whatever's coming out of your AirPort Express audio port.

5. Click OK.

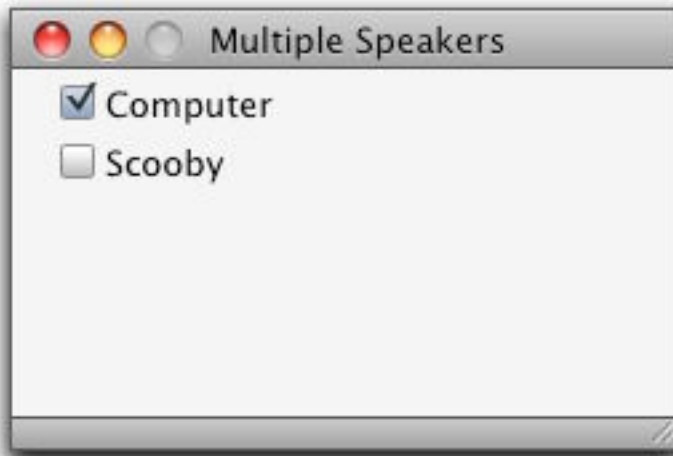
Now that you have a configured AirPort Express on the network and the Look for Remote Speakers Connected with AirTunes checkbox is selected, iTunes should display a new pop-up menu with a speaker icon next to it in the lower right of its main window (**Figure 72**).



**Figure 72:** At the lower right, choose the Express to stream through. A lock appears by those that are password protected.

6. In iTunes, choose a base station from the new pop-up menu. The menu lists all 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 choose 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 (**Figure 73**).



**Figure 73:** The Multiple Speakers window lets you choose one or more speaker sets to stream through.

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. 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.
- **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.

---

## SHARE WITH AIRFOIL

---

Rogue Amoeba's Airfoil software (<http://rogueamoeba.com/airfoil/>; \$25, downloadable demo version) for Mac OS X, Windows, and certain Linux systems lets you stream music from any computer you install their software on to any other computer with their free Airfoil Speakers

software installed, an Express (any model), or an Apple TV. You can choose which devices you stream to.

The advantage here is that you're not limited to iTunes, nor to playing back music only via an AirPort Express or Apple TV.

**Tip:** Airfoil can also play many kinds of video on a remote system.

To use Airfoil with an AirPort Express, follow these steps after downloading and installing the software from Rogue Amoeba:

1. Launch Airfoil. The main screen shows which targets are available on the local network (**Figure 74**).



**Figure 74:** The audio outputs available on the local network.

2. Click the speaker icon to the left of the AirPort Express; in this example, it's SushiExpress, which is protected with a password.
3. If there's a password, you're prompted, and can enter it, just as with iTunes.

Now you're connected. Any music playing on your system is now pumping out of the AirPort Express (**Figure 75**).



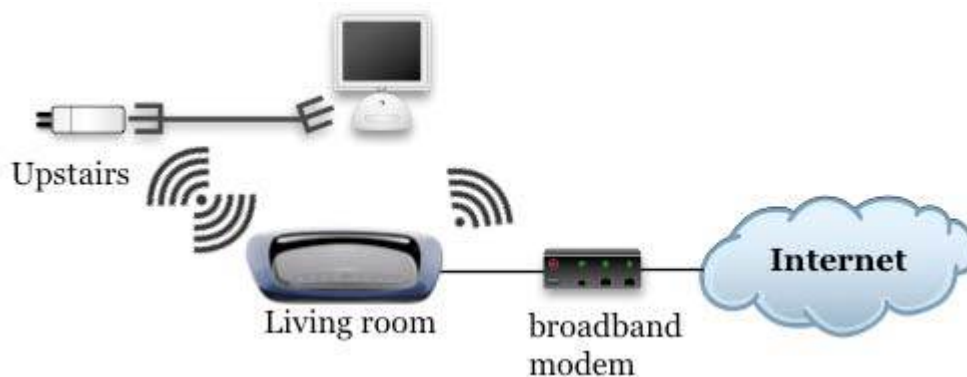
**Figure 75:** The Active label and the blue color in the speaker icon show that the Express can be used to play music.

---

## CONNECT TO ANY BASE STATION

---

The AirPort Express with 802.11n has a special, lightly documented mode that allows it to connect wirelessly to any Wi-Fi network, not just other Apple base stations, and share the connection via Ethernet (Figure 76). This mode, called *ProxySTA* by Apple but not mentioned by that name in Apple's documentation, is handy for using the Express N in circumstances where you can't control how the network works.



**Figure 76:** An AirPort Express (located upstairs here) can connect to any Wi-Fi network (such as the one from the living room shown here), and then share that network via its Ethernet port.

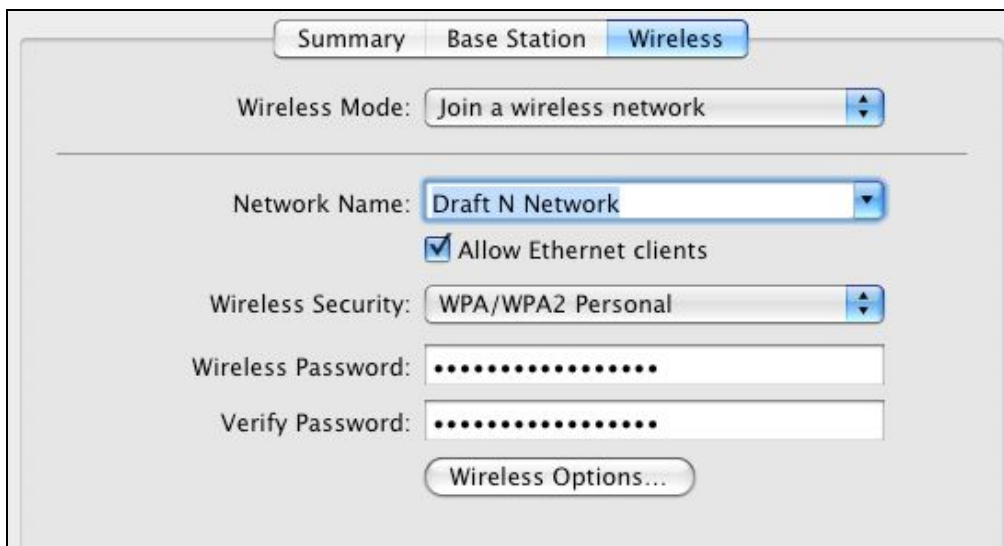
**Note:** The term ProxySTA refers to the base station acting as a *proxy*, a kind of intermediary, between your computers and a Wi-Fi network; and acting as a *station*, the technical 802.11 term (abbreviated *STA*) for an adapter. An *adapter* connects to what we and Apple call a base station, but which is known more precisely as an *access point (AP)*.

***Music streaming and printer sharing:*** These functions work no differently with ProxySTA than they do when you use them with Wireless Distribution System (WDS) or connect the base station via Ethernet to the rest of a network.

With ProxySTA, Ethernet clients—computers connected directly or multiple computers connected via an Ethernet switch—must obtain a DHCP address through a passthrough connection on the network that the Express has joined.

To use ProxySTA mode, follow these steps:

1. Launch AirPort Utility, select the Express N, and click Manual Setup.
2. Select the AirPort view, and click the Wireless button.
3. From the Wireless Mode pop-up menu, choose Join a Wireless Network (**Figure 77**).



**Figure 77:** Choose a network and enter its password, if any.

**Note:** Although you can choose Join a Wireless Network for an AirPort Extreme or Time Capsule by holding down the Option key before clicking Wireless Mode, it's not very useful. On those other two models of base station, joining only makes available shared hard drives and printers to the rest of the network; it doesn't bring access to those base station's Ethernet ports. It's in place for very remote cases in which it might be vaguely useful.

4. Choose the network from the Network Name pop-up menu (or for a closed network, type in a network name), choose the appropriate security method, enter the network's password, and re-enter it for verification. (AirPort Utility fills in the password if it's a network you've previously joined chosen to remember on this computer.)
5. You can check or uncheck the Allow Ethernet Clients box. Unchecking it still leaves printer sharing and music streaming over AirTunes available, if you're using the Express for either or both purposes.

**Note:** Why extend a network and not allow Ethernet clients? If you were using the Express solely for music streaming or printer sharing. This seems unlikely, but Apple predicts every need!

6. Click Update.

Now your Express N is connected to the Wi-Fi network, and any computer connected to its Ethernet port, or via an Ethernet switch plugged into its Ethernet port, can access that Wi-Fi network, and, presumably, the Internet via that Wi-Fi network.

# Connect Multiple Base Stations

Wi-Fi is described as reaching “only” about 150 feet, which is a rough estimate of the radius of older B and G devices. With an 802.11n base station, the distance can be much farther, although it varies by which band you choose.

But you can 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 important 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.

---

## KNOW THE BASICS

---

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 gateways.

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. Ethernet requires wires, of course, but has a huge speed benefit over wireless extensions.
- Add base stations wirelessly via Wireless Distribution System (WDS). This method avoids new wires, but can have severe speed limitations over Ethernet.

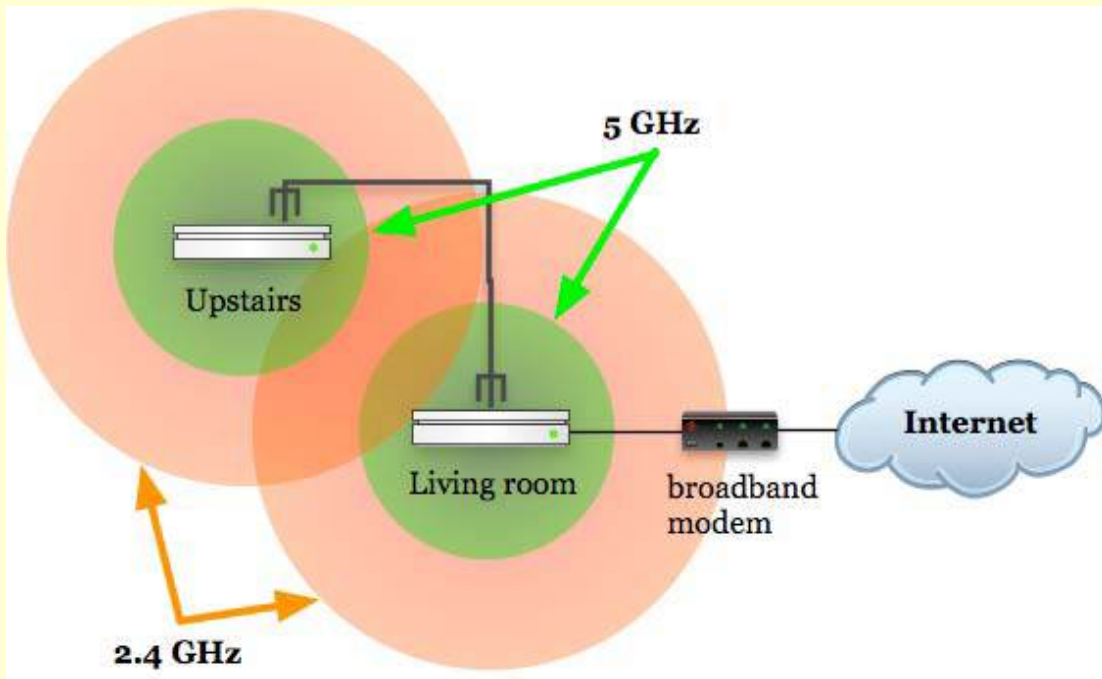
I write “mix and match,” because you can use any combination of Ethernet and WDS to build a network. Let’s start with the simpler case, which is extending a network via Ethernet.

**Note:** The ProxySTA mode of extending an existing Wi-Fi network with an Express N is another method, but it has its limits: it works only with a 2008 model AirPort Express, and it allows only the extension of the network via the Ethernet port on the Express. In contrast, linking base stations with Ethernet and WDS creates a larger and full-featured LAN with both Wi-Fi and Ethernet connectivity. See [Connect to Any Base Station](#), a few pages earlier, for details on ProxySTA.



## Spectrum Differences

The simultaneous dual-band base stations Apple released in March 2009 complicate planning a network of base stations because the two spectrum bands have different coverage areas. In **Figure 78** you can see a coarse look at the how the 5 GHz and 2.4 GHz ranges compare.



**Figure 78:** You can overlap just one band and still gain seamless coverage.

In the figure, note that the 2.4 GHz networks overlap in coverage, while the 5 GHz networks do not. This should work just fine because all your devices can either use only the 2.4 GHz band or can roam from 2.4 to 5 GHz and back again—as long as all the base stations and bands share the same network name. (I explain how to set this up next).

On each simultaneous dual-band base station, if you name the 5 GHz network with a different name than the 2.4 GHz network, then roaming will fail when you wander in an area where neither 5 GHz network has coverage.

---

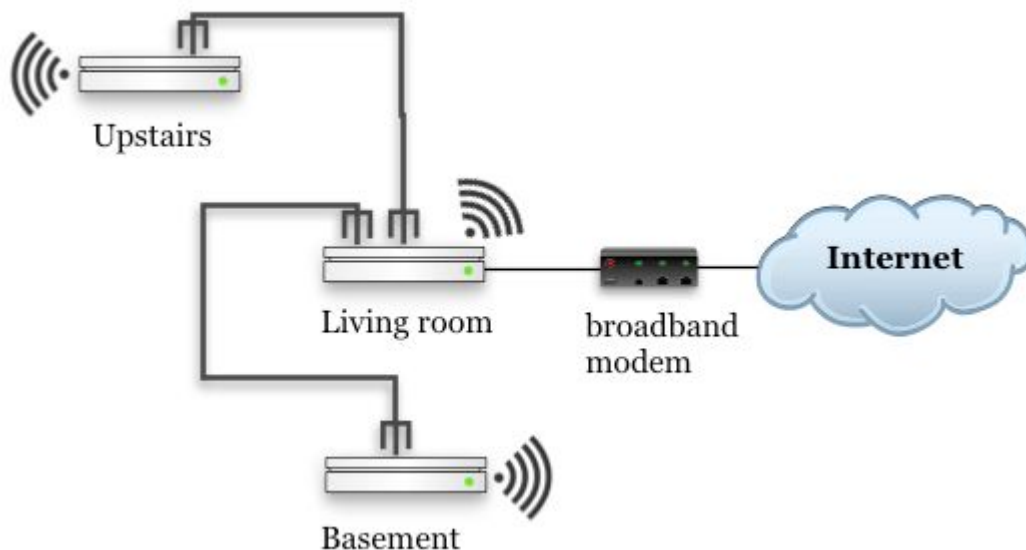
## ADD ACCESS POINTS VIA ETHERNET

---

The advantage of Ethernet is that you get the best possible speed between Wi-Fi clients connected via base stations to other computers, and among Ethernet-connected computers on the network. Using Ethernet lets you set each base station's 2.4 GHz and 5 GHz channels differently, allowing separate spectrum for each base station.

When you add access points that are intended to be part of the same Wi-Fi network, 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.

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 79**). 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 79:** A common Ethernet backbone connects one base station in the living room, another upstairs, and a third in the basement.

---

*Different names for seamless networks: In [Mix 2.4 GHz and 5 GHz 802.11n Networks](#), I advise you to set different network names for the old and new networks if you're trying to restrict certain kinds of devices to certain networks, such as keeping all 802.11n gear on the 5 GHz network. However, when adding access points to grow a single network, you keep the same name for all base stations and all bands so that the connecting computers see the network as a single entity.*

---

## Set Up a Main Wired Base Station

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

You have two options for proceeding:

- Let the base station automatically choose the channel it analyzes as best, based on a lack of interference from other networks or signals.
- Manually assign the channel, taking care to avoid overlapping with other base stations you're setting up and other nearby networks.

It's probably worthwhile to try the automatic approach because it requires the least work and is likely to choose the best channels.

If you're not getting the range you want—especially in the 5 GHz band—follow the directions in [Pick Compatibility and Optionally Set a Channel](#). As discussed in [Channels](#), you want to choose among channels 1, 6, and 11 in the 2.4 GHz band for overlapping base stations, and one of the upper four channels for 5 GHz to get the highest signal strength. (The lower four 5 GHz channels broadcast at 1/20th the strength of the highest-numbered channels.)

## Set Up Additional Wired Base Stations

Adding additional access points is straightforward:

1. Launch AirPort Utility, connect to the additional base station that you want to configure, and choose Base Station > Manual Setup.
2. In the Internet pane's Internet Connection view, choose Using DHCP from the Configure IPv4 pop-up menu and Off (Bridge Mode) from the Connection Sharing pop-up menu. (The main base station will handle distributing addresses, including to this additional base station.)

3. In the AirPort pane, switch to the Wireless view.
4. Enter the same Network Name as your main base station (this enables seamless roaming).
5. As with the main base station, either leave channel selection set to Automatic or you can choose a fixed channel. If you want to choose a channel, see [Pick Compatibility and Optionally Set a Channel](#) for specific directions, and choose in this manner:
  - For the 2.4 GHz band (B, G, or N), any three base stations can uniquely use channels 1, 6, and 11 with the least interference wherever signals overlap. If you set your main to 1, set an additional one to 6, for instance.
  - In the 5 GHz band (A or N), none of the channels are overlap. But with the “wide” channel mode, a base station 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. Pick 149 and 157 for the strongest signal.

**Tip:** As noted earlier in the section, you can set up overlapping 2.4 GHz networks where 5 GHz network coverage doesn't extend. In that case, you don't have to worry nearly as much about reusing the same channels in 5 GHz.

6. Choose the same Wireless Security option and enter the same Wireless Password as on your main base station.
7. Click Update to restart your base station with the new settings.
8. 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! For several years, electronics makers have been creating ever-faster *powerline networking* systems in which data is encoded as a component of the alternating current power that flows through homes and offices. The current fastest flavor is 200 Mbps.

With powerline networking, you typically use Ethernet wall plugs. Connect a computer or Ethernet switch into the network port on one of these bridges, and then plug the bridge into the wall. All similar bridges plugged into other sockets extend the network by communicating with all the other bridges.

There's no one standard, but the HomePlug Powerline Alliance has the only widely available standard that allows products to be certified to work together, sort of like Wi-Fi. A typical HomePlug offering is the Zyxel PLA401 (200 Mbps) sold as a pair for \$120 at [Amazon.com](https://www.amazon.com) (**Figure 80**). Trade off this price with the cost of adding a base station or installing Ethernet (professionally or by yourself). The additional advantage of powerline networks are that you can move the end points wherever you want.

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 powerline Ethernet bridges. And that's it.

Powerline networks must be plugged into wall sockets, not power strips, and they're often quite big wall warts.



**Figure 80:** The Zyxel PLA401 powerline adapter viewed on end.

---

## BRIDGE WIRELESSLY

---

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

Apple offers two flavors of WDS: *dynamic WDS*, which works only with 802.11n base stations models released in 2007 or later, and which requires minimal configuration; and *static WDS*, which is required for all the 802.11g base stations models released from 2003 to 2006, which uses many more fussy settings, and which newer base stations are backward compatible with. Apple doesn't use these terms in its manuals or products, but that's how the company describes the two forms of WDS.

### Mixing up Ethernet-Backed and WDS Networks

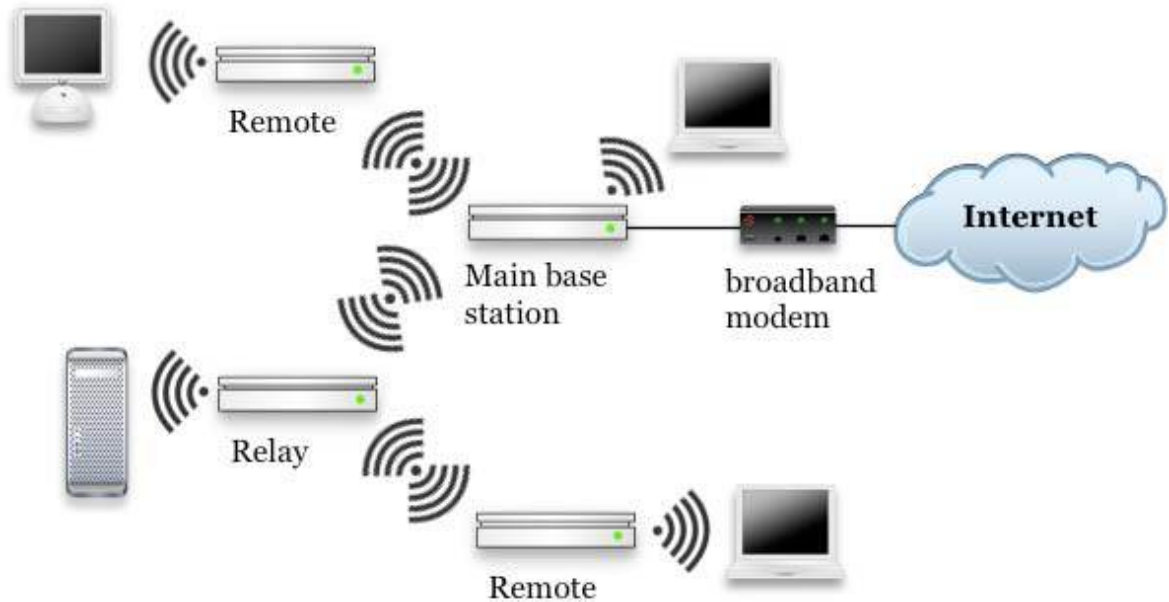
You can mix and match WDS with Ethernet-extended networks, too. Each cluster of WDS machines can work together, and then the "main" base station in that group—see below—can hook into a larger network via Ethernet as an additional base station.

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

Both dynamic and static WDS work 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 81**).



**Figure 81:** A main base station hands off access to remotes and relays, which in turn allow computers to connect.

All base stations must be in range of one another for WDS to work in either mode. With the simultaneous dual-band base stations, dynamic WDS tries to connect over both bands; if just one band can be reached on another device, the base station will still connect.

If you're not sure whether one base station can see another, use a laptop to test reception for a given location with an active base station. Base stations have far better antennas than laptops do, so even a marginally functional laptop Wi-Fi link suggests that you'll be able to use a WDS connection.

## WDS Downside

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, and because all WDS base stations are on the same channel, no base station can “talk” while another is “speaking.”

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.

This problem is especially bad if you have one 802.11g client that’s far enough away to operate at a slower speed, like 10 Mbps. You get half that speed for the overall network.

## 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.

## Distribute Wirelessly

If you have all 2007-or-later 802.11n base stations, your best bet is to use dynamic WDS. If you’re using a mix of older and newer base stations, skip ahead two pages to [Configure Static WDS](#).

---

***Not sure when your base station was released? Refer to [Table 2](#) and [Table 3](#), pp. 33–34, to match models, features, and dates.***

---

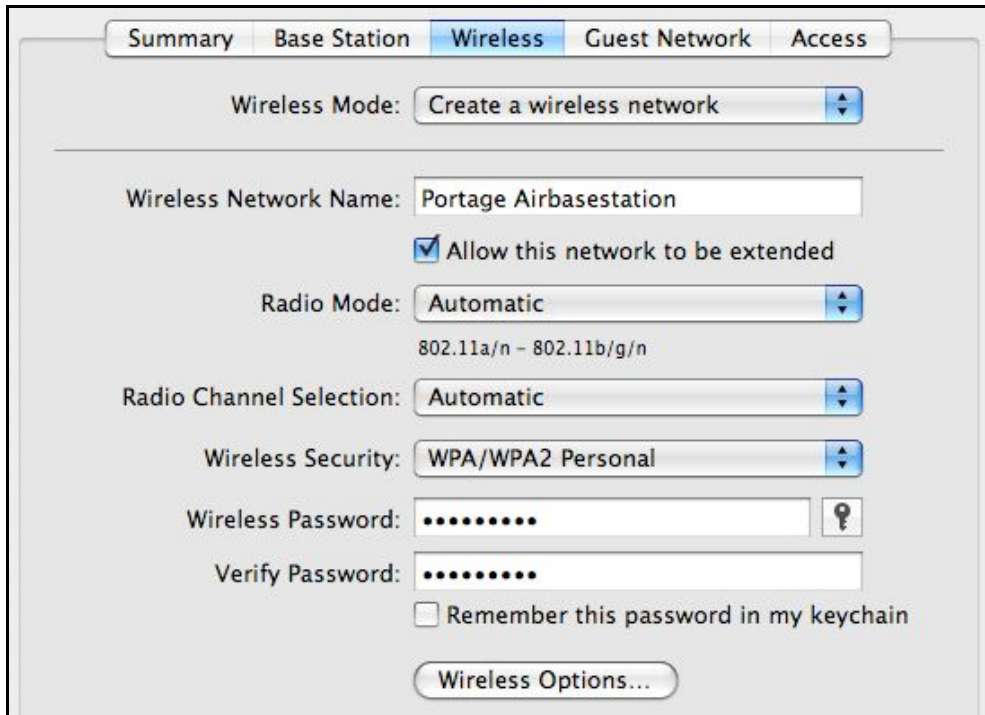


## Configure Dynamic WDS

With dynamic WDS, you change just a few settings to make a wirelessly connected network.

### Configure the main base station:

1. In the AirPort Utility, select your main base station and click Manual Setup; then in the toolbar, click AirPort.
2. In the Wireless view, choose Create a Wireless Network from the Wireless Mode pop-up menu (**Figure 82**).



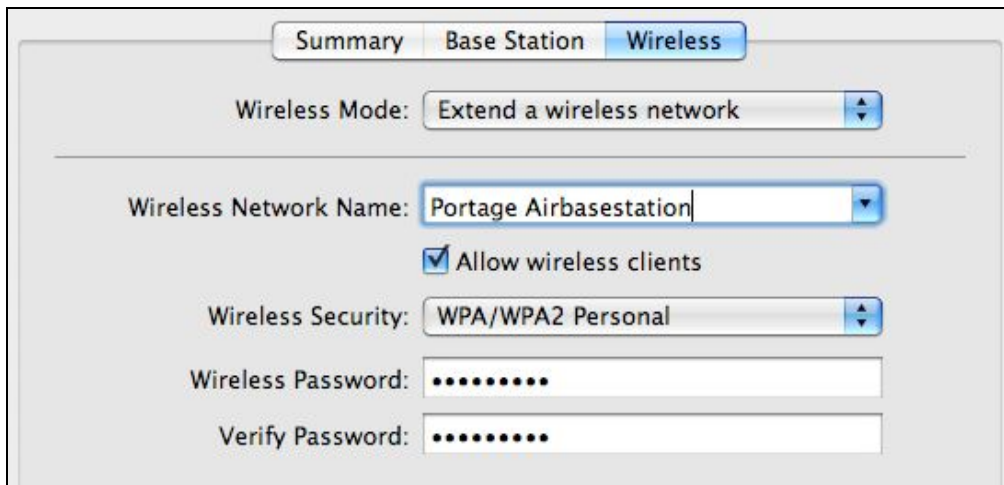
**Figure 82:** Set up a main base station by letting it create a network and allow its extension.

3. In the same view, check Allow This Network To Be Extended.
4. Set other base station options, such as wireless security.
5. Click Update to restart the base station with those settings.

### Configure additional base stations:

1. In AirPort Utility, select the appropriate base station and click Manual Setup; then in the toolbar, click AirPort.

2. In the Wireless View, choose Extend a Wireless Network from the Wireless Mode pop-up menu (**Figure 83**).



**Figure 83:** Other base stations connect back to the main by its network name, and can optionally allow Wi-Fi connections from clients.

3. Choose the Wireless Network Name from the pop-up menu, or enter a name if you're joining a network that's closed (not broadcasting its name).
4. Check Allow Wireless Clients if you want the base station to be available via Wi-Fi, not just to Ethernet-attached computers.
5. Set your Wireless Security choice and Wireless Password to be identical with your main base station.
6. 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.)

**Note:** It may take a moment after restarting for the base stations to find each other because each base station has to scan for other base stations. This is true even if you set the main base station to fixed 2.4 and 5 GHz channels.

### Configure Static WDS

The legacy version of WDS lets you connect 802.11n and earlier 802.11g base stations together. This isn't advised because of the huge speed drop. Nonetheless, here's how to do it.

In static WDS, 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 can serve as either remotes or relays. *Remotes* convey traffic to and from client devices, whereas *relays* connect a main and a remote. Relays can't connect to relays; remotes can't connect to remotes.

The limit is four remotes connected to each of four relays which connect to one base station, or 21 base stations. That's theory; in practice, bandwidth would far too constrained.

To start this configuration, you need to get organized:

1. Decide on the network name (SSID), spectrum band and channel, and encryption choice and password. Whatever you decide, you will be entering it identically for each base station in your network.
2. Use AirPort Utility or physically examine each base station to collect each AirPort ID, the unique network identifier for each base station (see [What and Where Is a MAC Address?](#), p. 97).

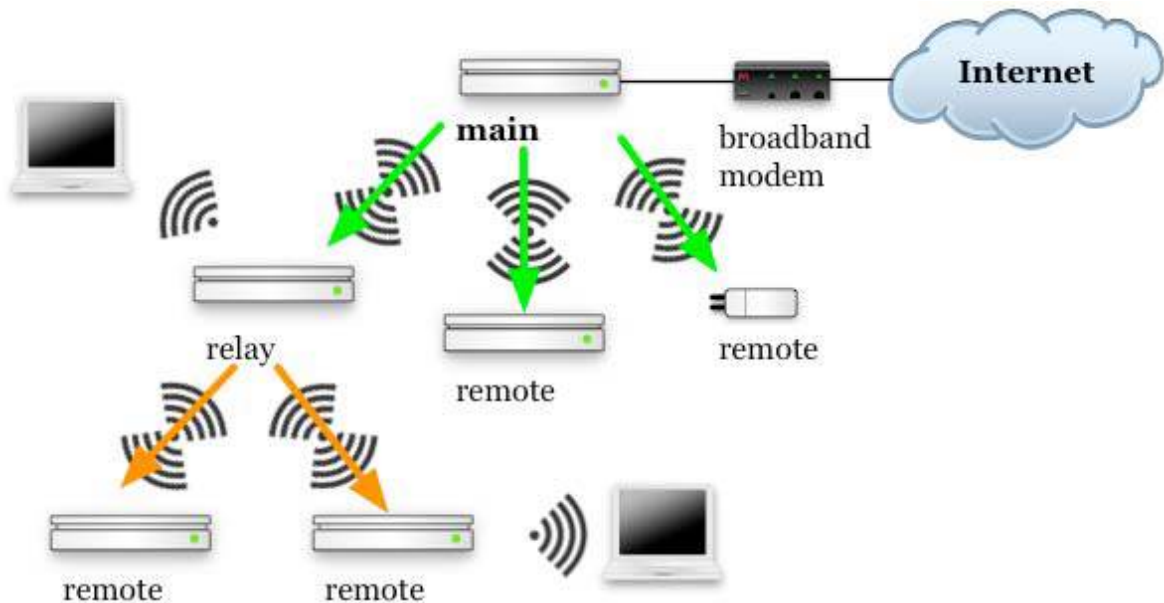
Now that you're organized, launch AirPort Utility and follow the steps below, repeating for each base station in a WDS network. Start with the main base station and then do the relays that connect to the main. This way, other base stations, when configured, will automatically connect to the main or relay when they reboot.

1. Select a base station to configure, and click Manual Setup.
2. In the AirPort pane, click the Wireless button.
3. Hold down the Option key and then select 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. Set the Allow Wireless Clients checkbox:
  - If client computers should be able to connect to the network via Wi-Fi using this base station, check the box.
  - Otherwise, don't check it; the base station will act as a conduit only.

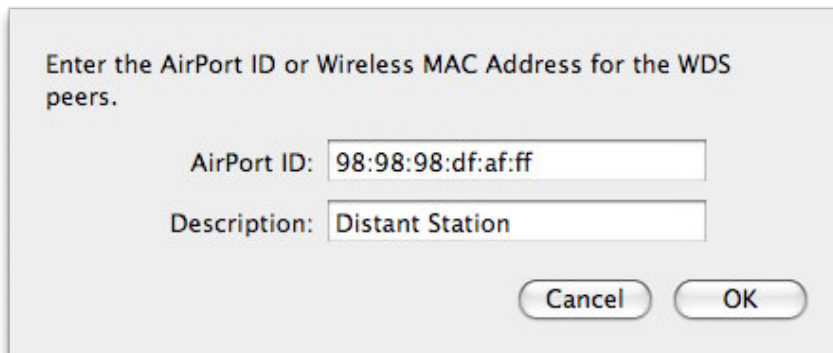
6. Set radio mode, channel, base-station password, wireless security method, and wireless password as you decided before starting, identically for every base station on the network:
  - In the AirPort pane, in Base Station view, set the Base Station Password.
  - In the AirPort pane, in the Wireless view, set the remaining items: Radio Mode, Channel, Wireless Security, and Wireless Password.
7. In the WDS view, you need to enter a value depending on the kind of base station you're configuring in this pass (consult **Figure 84**—and the list on the next page—to understand which values to enter):



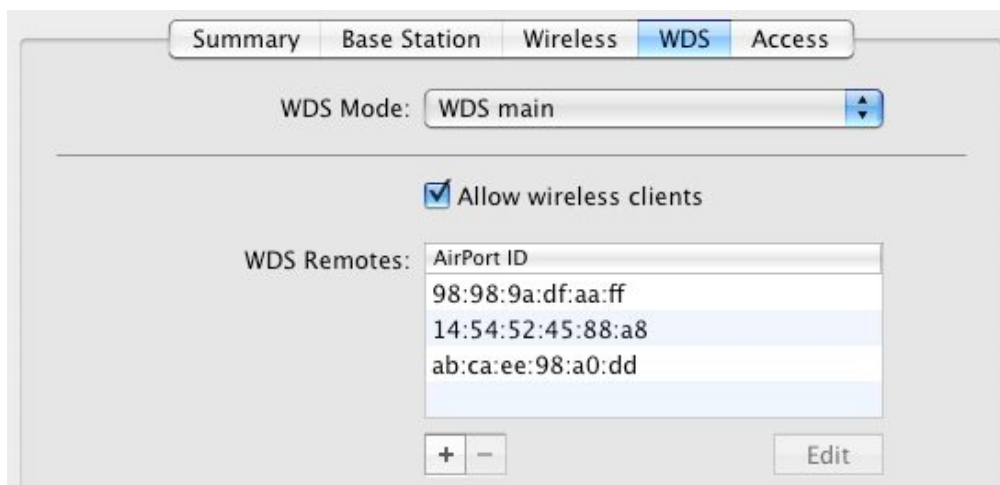
**Figure 84:** When setting up a WDS network, to configure the main base station, you enter only the MAC address values for the remote or relay base stations that directly use the main base station as a conduit. Here, those are connected by green arrows; likewise, those base stations use the main base station's MAC address as their conduit.


For a relay, you enter only the MAC addresses of remotes that directly use the relay as a conduit, shown here connected by orange arrows; and, similarly, the remotes use their relay's MAC address as their conduit.

- **Main base station:** Click the  button at the bottom of the WDS Remotes list to enter the AirPort ID of up to four base station(s) that you want to add as either relays or remotes (**Figure 85, Figure 86**).
- **Remote base station:** In the WDS Main field, enter the AirPort ID of the next-upstream device that the remote connects to wirelessly. This could be the main base station or a relay base station. That's the only value to enter.
- **Relay base station:** In the WDS Main field, enter the AirPort ID of the main base station and use the  to enter the MAC addresses for up to four WDS remote base stations that will connect to this relay.



**Figure 85:** Add a base station to the WDS list on the main base station.



**Figure 86:** When configuring a main base station, click the  button to enter up to four base stations 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 a base station 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 2.4 GHz and 5 GHz 802.11n Networks

In earlier editions of this book, this section was crucial, because many readers had older 802.11g gear (AirPort Extreme 2003–2006 or AirPort Express 2003–2007), and wanted to add a new 802.11n base station into the mix. I suggested that running one 2.4 GHz network using older equipment and one 5 GHz network using a newer base station was a great mix.

Apple made this option somewhat unnecessary in March 2009 by introducing simultaneous dual-band base stations that combine both bands in one box, and eliminate configuration hassles. However, if you're using newer and older gear, or have an AirPort Express base station in the mix—the Express offers only one band at a time—this technique could still be useful.

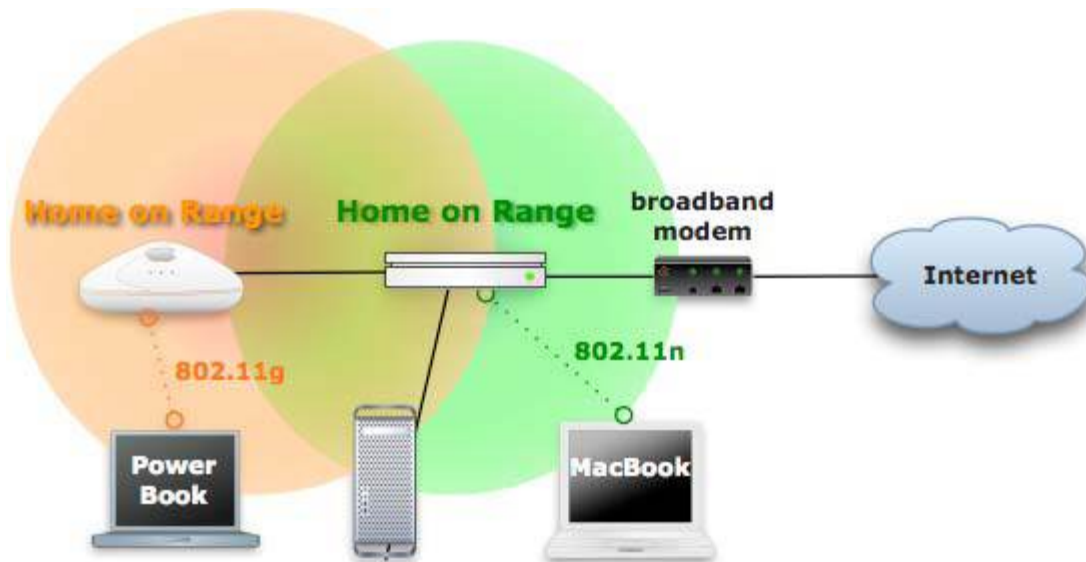
---

## KNOW THE GOAL

---

Setting up a two-band network isn't hard, particularly because the Extreme N and Time Capsule models have an Ethernet switch built in. The goal state for the network is shown in **Figure 87**.

To set this up with two base stations, you'll want a one-band-at-a-time Extreme N (2007 or 2008) or Time Capsule (2008) as your 5 GHz base station, and either an older 802.11g spaceship styled AirPort Extreme or any generation of AirPort Express as your 2.4 GHz base station.



**Figure 87:** 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.

### **AirPort Express Works Only as Extension**

In **Figure 87**, you see that the Extreme N acts as the interface between the broadband modem and the older network. This works because the Extreme N has a three-port Ethernet switch built in. (Four, but one is devoted to the WAN connection.) Because an Express N has just a single Ethernet port, that model can't act as your main base station connected to the broadband modem. It could act as a 2.4 GHz extension of a 5 GHz network when connected to a LAN port on the base station connected to the broadband modem.

---

## **SET UP YOUR 2.4 GHZ BASE STATION**

---

Start with an 802.11g base station or any vintage of AirPort Express (G or N) as the 2.4 GHz network hanging off the 5 GHz base station. You need to configure the base station with the following settings:

- The network name for the 2.4 GHz and 5 GHz networks should be the same if you want to let devices automatically roam from 2.4 to 5 GHz and back as they choose. You can set the network names distinctly to set devices to be either on the 2.4 or 5 GHz network.



- Connection Sharing must be 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 the 2.4 GHz base station to the 5 GHz base station. The 2.4 GHz 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:
  - Set the name the same as the 5 GHz base station if you want roaming. In the example, that's [Home on Range](#).
  - Set the name distinctly, like [TwoDotFour Home](#) if you'd rather fix which clients connect to which band.
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 your 802.11n base station that will handle the 5 GHz band.

---

***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 5 GHZ BASE STATION

---

Next, you need to set up your 802.11n base station to use the 5 GHz band:

1. Launch AirPort Utility, connect to the 802.11n base station, and switch to Manual Setup (Command-L).
2. Click the AirPort icon and then the Wireless button.
3. Change the Network Name to something descriptive:
  - Set the name the same as the 2.4 GHz base station if you want roaming. In the example, that's [Home on Range](#).
  - Set the name distinctly, like [FiveGig Home](#) if you'd rather fix which clients connect to which band.
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.

---

***Warning!*** *Certain countries, including the United States, allow wide channels, but not all. If your N base station is being used in a country that allows only regular 5 GHz channels, the option should be dimmed. You can still get the benefit of less interference and no channel overlap from using 5 GHz, however, as well as split up slower traffic in 2.4 GHz and faster in 5 GHz.*

---

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 an earlier edition of this book wrote in after reconfiguring their networks as described above because their printers stopped working. After some troubleshooting, we collectively realized

that printers needed to be moved from the old G network to the new 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 base station, or into a USB hub that's plugged into the base station.
3. Launch AirPort Utility, connect to the 5 GHz base station, 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 base station into a larger LAN, check the Share Printers over Ethernet WAN 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 having 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.

You can also access your base station remotely for file sharing and configuration using a MobileMe account and Back to My Mac, thanks to a new feature Apple added in March 2009 to all the 802.11n models it ever sold.

---

## KNOW YOUR OPTIONS

---

AirPort Utility paired with the first 802.11n base station marked a major breakthrough for Apple, finally adding features that had 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 several 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, 802.11n base stations also let 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 mapping system work consistently with less effort. I cover how to [Map Ports for Remote Access](#) on the next page, and that is the most sensible option for most purposes with an N base station.

- **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. This option works only when the software you're using is aware of NAT-PMP and can talk to the base station using this protocol, and when you have a publicly reachable IP address assigned to your base station. You can find out more in [Punch Through with NAT-PMP](#).
- **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 though it's directly connected to the Internet. This option is appropriate in limited cases where you want a machine to be reachable from the Internet on any of its ports without getting publicly reachable IP addresses from your ISP for computers on your network. I describe the *default host* option in [Set a Default Host for Full Access](#).
- **Configure and monitor your base station and mount attached disks via Back to My Mac:** The 7.4.1 firmware release for all 2007 and later 802.11n base stations adds a MobileMe view to the Advanced pane in AirPort Utility. When you enter your MobileMe account information, your base station becomes registered with your central MobileMe account. Once that's done, any Leopard or later system with Back to My Mac enabled using the same MobileMe account can access an internal Time Capsule hard drive, and any USB-attached external drives just as if the computer were on the same local network. The base station also appears in the list of available devices in AirPort Utility on that computer.

I provide directions in [Access a Base Station via MobileMe](#).

---

## 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 the 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 Skype and iChat 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:

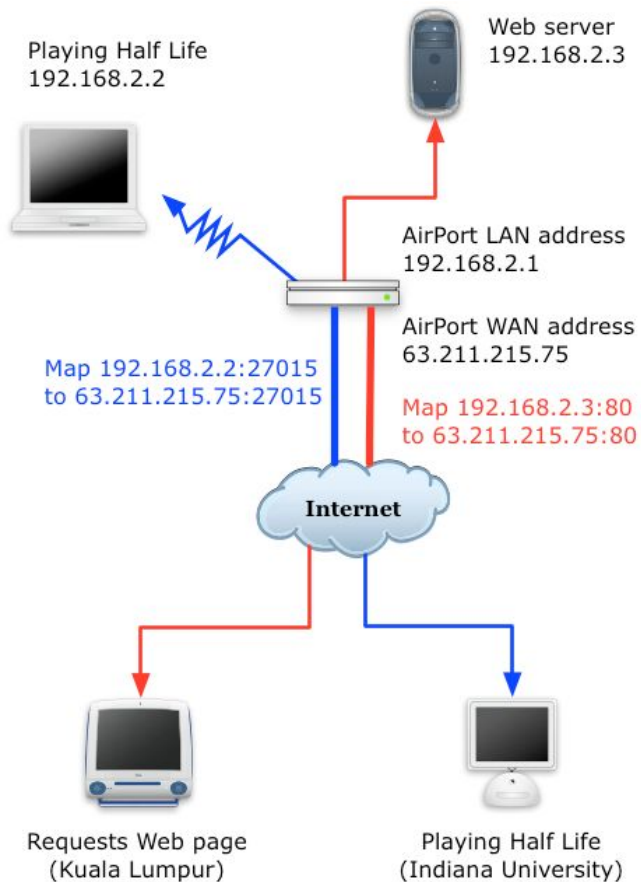
- In iChat, the central server is run by AOL, as iChat is part of the AOL Instant Messenger network. Each person using iChat connects to the AIM server, which maintains a persistent connection to iChat using the channel that iChat opened up. The server coordinates among everyone chatting to move messages among all those connections.
- Skype 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 you 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 88**). 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 88:** 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 first 802.11n Extreme appeared in 2007, you had to use a variety of complicated workarounds 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. As you work, I suggest that you create a text file or other simple list that includes the name of each computer (described, by its owner or its unique name) along with 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 base station configuration and restarting—which changes the IP addresses assigned dynamically!

---

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.

### **Set Base-Station-to-Computer Port Mapping for a Web Server**

To set up a Web server, we first need to configure the firewall on the computer that's acting as a Web server. The firewall protects the computer from unwanted inbound connections. Second, we need to set up the base station to pass traffic to the newly configured port.

### ***Running a Web server in Leopard or Snow Leopard***

The built-in firewall—configured in the Security pane of System Preferences, in the Firewall view—doesn't let you open up a specific port. Rather, it's based on applications and services.

Leopard has you set the firewall to allow access for “specific services and applications”; in Snow Leopard, you just press the Start button. In either version of Mac OS X, the only step you need to take is:

1. In the Sharing preference pane, check the box next to the Web Sharing service. This automatically opens an exception in the firewall for Web connections, if the firewall is engaged.

### ***Running a Web server in 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 below, in “Configure a Base Station to Pass Through to the Web Server.”


### ***Running a Web Server in Windows XP and Vista***

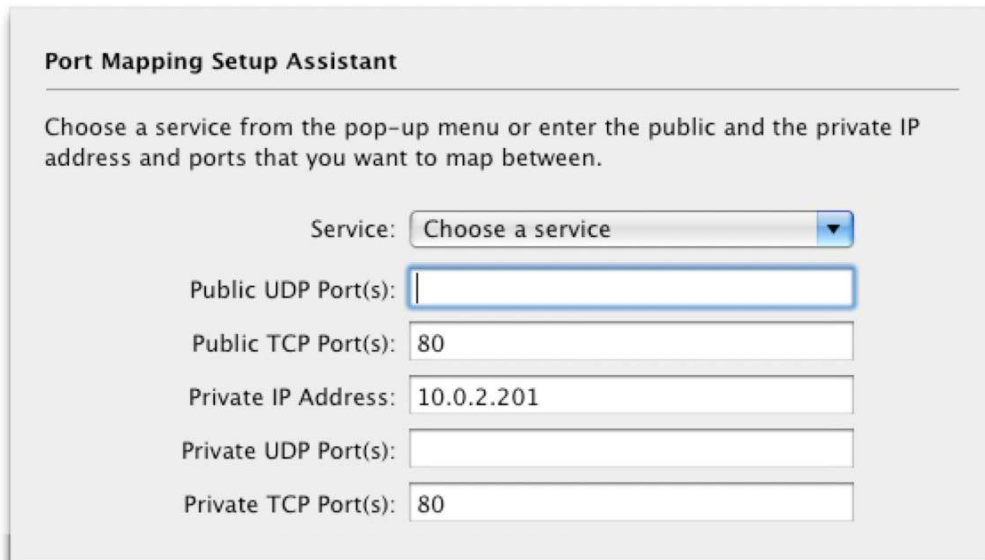
Typically, you use third-party firewall software for added security, and these packages allow you to enter exceptions for particular ports, such as port 80; read their instructions for details. But Windows XP and Vista each come with a built-in firewall package that you can configure quite simply:

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 that Don't Allow Exceptions is 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 a Base Station to Pass Through to the Web Server***

With the server set up to accept connections, we now can configure a base station in this fashion:

1. Launch AirPort Utility, select your base station, 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 89**).



**Figure 89:** 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 connect 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.

## 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.

## Set Base-Station-to-Computer Port Mapping 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 89**, previous page):

- **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](http://www.practicallynetworked.com/sharing/app_port_list.htm).

- **Public and Private UDP and TCP Port(s):** Public and private refer to the exposed ports (the public ones) and the ports on the local computer (the private ones). UDP and TCP are 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.

Each field for entering ports can handle a single number or a range as two numbers separated by a hyphen. You can also have multiple numbers or ranges separated by commas. For instance `407, 1216-1300, 6000-7000` would be a legitimate entry.

The ports must correspond in quantity from field to field. If you enter `407, 1000-1003` in the Public TCP Port(s) field, you must enter at least five (407, 1000, 1001, 1002, and 1003 comprising five) ports that correspond in the same order in the Private TCP Port(s) field.

---

## PUNCH THROUGH WITH NAT-PMP

---

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). NAT 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.

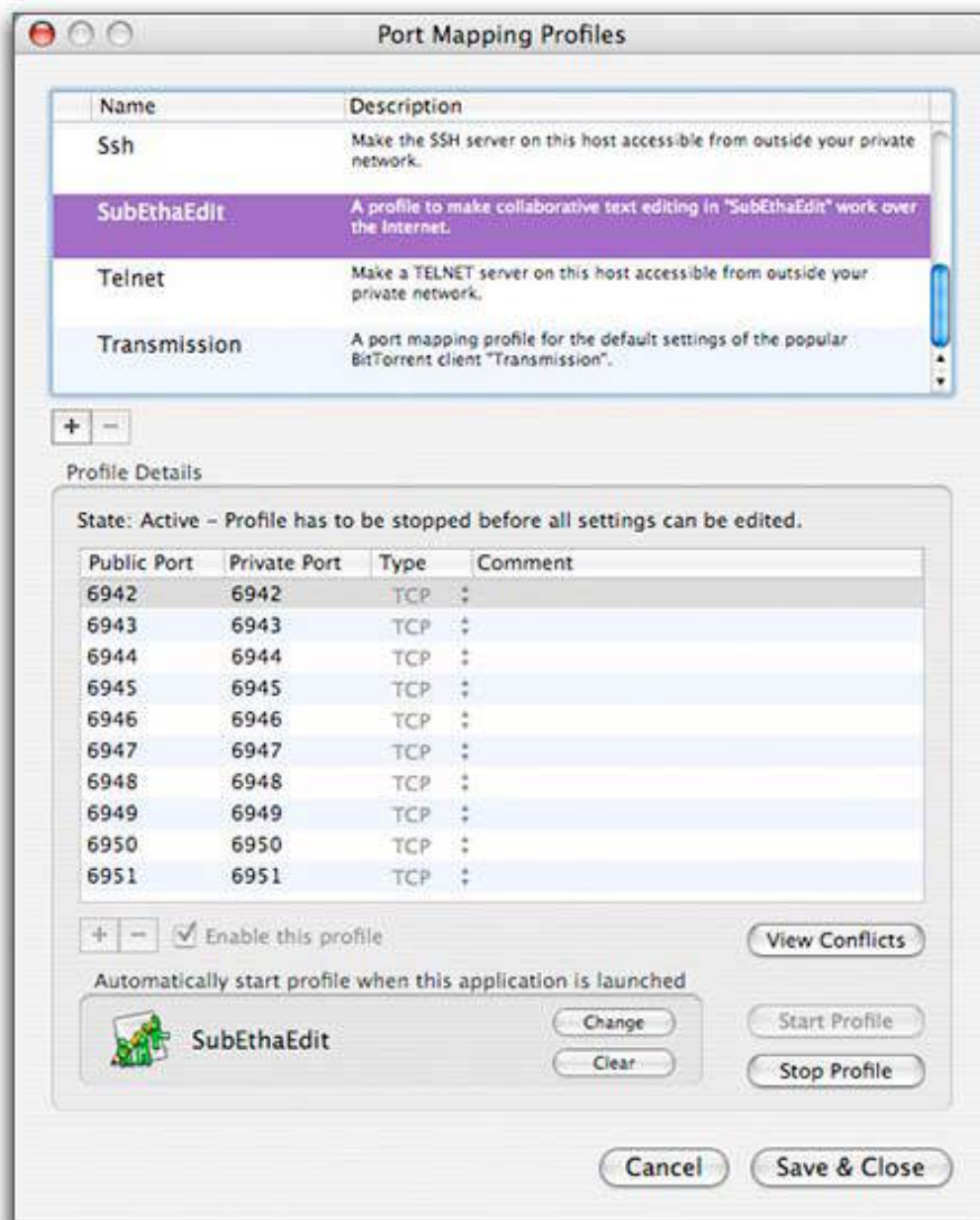
**Note:** NAT-PMP is a subset of features found in the more widely supported UPnP (Universal Plug and Play), which appears in most consumer Wi-Fi gateways as an option, but not in home DSL gateways provided by telephone companies.

You can also use a third-party program to set NAT-PMP mapping manually, which can be a nifty way to avoid the complexities of manual port mapping.

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. (It's generally already checked and available.)

The downside to NAT-PMP 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. There's not yet widespread use of NAT-PMP, because it's not found in routers outside Apple's.

This is where Lighthouse, from Codelaide Software, comes in (<http://codelaide.com/blog/products/>, \$13). Lighthouse is an interface for letting your Mac tell an Apple base station which ports it wants to use; it also works with any router that supports UPnP (**Figure 90**).



**Figure 90:** Lighthouse lets you choose which ports are mapped, and it tells a router to make it so.

### **Back to My Mac, MobileMe, iDisk, and iChat Use NAT-PMP**

Apple uses NAT-PMP to make Back to My Mac work, and NAT-PMP enhances MobileMe contact and calendar synchronizing, iDisk synchronization, and iChat file transfer and other tools. NAT-PMP lets Apple's servers contact your computer for these various services as needed.

MobileMe can sync its mountable iDisk more easily with NAT-PMP turned on, because that lets MobileMe 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.

With Back to My Mac, it provides a separate set of ports for each computer on a NAT-enabled network, making them individually reachable.

---

## **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 base station has a public IP address, your default host is as exposed as if it were on the public Internet.*

---

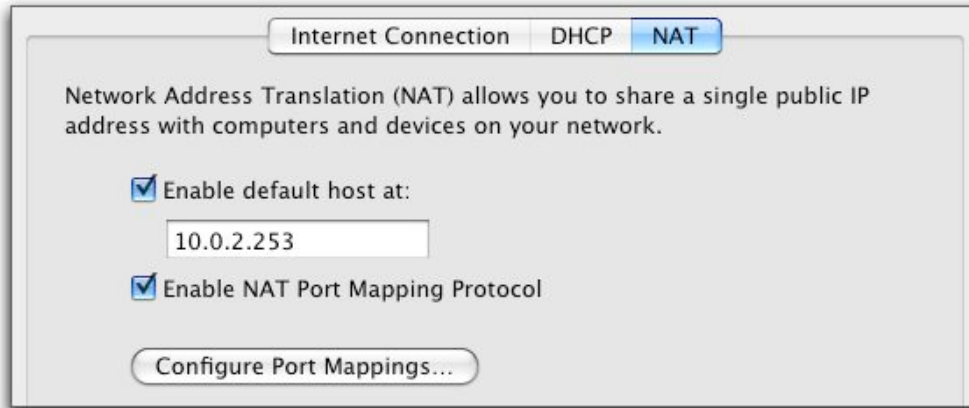
You should still use DHCP reservation to maintain the computer's private address over time; see [Reserved Addresses](#).

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 91**).



**Figure 91:** 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.

---

## ACCESS A BASE STATION VIA MOBILEME

---

There's one more way to gain remote access, but not to computers on your network. Using the Back to My Mac feature of MobileMe, you can access your base station from a Mac running Mac OS X Leopard 10.5 or later. Apple added support for Back to My Mac in March 2009 to the new AirPort Extreme and Time Capsule and—via the 7.4.1 firmware upgrade—to all 802.11n base stations released in 2007 or later.

This option lets you access a hard drive inside a Time Capsule or drives attached via USB to either an Extreme N or Time Capsule just as if you were on a local network (you can't attach a drive to an AirPort Express). Likewise, you can configure any supported base station model from AirPort Utility as if you were on the same network.

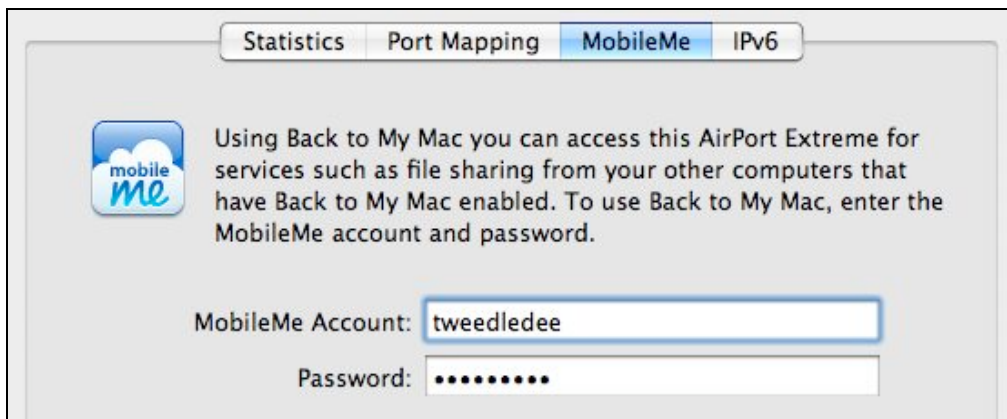
Introduced in Leopard, Back to My Mac uses MobileMe as a conduit for connecting Macs separated across networks, creating a secure connection between two computers that lets them appear to be on each other's local network. For a base station, Back to My Mac makes a one-

way connection, allowing a Leopard or Snow Leopard system to see a base station in the Finder window's sidebar under Shared or in the list of base stations in AirPort Utility.

**Note:** Learn more about MobileMe in Joe Kissell's *Take Control of MobileMe* or at <http://www.apple.com/mobileme/>.

If you configure a Back-to-My-Mac-savvy base station in AirPort Utility, you'll see a new MobileMe view in the Advanced pane (**Figure 92**). Enter your MobileMe user name and password, and click Update to restart the base station with the new credentials.

**Tip:** If you enter your credentials incorrectly, after you restart your base station, the LED on the base station will be amber and an amber light will show in AirPort Utility beside the base station in the list at the left.



**Figure 92:** Entering a MobileMe account allows any Leopard or Snow Leopard system with the same account entered and Back to My Mac active to configure the base station over the Internet.

Now from a remote Leopard or Snow Leopard system, follow these steps to connect to your base station:

1. Open the MobileMe system preference pane.
2. On the Account view, verify that you are signed in.
3. On the Back to My Mac view, verify that Back to My Mac is on. If it's not, click the Start button.

Now, you can:

- **Mount hard drives from an Extreme or Time Capsule:** In the Finder, open any window and look in the Shared section of the sidebar. The base station should appear as a listed server. Select the server and click Connect As to enter the password you set for access. The available shared volumes appear.
- **Configure the base station:** Launch AirPort Utility. In the device list at the left, the base station should appear. You can select and configure it just as you would any locally connected base station—even (as I did!) updating the firmware remotely.

Because Back to My Mac is a single-user remote access system, only one account can be used at a time for this remote option.

**Note:** You can't use Time Machine to back up volumes to a remotely mounted AirPort Extreme or Time Capsule volume over Back to My Mac. Time Machine uses a huge number of transactions to create its disk snapshots, and this wouldn't work well even over the fastest current broadband connections.

### **Back to My Mac Adds Remote Access to Computers**

With Back to My Mac active, you can access any service that uses Bonjour—including file sharing and screen sharing—from any computer in your Back to My Mac set. This doesn't help provide public access, but the service extends your personal remote access, when all the right pieces are in place.

I wrote *Take Control of Back to My Mac* to cover the intricacies of working with what should be a click-and-go option, and often isn't. When it works, it works well. I've also written a complementary book, *Take Control of Screen Sharing in Leopard*, which covers all the methods of accessing your screen remotely. An update for Snow Leopard is currently in the works.

# 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.

The AirPort Extreme and the Time Capsule can connect to one or more of both a printer and a hard drive via a USB hub. (To maximize reliability and performance, I recommend a Hi-Speed powered hub with external AC power.) The AirPort Express is designed to attach to one USB printer only, and cannot handle an attached hard drive.

In this section, I explain how to configure a base station for an attached printer, and how to print to that printer from Mac OS X and Windows.

---

## ADD A PRINTER

---

For each printer you want to attach to the base station:

1. Plug the printer into the base station (any model) or a USB hub (Extreme N, Time Capsule). 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](#), next page.
3. As needed, configure Macintosh computers to connect to the printer; [Add a Shared Printer in 10.5–10.6](#) and [Add a Shared Printer in 10.2–10.4](#) explain how.
4. As needed, configure Windows XP and Vista machines to connect to the printer; [Add a Shared Printer in Windows](#) has instructions.

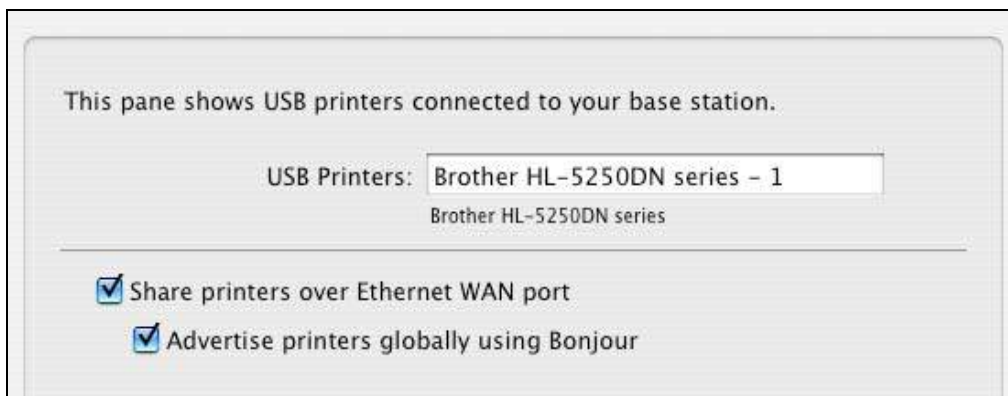
---

## 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 93**).



**Figure 93:** 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 or Time Capsule has a public IP address).

**Note:** Express N base stations can't advertise printers over their single Ethernet port.

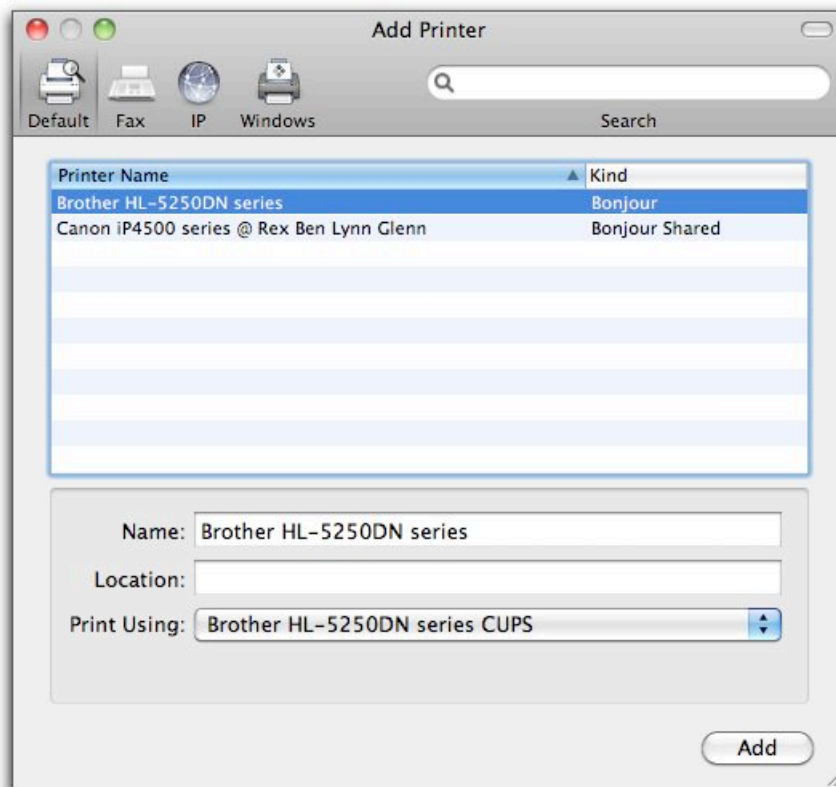
5. Check Advertise Printers Globally Using Bonjour to make the printer browsable over a larger LAN (outside the base station's private network) from all Mac OS X machines, and from Windows machines with Bonjour installed.
6. Click Update to save this change and restart the base station.

## ADD A SHARED PRINTER IN 10.5–10.6

To add a shared printer in Leopard or Snow Leopard, use these steps:

1. Open the Print & Fax system preference pane.
2. Click the  button near the bottom left of the window.

This launches an unlabeled floating printer browser; in Leopard, it can disappear behind other windows, but in Snow Leopard it always floats in front. The Default icon should be selected, and the printer list shows printers available over Bonjour (**Figure 94**).



**Figure 94:** The printer browser lets you choose the Bonjour-shared printer attached to a base station. The second printer above was found via Back to My Mac at a remote network, even.

4. Select the printer in the list. After a moment, Mac OS X should recognize the printer and display its driver in the Print Using pop-up menu. If it does not, find the driver manually.
5. Click Add.

The printer is now available.

---

## ADD A SHARED PRINTER IN 10.2–10.4

---

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 it 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

---

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 Bonjour for Windows package. You can download it 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. Click Next.
2. Select a printer. 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.macosxhints.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 the preceding steps to make sure you configured everything correctly or try the suggestions in [Troubleshoot an Unavailable Shared USB Printer](#), a few 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). To add a shared USB printer, make sure the printer is on and then follow these steps:

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 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.

4. Vista tries to find the appropriate printer driver. In my testing, it fails at this stage, and requires manual selection:
  - Should Vista find the right driver, resume at Step 7 on the previous page.
  - Otherwise, in the screen that appears—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 are in the list, select the maker on the left and 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. 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 still can't print to your shared USB printer, one of the following suggestions should shed light on the problem:

- Is the printer connected to the wrong base station? See [Put Printers in the Right Place](#) (p. 162).
- Make certain that the printer is powered up and not in an error condition (such as out of paper or out of ink).
- Check if the computer is on the same network as the base station. To do so, on the computer, launch AirPort Utility and see if 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](#), earlier in this section.
- Using AirPort Utility, restart the base station and try again.
- Consult the suggestions at <http://support.apple.com/kb/TS1253>. Note that the last suggestion, under "Still not working?" is to confirm that your printer is able to work with AirPort printer sharing.

# Set Up a Shared USB Disk

The AirPort Extreme N and the Time Capsule both add an interesting option to your network: they can share disks across a network without those disks being attached to a computer. Both models can accept one or more external drives plugged in via USB or via a USB hub; the Time Capsule also includes a non-removable internal drive.

Either model can share drives over a network with both the standard *Apple Filing Protocol* (AFP) format, the same format used with Personal File Sharing and Mac OS X Server share files, and *Samba*, a network file-sharing service compatible with Mac OS X, Windows, and Linux.

With a MobileMe account and Leopard or later on remote Macs, attached hard drives can be accessed over the Internet via AFP using Back to My Mac, too (see [Access a Base Station via MobileMe](#), p. 177).

In this section, I cover a handful of procedures for using the Time Capsule and the Extreme N to share USB disks. Topics covered include:

- Read [Prepare Your Drive](#), next page, to find out about physically attaching them and formatting them.
- [Work with Time Capsule](#) (p. 193) covers setting up Time Machine backups as well as how to use AirPort Utility to make a backup archive of a Time Capsule disk or to erase the disk.
- [Grant Access](#) (p. 199) and [Gain Access](#) (p. 202) look at how users on the network can best access the disks.

---

***Warning!*** You can't share volumes via either only AFP or only Samba; you must share through both.

---

---

***Slow speeds ahead!*** The performance of drives inside a Time Capsule or connected to the USB ports of either a Time Capsule or an Extreme N is creepingly slow when compared either with gigabit network throughput or a directly connected drive. Apple promises that Snow Leopard has improved on this; at this writing, I haven't run extensive tests.

*In my tests of the Extreme N (gigabit) under Leopard, I saw speeds about one-third that of directly connected USB drives with larger files. When I copied 8,000 tiny files, the transfer speed dropped to below 10 percent of directly connected USB. This is partly due to inefficiencies in copying many small files in Apple Filing Protocol (AFP), and partly due to the low-power, but adequate, processor in the Extreme N (both models). For faster speeds, use a computer-based fileserver or dedicated network-attached storage (NAS) device.*

---

---

## PREPARE YOUR DRIVE

---

The Time Capsule's internal drive comes preformatted, so it should be ready to go, but it can be erased to its pristine state through AirPort Utility (see [Erase](#), ahead).

You can connect a single drive to the USB port on the Extreme N or Time Capsule, 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 formatted and connected, you can access them and let others access them, too. You handle all the configuration in AirPort Utility in the Disks pane.

### Disks, Partitions, Volumes, Files and Folders

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

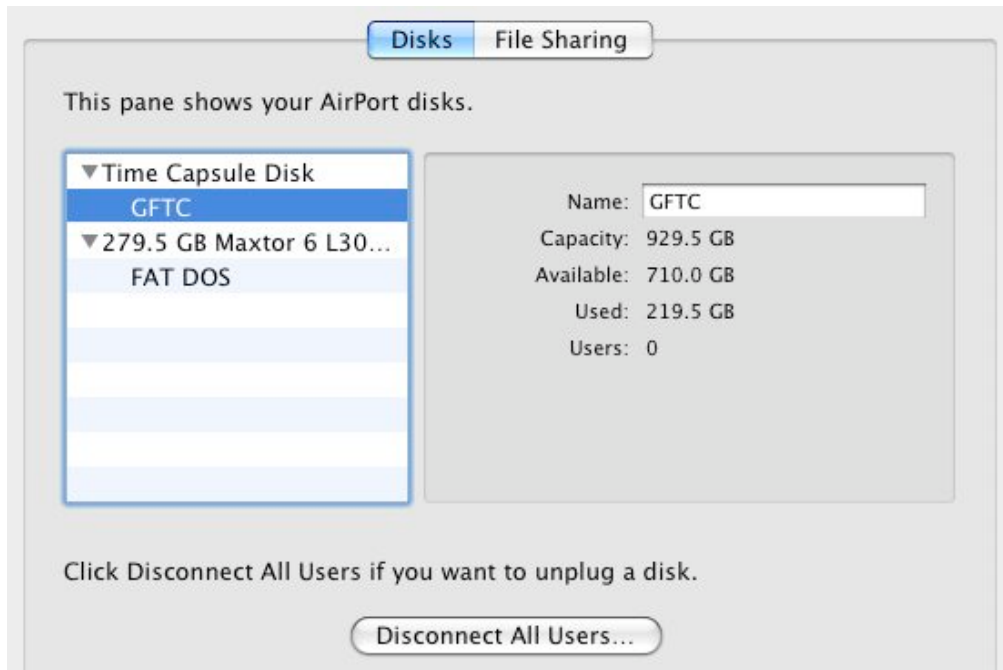
- **Hard disk:** A *hard disk* is a physical piece of hardware that contains data.
- **Partition:** A *partition* is a division of a disk's available storage into a separate logical compartment—part of the physical disk is written with certain kinds of data, and a disk-wide partition map is updated to 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, FAT32, 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, the base station makes folders into volumes, so that you can control access more finely, as described ahead.

---

## VIEW 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 95**). Selecting a partition reveals the capacity of that partition, the used and remaining storage, and how many users have mounted the partition.



**Figure 95:** In this example, AirPort Utility shows two drives, each with one partition. *Time Capsule Disk* is the internal drive on a Time Capsule, and it can be renamed in AirPort Utility. Select a partition to see its storage information and the number of connected users.

Clicking **Disconnect All Users** shuts down all file services, forcing connected users' computers to lose the connection with mounted volumes no matter whether they have open files or transfers in progress, so click it with care.

---

**Warning!** *You cannot disconnect individual users, nor can you bump users off just a single partition or drive.*

---

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 96**). This button appears even if no users are connected.

**Tip:** In AirPort Utility, you can rename a partition for a Time Capsule drive. For instance, you might want to give it a more descriptive name.

When no users are connected, the drive is in a standby state that lets you unplug it from the Extreme N or Time Capsule without harm, or turn off a Time Capsule without harming its internal drive.





**Figure 96:** 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).

---

## WORK WITH TIME CAPSULE

---

Once you've hooked your Time Capsule into your network and turned it on, you can configure the Time Capsule to accept Time Machine backups; I cover that procedure just ahead. A little farther along, I also explain how you get at the Time Capsule internal drive to perform functions such as making a backup archive or erasing the drive.

**Tip:** A Time Capsule's internal and external drives can be selected for use with Time Machine on multiple machines on a network.

### Time Machine Backups

The Time Capsule's very name indicates that it has something to do with the Time Machine backup feature. Any internal drive or external drive partition on a Time Capsule can be chosen as a Time Machine destination backup by any Mac running Leopard or Snow Leopard on the same local network.

---

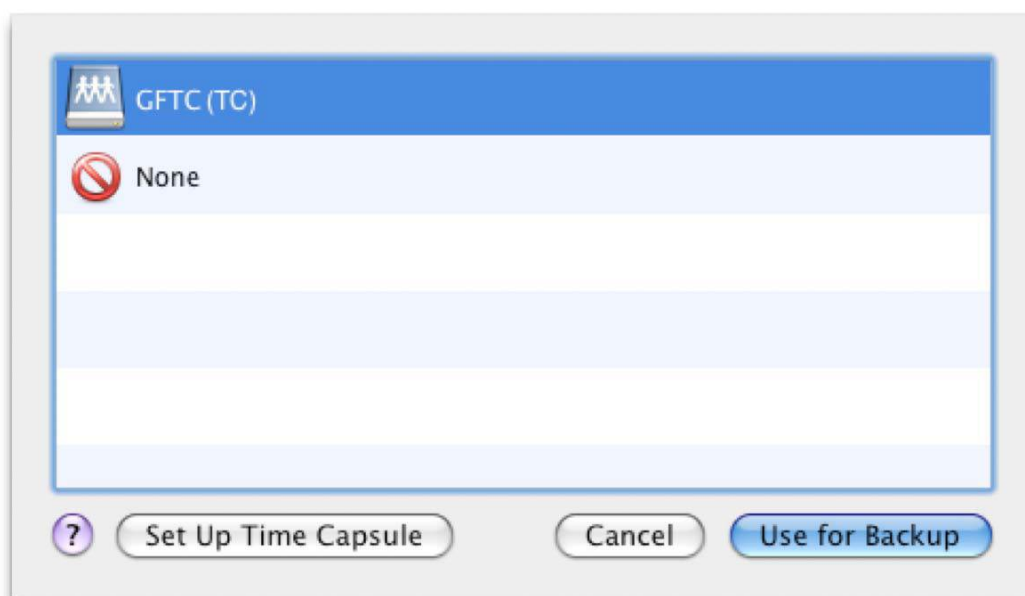
**Warning!** Apple promised that in Leopard, Time Machine would back up to Extreme N connected drives. But by the time Leopard shipped, Apple had removed the feature, angering some base station purchasers.

The Time Capsule supports Time Machine backups to both its internal drive and to any externally connected drives, and after an early update, that support extended to Extreme N external drives. This was apparently an accident: Apple never documented the feature and doesn't officially support it, and the feature is unreliable—backup images may become corrupted and drives may stop appearing as an option in the Time Machine drive selection dialog (**Figure 97**) after a few days or weeks goes by.

---

To use Time Machine with a Time Capsule volume, follow these steps:

1. Open the Time Machine System Preferences pane.
2. Click the Change Disk button.
3. In the dialog that appears, all locally available Time Capsule drives should appear (**Figure 97**). (Only HFS+ formatted drives, including the Time Capsule internal drive, show up.)



**Figure 97:** Time Machine shows available disks attached to your computer and over the network.

4. Select the disk and choose Use for Backup.

5. Time Machine will prompt you to enter the password to mount the drive in whatever fashion you've defined, if anything but Guest access with read and write has been selected. (See [Grant Access](#), a few pages ahead.) Enter that password and click Connect; the password is stored for future access.

Time Machine now proceeds with backups.

---

***Warning!*** *The first backup over Time Machine can take a very long time over Wi-Fi—even using 802.11n—because Time Machine backs up all files the first time. Subsequent backups copy only files that have changed in the interim. You may want to connect a Mac running Leopard or Snow Leopard via gigabit Ethernet to a Time Capsule overnight for the first backup.*

---

## Archive

The Archive feature lets you copy the entire contents of a Time Capsule's internal drive to an attached hard drive, making it easy to back up the entire internal Time Capsule drive. Such a drive might contain as much as a terabyte of backed up files from computers on your network! The Archive feature also makes it possible to take backups offsite for storage without requiring that you swap two Time Capsules in and out of your network.

**Note:** I advise taking an archived copy of your Time Capsule drive somewhere offsite, even to a safe-deposit box, to insure that you have access to it even if a disaster destroys the Time Capsule.

**Note:** External drives attached *to* a Time Capsule or Extreme N base station cannot be erased or archived via methods described here.

Time Machine writes its per-computer backups to Time Capsule's internal (and external) drives just as if they were normal disk images. You can take a drive with archived Time Capsule contents, mount it on a Leopard or Snow Leopard machine, and use Time Machine to restore files or systems.

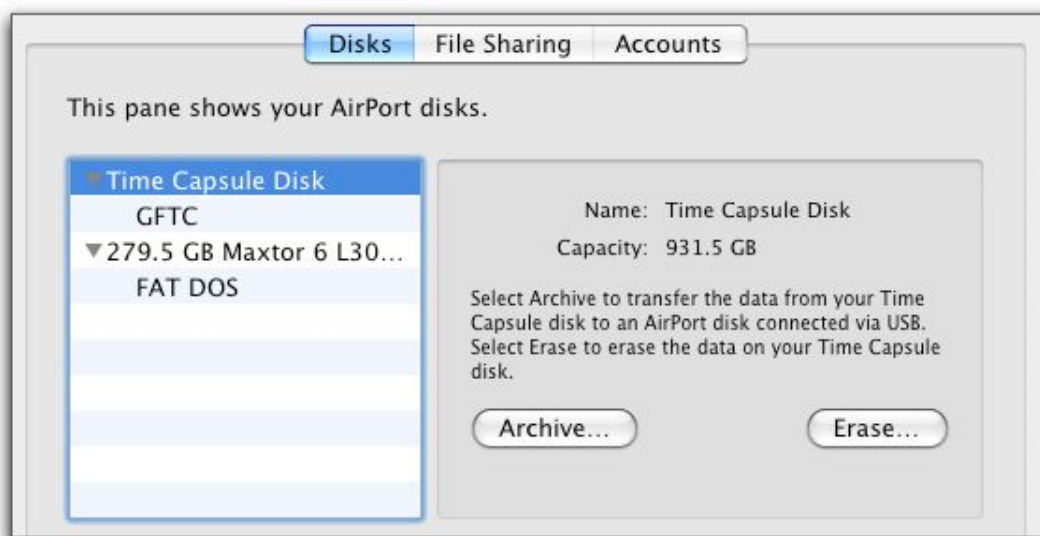
Although you could mount the Time Capsule internal drive on a Mac that had a spare hard drive attached and copy files to that extra drive, this process is tedious as it's limited to the speed that the Time Capsule

can copy over AFP (Apple Filing Protocol). In practice, this speed is 45–60 Mbps, even when you're connected via gigabit Ethernet. In contrast, the Archive feature in AirPort Utility copies directly over USB at speeds closer to 100 Mbps.

**Note:** Archive does not erase files from the drive onto which you are backing up your Time Capsule.

To archive files from an internal Time Capsule drive, follow these steps:

1. If you haven't already, connect a Mac OS X formatted external drive to the USB jack or a USB hub plugged into the USB jack of your Time Capsule.
2. In AirPort Utility, select your Time Capsule, click Manual Setup, and click the Disks button.
3. Select the internal volume, *Time Capsule Disk*, in the drive list.
4. Click the Archive button that appears at the right (**Figure 98**).



**Figure 98:** The Archive and Erase buttons appear when you select the item *Time Capsule Disk* in the drives list.

5. AirPort Utility asks you to select the drive to copy files to; that drive must have enough storage to hold all the files, as an archive operation cannot span multiple disks (**Figure 99**).



**Figure 99:** Choose the external drive onto which you want to archive files from the Time Capsule's internal drive.

For safety's sake, AirPort Utility warns you about the operation you're about to perform, which doesn't erase the target drive, but may take quite a while to complete and can't be interrupted (**Figure 100**).



**Figure 100:** You're given fair warning that proceeding makes the Time Capsule's non-networking features unavailable.

---

**Warning!** *While an archive operation is in process, the Time Capsule locks out Time Machine backups and file-server access to any volumes, internal or external. You should consider running this operation overnight or, in an office, over a weekend.*

---

When the Time Capsule's light stops blinking amber, the archive operation is complete, and you can remove the drive.

## Erase

If your internal Time Capsule drive becomes corrupted, or you want to remove its contents irretrievably—before selling the base station, for instance—the Erase feature is what you need.

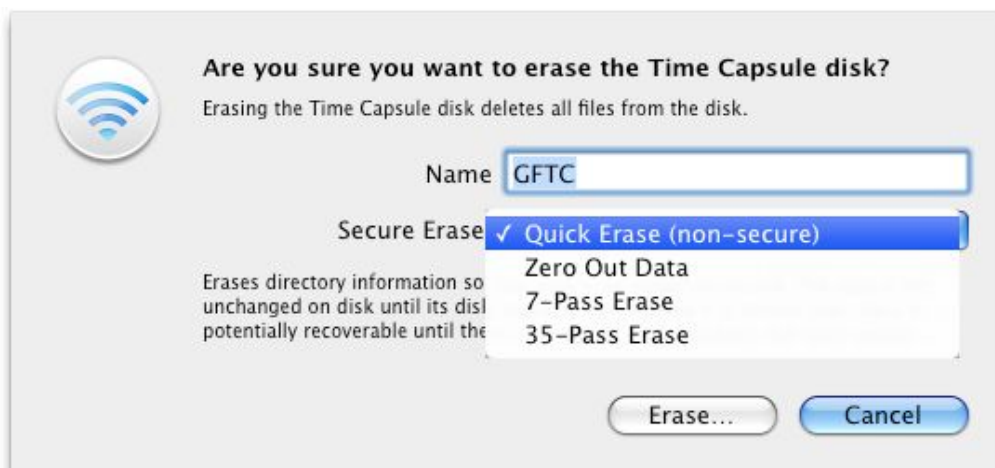
To reset the contents of your Time Capsule's internal drive, follow these steps:

1. In AirPort Utility, select your Time Capsule, click Manual Setup, and click the Disks view.
2. Select the internal volume, *Time Capsule Disk*, in the drive list.
3. Click the Erase button that appears in the pane at the right.
4. In the dialog that appears, rename the sole partition on the drive (if you like) and choose an erasure method. The Secure Erase pop-up menu shows several methods that range from smart to insanely paranoid. A 7-Pass Erase should provide security from all but national security agents. If you're erasing the drive to sell it, I suggest Zero Out Data; if you're erasing it for your own purposes to re-use, choose Quick Erase (**Figure 101**).

---

**Warning!** *Choosing 7 or 35 passes could take many, many, many hours to complete.*

---



**Figure 101:** You can go to rather extreme extremes to secure the erasure of your internal drive.

5. Click Erase.

---

**Warning!** While an erase operation is in process, the Time Capsule locks out Time Machine backups and file-server access to any volumes, internal or external.

---

6. You're prompted again to make sure you really want to erase the drive. Click Erase in this dialog to proceed.

---

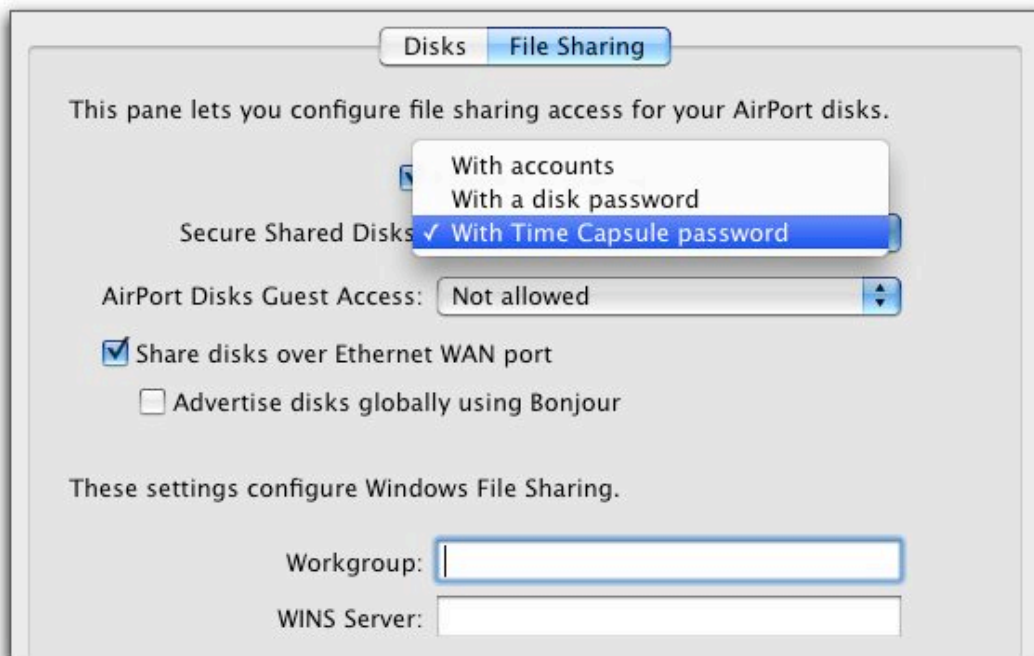
## GRANT ACCESS

---

Apple offers relatively little granularity in setting up security and access for hard disks you connect to an Extreme N or Time Capsule. 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 102**).



**Figure 102:** 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 it 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 someday (even though I've been hoping for nearly 2 years):

- ◇ **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 TB disk drive and a 1 GB flash drive to your base station, 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.

With a Time Capsule, user account folders are always placed on the internal drive.

---

***Single drive, no worries:*** *With a single hard disk that's formatted in HFS+ and attached to an Extreme N or using just the internal drive on a Time Capsule, 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.

## **Put Your Disks on a Larger LAN**

Also in AirPort Utility, in the Disks pane, in the File Sharing view, you can limit access to what network or part of a network is available through two checkboxes beneath the Guest Access pop-up menu:

- If you check Share Disks over Ethernet WAN Port, other computers on a larger LAN (one to which the base station connects via its WAN port) 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 or Time Capsule 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 base station and the larger world to provide additional access control, such as limited fileserver access to particular IP ranges that represent other locations.*

---

## Configure Windows File Sharing (Samba)

The other option in the bottom portion of the File Sharing view 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

---

File sharing with the Extreme N and Time Capsule uses standard methods: AFP, commonly known as AppleShare, and Samba, Windows's default method. You or users on your network can access base station file servers connected to an Extreme N or Time Capsule via normal file-sharing options, such as selecting the server from a Finder window's sidebar in the Shared section.

Before we look at methods of accessing shared disks, though, we need to figure out precisely which volumes are mounted based on the base station's settings, the disk's format, and what kind of access you're attempting to gain. I lay out the options in **Table 8**, next page, because they're too baroque to explain conversationally.

**Table 8: Comparing Methods of Serving Shared Disks**

<b>Access Control</b>	<b>Access Method</b>	<b>How Partitions Are Served</b>
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"> <li>• 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.</li> <li>• A folder named <i>Shared</i> is also created on one partition, and users mount it as a volume named with the partition name.</li> <li>• Any other partitions are served as volumes named with the partition name.</li> </ul> <p><i>FAT 16/32-formatted partition:</i></p> <ul style="list-style-type: none"> <li>• A folder named <i>Shared</i> is served. Users mount it as a volume having the partition name.</li> </ul>
	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>		

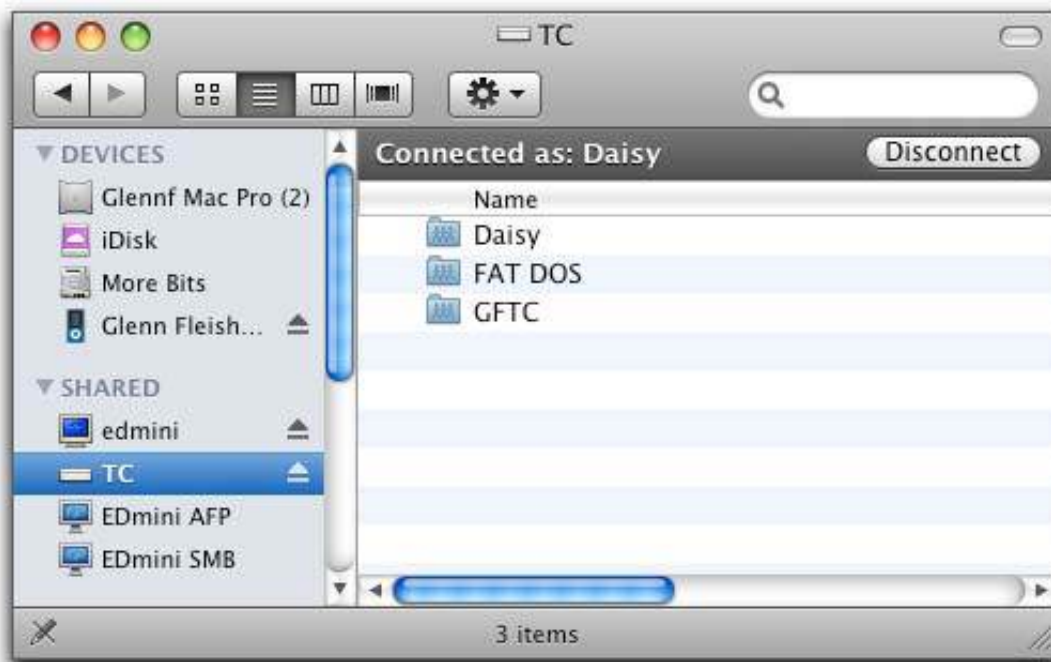
---

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

---

## Mount in Leopard and Snow Leopard

Leopard and Snow Leopard manages the base station server and disks through the Finder, just like any other network volume. Open any Finder window, and look in the sidebar for a list of servers in the Shared section (**Figure 103**). 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. If you are set up to [Access a Base Station via MobileMe](#) from that Mac, you'll also see base station(s) in that list.



**Figure 103:** The Shared section of the sidebar shows available servers. Select a server and enter its password, and volumes appear in the main portion of the window. The Connected As banner at the top shows which 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 in the Sharing section of the sidebar.
2. Now:
  - To connect as a Guest user, you need take no more steps. Leopard or Snow Leopard automatically tries to connect using the Guest login, and 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 and Snow Leopard are clever enough that for Extreme N and Time Capsule shared drives that use just a password for access—no user accounts—it prompts 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 mounted servers on the actual Desktop as an icon; this was fixed in Snow Leopard. This can be confusing! To fix this oversight, follow these steps:

1. Choose Finder > Preferences.
2. Click General.
3. Check Connected Servers under the Show These Items on the Desktop label.

---

***Unmounting:*** *To unmount a network volume, select the volume on the Desktop and press Command-E, or choose File > Eject "volume name". Or, you can unmount all volumes associated with a server by clicking the Eject icon in a Finder window sidebar next to the server's name, or clicking Disconnect in the server's Finder window (Figure 103, previous page).*

*In Snow Leopard only, a disk icon turns gray while Mac OS X is in the processing of removing its associations; it then disappears when the process is complete. Older versions of Mac OS X show the disk sitting there until the process is complete. If a file is in use by an application, Snow Leopard tells you which one; Leopard only tells you that it's in use.*

---

## **Mount in Tiger**

You can mount volumes in Mac OS X 10.4 Tiger 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.

(If the list doesn't appear, skip to the paragraph after Step 5.)

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 3–5.

---

***Unmounting:*** To unmount a volume or server, you can use the same options as with Snow Leopard and Leopard, described on the previous page.

---

## **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 3–5 on the previous page.

---

***Unmounting:*** To unmount a disk, find the volume under My Computers or on the desktop, right-click the volume, and select Disconnect.

---

# 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.

### 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.

### **Public Hotspots Carry Additional Risks**

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 violate 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 an example, see <http://bit.ly/Bad2v>.)



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. TJX Companies, the parent of discounter TJ Maxx, found this out the hard way when international criminals broke into their corporate network via poorly secured Wi-Fi at their retail stores in 2005 and 2006. Nearly 46 million credit card numbers were disclosed over 2 years, and the company paid tens in millions of dollars in settlements to affected card-issuing banks, among other fees.

### **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. Apple's 802.11n base stations can also control access by time of day and day of week for particular MAC addresses.

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

### Setting All Base Stations to Same Filtered Addresses

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 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.

To restrict access, first note the MAC addresses for devices you want to limit; see [What and Where Is a MAC Address?](#) (p. 97). You can also use AirPort Utility to extract the MAC address of the 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](#), p. 219, for more details.

To restrict access by MAC address on any 802.11n base station released in 2007 or later, 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 and choose Timed Access from the pop-up menu.
3. Repeat Steps 3a–3e for each Wi-Fi device you want to restrict:
  - a. Click the  button at the bottom of the access control client list.
  - b. In the Timed Access Control Setup Assistant, enter the MAC address of the device, or click This Computer to fill the field with the MAC address of the computer on which you are running AirPort Utility.
  - c. Enter a description of the computer you are adding.
  - d. 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 Everyday and All Day would be an ineffective barrier to access!)

- e. Click Done.
4. Edit the "(default)" entry in the access control client list. It's set at the factory to Unlimited. 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.
5. Click Update.

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. For a better defense, you must 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 must 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 the system uses 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 9**, next page, for side-by-side comparisons. I look at each option in more detail next.

### 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.

**Note:** Many retailers, such as the aforementioned TJ Maxx, still rely on WEP because their point-of-sale registers and other systems are outdated. This means that a credit card number you use at a retail store might be at greater risk than if you'd carried out the same transaction on a secure site online. Credit-card issuers have revised the rules around retail networks, and WEP will no longer be allowed by 2010. (About 5 years too late for my liking.)

**Table 9: Comparing Wi-Fi Security Methods**

<b>Name</b>	<b>What Can Use It?</b>	<b>Difficulties</b>
WEP	Any Wi-Fi adapter using 802.11a, b, or g, including the earliest made.	Encryption can be broken in under a minute using automated, free tools; deprecated since 2003.
TKIP (WPA Personal, WPA2 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.
AES-CCMP (WPA2 Personal)	Works only with gear shipped starting in late 2002, including AirPort Extreme, but requires Mac OS X 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 10.3 or later, or Windows XP SP2 or Vista.	Requires a back-end server to handle account management.

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 cases in Florida, Alaska, and Singapore indicate.

## **WPA & WPA2 Background**

WPA (Wi-Fi Protected Access) was released in 2003 by the Wi-Fi Alliance as an interim measure when work by an IEEE committee—802.11i—was taking too long. 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 Panther or later; see <http://support.apple.com/kb/HT2594> 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. All Apple base stations released starting in 2003 handle WPA2, but Mac OS X 10.3 or later is required to use it.

---

**Warning!** *The original AirPort Card cannot access WPA2-protected networks.*

---

### The Key to Keys

WPA2 is a superset of WPA. WPA supports just one new 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.

An Apple 802.11n base station 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. The option to create a long phrase gives a WPA/WPA2 passphrase the potential to be memorable, but more characters in the phrase also adds *entropy*, the principle in cryptography of introducing a greater inability for a key to be predictable and thus obtainable by someone who doesn't know it. A key could look like [my d000gs have lite\\_brite\\_hair!](#) I kid you not.

### **WPA Has a Weakness: Short Passphrases**

Researchers have found 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 on the previous page.

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.

### **Inexpensive Ways to Turn On the Enterprise Flavor**

Even small offices might like to use WPA/WPA2 Enterprise, and there are two affordable ways to add it to a network:

- Mac OS X Snow Leopard Server includes the necessary support for WPA/WPA2 Enterprise in its RADIUS server, which handles checking for valid user accounts. The \$500 ten-user version limits local logins (not accounts nor WPA/WPA2 Enterprise users) to only ten users; a \$1,000 unlimited user version is needed only if you want more than ten local users logged in at a time to certain services, like AFP file sharing (<http://www.apple.com/server/macosx/>, \$500 or \$1,000).
- You can buy server software from Periodik Labs (<http://www.periodiklabs.com/>, \$750).

### **Turning on WPA/WPA2 Personal**

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. Yes, I've said this before, but I'll keep saying it! Because it's utterly confusing: Your older Mac with an AirPort Card won't provide any feedback when it can't connect to the network.*

---

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 Security Network)**

WEP Transitional is supported in Apple's base stations; it's 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 while holding the Option key, choose WEP (Transitional Security Network). (Apple deprecates this option, so the firm hides it.)

**Note:** In the unlikely event that you need to use pure WEP (40 or 128 bit), you must first set Radio Mode in the Wireless view to a mode that doesn't include 802.11n. Hold down the Option key before selecting the pop-up menu to gain access to these extra modes: 802.11a and/or 802.11b, b/g, or g. With any of these modes set, hold down Option and open the Wireless Security pop-up menu to see WEP 40 bit and WEP 128 bit as options.

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 104**). 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 104:** The Equivalent Network Password dialog shows 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, your operating system will prompt you for a password. You can find details on connecting 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 anybody entering a key. Instead, in the two versions that Apple has implemented, users set up a profile with encryption to connect to a network without entering a password at all or by entering a short PIN (personal identification number). Apple's use of WPS requires that during set up you connect to the base station using AirPort Utility and, while connected, have the device that wants to join the network attempt to join.

Once you have completed a successful WPS connection, the device stores the encryption key for the network and uses it for future connections just as if you'd entered the key manually.

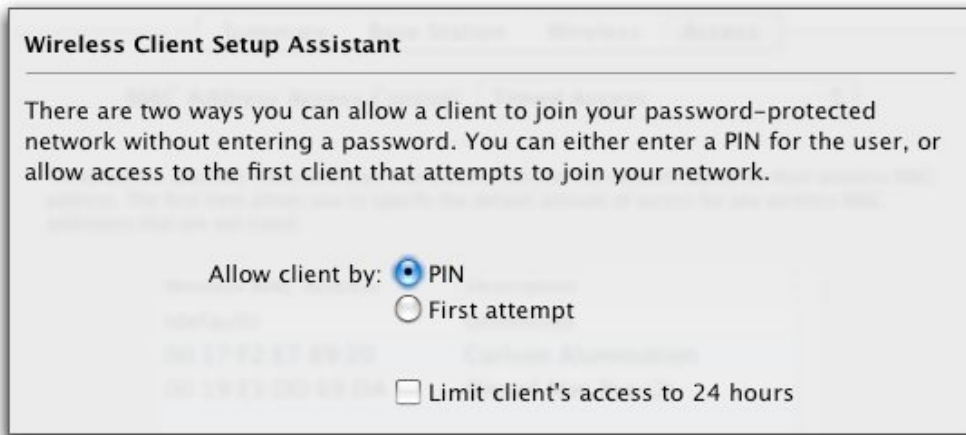
---

***WPS limited to Leopard and later:** Although WPS is an industry standard, I've been able to set up a WPS connection only between Apple 802.11n base stations and Macs with Apple 802.11n adapters running Leopard or later. The Linksys WRT610N comes with three different ways of using WPS, one of which triggers Mac OS X's WPS activation mode. But at that point, the connection fails: the system provides a key to enter, but the Linksys has nowhere to enter the key at that stage! I hope compatibility and availability of WPS improves.*

---

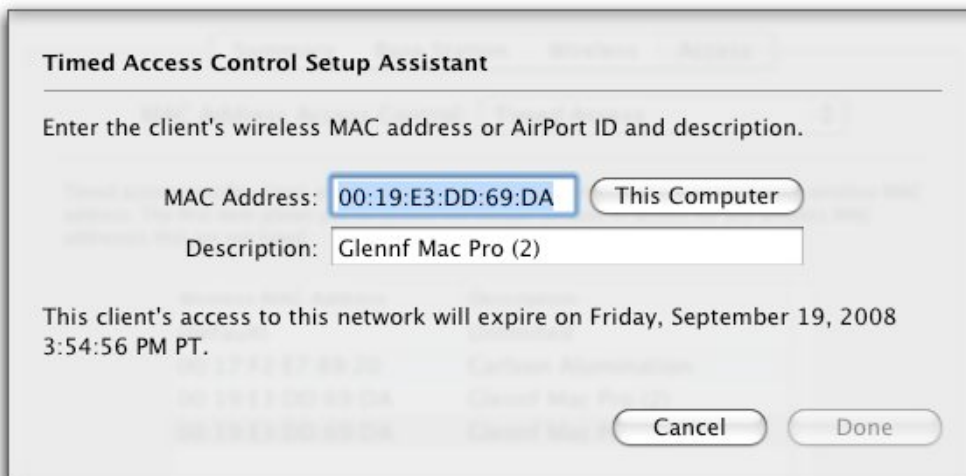
For either kind of WPS—no password or PIN—follow these steps to get set up:

1. Connect to your base station via AirPort Utility and click Manual Setup.
2. The first time you use WPS, click the Wireless button in the AirPort pane. In the Wireless view, confirm that WPA/WPA2 Personal or WPA2 Personal is selected in the Wireless Security pop-up menu and that you've entered a password. If not, see [Turning on WPA/WPA2 Personal](#), and follow those steps.
3. From the menu bar—not the blue “tab” buttons—choose Base Station > Add Wireless Clients to open the Wireless Client Setup Assistant (**Figure 105**).



**Figure 105:** The assistant allows a client to join the network without a password.

4. 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 the base station's access control settings after you finish the configuration (**Figure 106**). (See [MAC Address Filtering](#) for more detail.)

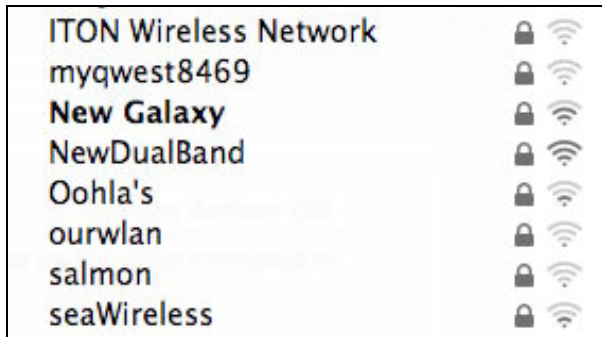


**Figure 106:** The special 24-hour limit entry for timed access can't be edited for time, only by name and MAC address.

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

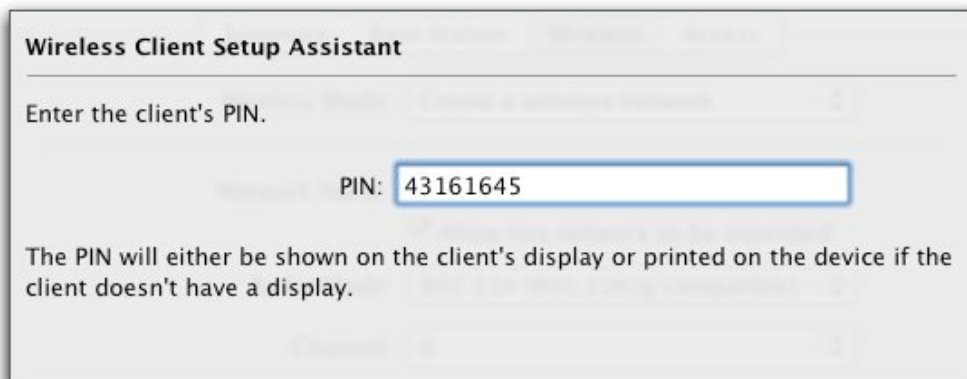
This puts AirPort Utility and the base station into a state of watchful awareness! It also sets the LED on the base station to a lovely shade of blue to indicate that the base station is receptive. AirPort Utility notes that it's waiting for a connection, and, if you've selected the First Attempt option, the first computer that tries to connect to the network will be presented with an encryption key automatically.

6. 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 107**).



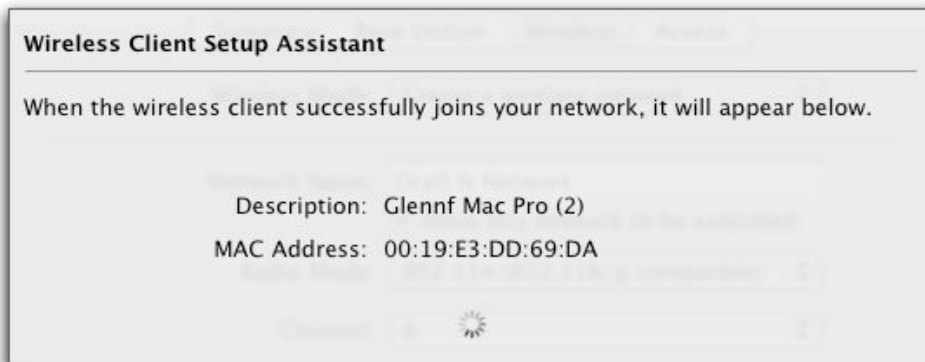
**Figure 107:** The network with WPS standing by appears in bold: Draft N Network.

7. If you've selected the PIN radio button in Step 3, the Mac OS X system that's trying to connect generates a code onscreen. Note that code and now enter it in AirPort Utility (**Figure 108**).



**Figure 108:** Enter the PIN provided when you select the network as in **Figure 107**.

A key is exchanged between that computer and the base station, and that computer joins the network (**Figure 109**).



**Figure 109:** AirPort Utility shows a successful addition of the client after the PIN was entered.

No matter which option you selected in Step 3, AirPort Utility’s watchful-waiting dialog disappears, and AirPort Utility confirms that the device has been added. Unlike many others, this operation does not require that you click the Update button to complete it.

The client is now connected.

---

## SET UP GUEST NETWORKING

---

If you want to preserve the security of your network while still allowing visitors and others to access it, you can take advantage of a new feature available only to the simultaneous dual-band models of the Extreme N and Time Capsule: Guest Network. This exceedingly nifty feature splits your Wi-Fi network into two separate networks (technically creating two *virtual LANs*) while using all the same actual hardware. The guest network provides users with Internet access, but doesn’t pass any traffic to or from the main network. People connecting to a guest network can’t access computers or devices on your main network, including printers. You can optionally allow guests to see each other’s traffic—useful for iChat over Bonjour with file transfer, for instance.

By setting either no network password or using a wireless password that differs from your main network, you don’t have to give out your main network password, either, which may be the same password you use in other places.

---

***No password, no problem:*** *If you don’t password-protect your guest network, guests can gain wireless Internet access with no hassle, and you’ve not put other network resources at risk.*

---

**Note:** A guest network must use both bands, and must have the same network name on both bands. There's no option to change either behavior. You also can't throttle a guest's access if they're using excessive bandwidth or most of your Internet connection.

**Note:** Hidden in the resource files for AirPort Utility are messages that relate to throttling or limiting the bandwidth available to guests. That feature isn't available, but might be something Apple was considering and rejected (but left traces of in the software), or a future option the company will add if it's useful.

To set up a guest network, follow these steps:

1. Launch AirPort Utility, connect to your base station, and click the Manual Setup button.
2. In the AirPort pane, click the Guest Network button (**Figure 110**).



**Figure 110:** Guest Network view lets you set options for visitors to use your Internet connection without accessing your main network.

3. Check Enable Guest Network and label the network. This name appears in the AirPort menu.
4. Optionally check Allow Guest Network Clients to Communicate with Each Other to provide Bonjour networking.
5. Optionally set a password by selecting either WPA2 Personal or WPA/WPA2 Personal from the Guest Network Security pop-up menu. Enter a password and then re-enter to verify it.
6. Click Update.

# 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 an AirPort network work well. Let's first look at eliminating sources of conflict, and then we'll look 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](#) (two pages 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.
- Is your Wi-Fi network 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 use wired Ethernet or upgrade to computers that can use the 5 GHz band 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 that use a band that doesn't interfere with your Wi-Fi network (swapping 2.4 GHz for 5.8 GHz or 900 MHz, or vice versa). Or upgrade your computers and Wi-Fi network to use 5 GHz instead of 2.4 GHz, a potentially expensive proposition, but one guaranteed to produce better results.
- In 5 GHz, use lower-numbered channels; 5.8 GHz falls within the highest range of channels supported by 802.11n base stations. (This also works for wISP interference.) This reduces the signal strength of your network by 95 percent, but it might be the only solution in extreme cases.
- Try T-Mobile's Unlimited Hotspot Calling, which offers cordless calling from a cell phone that also includes a Wi-Fi radio. You make and receive unlimited U.S. calls for \$10 per month (1–5 lines on one plan) over your own Wi-Fi network or any T-Mobile HotSpot (<http://www.theonlyphoneyouneed.com/>).

### **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.

### **Lower Power to Reduce Interference**

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.

In 5 GHz, you can switch from channel 149 or higher to channel 48 or lower to drop power output by 95 percent in 5 GHz while remaining the same in 2.4 GHz. See [Spectrum Trade-offs](#).

Or, to reduce the overall transmission power, run AirPort Utility, connect to the base station, click the Manual Setup button, and click Wireless Options in the AirPort pane's Wireless view. Set Transmit Power to a level below 100 percent, click Done, 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 its base stations, but not for 5 GHz, which doesn't need the additional "robustness," as there's much less interference. With the new simultaneous dual-band Time Capsule and Extreme N, the option to use interference robustness appears without an explanation, but still applies only to the 2.4 GHz network.

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. So, it seems that turning Interference Robustness on is helpful only if you use Wi-Fi at a short distance from a base station and if 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, 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.

**Note:** Mac OS X 10.4 Tiger has an option to enable Interference Robustness on a Mac, via the AirPort menu, but that was removed from 10.5 Leopard; Windows never had such an option.

To enable Interference Robustness on a base station, connect via AirPort Utility and click the Manual Setup button; 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 base station has the option enabled, there could be a performance improvement.

# Explore the Internet's Future with IPv6

IPv6 is the next big thing to hit the Internet—in 1999! This “new” technology was developed in the late 1990s to address a problem with IP addresses. The Internet as widely deployed into the 1990s uses IPv4 (version 4) networking, which has a relatively small number of possible addresses. IPv6 fixes a few other problems, but it mostly expands the address space from offering about 4 billion IP addresses to offering 4 billion raised to the fourth power. This increase in available addresses should let the Internet run until perhaps the end of time.

However, IPv4 addresses (as of mid-2009) still haven't run out, and the crisis continues to be averted by using techniques like NAT, which allow a single public IPv4 address to serve any number of private, off-the-direct-Internet IPv4 addresses.

Still, the transition is happening. In 2008, several significant events occurred that increase the likelihood that more people and companies will use IPv6 addressing in the next couple of years.

---

## IPv6 BACKGROUND

---

Because IP addressing is a fundamental part of how data travels between end points on the Internet, all the infrastructure that handles IP addressing must become IPv6 savvy. That's been both a delaying factor and part of the increased momentum: if you upgrade a bunch of core Internet routers, suddenly IPv6 works in a lot more places.

---

***Same Internet: IPv4 and IPv6 can work on the same Internet; I explain that shortly.***

---

IPv6 came into being because IPv4 addresses were predicted to run short sometime after the turn of the millennium. The Internet wasn't designed with billions of computers and devices in mind, and thus the possible addresses available to use in IPv4 weren't sufficient.

Running out of IP addresses was one problem, but we don't need all the tens of decillions of addresses that IPv6 provides, though we may need trillions some day. Rather, what we do need is the simplicity that IPv6 offers, giving us an abundance of addresses so that the tens of thousands of routers that handle the heavy lifting of the Internet needn't deal with thousands of tiny pieces of IPv4 network ranges.

In the early days of IPv4, many larger organizations, such as Stanford University and Apple, were assigned a vast number of address. Stanford had the entire 16 million addresses beginning with **36** (as in **36.0.0.4**, for instance). Over time, that kind of assignment became impossible and horribly inefficient.

A successful effort to forestall the day addresses ran out allowed very small ranges of addresses in the hundreds or thousands to be assigned to organizations. This led to very large *routing tables*: each router that can send a packet of data anywhere on the Internet, must keep an entry for every one of these tiny and large networks. (This is at a level somewhat above your home broadband network, but below the "top" of the Internet where routers exchange terabytes each day.)

IPv6 means that a lot of complexity in moving packets around is reduced, and the Internet becomes slightly less chaotic to operate.

Fundamentally, there are two big advantages to average folks for IPv6 addressing over IPv4 addressing:

- You can get a large range of publicly reachable IPv6 addresses from an ISP that supports IPv6, whereas most ISPs charge a small fortune for public IPv4 addresses or restrict how many public IPv4 addresses they assign out. (This tightness when handing out public IPv4 addresses comes from all the reasons above, plus the fact that IPv4 address ranges are increasingly hard for ISPs to obtain, too.)

As a consequence with IPv6, every computer, device, refrigerator, and Wi-Fi enabled plastic bunny on your network can be assigned its own public IP address, which is both good (for reachability) and bad (for security).

- Services that don't work today because the Internet's end-to-end principle is disrupted by NAT and other hacks to keep the Internet running will work with IPv6.

This might seem academic and even pedantic, since you're sitting at home with an IPv4 address on your home NAT or a publicly reachable IP address assigned to your computer. However, 802.11n base stations can reach out over the IPv4 network and use IPv6. Yup, that's right. Let me explain how, next.

### How to Write and Read IP Addresses

IPv4 addresses are typically written as four decimal (base 10) numbers, separated by periods, representing a 32-bit number, or 8 hexadecimal (base 16) digits: for example, `128.1.23.233`.

IPv6 addresses are written as eight sets of four hexadecimal digits, separated by colons, representing a 128-bit number. They look like this: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

For what networking engineers call simplicity's sake, internal leading zeroes can be omitted, so that `0034` is written as `34` or `0000` is written as `0`. Also, a range of zeroes in an address like `2001:0db8:0000:0000:0000:0000:1428:57ab` can be replaced with double colons to reduce the written address size; thus, with all extras removed, `2001:db8::1428:57ab`. Simple...right?

---

## IPv4 AND IPv6 TUNNELING

---

The two IP protocols can work together on the modern Internet through tunneling. IPv6 packets can be broken up and nested within IPv4 connections that terminate on an IPv6 network; the packets are *tunneled* from one IPv6 network to another and reconstructed on either end without any loss. Likewise, IPv6 networks can (more easily) smuggle IPv4 packets across their end points.

This tunneling would be of limited interest for average people not running their own high-end routers, except that good souls and organizations have set up IPv6 tunnel termination points, where anyone may pass their traffic through without any pre-existing relationship or payment.

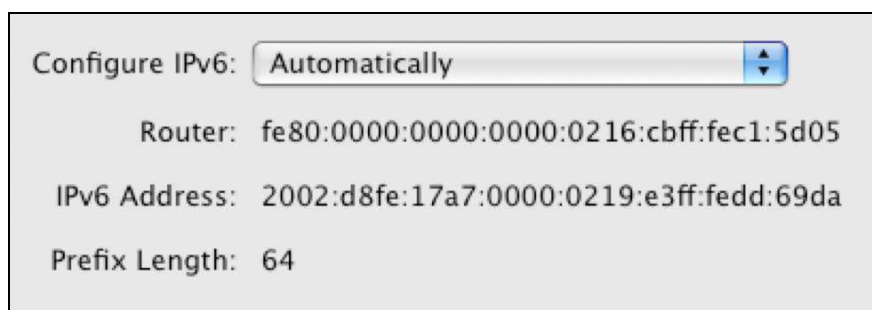
These pools of IPv6 mean that you could configure a 802.11n router at home and at work to use IPv6, allowing you access to each network even though the networks are also assigned IPv4 NAT addresses.

---

**Warning!** *At the moment, this appears to work only with public IP addresses. But that could change. Public IPv4 addresses can be automatically converted into IPv6 addresses (all of which start with 2002), making it an automatic process. But I expect that in the near future, you'll be able to get IPv6 addresses from many ISPs, and manually configure computers to use IPv6 tunnels.*

---

Mac OS X (since at least 10.3 Panther), Windows XP, and Windows Vista all support IPv6 natively. They include built-in tools necessary for handling the newer address protocol. Open up the Network preference pane, select your AirPort or Ethernet network adapter, and click Advanced. In the TCP/IP view, you'll see a section devoted to IPv6. Because I have a tunnel active on my AirPort network, I've been assigned one of these fancy long numbers by the tunnel operator (**Figure 111**).



**Figure 111:** IPv6 details in the TCP/IP tab of a network adapter.

---

**Warning!** *Not all Internet-capable software—such as Web browsers, FTP clients, and email programs—understands and can use IPv6, even though it should. Older software that wasn't designed with the future in mind can barf on IPv6 addresses. Current versions of Safari and Firefox handle IPv6 addresses.*

---

If you want to test the current state of the art, you should know a bit about the configuration options for Apple's 802.11n routers and IPv6.

---

## CONFIGURE IPv6 IN N ROUTERS

---

To start with, launch AirPort Utility, connect to your base station, click the Manual Setup button, and click the Advanced icon. One IPv6 button appears labeled simply IPv6; another button, IPv6 Firewall, shows up if you choose Tunnel from the IPv6 Mode pop-up menu.

---

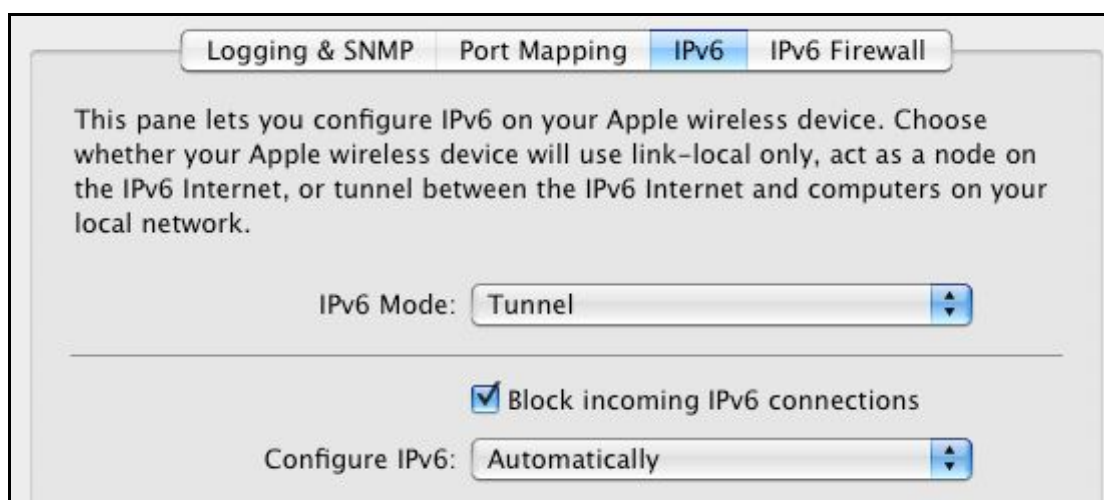
**Warning!** The first release of Apple's Extreme N base station included less-secure IPv6 support, which could have accidentally exposed otherwise unreachable computers. Apple revised its IPv6 default settings in mid-2007 and added firewall support. If you own and haven't upgraded the firmware of a 10/100 Mbps Extreme N, now's a good time.

---

## The IPv6 View

The IPv6 view (**Figure 112**) lets you choose among three possible modes:

- **Link-Local:** With this option chosen, you'll use IPv6 over the LAN. Link-Local can be useful in some organizations that are already routing IPv6 in their networks not only to avoid using NAT but also to better scale their networks.
- **Node:** Choose this option to put the base station directly on the Internet as an IPv6 node using a required IPv6-enabled connection to the Internet via your ISP.
- **Tunnel:** With Tunnel chosen, IPv6 packets are encapsulated inside an IPv4 tunnel to a location that handles routing among (currently) other public IPv4 addresses wrapped up in the same fashion. This mode also enables the IPv6 Firewall button.



**Figure 112:** IPv6 Mode options let you choose how the base station uses IPv6 addressing.



Both the Node and the Tunnel options let you configure an IPv6 address manually by choosing Manually from the Configure IPv6 pop-up menu:

- Node is straightforward: you enter an address that was assigned to the router by whomever handles your IPv6 routing.
- Manual configuration for tunnel is much more involved and beyond my IPv6 abilities! It requires a number of settings that only an expert would love. The Automatically option for tunnel provides the right settings, however.

If you check the Block Incoming IPv6 Connections box, you're cutting yourself off from the Internet as an active end point; this box is part of the result of the previously mentioned flaw in the security model in the first AirPort Extreme with 802.11n release. Even with this box checked, the base station can originate outgoing IPv6 connections.

## The IPv6 Firewall View

In the IPv6 Firewall view, you can set a couple of options that allow you greater flexibility and security:

- Checking Allow Teredo Tunnels can let IPv6 work with an IPv4 NAT, but, as with the Node option in the IPv4 tab, you must have a broadband modem or other device on the network that can use the Teredo protocol and talk to an Internet host that handles the conversion. Apple hasn't built in direct use of Teredo, which seems like a future step.

---

***If Teredo was built in:*** With Teredo tunneling built into a 802.11n router, you could let any computer with private IPv4 addresses be reachable from the public Internet via an IPv6 address.

---

- If you set Allow Incoming IPsec Authentication, you're offering the base station a chance to use encrypted IPv6 tunnels. IPv6 does not require encryption, but it allows strong encryption via *IPsec*, a method that's used for virtual private networks and to secure Back to My Mac, among many other purposes.
- The Exceptions list allows specific computers to punch through the IPv6 firewall.

---

## IPv6 ADVANCES

---

In the introduction to this section, I mentioned that a few significant events had occurred that made it more likely IPv6 would start taking off. You might want to know what those are!

- **Root DNS resolution:** While the software that turns domain names into numbers has long supported IPv6 addresses through a new record type, the *root nameservers*—the servers that handle .com, .net, .uk, .nu, and so forth—weren't IPv6 capable. Early in 2008, that switch was flipped. With that change in place, anyone who has a domain name can have their Web site, for instance, be available via an IPv4 address and an IPv6 address. Some Web browsers support IPv6 (like Safari); others do not yet.
- **Google launches IPv6 site:** Although technically this was a very minor move—just a matter of assigning a public IPv6 number to www.google.com, it's a big boost from the morale standpoint and now a pure IPv6 network can access Google without any fancy footwork.
- **IETF eats its own dog food:** At a conference in early 2008 of the *Internet Engineering Task Force*—a group that works together to set international standards, organizers planned and executed an IPv4 outage. Only IPv6 could be used for a few hours, though it was done on a voluntary basis. The results were enlightening, even to members who have been working on and with IPv6 for years, showing them where gaps exist and what's actually reachable. There's more movement to change as a result.
- **The U.S. government mandated IPv6 support among agencies:** In mid-2008, a long-expected mandate came into play that required all government agencies to be ready for IPv6. They didn't have to use it internally, but all their infrastructure had to be ready for it. Government agencies are just as likely to run out of IP addresses as the rest of us. Having the pieces in place makes it more likely that, as networks are redesigned or built, IPv6 will be a building block for those agencies.

# Appendix A: Apple TV and Wi-Fi

The Apple TV is a nifty device designed to act as a conduit to stream and sync content from computers on your network and present it on a home-entertainment system, most likely an HDTV set. The latest version can also access the Internet directly for watching YouTube videos, renting movies from the iTunes Store, and viewing pictures on Flickr and MobileMe.

The Apple TV was unveiled in early 2007 and shipped in March 2007; a major revision that upgraded all models was released in early 2008. The first release could store content on its internal drive as well as stream it from computers with iTunes running on the local network. The 2008 update added the capability to purchase and rent movies and TV shows directly from the iTunes Store via the Apple TV without using iTunes on a computer.

In this section, I cover how to set up your network for an Apple TV and how to configure an Apple TV to receive video and audio.

---

***Cheap music:*** *The AirPort Express is a great alternative to the Apple TV for transferring just audio over your network. You can connect to an Express N wirelessly or via Ethernet on an 802.11n network with no problems.*

---

The Apple TV can receive content from a single computer 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 the 2.4 GHz and 5 GHz bands, just like any 802.11n-savvy Mac. It has just 10/100 Mbps Ethernet, not gigabit Ethernet, which is peculiar for a device intended to receive a lot of data.

When connecting to a simultaneous dual-band base station, the Apple TV should automatically choose the 5 GHz network, which offers the best throughput.

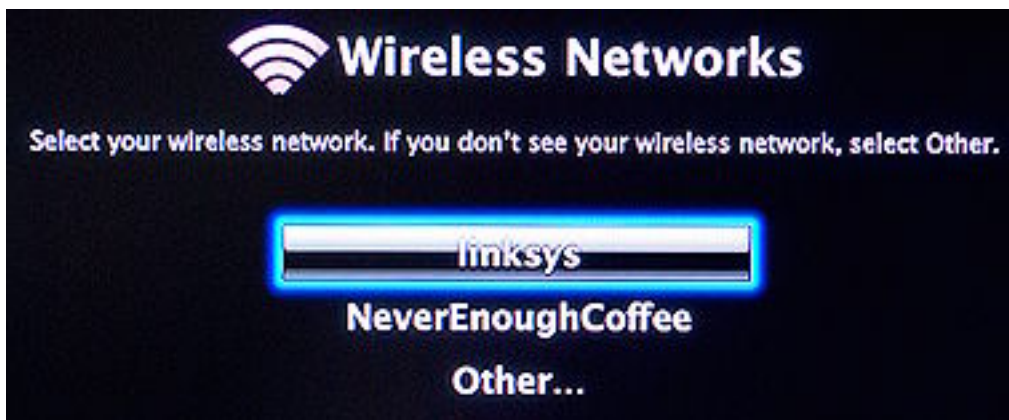
## Use Ethernet First, Then Unwire, for Best Initial Sync

If you're using an Apple TV with an 802.11g network or in the 2.4 GHz band, connecting via Ethernet lets the Apple TV sync with a 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://support.apple.com/kb/HT1784>.

**Tip:** Reports indicate that placing an object on top of the Apple TV can dramatically decrease the range of its Wi-Fi radio.

The Apple TV connects to a network in a straightforward way:

- If you plug the Apple TV into an Ethernet network with a DHCP server feeding out addresses—such as the default configuration for all Apple base stations—the device automatically obtains an address. You can later switch the Apple TV to use Wi-Fi after an initial synchronization. For now, connect the Ethernet cabling, skip ahead a page, and follow the directions *after* Step 5.
- If you'd prefer to avoid Ethernet and use Wi-Fi, 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 to view the Wireless Networks screen.
  3. Select your network (**Figure 113**), or if you have a [Closed Network](#), choose Other and enter a network name.



**Figure 113:** Choose your network from the list.

4. If your network has an encryption key or passphrase, use the Apple Remote to enter it (**Figure 114**), and then select Done. (The password is displayed on the TV screen as you type it.)



**Figure 114:** Use the Apple Remote to navigate the visual keyboard and select the letters in your network passphrase.

5. If your network uses static addresses or has other particular requirements, choose Configure TCP/IP from the Network screen to enter an IP address, set DNS servers, or control other details.

With either an Ethernet or Wi-Fi network connection in place, you can now pair the Apple TV to a particular Mac. If the Apple TV isn't already on the Computers screen, go through the Settings screen to the Computers screen. Select Connect to iTunes. Enter the code that appears on the Apple TV in the Mac's copy of iTunes (first select the Apple TV under Devices in the iTunes sidebar), and then syncing begins! It can take a while 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.

**Tip:** To learn more about the difference between *pairing* an Apple TV with one Mac (thus syncing content to the Apple TV) and *sharing* an Apple TV with one or more computers (thus streaming content to the Apple TV), and for detailed directions, see <http://support.apple.com/kb/HT1143>.

# Appendix B: AirPort Utility Extras

AirPort Utility has a few more tricks up its sleeve. Notably, you can back up, export, and import configuration profiles; connect over the Internet to configure a base station; and revert to an older version of the firmware. At the end of this appendix, I also clarify the use of a few settings in the AirPort pane and the Advanced pane.

---

## CREATE AND MANAGE PROFILES

---

The original AirPort Express compact base station released in 2004 included a unique feature: defining and storing multiple *profiles*. A profile is a complete set of configuration parameters; each profile resides on the base station in non-volatile (persistent) memory. Profiles are available on all 802.11n base stations.

---

***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 for initial setup of a base station, 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.

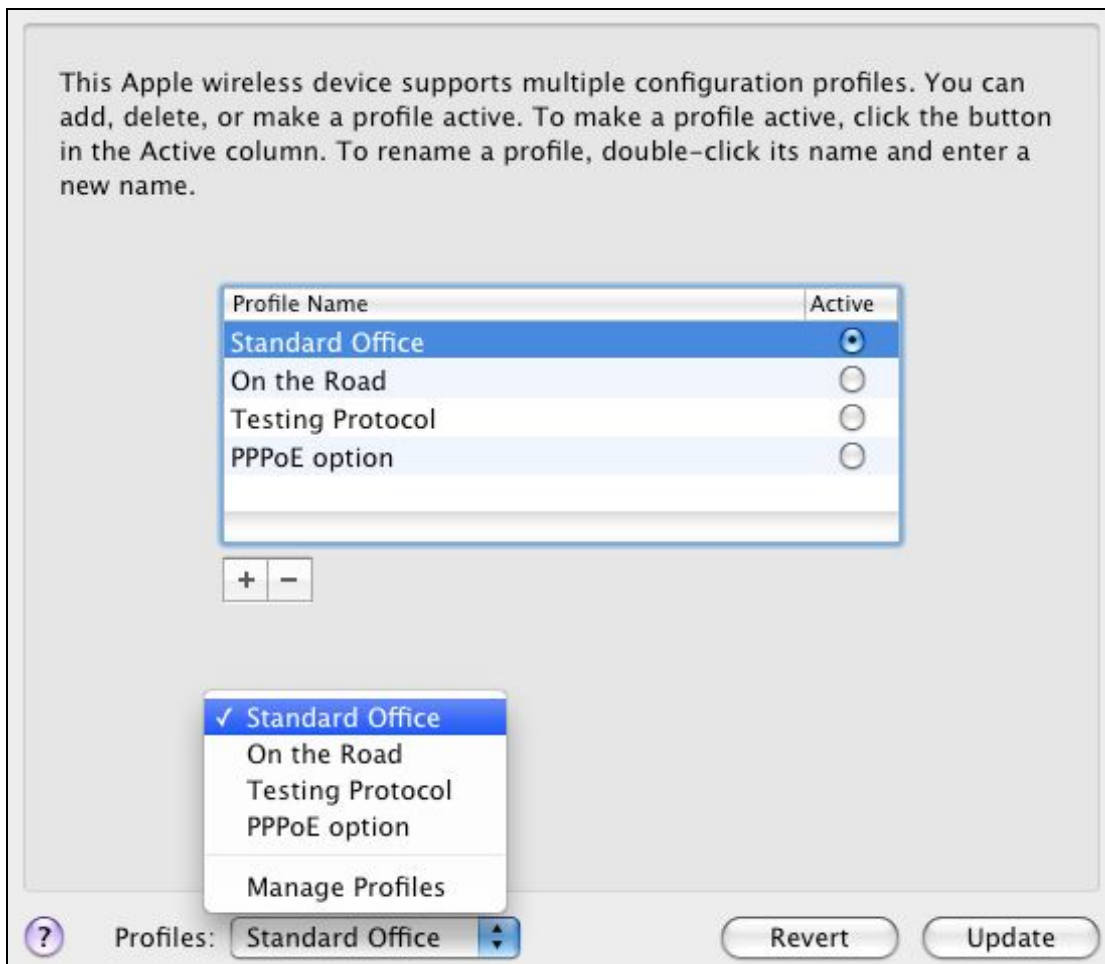
The screen that appears lets you create, activate, and delete profiles.

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

You should now see another profile in the list. 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 115**). You must click Update to activate a given profile, or to save changes that you make to the active profile.



**Figure 115:** 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 with 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 profiles 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 base station released starting in 2003; stored profiles are available only with the 802.11n series and original AirPort Express.

---

***Management utilities may never return:*** AirPort Management Tools lets you manage several original AirPort Extreme and Express base stations at once, including applying a model configuration file to them, but it doesn't work with the 802.11n models. The tool wasn't updated when the first Draft Extreme shipped in February 2007. Apple told me at that time that they'd revise the utility, but given that it's more than 2 years later with no news, I'm not holding my breath.

---

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:

---

**Warning!** Before importing a profile, you should save a copy of your current active profile using the steps just previously. Importing a profile overwrites your current active base station 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.

Base stations with 802.11n allow timed settings, which can restrict access to given computers at given times of the day or week; port mapping rules for allowing inbound access to local computers; accounts used for attached disks; DHCP reservations for assigning addresses to local computers; and miscellaneous other settings. You can choose to import one, two, a few, or all settings (**Figure 116**).



**Figure 116:** Select settings to import.

4. Choose which options you want to import and click OK.
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 items like Timed Access Control or DHCP Reservations lets you transfer just those settings among multiple base stations when you update them on one base station without resetting the base station's name or an assigned IP address.

---

## CONNECT REMOTELY

---

You may want to set up remote access to your base station, so that you can configure it via its WAN port—from either 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. Open the AirPort pane and click the Base Station button.
3. Check Allow Configuration over Ethernet WAN Port.

With remote access on, AirPort Utility can now access a remote 802.11n base station 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.

You can also use MobileMe to enable remote access from a Leopard or Snow Leopard system with Back to My Mac enabled. See [Access a Base Station via MobileMe](#).

---

***Secure connection:*** You can enter a base-station password and configure over a local or remote network without fear of interception. Apple confirmed for me that all management connections are securely encrypted; I tested and found that to be the case.

---

---

## 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 before. This has happened at times with AirPort base-station firmware, the software code that runs on the base station itself. Many firmware releases have had minor defects, often quickly fixed, that disable crucial features or make them erratic.

As long as the base station is responsive, you can go backward in AirPort Utility. (If it's not responsive, follow the advice in [Quick Troubleshooting Guide](#).)

1. Choose Base Station > Upload Firmware (**Figure 121**).

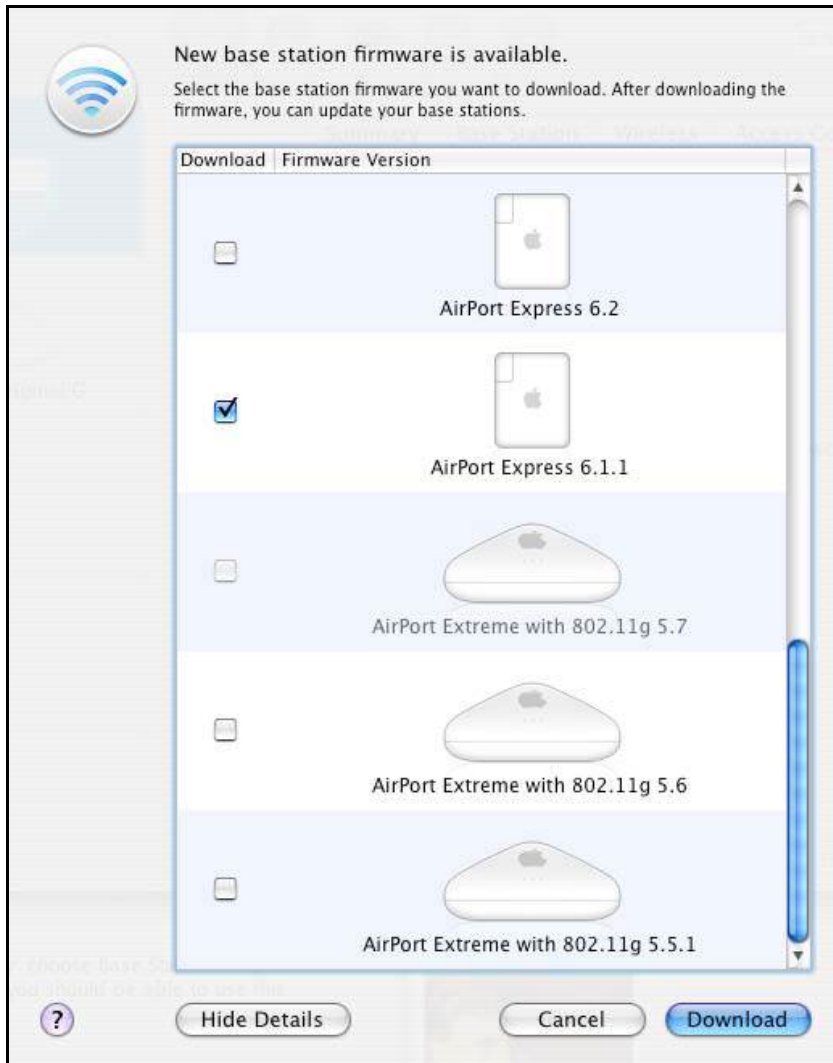


**Figure 121:** You can choose firmware that's stored in AirPort Utility, or choose a separate firmware file.

2. Look in the Upload Version pop-up menu to see if you already have previous versions of firmware downloaded:
  - If you do, choose the one you want and click OK. That's it! You can skip the rest of these steps.
  - If you don't, continue with Step 3.
3. Start retrieving 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 an image and a description of a model type, and a firmware release number (**Figure 122**).



**Figure 122:** AirPort Utility lets you retrieve any older versions of base station firmware.

4. Select the checkbox beside each firmware release you'd like to retrieve, and click Download. Entries that are already stored locally are dimmed out.
5. Once you've downloaded the older firmware into AirPort Utility, choose Base Station > Upload Firmware. Your desired older

firmware version should appear as an option in the Upload Version menu. Choose it and click OK.

**Note:** 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 pane beg for additional explanation.

### Base Station Settings

The Set Time Automatically controls allow you to set the time on any base station model released starting in 2003 via time servers operated by Apple or that you specify. With N routers, you prime the pump by choosing your time zone from the Time Zone pop-up menu. (It's unclear how older routers set the time zone automatically; my 2003 Extreme G always had the appropriate local time.) Hardware tends to lose track of time without external correction, so setting the time can ensure that any timed access rules you set function; see [MAC Address Filtering](#).

Click the Options button to set light options and update behavior:

- The Status Light pop-up menu controls whether the light on the front of the base station is green when everything is normal—Always On (Default)—or if it blinks with activity—Flash On Activity.
- Check for Firmware Updates allows the base station to communicate with Apple to figure out whether newer software is available. Check the box next to the menu and choose a frequency. Your base station's status light will slowly flash its amber color when there's an update. This option is separate from the AirPort Base Station Agent noted in [Launch AirPort Utility and Keep Up to Date](#).

### Wireless Settings

The Wireless view's Wireless Options dialog hides several useful controls for the built-in radio:

- **Country:** Change the country in which you are operating your base station; it should be preset to the country in which you purchased

the router. 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! And go to jail.

- **Multicast Rate:** This option concerns a subset of networking traffic that all connected computers can receive. Setting it higher can slightly improve the speed on a network with mixed 802.11g/n devices, but also locks out computers that are far enough away to need to connect at slower speeds.
- **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 long. It does not require that any computer log in to the network again.

## Access Settings

The MAC Address Access Control pop-up menu lists RADIUS as one option; Timed Access is discussed in [MAC Address Filtering](#). 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.

### Statistics Settings

An Apple base station 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 knowledge.)

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.

# Appendix C: Setting up a Software Base Station

You can use a Mac equipped with a Wi-Fi adapter card not just as a client on a Wi-Fi network, but also as a base station. In this appendix, I explain how to set up a software base station in Leopard and Snow Leopard, as well as how to use ad hoc networking, which has some elements in common with software base stations.

## Software Base Station or Ad Hoc Network?

A *software base station* walks and talks like a base station: it puts out the same kind of messages that other computers recognize from a base station. You need at least two network interfaces to turn on a software base station: an AirPort adapter plus another, like an Ethernet network connection.

*Ad hoc networking* is a computer-to-computer mode, and it doesn't require a second adapter to reach another network, although it can handle that. Ad hoc can be used sometimes by simpler devices.

Most operating systems distinguish between ad hoc networks (which are sometimes seen as more risky) and base stations. The fact that you can create software base stations eliminates the risk distinction; crackers use software base-station programs to lure hotspot users, for instance.

---

## SOFTWARE BASE STATION

---

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. Apple has avoided fixing this for years, and it's rather frustrating.

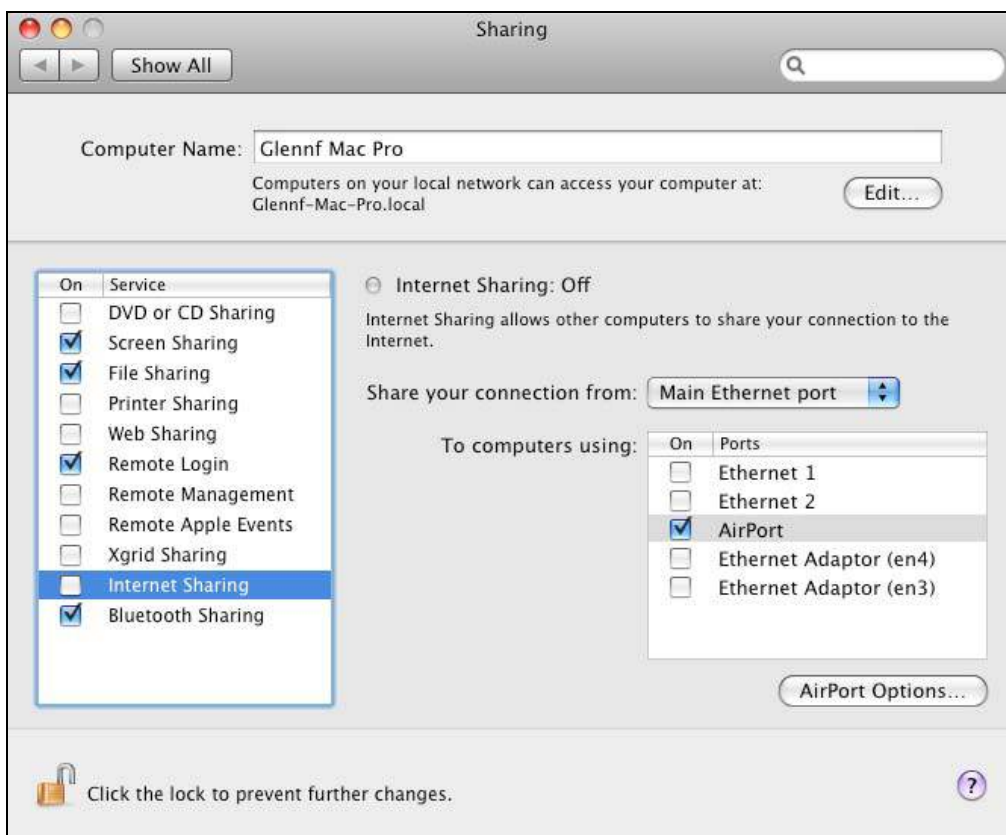


- **Frequency:** Even though 802.11n allows the use of the uncrowded 5 GHz band for less interference and better throughput, Internet sharing over AirPort works just with the busy 2.4 GHz band.

The Software Base Station feature is found in the Sharing preference pane. Before starting, make sure you have either another connection active in the Network preference pane—such as Ethernet or even machine-to-machine FireWire—because you can't create a software access point without another active network connection.

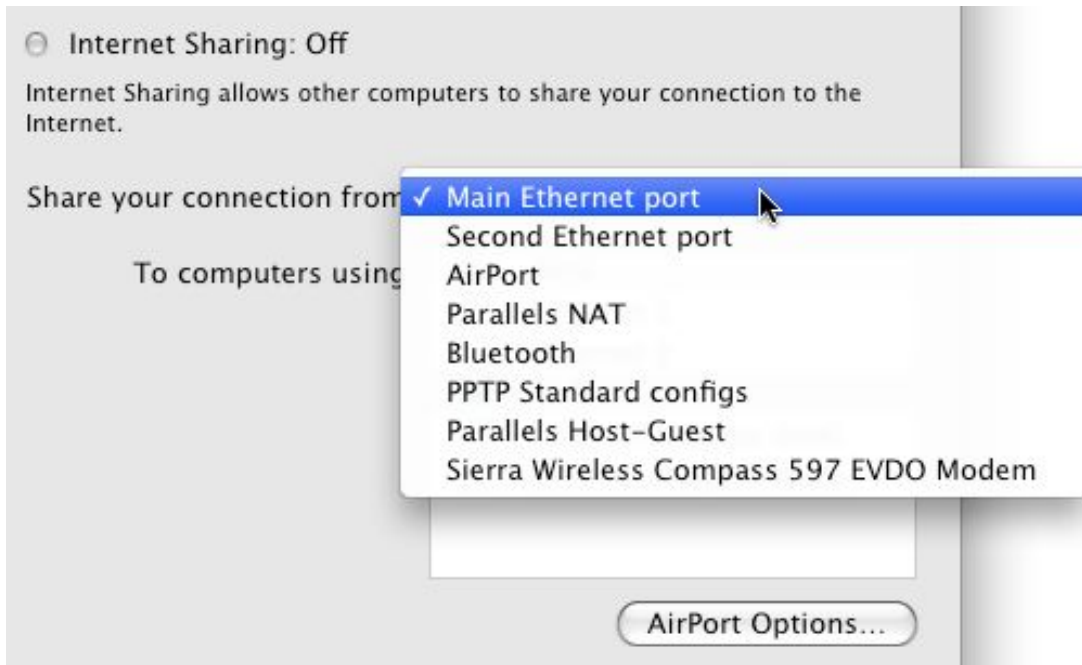
For this example, I assume your Internet connection comes via Ethernet from a cable modem. Here's what to do:

1. In System Preferences, open the Sharing pane and select the Internet Sharing service (**Figure 117**).



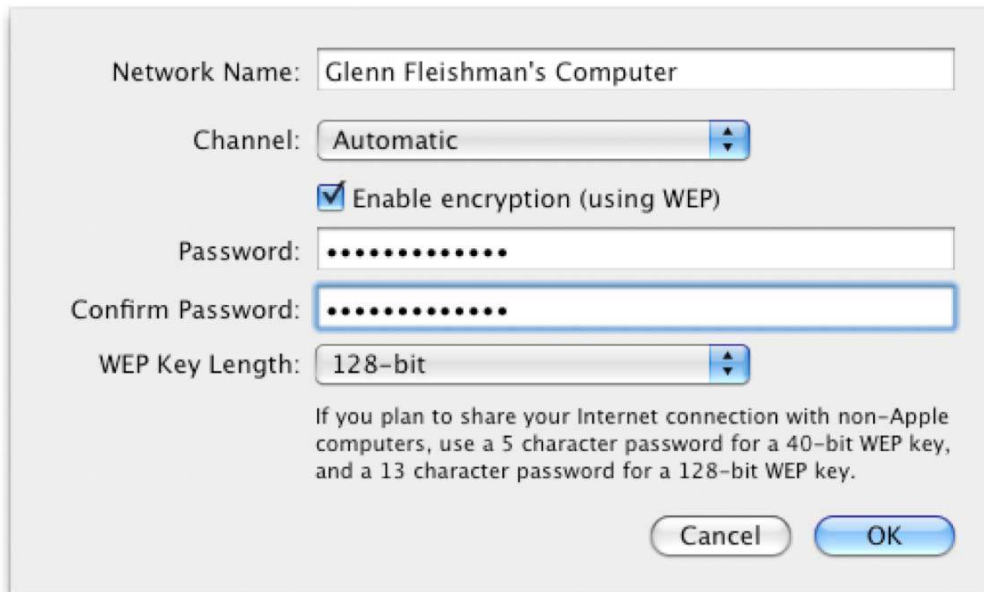
**Figure 117:** With Internet Sharing highlighted in the Sharing preference pane, you can share your wired Internet connection as a software base station by choosing, for example, Main Ethernet Port and checking AirPort. (The checkbox for Internet Sharing isn't enabled until you click the box in Step 5.)

2. From the Share Your Connection From pop-up menu, pick any of the available items (whatever matches how you access the Internet, see **Figure 118**), and then check AirPort in the “To computers using” list.



**Figure 118:** The Share Your Connection From menu lists all active network connections, including some obscure ones, like the virtual interface used with Parallels for Windows virtualization!

3. If you want to also share a connection to wired computers connected directly to your computer, check any of the other interfaces in the “To computers using” list.
4. Click AirPort Options to set the network name, channel, and, optionally, a WEP key (**Figure 119**). Click OK.



**Figure 119:** Set the wireless options you want for your software base station, including a WEP password.

### Use a Hexadecimal WEP Key for Ease of Connection

If you turn on WEP and anticipate computers other than Macs with 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. Check Internet Sharing box to start the service. An alert asks you to confirm that you want to turn on Internet Sharing; click Start.

---

**Warning!** *Internet Sharing could cause a problem by feeding out DHCP messages over a connection that already has DHCP traffic in place. For instance, if your ISP doesn't offer DHCP service in its broadband modem and you have just one Ethernet jack on your Mac, you might plug your Mac into an Ethernet switch into which you also plug the broadband modem. Using Internet Sharing, you could retrieve an address from the modem and feed out DHCP service on the same network segment. This can work, but Apple likes to warn you about it, because especially on work or school networks, you could disrupt the capability of other computers to connect.*

---

If it starts successfully, a green dot appears to the left of “Internet Sharing” above the Share Your Connection From pop-up menu, and the word Off changes to On.

---

## AD HOC NETWORKING

---

*Ad hoc networks* have no center: every computer that joins or advertises an ad hoc network is just as important as every other. If you network a group of machines together informally, with some coming and going now and again, ad hoc networking will work, whereas a software base station would fail if the central party was a laptop that left the network. For instance, you might create an ad hoc network in order to use Bonjour for file transfer among connected computers.

When you set up an ad hoc network, 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.

To set up ad hoc networking, follow these steps:

1. From the AirPort menu, choose Create Network.
2. Enter a network name, choose a channel (Automatic should be the best choice), and check Require Password if you want a modicum of protection (**Figure 120**). Enter a password and verify it; choose 128-bit WEP for a tiny bit more security.



**Figure 120:** Create an ad hoc network by filling in these settings.

3. Click OK to create the network.

Your AirPort menu now shows , which indicates that ad hoc networking is in use.

# Appendix D: Channels Explained

The ins and outs of channels used in each band have wound up in this appendix, as you may need to know the details only when something goes wrong—or if you just want to know more about the technical minutiae of Wi-Fi. In this appendix, you can learn about why 2.4 and 5 GHz channels are organized the way they are, and what happened to 15 missing 5 GHz channels.

See [Pick Compatibility and Optionally Set a Channel](#) to learn how to set your base station's channel in AirPort Utility.

Channels in both 2.4 and 5 GHz are 20 MHz wide; an optional 40 MHz wide or double-channel option was added in 802.11n, although Apple allows wide channels only in 5 GHz.

The two bands have very different ways of defining and making those channels available.

## MHz and Mbps

Megahertz does, in fact, correlate to megabits per second. *Shannon's Law* (or the Shannon-Hartley Theorem), 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 (**Figure 123**).

$$C = B \log_2 \left( 1 + \frac{S}{N} \right)$$

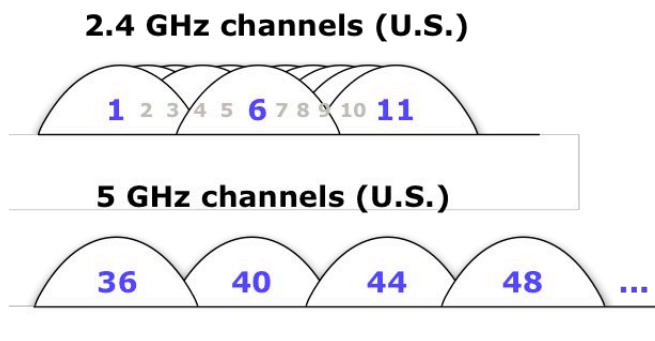
**Figure 123:** Shannon's Law (image via Wikipedia).

---

## 2.4 GHZ CHANNELS

---

In the United States, 802.11 standards can use any of 11 numbered, staggered channels in the 2.4 GHz band (**Figure 124**). 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, assuming you want the least interference. (In some countries, the 2.4 GHz band is slightly wider, allowing for four non-overlapping channels.)



**Figure 124:** 2.4 GHz 802.11 channels are staggered, with channels 1, 6, and 11 having the least overlap. 5 GHz 802.11 channels have little overlap; only the four lowest channels of 23 are shown.

All 2.4 GHz channels have the same power limits, but there's a distinct difference in the permitted level of signal strength—which affects the distance at which Wi-Fi can work and the top speeds available.

Also, due to the overlapping, staggered nature of the channels, there is room in 2.4 GHz 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.

**Note:** If you want the full detail about the limitations of wide channels in 2.4 GHz, read a long article I wrote for my Wi-Fi Networking News site about the three protection mechanisms: intolerance, clear-channel assessment, and politeness; <http://bit.ly/2InqXH>.

**Note:** Channel availability varies widely from country to country; most developing nations allow use in both 2.4 and 5 GHz. The United States generally has by far the most 5 GHz channels available; some countries offer a few more 2.4 GHz channels. Apple lists precisely which channels it supports in the technical specs for its base stations: <http://support.apple.com/kb/SP509>. You can also see a table of 5 GHz channels worldwide at [http://en.wikipedia.org/wiki/List\\_of\\_WLAN\\_channels](http://en.wikipedia.org/wiki/List_of_WLAN_channels).

---

## 5 GHZ CHANNELS

---

The 5 GHz band can be divided into 23 channels in the United States for 802.11a or n. The regular-width channels are the same 20 MHz width as the 2.4 GHz band channels; or you can pick one from among four possible wide channels. These channels overlap only at the fringes, and thus allow many different networks to work in the same space with little interference. (Why only four wide channels? Keep reading to find out.)

### Explaining Channel Numbering

Channels in both 2.4 GHz and 5 GHz are numbered in units of 5 MHz, even though Wi-Fi uses 20 MHz or 40 MHz channels. In 2.4 GHz, these channels are numbered sequentially from 1 to 11 because the channels overlap. 5 GHz channels jump and aren't sequential. Why? Two reasons:

- Because 802.11a/n channels don't overlap, the numbered channels increase by four (5 MHz multiplied by 4) for each selectable 802.11a or n regular-width channel, or by eight for 802.11n wide channels.
- 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.

The 5 GHz unlicensed band is sometimes called (for historical reasons) the *UNII* (Unlicensed National Information Infrastructure) band. This is divided into four pieces: 1 (4 channels), 2 (4 channels), 2 extended (11 channels), and 3 (4 channels).



Apple's base stations support just the UNII-1 and -3 sections, even though Apple's client hardware can use any UNII frequencies. UNII-1 (channels 36, 40, 44, and 48) have a maximum permitted signal strength that's 5 percent of that allowed in UNII-3 (149, 153, 157, and 161).

That's right: when broadcasting over the upper band, devices may emit *as much as 20 times the signal strength*. In the 2009 versions of the Extreme and Time Capsule, Apple increased the signal output to the legal maximum, up slightly from earlier models, providing even greater range.

**Note:** Apple didn't advertise this modest increase in power, but that bump in the upper 5 GHz band is enough to cover that last little bit in a house that a previous model might not have reached.

With 40 MHz channels, only channels 36, 44, 149, and 157 are available; since wide channels are really a set of two normal channels, a wide version of 36 is actually 36 plus 40, 44 is 44 plus 48, and so forth.

When any Apple 802.11n base station is set to choose a channel automatically, it tries to pick an upper-band channel in 5 GHz in order to broadcast with a greater signal strength. Interference will drive it to a lower channel, so it may be worth setting the channel manually for the extra distance, even if interference is an issue.

### **The Missing 15 Channels in UNII-2 and UNII-2 Extended**

It's no mystery where the UNII-2 and -2 extended channels went. These bands overlap with some American military radar use. A compromise among industry, regulators, and the military opened up 11 new channels (the 2 extended section), but also imposed new rules on the existing four channels in UNII-2.

To use these 15 channels, chipmakers and manufacturers must put procedures in place to avoid interfering with radar, despite these uses of radar being high-power, used at limited times, and restricted to relatively small parts of the United States. A device must sense radar patterns and stop using a channel for 10 minutes when it detects a radar pattern, and it must also automatically use the least amount of power necessary. (These requirements were bundled in 802.11h, a standard developed to meet European requirements, and they are also used in the United States in the affected channels.)

False positives for detecting radar are frequent, and thus equipment makers like Apple choose to not offer them, in order to avoid frustration and dropped network signals. Change may be afoot to make these rules more sensible, at which point firmware updates could make them available.

Wide channels aren't available for use in these bands, either, which makes the channels less interesting for ordinary home use. 5 GHz signals drop off so much more rapidly than 2.4 GHz signals that even in an apartment building it's highly unlikely that a base station wouldn't be able to use one of the four wide channel options in 5 GHz.

The -2 and -2 extended bands can use about five times as much power as the UNII-1 band and one-quarter as much as the UNII-3 band.

# Appendix E: AirPort Command-Line Utility

Hidden in the bowels of Mac OS X is a command-line utility that can reveal much more information about your AirPort adapter's status than any other tool Apple provides.

---

**Warning!** Proceed only if you're comfortable working with the command line via Terminal.

---

To use `airport`, a program that reveals lots of detail about your Wi-Fi connection, follow these steps:

1. Launch Terminal from `/Applications/Utilities`.
2. Enter:

```
cd /System/Library/PrivateFrameworks/  
Apple80211.framework/Versions/Current/Resources/
```

This puts you in the right directory to use the program.

3. Enter:

```
./airport --help
```

That shows all the tools and how to configure them, which is beyond the full scope of what I show here.

---

**Warning!** The Snow Leopard version of `airport` removed several options present in Leopard, including a repeat mode for scanning, an associate (or join) command, and others. The reason is unknown.

---

---

## SCAN

---

One of the more interesting options is scanning. You can scan and output the networks and their security settings around you.

Enter:

```
./airport -s
```

You'll see output like that in **Figure 125**:

```
      SSID  BSSID          RSSI  CHANNEL  HT  CC  SECURITY (auth/unicast/group)
NewDualBand 00:24:36:a4:a4:ae -31  149,+1  Y  US  WPA(PSK/TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
@HomeD6E0  00:1b:11:25:c5:a0 -84   2       N  --  WPA(PSK/TKIP/TKIP)
SKYNET     00:1e:58:25:14:7d -74   2       Y  --  WPA(PSK/TKIP,AES/TKIP) WPA2(PSK/TKIP,AES/TKIP)
Yak's     00:21:43:52:c0:e0 -89   1       N  --  WEP
ourwlan   00:0f:66:8e:49:50 -82   1       N  --  WPA(PSK/TKIP/TKIP)
bks       00:0f:b5:5a:3e:ea -70  11       N  --  WEP
Oohla's   00:15:e9:ec:cd:78 -67  10       N  --  WEP
seaWireless 00:21:91:d4:02:d5 -63   8       Y  --  WPA(PSK/TKIP,AES/TKIP) WPA2(PSK/TKIP,AES/TKIP)
dwtjain   00:1c:df:b9:a6:3d -70   6       N  US  WPA(PSK/TKIP,AES/TKIP)
salmon    00:13:10:36:4f:59 -84   6       N  --  WPA(PSK/TKIP/TKIP)
New Galaxy 00:19:e3:32:c3:6f -49   6       Y  US  WPA(PSK/TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
ZaazOutpost 00:1c:10:92:71:92 -63   6       N  --  WPA(PSK/TKIP/TKIP)
BasketballNet 00:1c:10:99:89:53 -55   6       N  --  WPA2(PSK/AES/AES)
```

**Figure 125:** A Terminal dump from the `airport` command-line program.

The output consists of a text table having these headers: SSID (plain text network name), BSSID (the MAC address of the adapter as broadcast), RSSI (signal strength measure), channel, HT (high throughput), CC (country code), and security (authentication type, per-computer or unicast method, and broadcast or group method).

I've explained most of these terms elsewhere in the book. The HT flag (yes or no) indicates whether an 802.11n-style higher-throughput encoding is used; 802.11n improved on 802.11g maximum throughput. The CC code shows the regulatory domain for devices that advertise that information.

If you want to monitor a particular network, you can specify its name, as in:

```
./airport -s BasketballNet
```

which will produce results for Basketballnet.

---

## GETINFO

---

The getinfo option simply dumps information about your current connection:

```
./airport -I
```

```
agrCtlRSSI: -49
agrExtRSSI: 0
agrCtlNoise: -89
agrExtNoise: 0
state: running
op mode: station
lastTxRate: 216
maxRate: 270
lastAssocStatus: 0
802.11 auth: open
link auth: wpa2-psk
BSSID: 0:24:36:a4:9a:e4
SSID: Portage Airbasestation
MCS: 13
channel: 149,1
```

# About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments at [tc-comments@tidbits.com](mailto:tc-comments@tidbits.com). Keep reading in this section to learn more about the author, the Take Control series, and the publisher.

---

## ABOUT THE AUTHOR

---



Glenn Fleishman contributes regularly to *Macworld*, the *Economist*, *Popular Science*, and the *Seattle Times*. He's the Macintosh columnist for the *Seattle Times*, and a contributing editor at *TidBITS*, where he's built the content management software.

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/>). Glenn also appears regularly 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."

---

## AUTHOR'S ACKNOWLEDGMENTS

---

This book has gone through many changes since its first edition in 2005, when Draft N was still a pipe dream, and networks were simpler beasts, even though quite complex.

I want to thank Tonya Engst for her continued work in developing this book through now its third edition, and her attention to detail as we fiddle with the fine points. Adam Engst also continues to help improve this title through brainstorming and great feedback. Thanks to Jeff Carlson for the use of his Apple TV screen photos.

---

## SHAMELESS PLUG

---

I spend my days writing about technology, often related to Wi-Fi. My blog Wi-Fi Networking News (<http://wifinetnews.com/>) covers as much in the field that's interesting as I can find each day, from in-flight broadband over Wi-Fi to finding Wi-Fi at a base camp on Mt. Everest (not me finding it, personally).

---

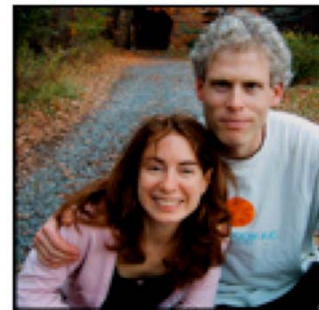
## ABOUT THE PUBLISHER

---

Publishers Adam and Tonya Engst have been creating Macintosh-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.

**TidBITS**  
Mac news for the rest of us



---

## PRODUCTION CREDITS

---

Take Control logo: Jeff Tolbert

Cover design: Jon Hersh

Editor in Chief and template master: Tonya Engst

Publisher and grep automation master: Adam Engst

*Thanks to Glenn for his ongoing enthusiasm for writing books about wireless networking and to Julie Kulik for production assistance.*

# Copyright and Fine Print

*Take Control of Your 802.11n AirPort Network*

ISBN: 978-1-933671-50-5

Copyright © 2008, 2009, Glenn Fleishman. All rights reserved.

TidBITS Publishing Inc.

50 Hickory Road

Ithaca, NY 14850 USA

<http://www.takecontrolbooks.com/>

Take Control electronic books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control ebooks also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

This electronic book doesn't 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 information 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 ebook 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 the trademarks and of the registered trademarks of Apple Inc., you can visit <http://www.apple.com/legal/trademark/appletmlist.html>.



# Featured Titles

Now that you've seen this book, you know that 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 title below or [visit our Web catalog](#) to add to your Take Control collection!

*[Take Control of Exploring & Customizing Snow Leopard](#)* (Matt Neuburg): Make the Finder work for you and get more out of many special Mac OS X features! \$15

*[Take Control of Mac OS X Backups](#)* (Joe Kissell): Set up a rock-solid backup strategy so that you can restore quickly and completely, no matter what catastrophe arises. \$15

*[Take Control of MobileMe](#)* (Joe Kissell): This ebook helps you make the most of the oodles of features provided by a \$99-per-year MobileMe subscription. \$10

*[Take Control of Passwords in Mac OS X](#)* (Joe Kissell): Create and manage strong passwords that keep your data safe without taxing your memory! \$10

*[Take Control of Screen Sharing in Snow Leopard](#)* (Glenn Fleishman): Understand the options and technologies and start controlling and viewing other Mac screens from afar. \$10.

*[Take Control of Sharing Files in Snow Leopard](#)* (Glenn Fleishman): Learn about all the ways you can share files in Leopard, along with advice on selecting the right hardware and software, and setting up proper security. \$10

*[Take Control of Your Domain Names](#)* (Glenn Fleishman): Get expert help with registering, configuring, and managing your Internet domain names like a pro! \$10

*[Take Control of Your Wi-Fi Security](#)* (Adam Engst & Glenn Fleishman): Learn how to keep intruders out of your wireless network and protect your sensitive communications! \$10