Check for Updates
Make sure you have the latest information!

TidBITS Publishing Inc.

Take Control of Your 802.11n AirPort Network

v3.0

Glenn Fleishman

THIRD EDITION

COVERS AIRPORT UTILITY 6

$20

Help | Catalog | Feedback | Blog | Order Print Copy

Table of Contents

Read Me First

Introduction

Quick Start to AirPort Networking

Quick Troubleshooting Guide

Mac Wi-Fi Iconography

Light Reading

Learn Wireless Basics

Wi-Fi Gear from Apple

Plug In Your Base Station and Get Started

Set Up a Network

Pick the Right Place and the Right Channel

Advanced Networking

Connect Your Devices

AirPort Express Extras

Connect Multiple Base Stations

Reach Your Network Remotely

Set Up a Shared USB Printer

Set Up a Shared USB Disk

Read Me First

Welcome to *Take Control of Your 802.11n AirPort Network, Third Edition,* version 3.0, published in May 2012 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and edited by Tonya Engst.

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—using AirPort Utility 6 on the Mac or AirPort Utility in iOS, this book will help you get the fastest network with the least equipment and fewest roadblocks. This book also has advice on connecting to a Wi-Fi network from older versions of Mac OS X and Windows 7.

Copyright © 2012 Glenn Fleishman. All rights reserved.

Updates and More

You can access extras related to this book on the Web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or purchase any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and—usually—Mobipocket. (Learn about reading this ebook on handheld devices at http://www.takecontrolbooks.com/device-advice.)
- Read postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.
- Get a discount when you order a print copy of the ebook.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

Basics

Here are a few “rules of the road” that will help you read this book:

- **Path syntax:** I occasionally use a *path* to show the location of a file or folder in the Mac’s 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.”

- **Big cats:** I often mention features specific to a particular version of Mac OS X, which Apple usually refers to by their “big cat” names:
    - Mountain Lion: 10.8
    - Lion: 10.7
    - Snow Leopard: 10.6
    - Leopard: 10.5
    - Tiger: 10.4
    - Panther: 10.3

- **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 Apple > 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 Wi-Fi view in the Network preference pane, you would click the Wi-Fi item in the list at the left of the pane.

- **Wi-Fi menu:** The Wi-Fi 📶 status menu appears near the right side of the menu bar on a Macintosh. If yours isn’t showing, you can turn it on via a checkbox in the Network system preference pane, in the Wi-Fi view. To learn about the icons that may mark the top of this menu, see Mac Wi-Fi Iconography.

- **Configuring a base station:** Throughout the book, I refer to using a program called AirPort Utility to configure a base station. In almost all cases, to configure a base station in AirPort Utility 6 on the Mac or in AirPort Utility in iOS (both versions are covered in the book), you select the base station in the AirPort Utility graphical display, and then click or tap the Edit button that appears. (You may have to enter a password for the base station first.)

What's New in the Third Edition

This third edition has a significant change: it replaces its former coverage of AirPort Utility 5 in favor of focusing on AirPort Utility 6, which was released in February 2012. *AirPort Utility 6 runs on 10.7 Lion or later*. AirPort Utility 6 has many of the features that are documented in previous editions of this book, but it omits several options designed for mixed 802.11g and 80211.n networks and it can't configure 802.11b and 802.11g AirPort base station models (any base station released from 1999 to 2006). Also, it supports only iCloud, not MobileMe, for remote connections.

The big new feature in AirPort Utility 6 is a graphical depiction of the layout of an AirPort network. This is terrific for visualizing how parts are connected and seeing where errors lie.

This third edition also discusses AirPort Utility for iOS, which has a similar approach to AirPort Utility 6, and makes it possible to configure and manage an Apple base station without a desktop computer. That's a first for Apple.

Older versions of AirPort Utility remain available:

- AirPort Utility 5.5.3 for Leopard and Snow Leopard and 5.6 for Lion are the latest releases of the previous version of AirPort Utility.
- AirPort Utility for Windows XP, Vista, and 7 is, at this writing, nearly identical to version 5.5.3/5.6 for Mac. I expect that Apple will update the Windows version of AirPort Utility to be feature identical to the latest Macintosh version.

Free download: *If you need help with AirPort Utility 5, you can refer the previous edition of this ebook—there's no extra charge. Follow the "access extras" link in Ebook Extras, and look in the blog.*

Introduction

Apple introduced integrated Wi-Fi 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 costs were high, speeds were low, and complexity was manifest. Apple's products shot off the shelves due to their relatively low initial price, simple configuration interface, and excellent performance.

Apple originally required add-on cards for Macs to use Wi-Fi; a few years ago, the Mac Pro became the last model for which Wi-Fi was an extra-cost option. Apple now builds the fastest flavor of Wi-Fi, called *802.11n,* into every Mac it sells, as well as every iPhone, iPod touch, and iPad.

Despite Apple's 13-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 an 802.11n AirPort network and offers tips to help save time, improve security, extend range, and enjoy a technical edge when working with Wi-Fi.

Although this book focuses on using AirPort Utility 6 (with Lion and later) and AirPort Utility (for iOS) to configure your network, I also cover compatibility and connections with older computer hardware, and how to connect to 802.11n via Mac OS X and Windows 7. I also provide some information to help you use Wi-Fi with 10.6 Snow Leopard and 10.5 Leopard.

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.

Free download: *If you need help with AirPort Utility 5, you can refer the previous edition of this ebook—there's no extra charge. Follow the "access extras" link in Ebook Extras, and look in the blog.*

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 a few pages to the Quick Troubleshooting Guide or see Light Reading to learn what the light on your AirPort base station is trying to tell you. Also, you may especially wish to consult Overcome Interference.*

Learn wireless basics:

- Get a quick grounding in Learn Wireless Basics.
- Familiarize yourself with Wi-Fi Gear from Apple.

Plan your network:

- For common configurations, see Picture Your Scenario and focus on the diagrams and descriptions at the beginning of: New Network, Single Base Station, Extend a Network via Ethernet or Wi-Fi, and Replace an Existing Base Station.
- For ideas on using the AirPort Express, skim AirPort Express Extras.
- For more advanced possibilities, consult Connect Multiple Base Stations, 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 covers creating a Software Base Station and Ad Hoc Networking.

- Although it's not necessary for a basic setup, you can consider the channels and bands that your Wi-Fi network will use in Spectrum Trade-offs.

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. 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.
  - For existing networks, find what you need to Extend a Network via Ethernet or Wi-Fi or Replace an Existing Base Station.
  - When wireless is the way to go, learn what you need to extend a network using only Wi-Fi. See Bridge Wirelessly.
  - Hook up a larger network with many base stations. See Connect Multiple Base Stations 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.
- Pick the Right Place and the Right Channel 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 Spectrum Trade-offs.
- Share a printer or a hard drive. See Set Up a Shared USB Printer or Set Up a Shared USB Disk.
- Set up Time Machine backups with a Time Capsule base station. Read Work with Time Capsule.

Connect to your base station:

- Find out how to connect Macs and systems running Windows to a base station in Connect Your Devices.
- Access your network when you're not physically on it. See Reach Your Network Remotely.
- Access your base station with the Back to My Mac service in iCloud. See Access a Base Station via iCloud.

Add music and video:

- Use the AirPort Express to stream music. See Stream Audio with AirPlay and Share with Airfoil.
- Get jiggy with a video- and audio-streaming set-top box, the Apple TV. See Appendix A: Apple TV and Wi-Fi.

Connect between Macs:

- Understand the new AirDrop peer-to-peer file-transfer feature in Lion, and see if your hardware and situation are a good fit to use it. Read Share Files with AirDrop.

Secure your network:

- Avoid security tricks that don't work. Consult Simple Tricks That Don't Work.
- Apply encryption using the best—and often simplest—method. See Use Built-In Encryption.
- With a 2009 or later AirPort Extreme or Time Capsule, you can Set Up Guest Networking.

Learn still more advanced topics:

- Stop pulling your hair out over a problem with new firmware you install that doesn't work. See Revert to Older Firmware.
- Get a few details about saving and re-using an AirPort base station's settings in Appendix B: Configuration Files.

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 about a problem by decoding 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 Wi-Fi menu as an available network, nor in AirPort Utility as an available base station, or AirPort Utility identifies it as missing, 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 unplugging a Time Capsule. Make sure Time Machine backups or other transfers aren't in progress before you power cycle a Time Capsule—for each computer on your network that uses the Time Capsule, eject any mounted Time Capsule volumes and halt Time Machine backups. The easiest way is via the Time Machine system preference pane: flip On to Off. After you power cycle the Time Capsule, you can flip Time Machine back on for each computer.*

   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 see if it appears in 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 Appendix B: Configuration Files).

   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 triangle reversed out of a gray circle (**Figure 1**).

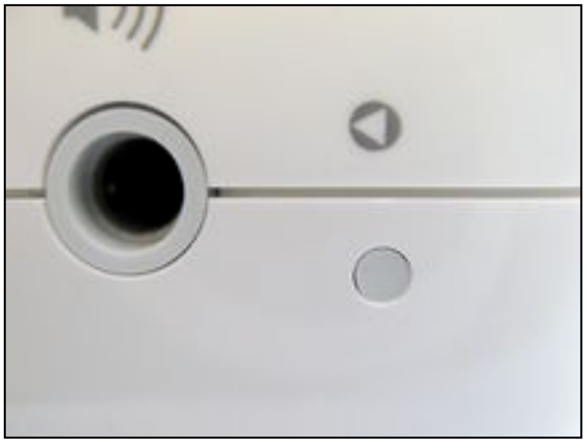


Figure 1: The reset button is located below the reversed-out white triangle; here, it's next to the audio port of an AirPort Express.

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 if the unit is under warranty. If not, it may be time to invest in a new one.

Other Troubleshooting

Can't see base station's network from a device

Did you set the base station to use just the 5 gigahertz (GHz) band? Only Mac models released starting in 2005 with built-in 802.11a or 802.11n can connect, and no iPhone nor iPod touch supports 5 GHz (all models of the iPad do, however).

Or, did you set the base station to allow 802.11n-only connections in 2.4 GHz? Late 2006 and later Macs have 802.11n built in, and the iPhone and iPod touch added it in 2010. It's also included in all iPad models. For more help, read Pick the Right Place and the Right Channel.

Further, computers can sometimes temporarily lose their capability to find Wi-Fi networks—and don't ask me why! It's a mystery of many years. Try turning the adapter off and back on—on a Mac, choose Turn Wi-Fi Off from the Wi-Fi 🛜 menu, and then choose Turn Wi-Fi On. Another common fix is to restart the computer.

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

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

- Did you inadvertently set the base station to allow 802.11n-only connections in the 2.4 GHz band? See Connect Your Devices (look for the first Warning in the chapter).
- Interference from other networks may be the problem. Consult Overcome Interference.

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 Turn On WPA/WPA2 or WPA2 Personal.

Can't connect to a base station via Ethernet in AirPort Utility after selecting it and seeing the summary screen

You might have hit an unusual bug. 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 Preferences pane, select your Ethernet adapter, then click Advanced. In the Hardware view, choose Manually from the Configure pop-up menu and then Standard (1500) from the MTU pop-up menu. Now, click OK, and then click Apply.

Firmware update makes base station act erratically

Try to Revert to Older Firmware.

Network works erratically

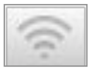
Another network might be interfering with yours. See Overcome Interference.

Conflicting signals seem to cause network problems

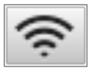
Read Overcome Interference.

Mac Wi-Fi Iconography

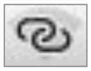
The Wi-Fi menu—located on the system menu bar—reveals what kind of connection is in progress on your computer. Knowing what the icons mean can help you troubleshoot problems. This icon is always at the top of the Wi-Fi menu.



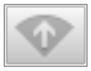
A gray fan indicates an active Wi-Fi network adapter that isn’t currently connected to any network. Read Connect Your Devices to get started.



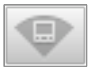
A full fan with one or more black bars—the bars represent current strength—indicates a current Wi-Fi connection to either a base station or a network created through the Sharing preference pane’s Internet Sharing service. (An animation of each wave turning black in turn occurs while the connection is underway.) For more information, consult Connect Your Devices and Appendix C: Setting Up a Software Base Station.



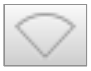
iOS devices may share a cellular connection via Wi-Fi using the Personal Hotspot feature. When a Mac connects to such a network, the fan icon is overlaid with interlinked loops. Apple also uses this symbol in iOS to indicate a tethered connection of this kind.



A fan showing an up arrow indicates that the Internet Sharing service is active on this computer. See Software Base Station.



A fan containing a computer shows that the Mac has created an *ad hoc network,* a method of handling Wi-Fi communication among multiple computers without a base station—not even the “software” base station that’s created by Internet Sharing. See Ad Hoc Networking, in Appendix C.



An empty fan outline indicates that either there’s no Wi-Fi adapter in the computer, or the Wi-Fi adapter is off. To turn it on, choose Turn Wi-Fi On from the menu. If the Wi-Fi 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.

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 or a bad cord.

🟢 **Blinking green:** The base station light blinks or flashes green in two 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.

🟢 **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:** A blinking amber light has several meanings:

- The base station has a configuration problem, has lost its network connection, or is suffering from another problem. Use AirPort Utility to troubleshoot the problem.
- A Time Capsule may have a Disk Integrity problem.

Learn Wireless Basics

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

Adapters and Access Points

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 calls its wireless gateway a *base station*.

Apple's line-up of base stations includes the AirPort Extreme, the AirPort Express, and the Time Capsule. When I talk about "AirPort equipment," I mean all Apple base stations, including Time Capsules. 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—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.

What's Wi-Fi?

The name *Wi-Fi* is a certification guarantee for which The Wi-Fi Alliance trade group owns the rights and controls the testing. *Wi-Fi* doesn't stand for anything—it's a made-up name—but it loosely connotes *wireless fidelity,* in the sense of *faithfulness*: devices with Wi-Fi stamped on them work with other Wi-Fi devices following the same standards, or are faithful to one another.

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 Wi-Fi menu in the menu bar, and the Wi-Fi 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.

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.

With newer adapters, a connection may be made directly to another device with peer-to-peer networking at the same time that an adapter is connected to a regular Wi-Fi network. The Wi-Fi trade group calls this *Wi-Fi Direct*, and it's not yet implemented in Mac OS X. Lion's AirDrop feature is a preview of things to come (see Share Files with AirDrop).

The Spectrum Part of Wi-Fi

Wi-Fi networks use *unlicensed spectrum,* so called because regulatory agencies allow license-free use of those airwaves by everyone in a given country. 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.*

Spectrum *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 won't encounter 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 1.9 GHz band is used by newer home cordless telephones.) 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 from 1999–2006 works only in the 2.4 GHz band.

  Previous edition: *You can download the previous edition of this book at no cost to find coverage of how to make older and newer AirPort equipment work together. See Ebook Extras (once you reach the Take Control site, look for the ebook's Blog).*

- **Dual band:** All 2007 and 2008 Apple base stations can use either the 2.4 or the 5 GHz band, but you must choose one before starting or restarting, and use that one until a change is made and the unit is restarted again.
- **Simultaneous dual band:** The AirPort Extreme and Time Capsule models released starting in 2009 can use both bands at once.

For more on the differences between 2.4 and 5 GHz, see Spectrum Trade-offs.

Warning! *Many manufacturers, including Apple, sell specific hardware for each country or regulatory domain in which they do business. Because laws can vary by country and 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. The original popular flavor of Wi-Fi was known as 802.11b, or sometimes just “B.” Somewhat faster and more robust was 802.11g, or “G,” introduced in 2003. The current fastest generation is known as 802.11n, or “N.”

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, 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. 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?

The 802.11a protocol was approved in 1999 even before 802.11b. 802.11a may use only the 5 GHz band, and it never quite caught on because it wasn’t backward compatible with 802.11b or 802.11g, which relied on the 2.4 GHz band. Building an affordable single adapter or base station with both bands that could work at once wasn’t possible until about 2009.

Apple shipped some early Intel-based Macs with 802.11a quietly enabled because it was built into the chips that Apple used for Wi-Fi. It still works in Macs today for compatibility’s sake.

A few years ago, a colleague 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-based Macs with 802.11a. You may want to disable 802.11a in the 5 GHz band on your router to avoid having it slow down your network’s 802.11n devices.

802.11n Technology

802.11n can be ten or more times faster than its predecessor, 802.11g, in typical circumstances when measuring real data passed over a network. 802.11n typically uses several antennas, with at least two receiving and two transmitting data (called 2x2), 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 a different path through space using the same frequencies! Think of this like pool balls on a pool table. A sending base station is the equivalent of two pool players shooting a series of balls that uniquely ricochet across the table (sometimes striking and passing through each other in a ghostly fashion) until they sink into different holes at the other end.

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 75–450 Mbps (megabits per second) in current versions and up to 600 Mbps in advanced versions used in corporate campuses. Apple's current generation of AirPort Extreme and Time Capsule uses three data streams for a maximum raw rate of 450 Mbps with a 3x3 antenna array. The latest Mac hardware has a similar Wi-Fi radio system installed, allowing for the greatest range and speed.

Single-Stream Radios

A form of 802.11n called *single stream* uses one or two antennas and a single data stream, which limits a device to raw rates of 75 Mbps in 2.4 GHz and 150 MHz in 5 GHz (if wide channels are also supported in 5 GHz).

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* lets 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.

Apple has included single-stream 802.11n in all iPhone models introduced starting in 2010 (iPhone 4) and all iPod touch models since 2009 (3rd-generation). The iPad has included single-stream 802.11n from its first model. The iPad handles both 2.4 and 5 GHz networking, while the iPhone and iPod touch are 2.4 GHz only.

The speed of a Wi-Fi network drops somewhat when other Wi-Fi networks are used in the vicinity, when the network is set for backward compatibility (up to 10 percent of the top speed is lost), when older 802.11 devices are used on the network (but only while they actively send or receive data), or when 802.11n adapters are far enough away from the base station to require slower transmission rates.

Compatibility among 802.11 Flavors

While each 802.11 evolution brings unique elements to the table, all 802.11 versions designed for the same band can work together. Newer versions are designed not to tramp all older versions, and base stations can be set to allow all, some, or no backward compatibility.

With Apple gear, for instance, the original AirPort handled just 802.11b, and the AirPort Extreme 2003 added 802.11g, which can talk to B devices with full support. Likewise, Apple's 802.11n base stations handle the older 802.11a/b/g standards.

At one time, Wi-Fi devices using 802.11n were *required* to support older 802.11a/b/g devices, but we'll see more and more hardware in the future that's solely 802.11n. All equipment I've tested calls multiple standard support a *mixed* mode. Apple's 802.11n hardware sports controls that let you choose in 2.4 and 5 GHz which standards to allow.

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 10–30 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.

Upcoming: 802.11ac and 802.11ad

The IEEE has newer standards on the horizon for wireless LANs: 802.11ac, which updates the current standards to 1 Gbps or faster networking in 5 GHz (2.4 GHz speeds stay the same), and 802.11ad, which will use new spectrum way up the dial at 60 GHz for rates as high as 7 Gbps over very short distances, such as within a single room. Devices are planned that will incorporate current 802.11n alongside 802.11ac and 80211.ad in a single package.

Chips with 802.11ac built in will ship during 2012, but it's anyone's guess when you'll be able to buy a base station with this faster 5 GHz flavor. Apple never announces plans, and it's unclear how fast the rest of the industry will upgrade.

Wi-Fi Gear from Apple

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 AirPort Base Station Models and the options for Adapters in Macs and iOS Devices.

At the end of this chapter, you should better understand the gear that you already have, or be in a better position to shop for new equipment.

802.11n and Apple's Choices

Although Apple has made distinct choices when implementing 802.11n, all three of Apple's current 802.11n base stations can handle both the 2.4 band and the 5 GHz band. Current AirPort Extreme and Time Capsule base stations can manage networks on both bands at the same time. The AirPort Express requires that you choose one band or the other.

Note: The 2007 and 2008 models of AirPort Extreme and Time Capsule could only use a single band at a time as well.

For the 5 GHz band, Apple enables just 8 of the 23 possible channels in the United States for use in a base station. This is because of a compromise among the radio equipment industry, the military, and the FCC. This compromise protects 15 of the possible 23 channels for limited military use, but it also makes it more difficult to use those channels for home networks. Apple has chosen not to support those 15 channels in its base stations. The company doesn't think that they would be consistently available in a way that would be useful to most consumers and small offices who would buy AirPort gear.

Note: The adapters in a Mac can, in fact, connect to all the 23 legal channels in the United States. Some companies may deploy Wi-Fi networks using non-Apple base stations that allow the use of all 23 channels, as they're more likely to be available without hitting military rules inside buildings.

Apple also chose to limit wide channels to the 5 GHz band. *Wide channels* are an 802.11n feature that uses two adjacent channels at once—this doubles the raw bandwidth. Apple's choice was an option under the Wi-Fi Alliance's certification rules, but some vendors offer wide channels in 2.4 GHz.

In practice, 2.4 GHz wide channels don't work well, because 802.11n 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's current line-up of base stations that offer Wi-Fi comprise the AirPort Extreme, a solid offering for home networks and small offices; Time Capsule, a backup system coupled with Extreme features; and AirPort Express, a compact router good for extending a network and for travel. **Table 1** (ahead shortly) summarizes the differences between these devices, and I discuss each device in the pages ahead.

Field Guide to Base Stations

Apple confusingly has kept the same name for five generations of the 802.11n AirPort Extreme and four versions of the Time Capsule base stations. The dates for these generations were 2007 (AirPort Extreme only), 2008, early 2009, late 2009, and second-quarter (June) 2011. This can make it difficult to figure out which unit you own.

However, in AirPort Utility 6, for any supported model, you can see a unit's name by clicking its name in the graphical view, and then hovering over its name in the popover.

An additional resource is a set of tables on Apple's tech-support site that match model numbers, names shown in AirPort Utility—like "AirPort Extreme 802.11n (3rd Generation)", and release dates, though Apple has not yet added the June 2011 models, which is rather peculiar. Visit http://support.apple.com/kb/HT4635.

The names shown in the **Table 1** (next) correspond to those shown in AirPort Utility 5.5.3

Table 1: Current Apple Wi-Fi Hardware (March 2012)

(AU is the AirPort Utility description)

Name	Features	Price
AirPort Extreme Base Station (June 2011)	• Four gigabit Ethernet ports (three LAN, one WAN). • USB disk and printer sharing (any number of each). • Simultaneous dual-band networking using two radios. • Guest networking option. • Three-stream (450 Mbps) 802.11n. • AU shows "AirPort Extreme 802.11n (5th generation)".	$179
Time Capsule (June 2011)	• All AirPort Extreme features. • Built-in 2 TB or 3 TB hard drive for network-attached storage or Time Machine networked backup. • AU shows "Time Capsule 802.11n (4th Generation)".	$299 (2 TB), $499 (3 TB)
AirPort Express Base Station (Mar. 2008)	• One 10/100 Mbps Ethernet port (LAN or WAN). • Audio streaming. • USB printer sharing (one printer). • 802.11n. • AU shows "AirPort Express 802.11n".	$99; $39 for audio/power extension kit

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

AirPort Extreme

Over the years, Apple has enhanced the wide range of features now available in the AirPort Extreme:

- **Simultaneous dual-band networking:** With two internal radios, the early 2009 and later models of the Extreme 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:** Starting with the early 2009 model of the Extreme, you can set up a separately named Guest Network in addition to the network that you normally access. This feature broadcasts a *virtual* network that shares the same networking hardware, but appears as a unique name in the Wi-Fi 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 base station has four gigabit Ethernet ports, three of which are for the LAN, leaving one for the WAN (**Figure 2**).

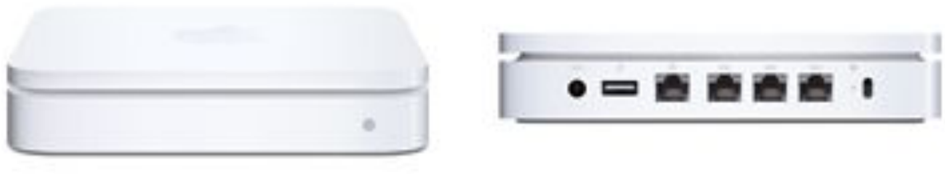


Figure 2: The tilted front view (left) and straight-on back view (right) of the AirPort Extreme Base Station. The back ports are, left to right, power, USB, one WAN Ethernet jack, three LAN Ethernet jacks, and a security slot for physical lock-down.

- **450 Mbps throughput:** Starting with the late 2009 model of the Extreme base station, it can pump out up to 450 Mbps of raw data in the 5 GHz band by using a wide channel (150 Mbps) across three separate spatial streams. In practice, this keeps data rates consistent over longer distances from the base station rather than providing overall faster throughput. Throughput is limited to half that in 2.4 GHz, because only normal-width channels are allowed.

***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 802.11n 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 (or Time Capsule) can be used as switched LAN ports if the base station is set to bridging mode. In this mode, the Extreme just passes through traffic from the network to which it’s connected. See Passthrough and Bridging for more details.

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

Time Capsule

The Time Capsule (**Figure 3**) is a backup appliance with all the technical characteristics and external ports found in an Extreme, but with the addition of an internal 2 TB or 3 TB drive. (In the June 2011 model, Apple changed the storage capacity for the second time in the Time Capsule's history.)

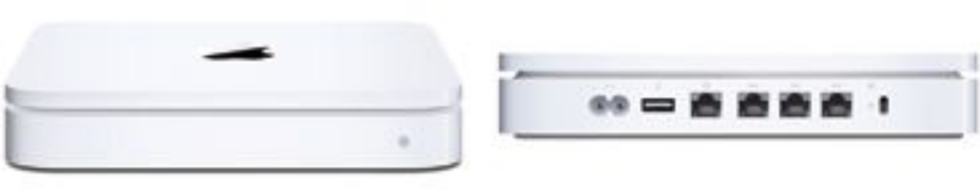


Figure 3: The Time Capsule combines an internal hard drive for backup with all the features found in an Extreme base station.

Apple designed the Time Capsule to pair with Mac OS X's Time Machine feature for network backup. Any computer with 10.5 Leopard or later installed can back up files over Wi-Fi or Ethernet to a Time Machine's internal drive or an externally connected drive.

The Time Capsule is slightly larger than an Extreme in order to accommodate the drive. Also, Apple did a little extra engineering to put the power supply inside the Time Capsule: a 6.5 foot/2 meter external AC power cord connects the Time Capsule to a power socket.

Extra options for the internal drive: *In AirPort Utility, you can erase the internal drive in a Time Capsule.*

AirPort Express

Apple upgraded the AirPort Express to 802.11n in 2008, and hasn't modified the base station since. The Express lacks simultaneous dual-band networking: you must choose 2.4 or 5 GHz and boot it into that mode. It also has just a "2x2" radio setup, allowing a maximum of 300 Mbps of raw speed in 5 GHz and half that in 2.4 GHz.

The Express 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 802.11n traffic that can pass between it and Ethernet. The Express also has a USB port for sharing a single printer, but it can't share multiple printers nor a hard drive.

The Express 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.

Due to its integral power plug, the Express can hang from a power outlet (**Figure 4**). Apple used to sell a special extension cord as part of a $39 audio kit that could be used in place of the integral plug, and which terminated in a three-prong plug. That's no longer available; use a simple extension cord instead.

Figure 4: The 802.11n AirPort Express streams audio, shares a USB printer, and connects to a LAN network via Ethernet or Wi-Fi.

Common ways to use an Express include:

- To connect an Express 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, you have two options:
  - Via Wireless Distribution System (see Bridge Wirelessly) for an Apple network extension.
  - Via a special mode called ProxySTA to Connect to Any Base Station and relay that connection through the Express's single Ethernet port.
- To Stream Audio with AirPlay from Macintosh or Windows or an iOS device to stereo speakers connected to the Express.

Adapters in Macs and iOS Devices

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 802.11n 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 include Wi-Fi and have dual-band 802.11n built in. See **Table 2** for the full rundown by model over AirPort's history.

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 10.5 Leopard or later automatically chooses the fastest and best connection. This ensures that the connection will always be the best one for the circumstances.

Table 2: Wi-Fi Flavor by Model

Model(s)	Fastest Supported Wi-Fi Type
iPhone 4 (2010), 4th generation iPod touch (2010), iPhone 4S (2011), 5th generation iPod touch (2011)	802.11n (2.4 GHz only)
iPad (2010), iPad 2 (2011), 3rd-generation iPad (2012)	802.11n (dual band)
All Core 2 Duo, i5, and i7 Macs: MacBook and MacBook Pro (2006–), Mac Pro (2008–), and Mac mini (2009–), iMac (2006–, except 1.83 GHz 17-inch)	802.11n (dual band)
iPhone, iPod touch (2007–2009)	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
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
iBook G3, iMac (2000–2003), G4 Cube, Power Mac G4 (1999–2002), PowerBook G3 (2000–2002), PowerBook G4 (2001–2002), eMac (2002)	802.11b

Adapters for Older Macs

If your Mac lacks a built-in adapter, or its built-in adapter has failed and your computer is out of warranty, or you're stuck with 802.11g and want to use 802.11n, you're not out of luck. Apple doesn't have an answer, but some third-party firms do—and inexpensively!

I suggest visiting Other World Computing's wireless products page to find the best adapter for your Mac (http://eshop.macsales.com/shop/wireless/).

Plug In Your Base Station and Get Started

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

(The next chapter, 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 Devices, 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:**

   - **AirPort Extreme and Time Capsule:** The Extreme box and the Time Capsule box each include just a few necessary parts: the square base station, a thick setup booklet, a booklet full of software licensing information (silly, but required), and an AC power cord. The Extreme box also has a power adapter, which is integral to the Time Capsule.

   - **AirPort Express:** The Express box includes just the Express with its integral AC plug snapped away for storage and the booklets noted above.

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

   - **AirPort Extreme:** The power cord and adapter's combined length—17 feet/5.2 meters—should aid in placement, but to position the device even farther from a power outlet, you can use a lightweight extension cord. In the U.S. version, the AC end of the Extreme's power cord terminates in a non-polarized two-prong plug—both prongs are the same width—which can work in any outlet in either orientation.

- **Time Capsule:** Plan to buy an extension cord if the included 6.5 foot/2 meter cord is too short for your purposes. The Time Capsule has a non-polarized two-prong plug in the U.S. version.
- **AirPort Express:** If you need to locate the Express where you can't attach it to a power outlet, you can use a simple extension cord. Apple once offered a custom extension cable (paired with audio cords), but that was discontinued in 2011.

The Extreme 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. **Do you need an Ethernet cable?**

   Configuring a base station may be simpler if you temporarily hook it to your computer or existing LAN with an Ethernet cable.

   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 in order to make that connection. 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.

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

Now it's time to power up. Plug your base station into an electrical outlet, and plug an Ethernet cable from your Mac into any of the three LAN ports on the Time Capsule or Extreme, or the single Ethernet port on the Express. If you'd rather have mobility while configuring, you can also set up via Wi-Fi, but you must reconnect after each time you change password or naming options.

Flashy: *In a neat addition, all the Ethernet ports on an Extreme 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 (**Figure 5**). Also, a green/amber 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.*

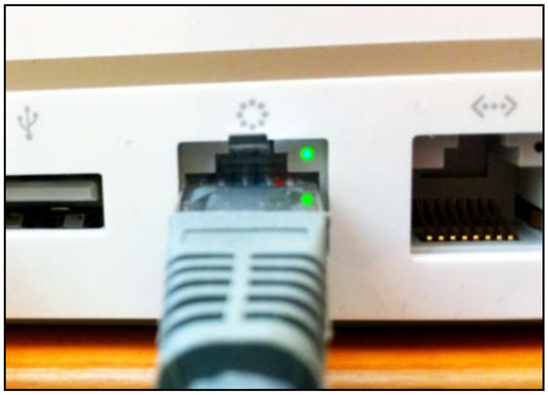


Figure 5: A tiny light inset into the Ethernet port shows a good Ethernet connection and reveals activity.

I recommend not connecting a 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.

Use AirPort Utility

AirPort Utility lets you manage base stations from a Mac, a Windows system, or an iOS device. Apple doesn't offer Web-based configuration of its base stations. As noted in the Introduction, this book covers just AirPort Utility 6 for Mac OS X and the AirPort Utility iOS app.

Let's look at AirPort Utility and examine its graphical approach for showing a network's composition, and then discuss making sure your software is up to date.

Note: On the Mac, you can launch AirPort Utility from `/Applications/Utilities`. In iOS, first download the app from the App Store (it's free), and then tap its icon to launch it.

View a Network Graphically

From the first release of the iOS app and starting with the 6.0 release of the Mac OS X version, AirPort Utility uses a graphical display of your network's *topology*, the interconnection among its networked parts, to show which base stations are available and their respective statuses. In **Figure 6**, AirPort Utility shows that AirPortage Bay is connected to the Internet, while Downstairs AirPort and Guest Room Apr2011 connect via AirPortage Bay for their network needs. (They look to AirPortage Bay for DHCP and NAT address handling.)

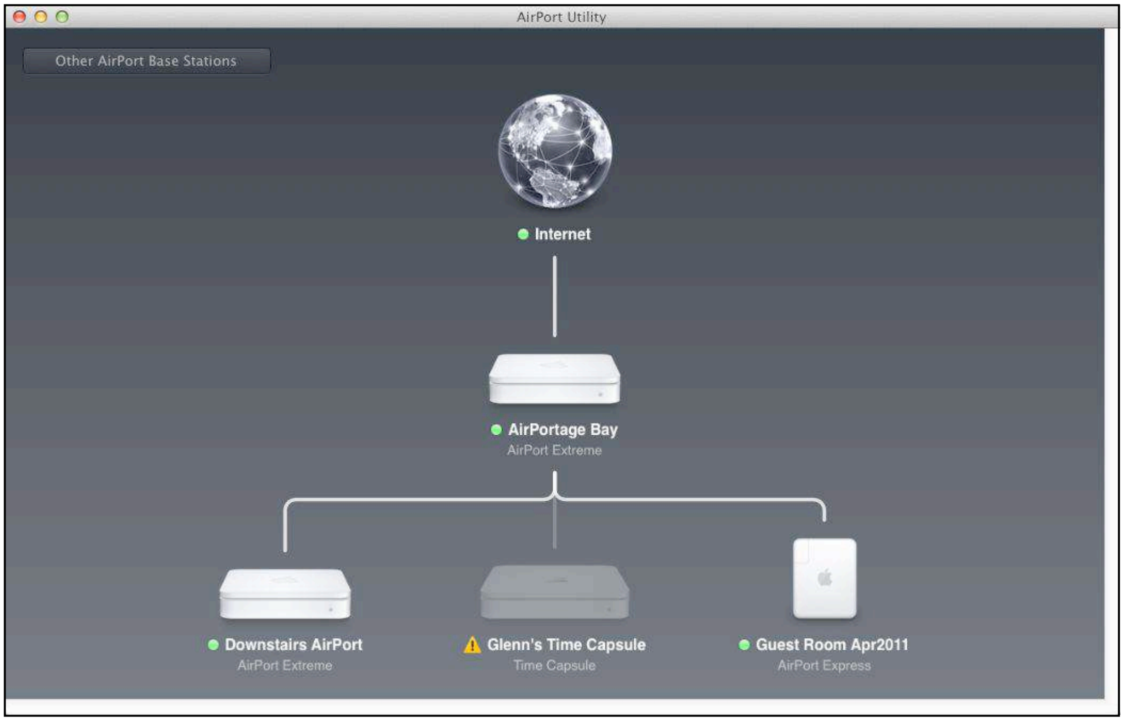


Figure 6: AirPort Utility offers a graphic depiction of your network and its interconnections.

The topology represents Ethernet connections with solid lines and wireless connections with dotted lines (**Figure 7**).

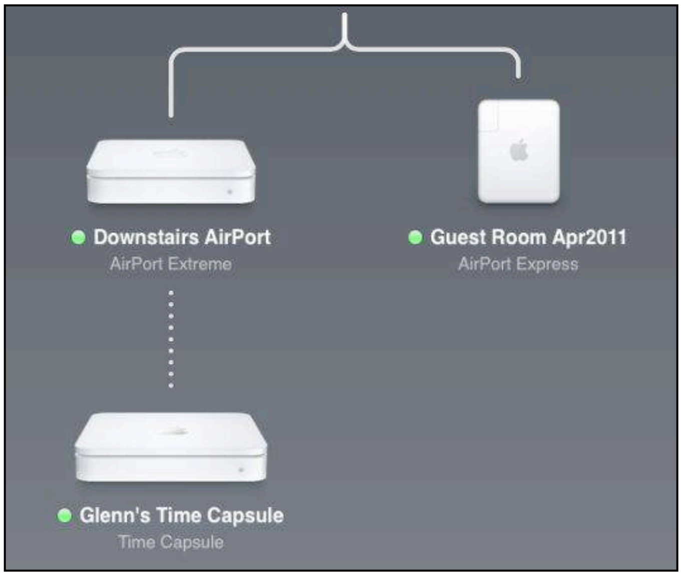
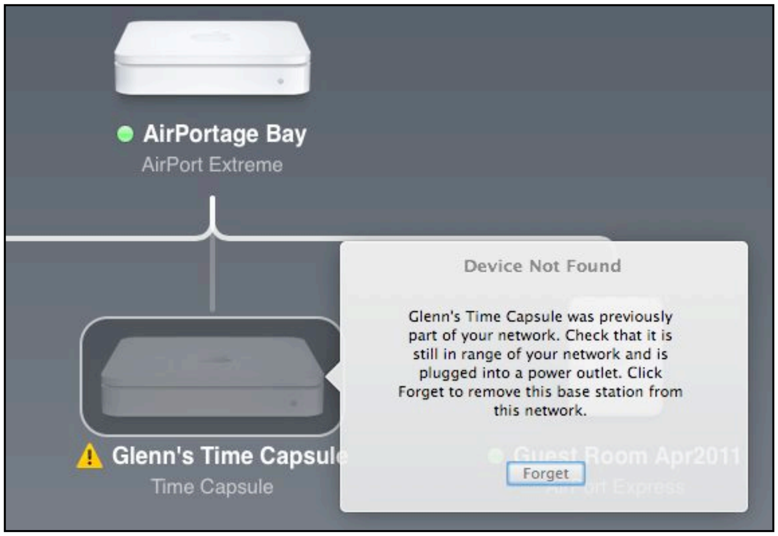


Figure 7: A solid line means an Ethernet hookup, while a dotted line indicates a Wi-Fi connection.

A green dot appears to the left of all correctly functioning base stations and an active and happy Internet connection. A yellow dot indicates a problem (such as a dead Internet feed), while a yield sign means a base station that was once available can't be found (**Figure 8**).

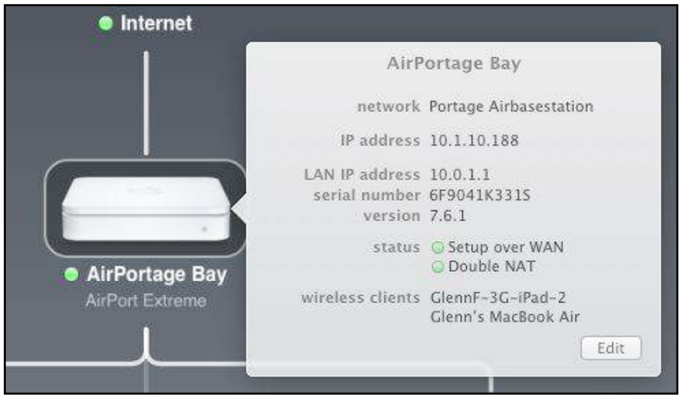


Device Not Found

Glenn's Time Capsule was previously part of your network. Check that it is still in range of your network and is plugged into a power outlet. Click Forget to remove this base station from this network.

Figure 8: A missing base station icon, when clicked, provides suggestions on how to fix the problem.

Click or tap on a base station, and basic details are revealed, such as its name, IP address, and firmware revision (**Figure 9**).



AirPortage Bay

network Portage Airbasestation
IP address 10.1.10.188
LAN IP address 10.0.1.1
serial number 6F9041K331S
version 7.6.1
status Setup over WAN
Double NAT
wireless clients GlennF-3G-iPad-2
Glenn's MacBook Air

Figure 9: Tap or click a base station to reveal details.

Click or tap Edit and—after entering a password if it's not already stored—you can configure the base station. (In the steps ahead, if I tell you to "edit your base station's configuration," simply click or tap the base station icon and then click or tap the Edit button.)

Warning! *After you initially enter a password in AirPort Utility on your Mac or in iOS, the software remains logged in, and it doesn't require the re-entry of the password. AirPort Utility will also reveal the password on demand. Make sure you don't allow easy access to an unlocked iOS device or computer if you need to keep such passwords secret.*

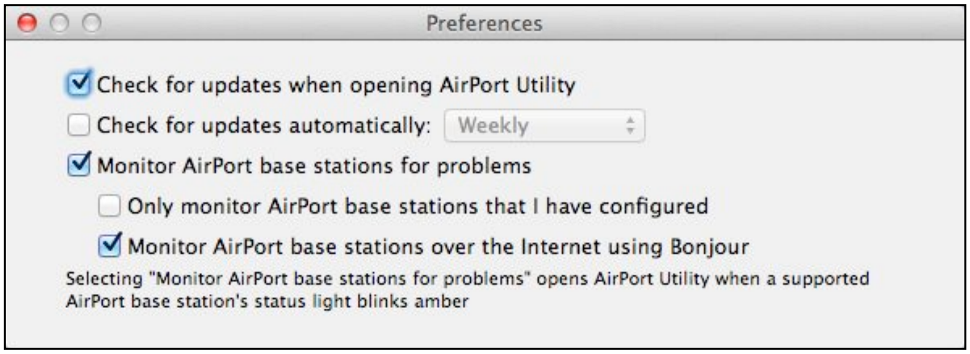
You can also tap the Internet icon, a globe familiar to Mac users from its use in the Finder, to show a few details about the connection to the larger Internet.

Keep Up to Date

If your desktop or iOS copy of AirPort Utility isn't up to date, you should update it before proceeding, and then update any base stations' firmware that is out of date.

The first time you run AirPort Utility on the Mac, it asks if it should check for updates automatically. Although Software Update (choose 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. A background process monitors for updates at the interval you specify, and then launches AirPort Utility if an update is available. You can adjust how often updates are checked in AirPort Utility's Preferences window (**Figure 10**).



☑ Check for updates when opening AirPort Utility

□ Check for updates automatically: Weekly

☑ Monitor AirPort base stations for problems

□ Only monitor AirPort base stations that I have configured

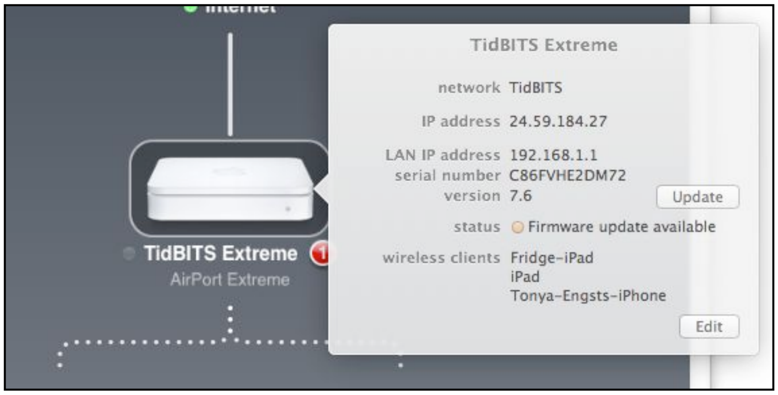
☑ Monitor AirPort base stations over the Internet using Bonjour

Selecting "Monitor AirPort base stations for problems" opens AirPort Utility when a supported AirPort base station's status light blinks amber

Figure 10: The Preferences window lets you choose to check for updates regularly—or not.

Note: iOS handles its own updates through the App Store app or iTunes if you sync via a computer. Windows sports a version of Apple's Software Update to manage new versions of AirPort Utility.

AirPort Utility can also tell you if there's a firmware update available. On the Mac, select your base station, and click Edit. If a firmware update is available, that information will appear in the status area (**Figure 11**). To update the firmware, click Update.

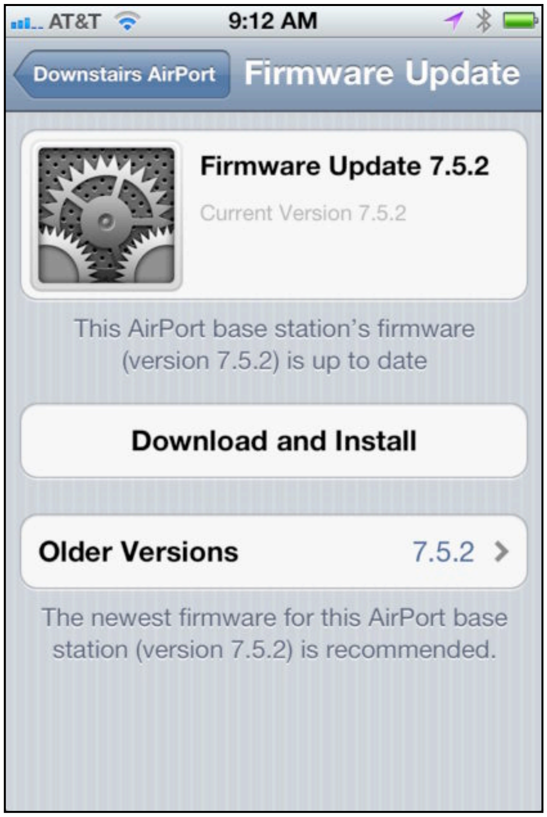


TidBITS Extreme

network TidBITS
IP address 24.59.184.27
LAN IP address 192.168.1.1
serial number C86FVHE2DM72
version 7.6
status Firmware update available
wireless clients Fridge-iPad
iPad
Tonya-Engsts-iPhone

Figure 11: Select your base station to view a summary pane which alerts you if an upgrade is needed.

You can also update firmware from the iOS version of AirPort Utility, which is useful if you don't have a computer nearby and need the latest base station features. Tap the icon for the base station, tap Version, and then on the Firmware Update screen (**Figure 12**), tap Download and Install.



Firmware Update 7.5.2
Current Version 7.5.2

This AirPort base station's firmware (version 7.5.2) is up to date

The newest firmware for this AirPort base station (version 7.5.2) is recommended.

Figure 12: The iOS app also lets you apply firmware updates to base stations.

Revert to Older Firmware

In the event that a firmware update causes trouble with your network, and that has been known to happen, you can reload (revert to) a previous firmware release. In the desktop version of AirPort Utility, select your base station and Option-click the firmware number next to the Version label. A pop-up menu appears, listing all the previous firmware available. Choose the release you want to install (typically the immediately previous version), and then click Continue.

Connect to a New Base Station

The moment a new base station is powered on either in the radio vicinity of a computer's Wi-Fi receiver or near an iOS device, AirPort Utility on that computer or iOS device recognizes the base station. You can also plug in a base station via Ethernet to a switch or base station on the network to which your computer or iOS device is connected.

To start configuring, you have the following choices:

- On a Mac, select the base station from the Wi-Fi menu in the area near the bottom below a gray label reading New AirPort Base Station; the type of base station is listed (**Figure 13**). This launches AirPort Utility and opens a configuration setup dialog. Mac OS X finds these base stations even if you're connected to an active Wi-Fi network, and it doesn't drop your current connection.

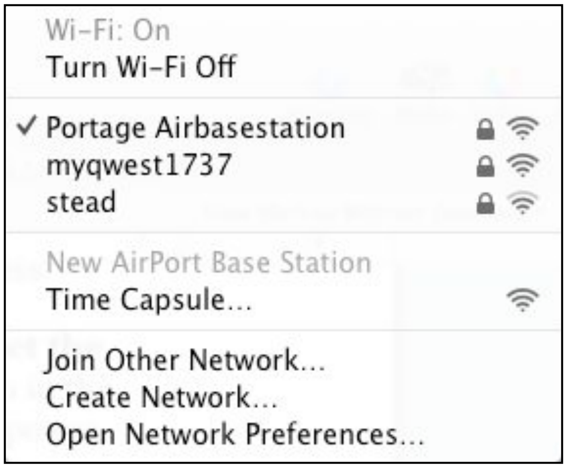


Figure 13: The Wi-Fi menu in Lion and later reveals unconfigured base stations in the vicinity, even ones to which you're not connected.

- On a Mac, launch AirPort Utility and click the faint Other AirPort Base Stations button at the upper left (**Figure 14**). Select the base station from this list to start configuring it.

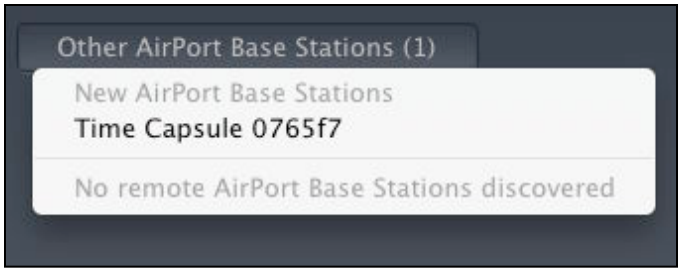
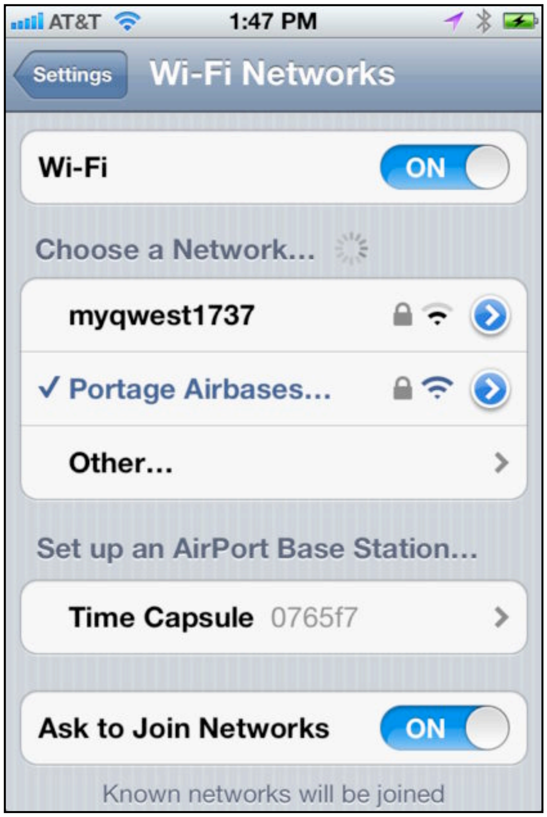

Other AirPort Base Stations (1)
New AirPort Base Stations
Time Capsule 0765f7
No remote AirPort Base Stations discovered

Figure 14: AirPort Utility shows base stations in the vicinity that you can configure.

- In iOS, launch Settings, tap Wi-Fi, and choose the base station by type beneath the Set Up an AirPort Base Station label (**Figure 15**). This starts the AirPort Setup process.



Wi-Fi ON

Ask to Join Networks ON

Known networks will be joined

Figure 15: Unconfigured base stations are listed near the bottom.

Now you can proceed to one of the scenarios listed at the beginning of the next chapter, a page or so ahead.

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 hexadecimal 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 Other AirPort Base Stations list as `Base Station Name 003FF`, with the appropriate model type, like AirPort Extreme, replacing `Base Station Name`.

The AirPort ID is a MAC (Media Access Control) address. Read Appendix E: What and Where Is a MAC Address? to find more information about MAC addresses.

Set Up a Network

How you configure your base station depends on the type of network you're building. In this chapter, I look at *scenarios*: pairing the kind of network that you want to with an explanation of how to use AirPort Utility for a basic configuration of that scenario. The next chapter helps you tweak your selection of channels and determine exactly where to place your base station. More advanced scenarios and configurations are covered later in the book.

Placing a Base Station

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

Picture Your Scenario

What kind of network are you building? The scenarios in this chapter cover common situations. Pick a scenario and proceed as directed, each scenario begins with a diagram and explanation of the type of network and then gives 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.
- Extending an existing network? See Extend a Network via Ethernet or Wi-Fi.
- Replacing an existing base station with a new unit and want exactly the same settings? See Replace an Existing Base Station.
- None of the above. If your scenario isn't in this list, consult later sections in the book, which examine advanced options.

Note: AirPort Utility used to have a Setup Assistant with many different branching paths. That's now folded into the far simpler, but unnamed, configuration helper discussed in this chapter.

New Network, Single Base Station

In the simplest setup, where you have a single base station and are connecting it directly to a broadband modem (**Figure 16**), you can breeze through setup.

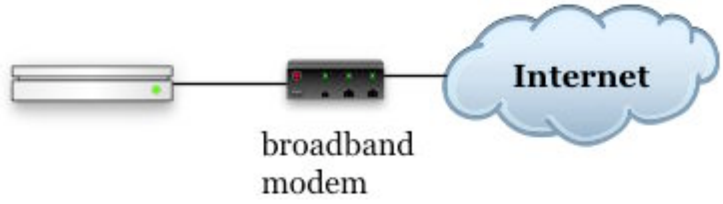
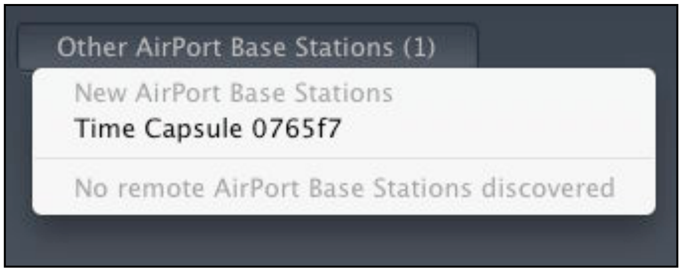


Figure 16: A simple network connects a base station via a broadband modem to the Internet.

To configure a new base station to create a new Wi-Fi network, follow these steps:

1. Select the base station (for more detail, see Connect to a New Base Station, in the previous chapter):

   - On a Mac, launch AirPort Utility and click the faint Other AirPort Base Stations button at the upper left (**Figure 17**). Select the base station from this list. (Or choose the base station from the New *base station type* item in the Wi-Fi menu on the menu bar.)

   Other AirPort Base Stations (1)

   New AirPort Base Stations

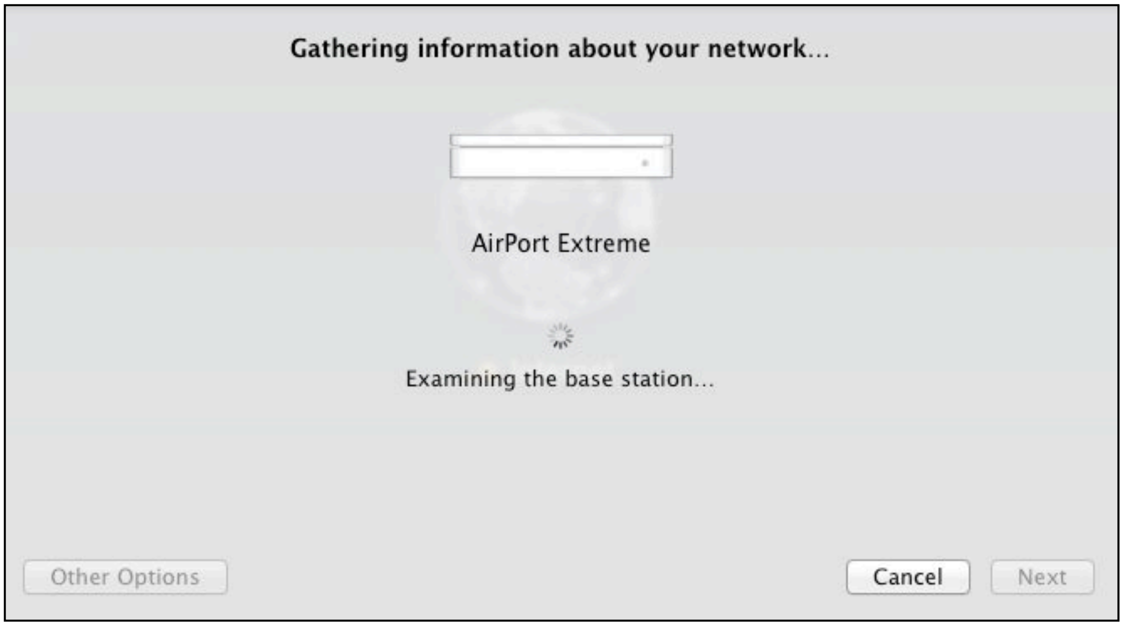
   Time Capsule 0765f7

   No remote AirPort Base Stations discovered

   Figure 17: AirPort Utility shows base stations in the vicinity that you can configure.

   - In iOS, launch Settings, tap Wi-Fi, and choose the base station by type beneath the Set Up an AirPort Base Station label. This starts the AirPort Setup process.

2. AirPort Utility (or AirPort Setup in iOS) shows its progress while it gathers information (**Figure 18**). Since there are no other base stations to which you're connected, wait until it says, "This *base station type* will create a network." Then, click the Next button.



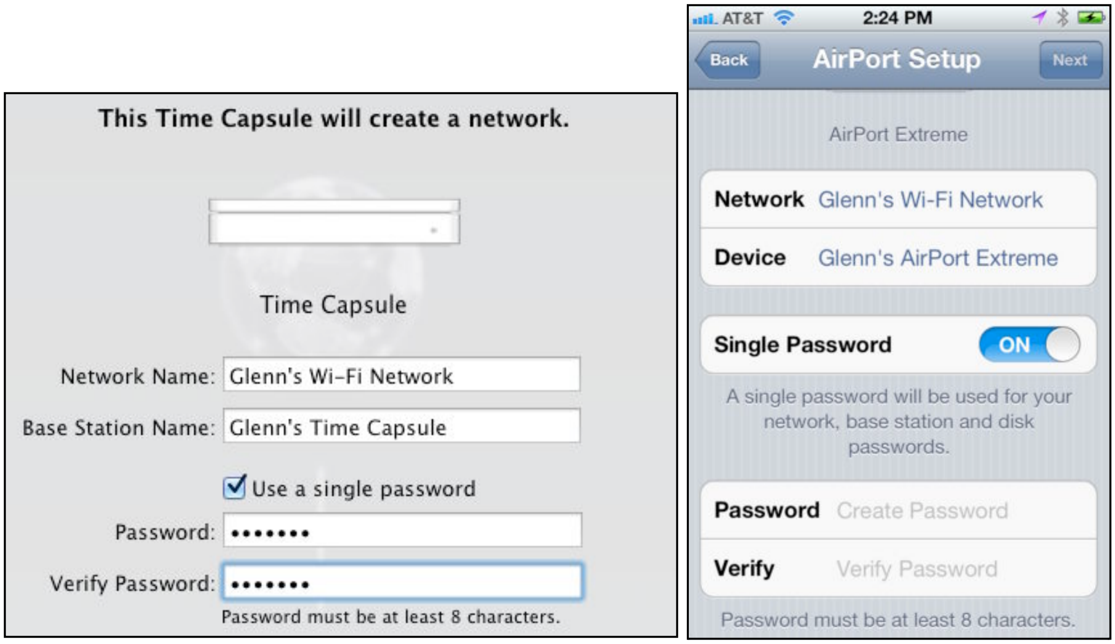
Gathering information about your network...

AirPort Extreme

Examining the base station...

Figure 18: AirPort Utility gathers information.

AirPort Utility (or AirPort Setup) now lets you fill in the details about your new network (**Figure 19**).



This Time Capsule will create a network.

Time Capsule

Network Name: Glenn's Wi-Fi Network

Base Station Name: Glenn's Time Capsule

☑ Use a single password

Password: •••••••

Verify Password: •••••••

Password must be at least 8 characters.

AirPort Extreme

Network: Glenn's Wi-Fi Network

Device: Glenn's AirPort Extreme

Single Password: ON

A single password will be used for your network, base station and disk passwords.

Password: Create Password

Verify: Verify Password

Password must be at least 8 characters.

Figure 19: Name and protect the base station.

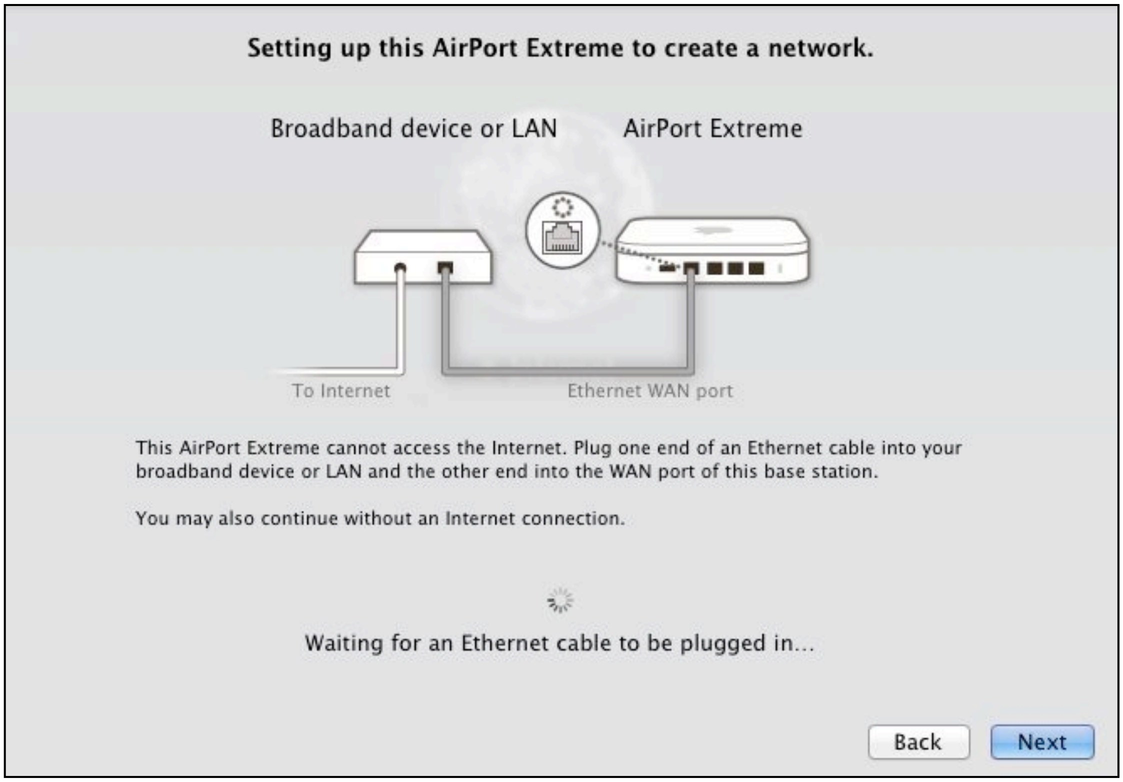
3. Fill in the details:

    - **Network Name (Mac)/Network (iOS):** This is the name that the base station broadcasts, and which appears in Wi-Fi selection menus on devices and computers.

- **Base Station Name (Mac)/Device (iOS):** Enter the Bonjour name that will be used to identify the base station in AirPort Utility, as well as in the Finder sidebar if a hard disk is connected to the base station or inside of it.
- **Single Password:** You can choose to set different passwords for configuring a base station, disk access, and network access. With this box checked (or switch set to On, in iOS), one password works for all purposes. (I discuss the details, in Turn On WPA/WPA2 Personal or WPA2 Personal.)
- **Password/Verify:** This password allows encrypted access to the network and prevents unwanted people from connecting to the base station and changing its settings.

Click Next.

4. If you haven't plugged in an Ethernet cable to your broadband modem and base station, AirPort Utility explains that you need to at this point (**Figure 20**). If you see this screen (or a similar message in iOS), plug in your cable or check your connections.



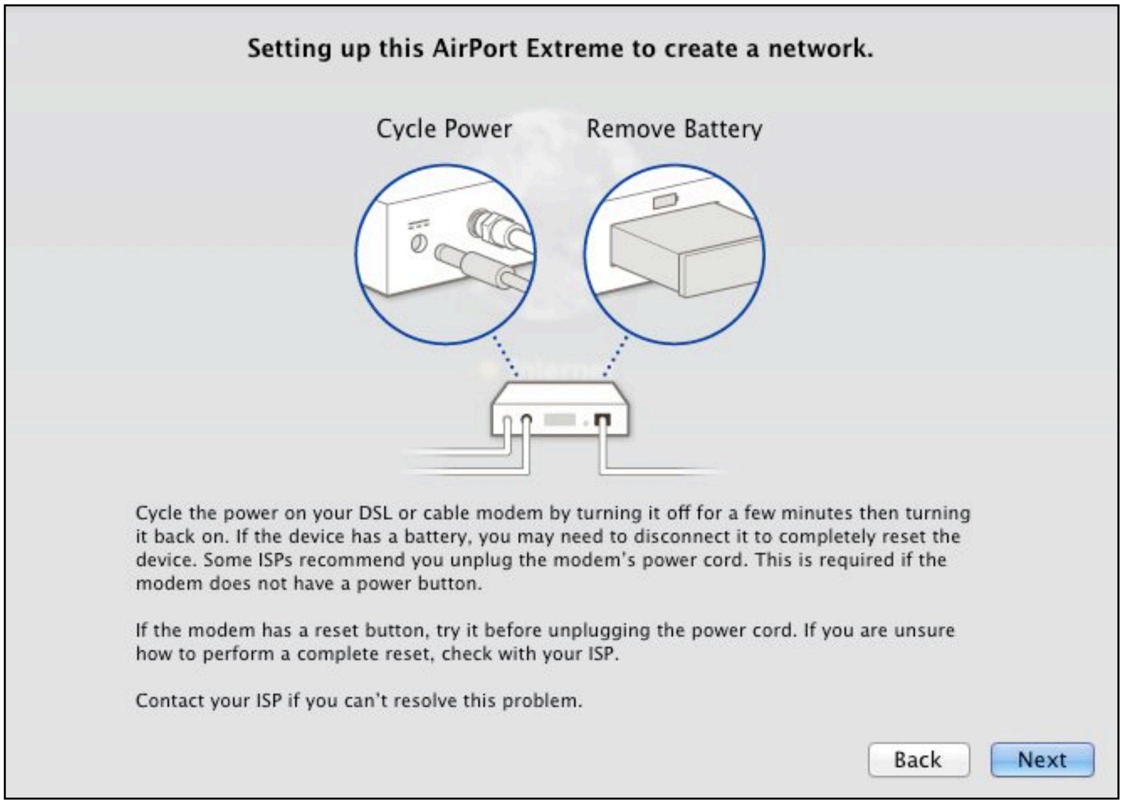
This AirPort Extreme cannot access the Internet. Plug one end of an Ethernet cable into your broadband device or LAN and the other end into the WAN port of this base station.

You may also continue without an Internet connection.

Waiting for an Ethernet cable to be plugged in…

Figure 20: Plug in your Ethernet cable if you haven't already, or check your cables.

5. AirPort Utility (or AirPort Setup, in iOS) completes the setup. It may suggest you power cycle your broadband modem as in **Figure 21** (click Next to proceed). In my testing, I found that setup can take a minute or two to finish. Click Done when the dialog says "Setup Complete."



Setting up this AirPort Extreme to create a network.

Cycle the power on your DSL or cable modem by turning it off for a few minutes then turning it back on. If the device has a battery, you may need to disconnect it to completely reset the device. Some ISPs recommend you unplug the modem's power cord. This is required if the modem does not have a power button.

If the modem has a reset button, try it before unplugging the power cord. If you are unsure how to perform a complete reset, check with your ISP.

Contact your ISP if you can't resolve this problem.

Figure 21: Apple provides some final advice on making sure your new network works as expected.

Run setup again: *You must reset a base station to factory defaults to go through the setup process described above again.*

Now that you've configured your base station, you may want to add a printer, configure special settings, or add another base station. To consider your options, read Quick Start to AirPort Networking, earlier.

Extend a Network via Ethernet or Wi-Fi

If you already have a network in your home or office, you may simply want to plug in another base station to extends its range. You have two options—via Ethernet or via Wi-Fi:

- **Ethernet:** The most reliable way uses Ethernet to connect the first base station with any subsequent base stations (**Figure 22**). The first base station must be connected to the Internet, but the rest can connect via that base station for Internet access. Each base station should be given a unique name, but the network name is the same for all of them.

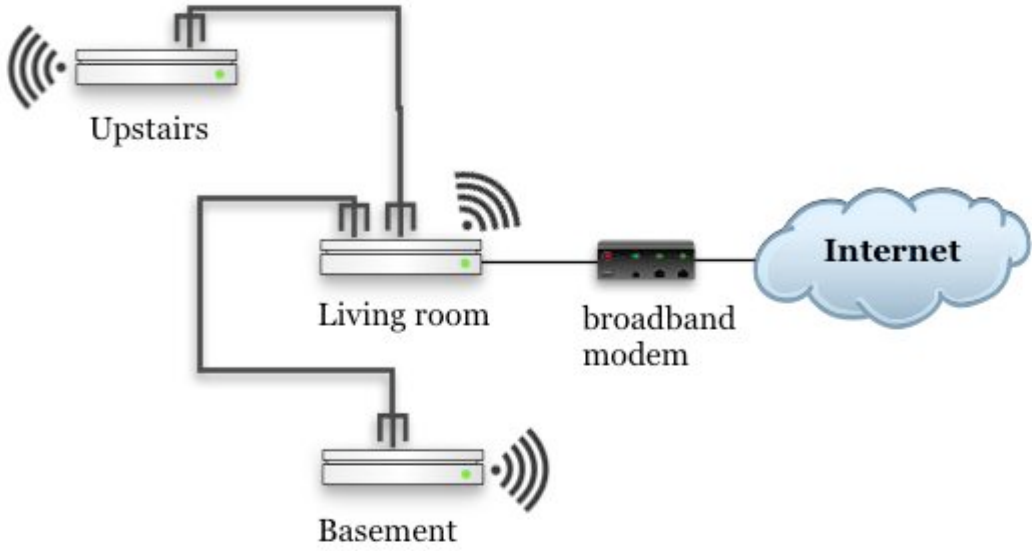


Figure 22: Ethernet lets you connect a number of base stations together to form one seamless network across a home or office.

This method 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 set up with the same network name.

Because the Extreme and Time Capsule each have four gigabit Ethernet jacks built in, you will likely connect 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.

- **Wi-Fi:** You can also opt to connect base stations wirelessly. With a wireless connection, base stations communicate with each other via Wi-Fi instead of Ethernet (**Figure 23**).

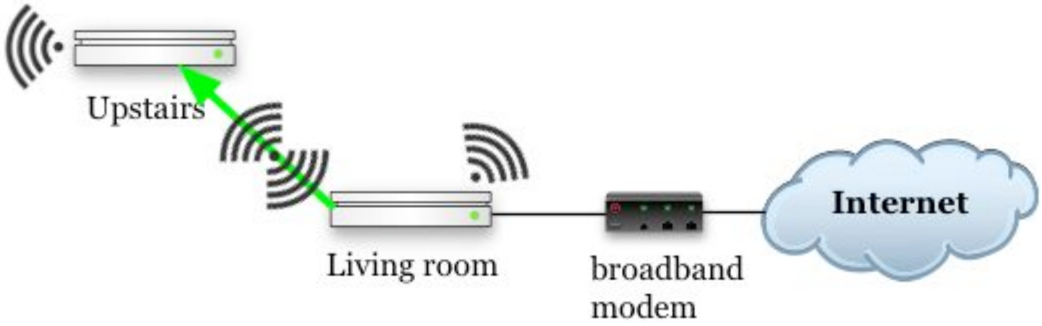


Figure 23: Extending via Wi-Fi lets you avoid running a cable.

Note: With an 802.11n AirPort Express, you can extend any Wi-Fi network, using Apple equipment or otherwise, through a special, lightly documented mode called ProxySTA. See Connect to Any Base Station.

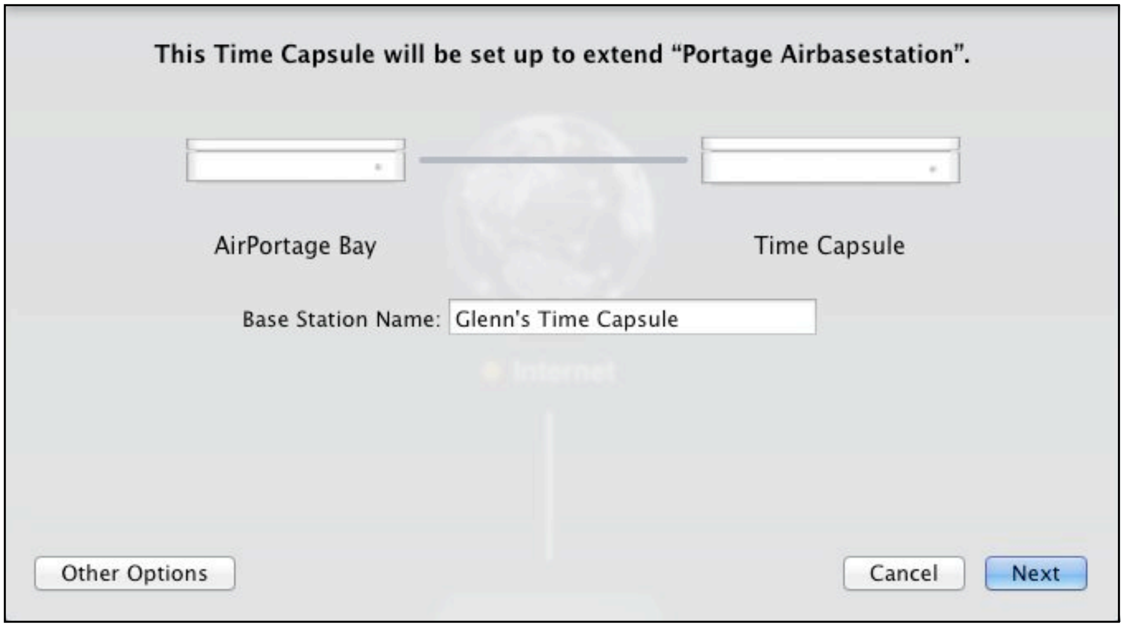
You can mix and match Ethernet and Wi-Fi network extensions, too. If you aren't sure how you want to extend your network, think you have an unusual situation, or want to better understand the technical details, flip ahead to Connect Multiple Base Stations.

Note: The iOS version of the setup assistant is quite similar; to avoid replication, I'm not including the screen captures and steps here.

To extend your network with Ethernet or Wi-Fi in AirPort Utility, follow these steps:

1. Connect to the base station using a method noted in Connect to a New Base Station, such clicking the Other AirPort Base Stations button at the upper left of AirPort Utility.

   AirPort Utility should recognize that the base station has been connected to an existing network and suggest how to configure the base station in that context (**Figure 24**).



This Time Capsule will be set up to extend "Portage Airbasestation".

Base Station Name: Glenn's Time Capsule

Figure 24: AirPort Utility helpfully suggests how to extend your existing network with the new base station.

2. Enter a base station name if you don't like the one filled in for you, and click Next.

   AirPort Utility connects to the new base station, configures it to extend your existing network, and restarts the base station. You will see a series of status messages as this progresses.

3. When you see the message Setup Complete, click the Done button.

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 your options, see Quick Start to AirPort Networking.

Replace an Existing Base Station

This option lets you replace an Apple base station (or a non-Apple router) that's already in use or that was in use on your network. For instance, you might be updating a network that had a single-band-at-a-time 802.11n base station by replacing that older one with a new 802.11n unit that works over both frequency bands at once (**Figure 25**). You can use the setup assistant to replace the base station in moments.

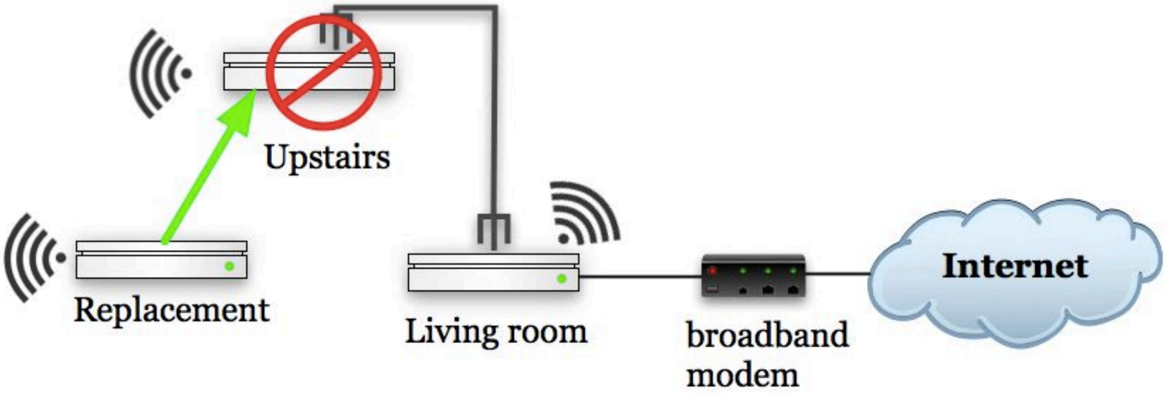


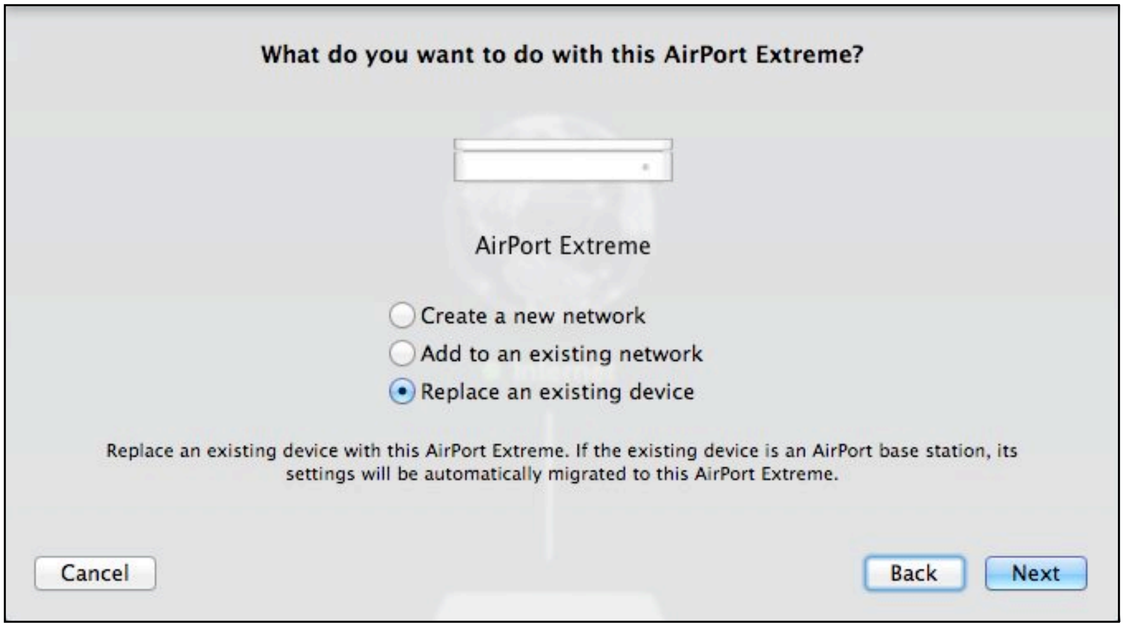
Figure 25: You might want to replace an existing base station with a newer, faster one, without having to re-enter all of the current base station's configuration details.

Tip: If you're swapping in a wired base station, put your new base station near your old base station for ease of swapping cables.

Note: The iOS version of the setup assistant is quite similar; to avoid replication, I'm not including the screen captures and steps here.

Follow these steps:

1. Connect to the new base station using any method noted in Connect to a New Base Station, such as clicking the Other AirPort Base Stations button at the upper left of AirPort Utility.
2. AirPort Utility will try to sort out the existing network, and offer to let you extend the network. Instead, click the Other Options button.
3. Select Replace an Existing Device, and click Next (**Figure 26**).



What do you want to do with this AirPort Extreme?

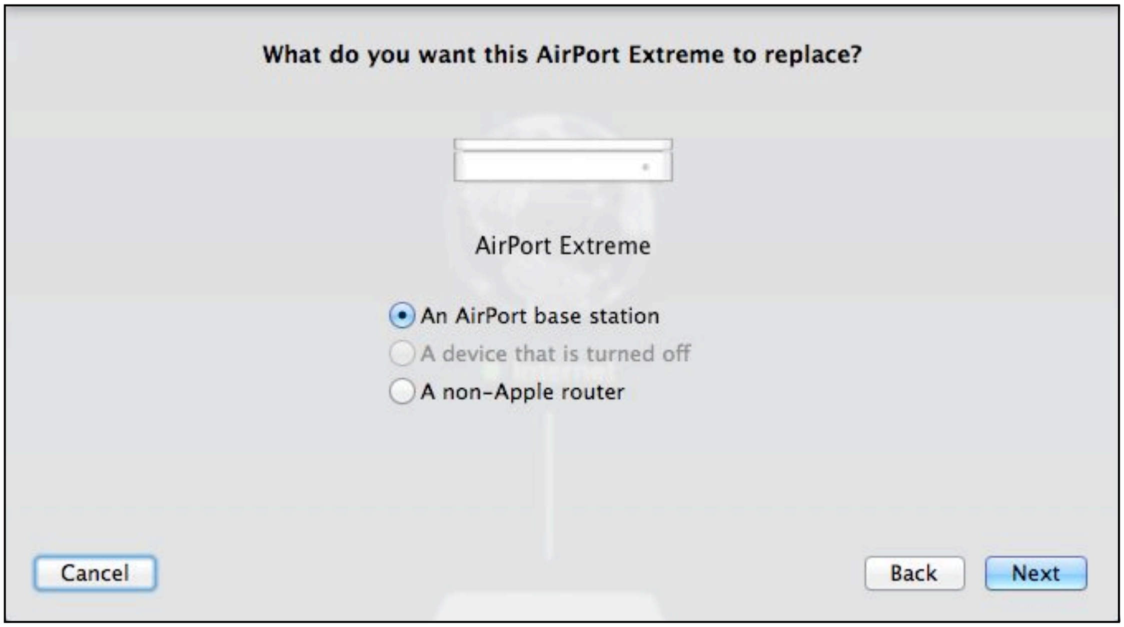
AirPort Extreme

○ Create a new network
○ Add to an existing network
● Replace an existing device

Replace an existing device with this AirPort Extreme. If the existing device is an AirPort base station, its settings will be automatically migrated to this AirPort Extreme.

Figure 26: Select Replace an Existing Device to proceed.

AirPort Utility asks how to proceed (**Figure 27**).



What do you want this AirPort Extreme to replace?

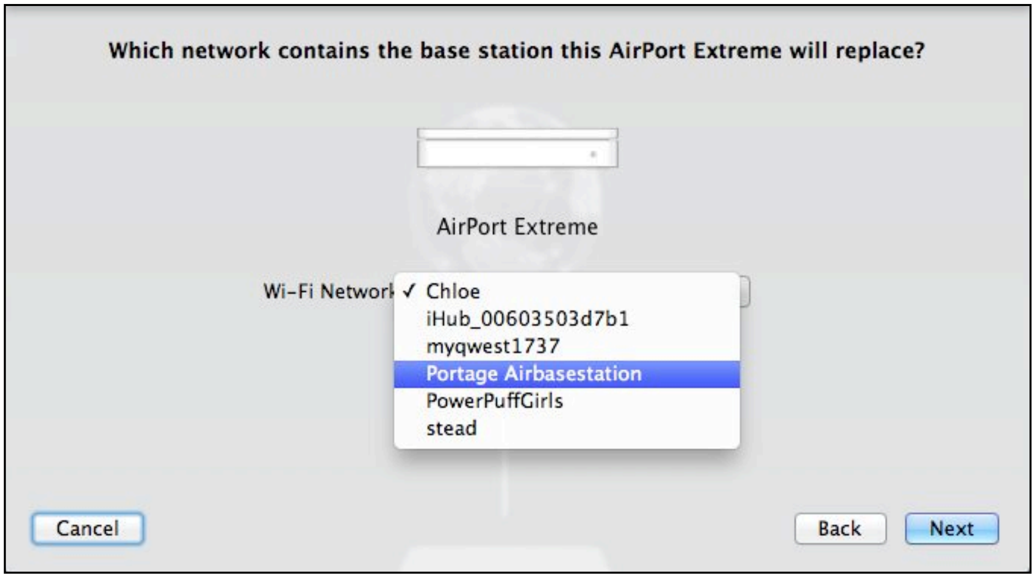
AirPort Extreme

● An AirPort base station
○ A device that is turned off
○ A non-Apple router

Figure 27: Pick the kind of router you’re replacing.

4. Now, depending on what type of device you are replacing:
    - If you are replacing an AirPort base station:
        a. Select An AirPort Base Station. Click Next.

b. From the Wi-Fi Networks pop-up menu (**Figure 28**), choose the network that contains the base station you want to replace. Click Next.



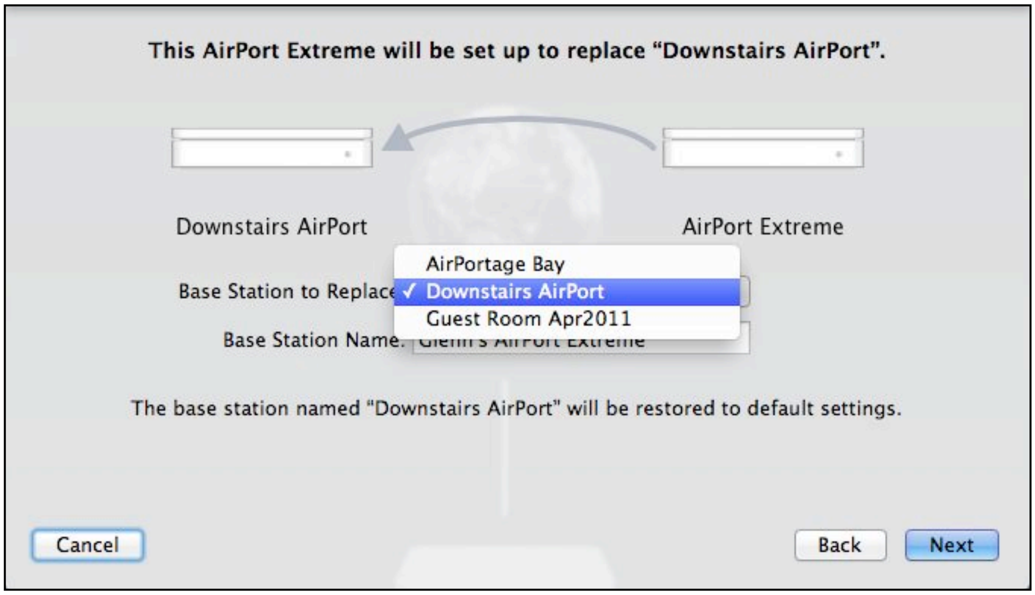
Which network contains the base station this AirPort Extreme will replace?

AirPort Extreme

Wi-Fi Network: Portage Airbasestation

Figure 28: Pick the network that contains the base station you want to replace.

c. From the Base Station to Replace pop-up menu (**Figure 29**), choose the base station that you want to replace (if you can't figure out the correct name and don't want to interrupt this sequence, use AirPort Utility on another device). Name the new base station something descriptive, and click Next.



This AirPort Extreme will be set up to replace "Downstairs AirPort".

Downstairs AirPort

AirPort Extreme

Base Station to Replace: ✓ Downstairs AirPort

Base Station Name: Glenn's AirPort Extreme

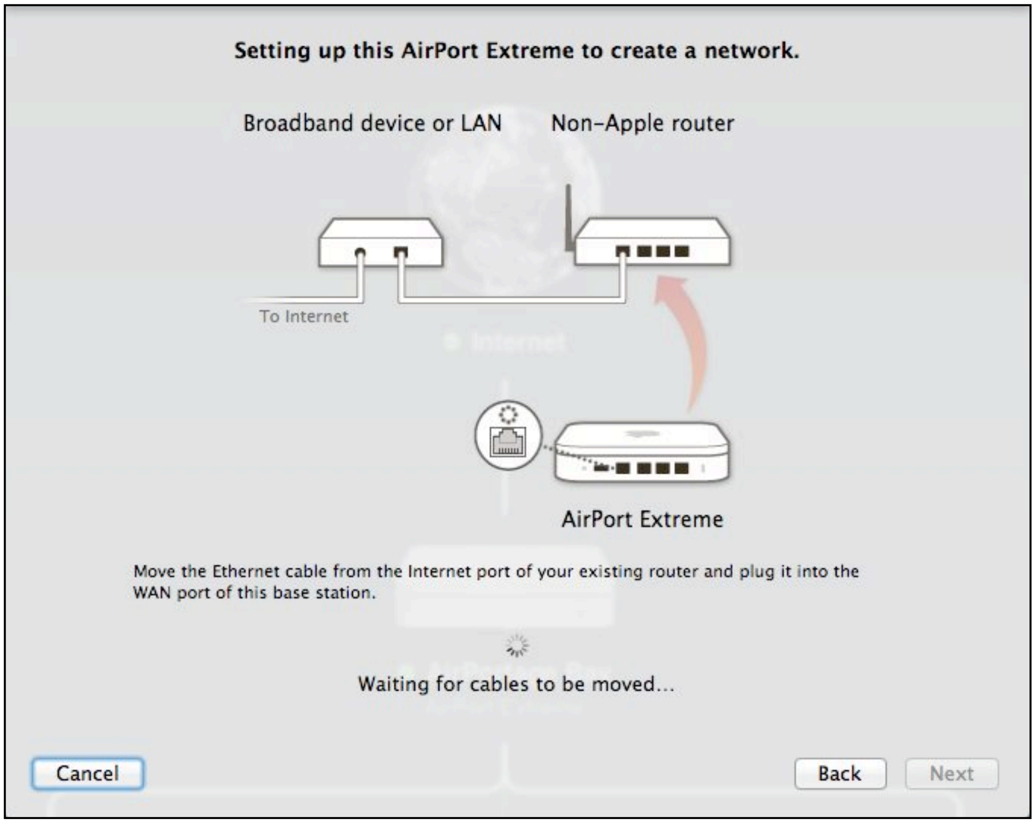
The base station named "Downstairs AirPort" will be restored to default settings.

Figure 29: Pick the base station to replace.

- If you want to replace a router that is not an Apple base station:

  a. Select A Non-Apple Router (**Figure 27**, earlier). Click Next.

  b. Follow the directions shown in AirPort Utility for how to attach the new Apple base station in your existing network, and click Next (**Figure 30**).



Setting up this AirPort Extreme to create a network.

Move the Ethernet cable from the Internet port of your existing router and plug it into the WAN port of this base station.

Waiting for cables to be moved...

Figure 30: Use the illustration as a guide for how to swap in your new Apple device.

  c. Click Done.

AirPort Utility connects to the new base station, configures it to extend your existing network, and restarts the base station. You'll see a series of status messages as this progresses.

5. When you see the message Setup Complete, click the Done button.

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 a Mac can't access the Internet, open its Network preference pane, select the Wi-Fi 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 re-appear. Click OK, and then click 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 Hand Out LAN Addresses.

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.

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 Appendix B: Configuration Files), 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, click the Edit button, and then choose Base Station > Restore Default Settings. Click Continue 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 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.)

Create Separately Named 2.4 and 5 GHz Networks

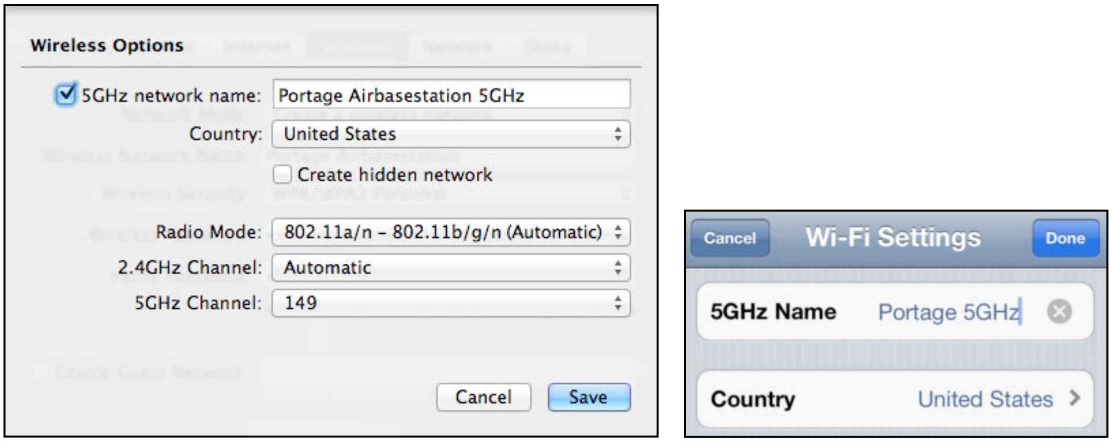
Apple's simultaneous dual-band Time Capsule and AirPort Extreme base stations are designed to a let a Wi-Fi client pick the best network at any given time, so by default both networks must use the same name. Mac OS X has been optimized to balance speed and range in choosing a given band's network, so 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 iPhones and iPod touch models before 2010. 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 slightly; here's how you access it:

1. Make sure your new base station is prepped as explained in Connect to a New Base Station.
2. In AirPort Utility (Mac or iOS), edit the base station's configuration.
3. On the Mac, click the Wireless button, click Wireless Options, and then select the 5 GHz Network Name checkbox. Or in iOS, tap Advanced > Wi-Fi Settings, and then tap the 5GHz Name field.
4. Enter a different name than the name shown in the main Wireless view (**Figure 31**).



Wireless Options

☑ 5GHz network name: Portage Airbasestation 5GHz

Country: United States

□ Create hidden network

Radio Mode: 802.11a/n – 802.11b/g/n (Automatic)

2.4GHz Channel: Automatic

5GHz Channel: 149

5GHz Name: Portage 5GHz

Country: United States

Figure 31: Name the 5 GHz network separately (Mac OS X left, iOS right).

5. On the Mac, click Save and then click Update. In iOS, tap Done repeatedly to reverse through several configuration screens and then tap Update.

Pick the Right Place and the Right Channel

This chapter helps you tune your network for the optimum performance. It starts by helping you understand more about the portion of the radio frequency spectrum that your base station uses and how to determine the right channel to use in each frequency band. After that it explains how you can use AirPort Utility to Pick Compatibility and Set a Channel.

Finally, you'll learn how to Pick the Right Place for a base station with General Testing Advice as well as details on Testing from Client to Base Station and Testing from Base Station to Client.

Note: Before the early 2009 Extreme and Time Capsule, all 802.11n Apple base stations could use only one band at a time. That's still true for the Express. The simultaneous dual-band base stations introduced in early 2009 remove most of the complexity.

Spectrum Trade-offs

Shortly, I explain how to select channels for a base station. To make the best choice, you may need some background on spectrum and channel choices. (If you don't know the basics of spectrum bands and channels, read The Spectrum Part of Wi-Fi, before proceeding here.)

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

Note: Future 802.11ac networks will be able to use quadruple wide channels, and have a raw data rate of over 1 Gbps in the right circumstances.

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.)

Problems with Wi-Fi networks often stem from your own or your 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

The 5 GHz band offers consistent *throughput*—the amount of actual data passing over the network exclusive of overhead used to transmit it. With 2.4 GHz, however, throughput is all over the place. When other technologies cause interference in the 2.4 GHz band, Wi-Fi devices and base stations are forced to slow down.

The highest possible 802.11n rate happens when two adapters use the 5 GHz band with wide channels. However, the maximum potential throughput is reduced because the signal must go from one adapter to the base station and then from the base station to the other adapter. You'll see the fastest possible speeds from an 802.11n adapter connected via a 5 GHz wide channel to a computer connected to the base station via gigabit Ethernet. (The Express has just 10/100 Mbps on its single Ethernet port, limiting its top network transfer speed to and from an Ethernet network to devices.)

Compatibility

An 802.11b or 802.11g device—such as a Mac with an original 802.11g AirPort Extreme built in—can't connect to a 5 GHz network, which is a reason Apple offers both 2.4 GHz and 5 GHz on its base stations. (Apple has never sold a device that can connect only in the 5 GHz band.) A visitor with an older adapter would be out of luck if a base station offered only a 5 GHz connection, as would anyone with an iPhone or iPod touch, or most any smartphone. **Table 2**, earlier, summarizes which 802.11 standards are supported by which Apple devices.

Channels

Now that you understand the limits of the bands over which your base station broadcasts, it's time to consider which channels to use. The regular and wide channels that 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, when an Apple base stations is set to Automatic, it does a great job 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 14, although just 1 to 11 are available in the United States. Channels 1, 6, and 11 are typically chosen in the United States because they lack any real overlap with each other. In countries in which 14 channels are available, 1, 6, 10, and 14 may be used with little overlap. (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 in the United States has a bigger tradeoff: Apple makes 8 out of 23 possible channels available: 36, 40, 44, and 48 in the lower set, and 149, 153, 157, and 161 in the upper part (see Appendix D: Channels Explained for more details). (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 picks an upper-band channel, unless it senses interference in all the available choices and opts for a lower-band channel to make sure the network will work.

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 around the neighborhood.

The 5 GHz band is much less available in most other countries, some of which allow a small slice of 4.9 GHz spectrum to be used instead.

Pick Compatibility and Set a Channel

To configure a base station's band, compatibility, and channel (or as many of those as you want), launch AirPort Utility, and edit the base station's configuration. On the Mac, click the Wireless button, and then the Wireless Options button. In iOS, tap Advanced > Wi-Fi Settings.

Set the Radio Mode

The radio mode option is handled differently in Mac OS X and iOS. In Mac OS X, you choose an option from a pop-up menu (**Figure 32**), which—if you press Option while opening the menu—offers a multitude of choices in every combination.

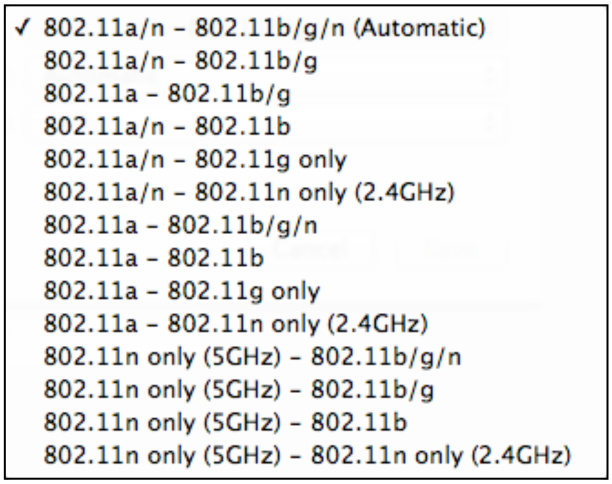
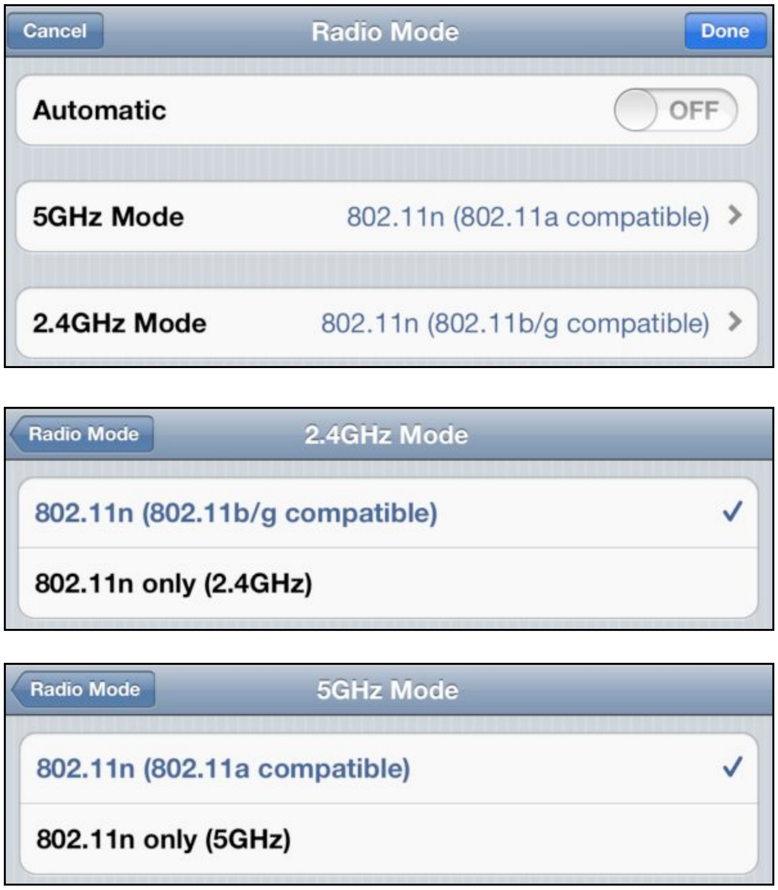

✓ 802.11a/n – 802.11b/g/n (Automatic)
802.11a/n – 802.11b/g
802.11a – 802.11b/g
802.11a/n – 802.11b
802.11a/n – 802.11g only
802.11a/n – 802.11n only (2.4GHz)
802.11a – 802.11b/g/n
802.11a – 802.11b
802.11a – 802.11g only
802.11a – 802.11n only (2.4GHz)
802.11n only (5GHz) – 802.11b/g/n
802.11n only (5GHz) – 802.11b/g
802.11n only (5GHz) – 802.11b
802.11n only (5GHz) – 802.11n only (2.4GHz)

Figure 32: When you configure a simultaneous, dual-band base station, the Radio Mode pop-up menu offers "802.11a/n – 802/11b/g/n (Automatic)" along with two standard options (the top three of the many options shown here), but reveals eleven more options—as shown—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.

AirPort Utility suppresses radio and channel options if a base station is a wireless extension of a network, as it must have the same settings as the base station connected to a broadband modem or larger network.

iOS has a different approach. Tap Radio Mode, and set Automatic to Off (**Figure 33**). This lets you select 5GHz Mode and 2.4GHz Mode options. 5GHz Mode can be set to just 802.11n (with 802.11a compatibility) or 802.11n only operation. Likewise 2.4GHZ Mode offers just two options: 802.11n with 802.11b/g compatibility or 802.11n only. If you need a greater range of options, use the Mac version of AirPort Utility.



Automatic OFF

5GHz Mode 802.11n (802.11a compatible) >

2.4GHz Mode 802.11n (802.11b/g compatible) >

802.11n (802.11b/g compatible) ✓

802.11n only (2.4GHz)

802.11n (802.11a compatible) ✓

802.11n only (5GHz)

Figure 33: The Radio Mode screen (top) lets you choose from two major options for the 2.4 GHz band (middle) and for the 5 GHz band (bottom).

Let's look at the radio mode options:

- **Automatic (Mac and iOS):** This default pop-up menu on the Mac and an On/Off switch in iOS works with a simultaneous dual-band base station to provide full compatibility with different types of 802.11 devices: 802.11a/n in 5 GHz, and 802.11b/g/n in 2.4 GHz.

- **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. Choose "802.11a/n – 802.11b/g/n (Automatic)" or "802.11a/n – 802.11b/g" on a Mac, or tap "802.11n (802.11a compatible)" in the 5GHz Mode view in iOS.

- **802.11b/g/n:** This option is fully backward compatible in 2.4 GHz. Choose “802.11a/n – 802.11b/g/n (Automatic)” on a Mac, or tap “802.11n (802.11b/g compatible)” in 2.4GHz Mode view in iOS.
- **802.11a, 802.11b, 802.11g only, 802.11b/g (Mac only):** These modes, available as various menu items in combination with other modes, lock out various faster and slower modes, and are for compatibility only. The only reason to use these modes is to set up an older form of network security called WEP that provides no protection. On a network with 802.11n, WEP can be used only in a deprecated and broken form called Transitional. See Enter an Encryption Key (WPA/WPA2 Personal, WEP).
- **802.11n only (5 GHz), 802.11n only (2.4 GHz) on the Mac and in iOS:** These modes disable the special backward-compatible *preamble* that’s transmitted at the slowest speed, removing overhead and disabling adapters that can’t talk 802.11n from using either or both bands.

Set the Channel

The channel selection options let you choose channels in one or both bands depending on your base station model. AirPort Utility defaults to Automatic for both bands, where the base station picks a channel based on which channel has the least amount of radio activity:

- In AirPort Utility on the Mac, while working in the Wireless Options dialog discussed in the previous topic, choose any channel listed in the 2.4GHz Channel or 5GHz Channel pop-up menu.
- In AirPort Utility for iOS, in the Radio Channel view described just previously, turn off the Automatic Channel switch for either or both the 5 GHz or 2.4 GHz bands, and then tap the respective channel label to select a fixed channel.

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 situation 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 or 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) 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?

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 wireless network access. Write down the current location of the base station and the signal strength that you're seeing at that location so it's easy to determine the ideal placement of the base station later.

- The Extreme 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 Client to Base Station

There are several ways you can test how well a client can interact with a base station:

- To test the connection between a single Mac and the base station, use Mac OS X's hidden Wi-Fi Diagnostics program (added in Lion) or use your Mac's built-in but rough signal strength information in the Wi-Fi menu. I talk about each of these options next.

- To monitor all the base stations and networks in your vicinity, you can Measure with iStumbler.

- You can also bring out the big guns and Run a Spectrum Analyzer to troubleshoot why a network won't work in a channel or area.

Use the Wi-Fi Diagnostics Program

Apple has a hidden diagnostics program that the firm apparently uses when you take your computer into an Apple Store or when you call for phone-based technical support. However, it's not difficult to use, and I find it a great help in placing a base station.

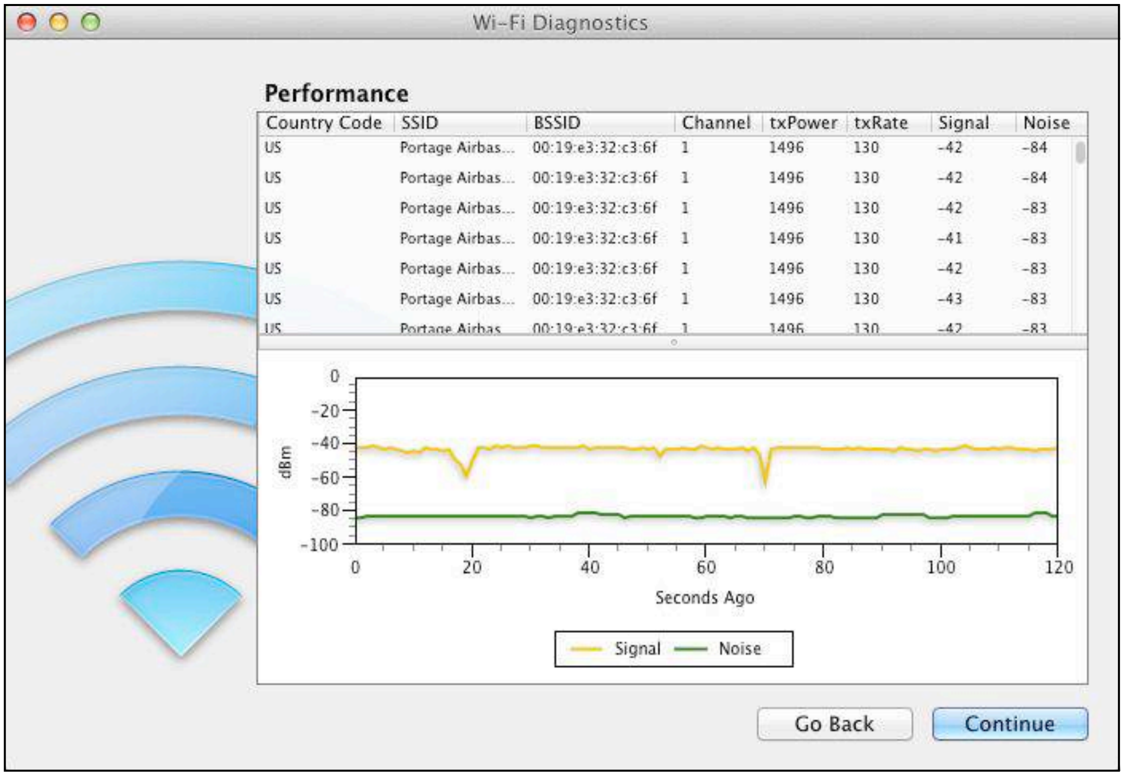
The program is called Wi-Fi Diagnostics, and it's in the root `/System` folder. To use the program to help you track signal strength over time (and space) in a base station connection, follow these steps:

1. In the Finder, choose Go > Go To Folder.

2. Type `/System/Library/CoreServices` and click Go.

   The Core Services folder opens.

3. From within the Core Services folder, launch Wi-Fi Diagnostics.
4. Select Monitor Performance, and click Continue
5. The Performance display is in two parts, and it shows continuous monitoring, updated every second, of the computer's connection to a base station (**Figure 34**). Walk around with your laptop or relocate your base station, and monitor results.



Country Code	SSID	BSSID	Channel	txPower	txRate	Signal	Noise
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-42	-84
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-42	-84
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-42	-83
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-41	-83
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-42	-83
US	Portage Airbas...	00:19:e3:32:c3:6f	1	1496	130	-43	-83
US	Portage Airbas	00:19:e3:32:c3:6f	1	1496	130	-42	-83

Figure 34: Monitor the quality of a connection to a base station continuously with Wi-Fi Diagnostics.

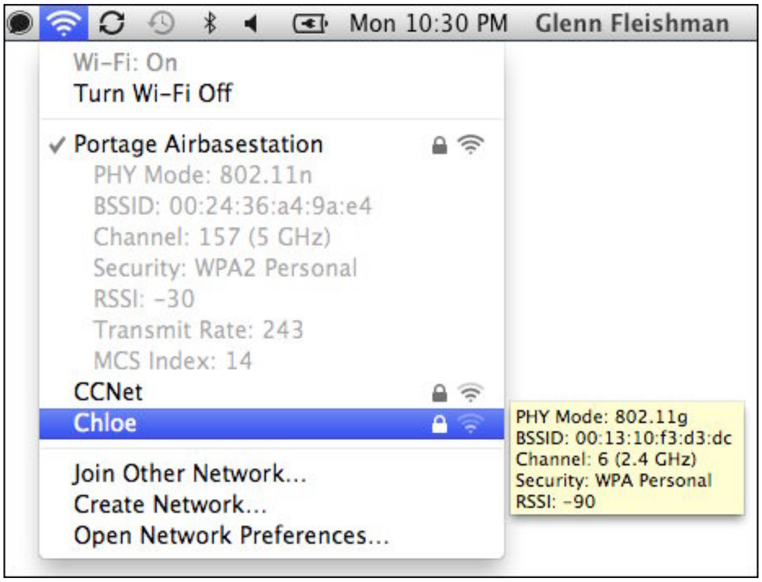
The columns show the network name (SSID), the unique adapter identifier (BSSID), the base station's channel, the transmit power (txRate)—not useful as it is a constant number set by the base station, transmission rate (txRate)—Mbps for the connection, signal, and noise.

Aim for the highest txRate (a higher number is better), the lowest noise (closer to -100 than 0), and the highest signal level (closer to 0 than to -100).

6. When you are finished, click Continue, and then choose Wi-Fi Diagnostics > Quit Wi-Fi Diagnostics (Command-Q).

Use the Wi-Fi Menu

The Wi-Fi menu in the menu bar offers connection information useful for troubleshooting in Snow Leopard and later (**Figure 35**).



PHY Mode: 802.11n
BSSID: 00:24:36:a4:9a:e4
Channel: 157 (5 GHz)
Security: WPA2 Personal
RSSI: -30
Transmit Rate: 243
MCS Index: 14

PHY Mode: 802.11g
BSSID: 00:13:10:f3:d3:dc
Channel: 6 (2.4 GHz)
Security: WPA Personal
RSSI: -90

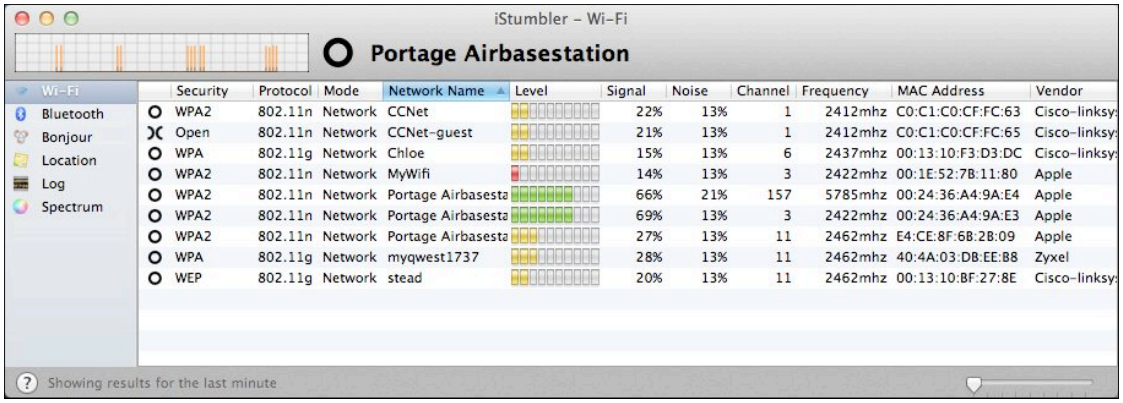
Figure 35: The Wi-Fi menu displays signal information.

Hold down the Option key and select the menu, then hover over any network to get answers to several key questions:

- **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.
- **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. 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 flavor in the Time Capsule and AirPort Extreme models can operate at a raw rate of up to 450 Mbps (in 5 GHz) or 225 Mbps (in 2.4 GHz); for example, in **Figure 35** (above), for the Portage Airbasestation, the rate is 243 Mbps using 5 GHz channel 157. The transmit rate can change constantly, as the adapter and base station negotiate for faster or slower connections as problems are encountered.

Measure with iStumbler

iStumbler (http://www.istumbler.com/) provides a continuous scan with information about signal and noise for all the 2.4 and 5 GHz networks in your vicinity, including each base station in a multi-base station network, such as Portage Airbasestation, shown in **Figure 36**.



	Security	Protocol	Mode	Network Name	Level	Signal	Noise	Channel	Frequency	MAC Address	Vendor
○	WPA2	802.11n	Network	CCNet		22%	13%	1	2412mhz	C0:C1:C0:CF:FC:63	Cisco-linksy
)(	Open	802.11n	Network	CCNet-guest		21%	13%	1	2412mhz	C0:C1:C0:CF:FC:65	Cisco-linksy
○	WPA	802.11g	Network	Chloe		15%	13%	6	2437mhz	00:13:10:F3:D3:DC	Cisco-linksy
○	WPA2	802.11n	Network	MyWifi		14%	13%	3	2422mhz	00:1E:52:7B:11:80	Apple
○	WPA2	802.11n	Network	Portage Airbasesta		66%	21%	157	5785mhz	00:24:36:A4:9A:E4	Apple
○	WPA2	802.11n	Network	Portage Airbasesta		69%	13%	3	2422mhz	00:24:36:A4:9A:E3	Apple
○	WPA2	802.11n	Network	Portage Airbasesta		27%	13%	11	2462mhz	E4:CE:8F:6B:2B:09	Apple
○	WPA	802.11g	Network	myqwest1737		28%	13%	11	2462mhz	40:4A:03:DB:EE:B8	Zyxel
○	WEP	802.11g	Network	stead		20%	13%	11	2462mhz	00:13:10:BF:27:8E	Cisco-linksy

Showing results for the last minute

Figure 36: iStumbler shows nearby networks.

iStumbler uses percentages for signal and noise, where a higher number (closer to 100% than 0%) is better for signal, as it means a stronger signal, and a lower number (closer to 0% than 100%) is better for noise, as it indicates less noise.

Run a Spectrum Analyzer

If you're truly frustrated with finding a good connection, you could buy a spectrum analyzer, an expensive piece of hardware. 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.

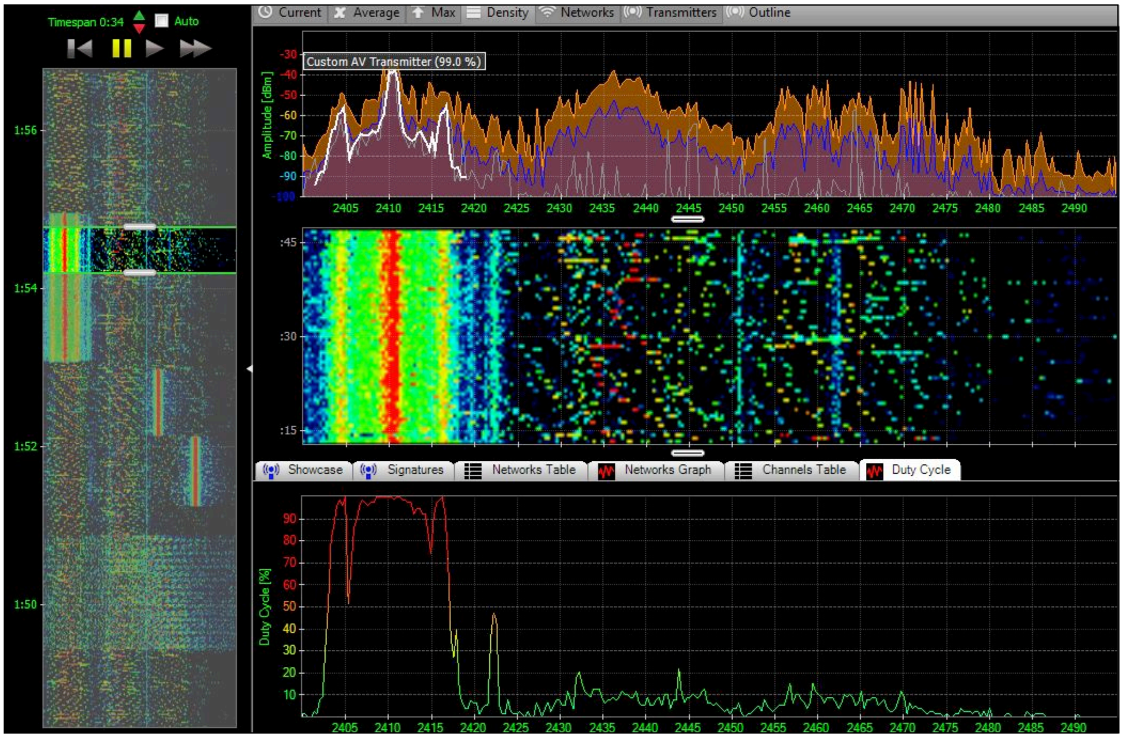


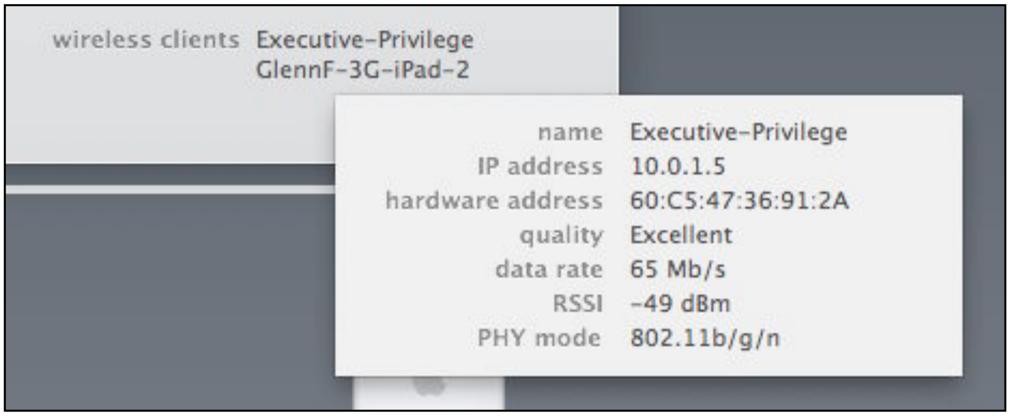
Figure 37: Chanalyzer software from MetaGeek provides a rich visualization of what's happening in the radio spectrum around you.

MetaGeek makes spectrum analyzers that run from $199 for a 2.4 GHz only unit with basic software that's useful for spotting and troubleshooting interference, up to a $999 pro version for examining the 2.4 and 5 GHz bands with sophisticated analysis software (http://www.metageek.net/).

Testing from Base Station to Client

The saddest change from AirPort Utility 5 to 6 is the elimination of some useful monitoring tools hidden deep in the program that helped you watch client connections in real time. Apple left a little bit of help in, but you have to look for it.

In the Mac version of AirPort Utility, select a base station and note the list of entries at the bottom next to the label Wireless Clients (if any hardware is connected). Hover over, but do not click, any client name, and a floating panel appears (**Figure 38**), showing connection details: the data rate, RSSI, and PHY mode, as described earlier in this section, in Use the Wi-Fi Menu.

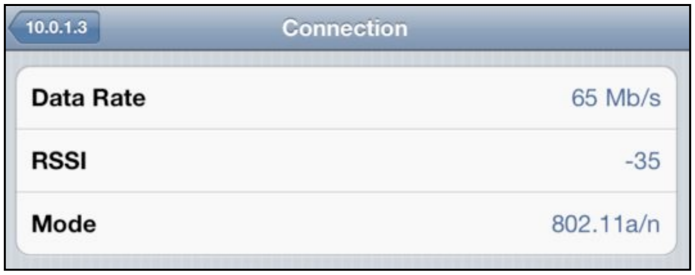

wireless clients Executive-Privilege
GlennF-3G-iPad-2

name	Executive-Privilege
IP address	10.0.1.5
hardware address	60:C5:47:36:91:2A
quality	Excellent
data rate	65 Mb/s
RSSI	-49 dBm
PHY mode	802.11b/g/n

Figure 38: The Wireless Clients entry mouseover shows connection information.

The same information is available in iOS, nested a few layers deep. Select a base station, then tap Wireless Clients (you may have to slide down), and then tap a client name.

Unlike AirPort Utility on the Mac, the iOS app seems to miss the Bonjour names of clients more often then not, and it instead shows just the local network's IP address. In the Wireless Clients view, tap an entry, and then tap Connection to get the details on Data Rate, RSSI, and (PHY) Mode (**Figure 39**).



Data Rate	65 Mb/s
RSSI	-35
Mode	802.11a/n

Figure 39: AirPort Utility for iOS nests connection status a little deeper than the Mac version.

Advanced Networking

Did the simplified setups explained in Set Up a Network not cover everything you needed to get up and running? In this chapter, I spell out 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 chapter 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 40**).

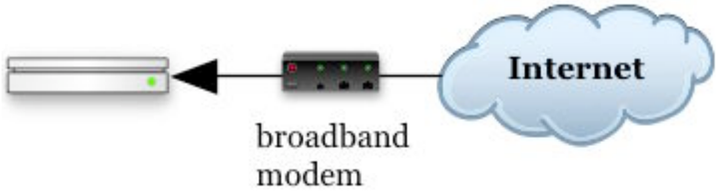


Figure 40: Plug your broadband modem into the base station's WAN port.

For an Express, that's the only port, and it's labeled as a standard Ethernet port (**Figure 41**, left); for an Extreme or Time Capsule, it's a port labeled with a circle of dots (**Figure 41**, right).

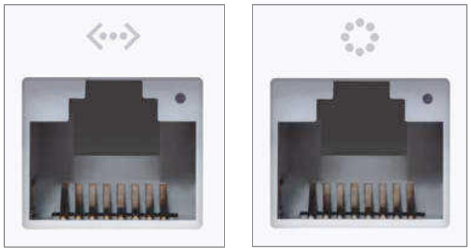


Figure 41: The single Ethernet port on an Express (left); the WAN port on the back of an Extreme or Time Capsule (right).

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.

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, just ahead.

- A static address is more typical for small and large offices. For setup information, read Static Addressing, a few pages ahead.

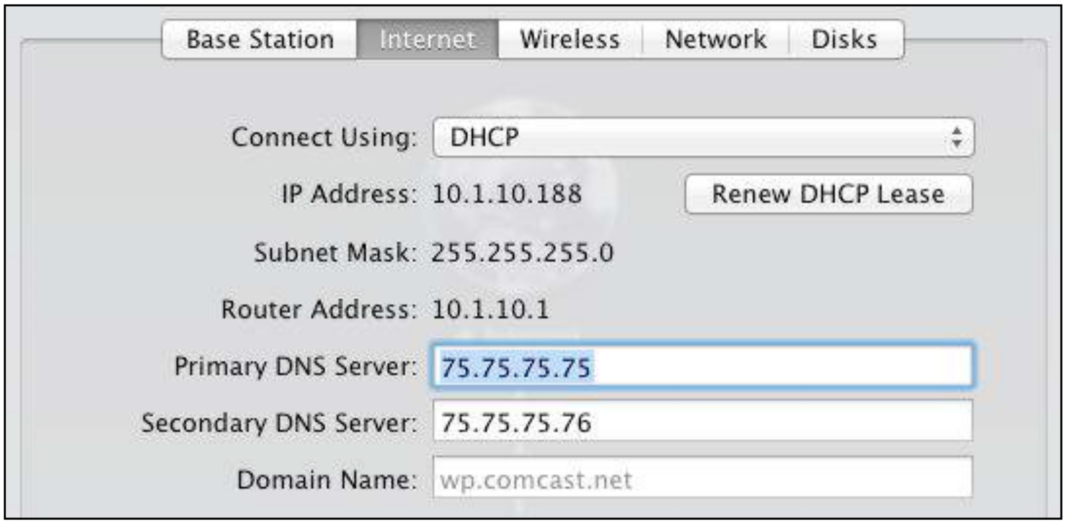
Dynamic Addressing

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 request 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 42**).



Connect Using: DHCP
IP Address: 10.1.10.188
Subnet Mask: 255.255.255.0
Router Address: 10.1.10.1
Primary DNS Server: 75.75.75.75
Secondary DNS Server: 75.75.75.76
Domain Name: wp.comcast.net

Figure 42: 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. DHCP server DNS addresses are shown in the DNS Server(s) fields in gray. In the Mac version of AirPort Utility, select your base station and click Edit, and then in the Internet view (**Figure 42**, above), you can click to type and replace them.

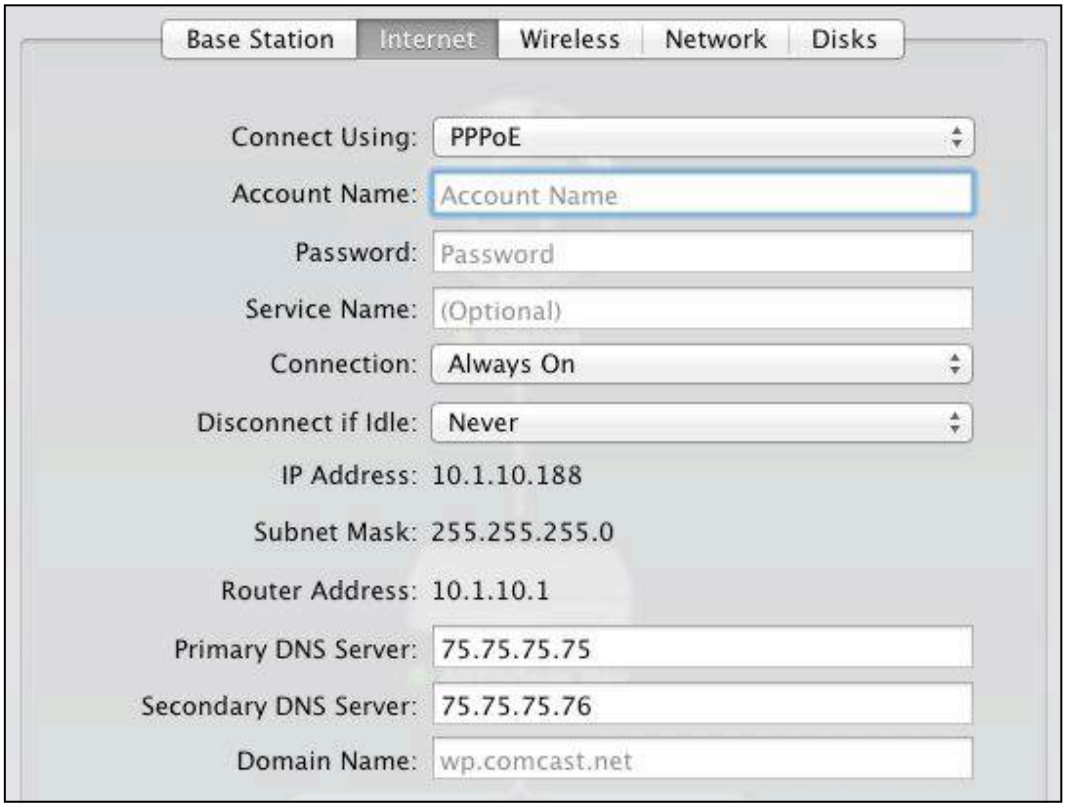
- If you need to use PPPoE or have MAC address issues with configuration, then New Network, Single Base Station may not have answered all your questions; keep reading in this chapter to find directions for how to log in via PPPoE over Broadband DSL (just ahead) and how to Deal with MAC-Address-Restricted Cable Broadband.

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 *PPPoE* (PPP over Ethernet) when connecting to their network. With PPPoE, you log in with a username and password to your ISP over your DSL connection, at which time you are automatically assigned an IP address and the connection works just like any other broadband connection.

If you need PPPoE, configure it in the Internet pane of AirPort Utility for the Mac by choosing PPPoE from the Connect Using pop-up menu (**Figure 43**). The base station connects per the setting you choose in the Connection pop-up menu: Always On is the most likely choice.



Connect Using: PPPoE
Account Name: Account Name
Password: Password
Service Name: (Optional)
Connection: Always On
Disconnect if Idle: Never
IP Address: 10.1.10.188
Subnet Mask: 255.255.255.0
Router Address: 10.1.10.1
Primary DNS Server: 75.75.75.75
Secondary DNS Server: 75.75.75.76
Domain Name: wp.comcast.net

Figure 43: PPP over Ethernet connects with 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.

ISPs use two common methods to restrict access by MAC address:

- In the less annoying method, the cable modem powers up and then locks on to the MAC address of the device that's 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.

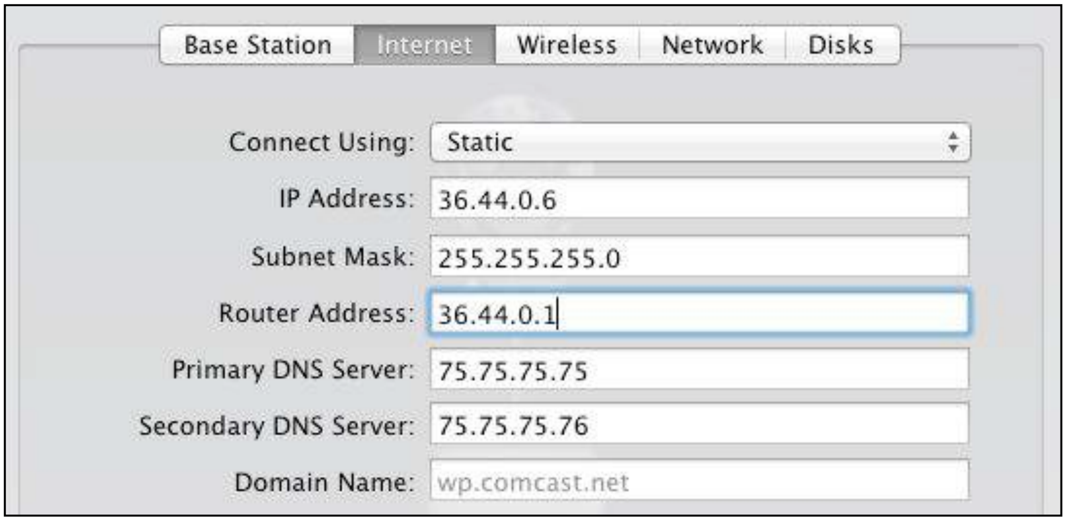
Note: To learn more about MAC addresses, read Appendix E: What and Where Is a MAC Address?.

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 outgoing 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 the IP address for 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 configure static addressing, edit your base station in the Mac version of AirPort Utility, click the Internet button, choose Static from the Connect Using pop-up menu, then enter the values (**Figure 44**).



Connect Using: Static

IP Address: 36.44.0.6

Subnet Mask: 255.255.255.0

Router Address: 36.44.0.1

Primary DNS Server: 75.75.75.75

Secondary DNS Server: 75.75.75.76

Domain Name: wp.comcast.net

Figure 44: Configure the Internet connection manually by entering the static values provided by your ISP or network administrator.

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 are providing services and 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.

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 topic to set up the base station; you can skip ahead to Connect Your Devices. However, should you want to control which addresses are assigned or manage other details of NAT and DHCP, read on.

In AirPort Utility for the Mac, edit your base station, click the Network button at the top of the window, and choose DHCP and NAT from the Router Mode pop-up menu.

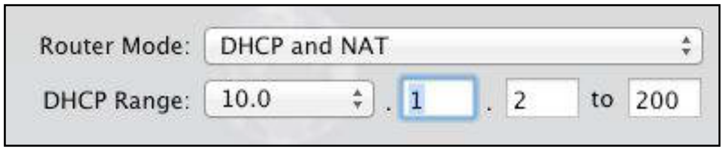
The DHCP Range pop-up menu lets you set the numbers and range of addresses used for DHCP address assignment on your network, as well as a few other DHCP properties. The only reason to change the range of numbers is if you want to create and assign *private* addresses that remain static instead of being 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, discussed later in this chapter.

DHCP addresses are drawn from one of three reserved ranges of private addresses—10.0.*.*, 172.16.*.*, or 192.168.*.*. The * refers to a number in an appropriate range, typically 0 or 1 through 254 or 255. These prefixes are reserved by the global numbering authority, and they are guaranteed to not be in use on any public Internet network. You can choose any of these three starting points, although Apple uses the 10.0 prefix by default.

To configure the rest of the DHCP addresses for assignment, carry out the following :

1. Type the third number in the IP address in the field to the right of the pop-up menu (**Figure 45**). 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.



Router Mode: DHCP and NAT

DHCP Range: 10.0 . 1 . 2 to 200

Figure 45: The DHCP Range controls comprises a pop-up menu for selecting one of three private address ranges, a field for setting the third number in the IP address, and fields for entering the start and end range of your addresses.

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.

***2^8-2:** 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.*

3. The final number, following “to” is the end of the range. It may be from any number starting at or including the starting address number all the way to 254. Apple, by default, sets this field to 200. You might choose to set this to a lower number if you have a complicated network. But in most cases, you can leave the default setting in place.

In the DHCP Lease field, 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. You can opt to set units of time in minutes, hours, or days in the pop-up menu.

NAT (Network Address Translation) is handled in the bottom half of the Network view. The view offers 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.

Note: I explain DHCP reservations in Reserved Addresses (ahead shortly), the options for port mapping in Map Ports for Remote Access, and how to limit access in Timed Access Control.

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 on the Mac, select the base station, click Edit, and then click the Internet button.
2. Choose DHCP Only from the Router Mode pop-up menu.

   In this mode, the NAT options are dimmed because there's no translation going on.
3. In the DHCP Range fields, enter values for the beginning and the ending addresses. 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 Internet. This makes computers susceptible to direct attacks by ne'er-do-wells. For example, someone could attempt to break your Web server by sending it a maliciously crafted request.*

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.

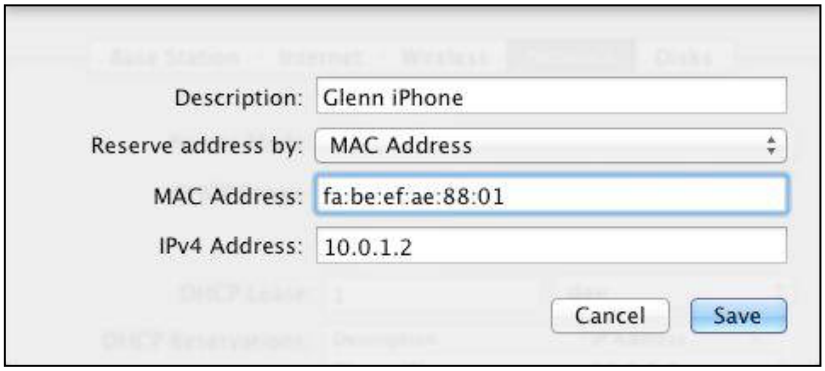
The reserved address is never assigned to another computer, and if the computer in question restarts or shuts down, the next time it powers up and its network adapter is active, it receives its reserved address.

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 reserved addresses:

1. In AirPort Utility on the Mac, select your base station and click Edit. Then, below the Network pane's DHCP Reservations list, click the plus + button.

   A dialog for entering the reservation appears (**Figure 46**).



Description: Glenn iPhone

Reserve address by: MAC Address

MAC Address: fa:be:ef:ae:88:01

IPv4 Address: 10.0.1.2

Figure 46: 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.

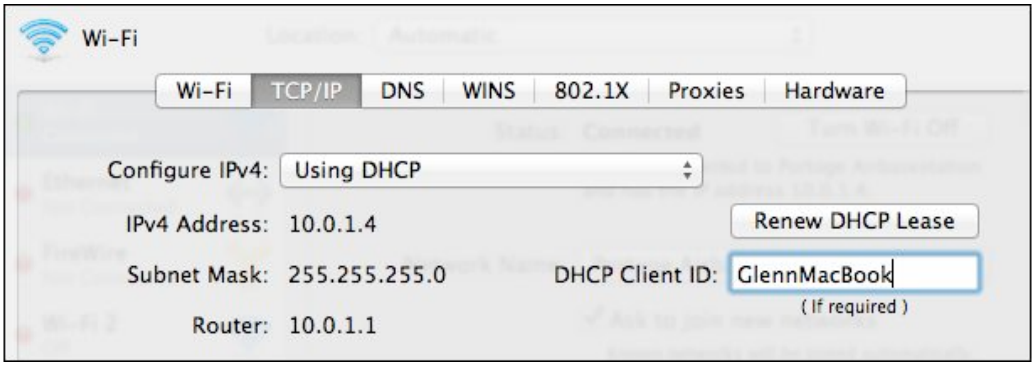
3. Select whether to reserve an IP address by a Wi-Fi adapter's MAC address or by its DHCP Client ID. DHCP Client ID is easier to set up, but it works only with Mac OS X (and earlier Mac systems).

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), and enter the last number in the IP range that you want to reserve. If you need help locating the MAC address, see Appendix E: What and Where Is a MAC Address?.

   - **If you reserved by DHCP Client ID:** The DHCP Client ID is a text tag that you assign to a Wi-Fi or Ethernet adapter. When an adapter requests a dynamic address, it transmits the text, and then the base station uses the tag to assign a reserved IP address:

     a. Set the DHCP Client ID on a client Mac: 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 47** shows the DHCP Client ID set to *GlennMacBook*.



Configure IPv4: Using DHCP

IPv4 Address: 10.0.1.4

Subnet Mask: 255.255.255.0

Router: 10.0.1.1

DHCP Client ID: GlennMacBook

(If required)

Figure 47: The DHCP Client ID field is found in the TCP/IP view when the Configure IPv4 pop-up menu is set to Using DHCP.

***Warning!** To avoid confusing the base station, make sure that each Mac's DHCP Client ID is unique.*

     b. In AirPort Utility, enter the DHCP Client ID that you just set up on the Mac in the reservation dialog and then enter the last number in the four-number IP address (**Figure 46**, earlier).

(If the number is reserved already, in use by another device, or not in the legal range, the Done button can't be clicked.)

5. Click Save.

***More than one?** As needed, repeat Steps 1–5 until you've set up all your reservations.*

6. After completing all the reservations you need, click Update.

When the base station is finished restarting, the DHCP Reservations list shows the entries you made and any computers listed will have retrieved their new addresses.

***If a Mac still shows its old address:** Open the Network system preferences pane, select the adapter, and click the Advanced button. Click TCP/IP, and then click Renew DHCP Lease. The IPv4 Address field should clear 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 on the Mac, select your base station, click the Edit button, and click the Network button.
2. Choose Off (Bridge Mode) from the Router Mode pop-up menu. (The DHCP and NAT features dim.)
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.

Connect Your Devices

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 chapter to learn how to Connect in Lion (with notes on 10.5 Leopard and 10.6 Snow Leopard), Connect in iOS, and Connect in Windows 7. These topics discuss not just how to connect to networks, but also how to 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 Lion

You connect in Lion, as with previous versions of Mac OS X, through either the Wi-Fi menu, a status menu near the right of the menu bar, or the Network system preference pane. If you don't see the Wi-Fi menu, launch System Preferences and select the Network preference pane. Select the Wi-Fi adapter at the left, and then check Show Wi-Fi

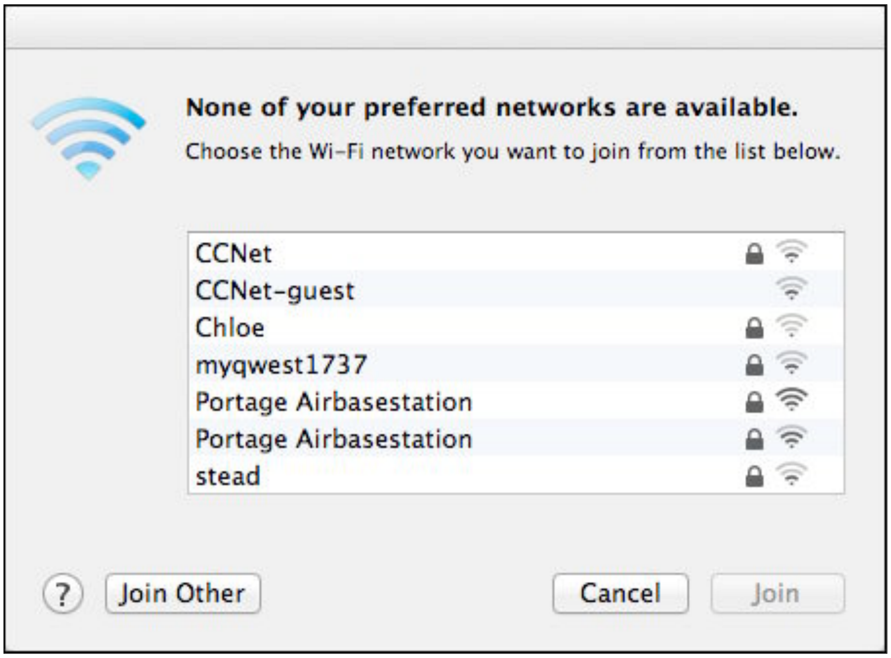
Status in Menu Bar. (To learn what the different icons for the Wi-Fi status menu mean, consult Mac Wi-Fi Iconography, much earlier.)

Tip: 10.5 Leopard and 10.6 Snow Leopard have nearly identical choices as Lion for connecting to a Wi-Fi network.

Find a Network and Connect

Mac OS X constantly looks for networks, and a list of any found networks appears in the Wi-Fi menu when the Wi-Fi adapter is on. (If it's off, choose Wi-Fi > Turn Wi-Fi On.)

If a Wi-Fi network appears nearby 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 will alert you (**Figure 48**). From that alert, you can then connect to the network.



None of your preferred networks are available.

Choose the Wi-Fi network you want to join from the list below.

CCNet
CCNet-guest
Chloe
myqwest1737
Portage Airbasestation
Portage Airbasestation
stead

Figure 48: Mac OS X alerts you to a new network.

Your Mac automatically joins any network that it's been told to remember. It will connect when you wake it up or turn it on, when you turn Wi-Fi 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.

Tip: You can disable new network alerts in the Network system preference pane.

Let's walk through the various connection methods. Connecting to a named network is by far the most common option and I discuss it just below. After that, I cover how to make more complex connections.

Connect to a Named Network

To join a Wi-Fi network when the network broadcasts its name—as most do—choose the network name from the Wi-Fi status menu (**Figure 49**). Starting in 10.6 Snow Leopard, Mac OS X animates the bars in the Wi-Fi icon, lighting them up one at a time in a back-and-forth pattern while the connection is in progress. After connecting, the Wi-Fi menu's icon switches from gray to black, with the number of black waves indicating signal strength by their quantity.

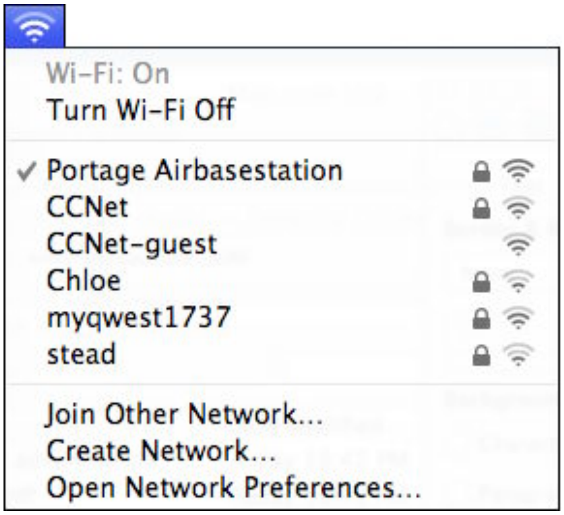


Figure 49: Choose a network from the list or choose Join Other Network to join a closed network by entering its name.

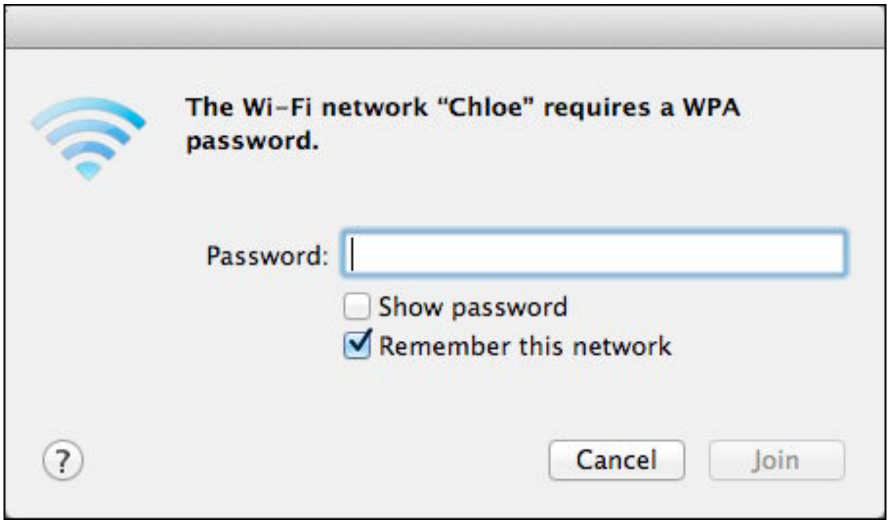
Warning! *Wi-Fi networks that use base stations appear as in* ***Figure 49****, above. Ad hoc and peer-to-peer networks are listed lower down under the Devices heading. Public Wi-Fi networks won't appear in the Devices list; if a public-sounding network appears there, it is likely a compromised computer, a bad configuration, or a hacker trying to get you to connect to a honeypot.*

Use Diagnostics to Solve Connection Problems

Starting in 10.5 Leopard, Mac OS X has a feature called Network Diagnostics; if you can't get your Wi-Fi 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.

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

If encryption is active on the network, after you choose the network name, you are prompted by a dialog to enter an encryption key (your encryption key is your password) (**Figure 50**).



The Wi-Fi network "Chloe" requires a WPA password.

Password: |

□ Show password
☑ Remember this network

Figure 50: When you attempt to join a network that's protected by encryption, you're prompted for its password.

Typically, the Wi-Fi 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 Join to connect to the network.

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

Save the key, save time: *You can store the key in the Keychain by leaving Remember This Network checked; this prevents you from having to retype the password in the future.*

Encryption Key, Password, Passphrase

In this chapter, 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 often 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. (I discuss how to set up network security in Secure Your Network, later).

WPA and WPA2 Personal both use a passphrase to create an encryption key, but with different methods. But the passphrase can be the same for both WPA and WPA2, neatly enough: you don't need to set a different one for each encryption method. This lets you upgrade a network from WPA or mixed WPA/WPA2 to WPA2 only or the reverse without having to reset the passphrase on devices that connect to the network.

You can set up WPA/WPA2 Personal or WPA2 Personal in one of two ways, the first of which is what you will see nearly all the time:

- **Passphrase:** Enter the passphrase exactly as it was typed in the base-station configuration software. Mac OS X (like all operating systems that handle WPA and WPA2) converts the passphrase into the long hexadecimal key used to join the network.

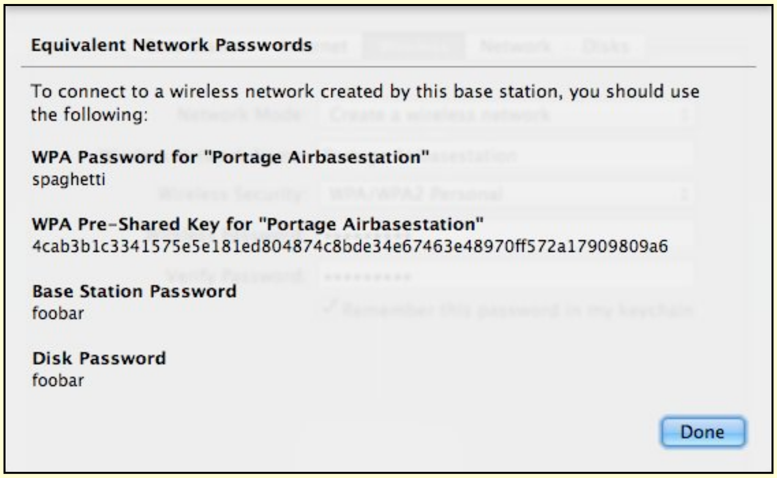
- **Full hex key:** In rare cases with WPA or WPA2, you may need to enter the 64-digit hexadecimal encryption key that's typically hidden from view. In nearly a decade of using WPA and then WPA2, I have never had to enter such a key.

  To enter this in Leopard or later, hold down the Option key before you choose the network from the Wi-Fi menu. An extra large field appears, allowing entry. Yes, it's a pain to enter 64 hex digits. It's there for full compatibility's sake.

Extracting the Full WPA Key

A vanishingly small number of devices might need you to enter the full hex key instead of a WPA or WPA2 Personal passphrase. AirPort Utility (on the Mac) can show the conversion of the passphrase into a 64-digit hex key. Edit your base station and then choose Base Station > Show Passwords (**Figure 51**).

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.)



Equivalent Network Passwords

To connect to a wireless network created by this base station, you should use the following:

WPA Password for "Portage Airbasestation"
spaghetti

WPA Pre-Shared Key for "Portage Airbasestation"
4cab3b1c3341575e5e181ed804874c8bde34e67463e48970ff572a17909809a6

Base Station Password
foobar

Disk Password
foobar

Figure 51: *The horror that is the very long WPA Pre-Shared Key shown in hexadecimal.*

Although WEP is much less commonly used these days, you may yet encounter it. It 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 hexadecimals 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 exactly 5 or 13 characters long.

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 (found inside `/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*".

Connect to a Closed (Hidden) Network

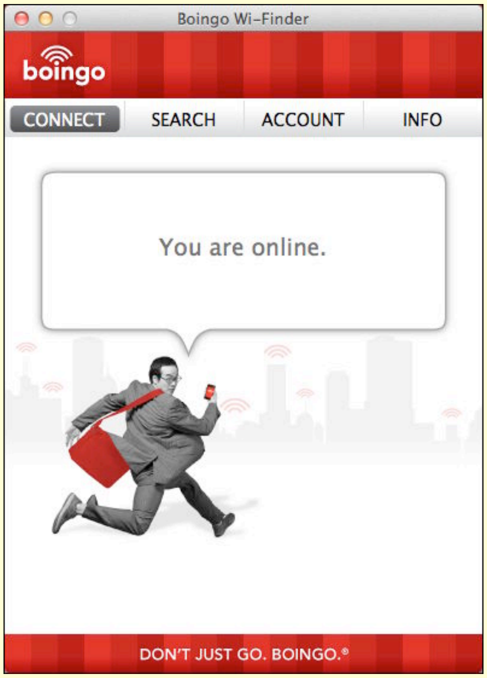
For a closed network, choose Join Other Network from the Wi-Fi status menu. In the resulting dialog, enter the network's precise name (close doesn't count), and choose None from the Security menu or pick the form of encryption and enter the username (if required) and password. Click Join.

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 in many cases if you use Boingo Wireless, a hotspot access reseller that aggregates access to thousands of networks. With Boingo's Boingo Wi-Finder 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 for two Wi-Fi devices, whether laptops or mobiles. Extra devices add $5 per month each. Global and mobile-only plans are also available (http://www.boingo.com/).

The software can also be set up to connect with no dialog to hundreds of thousands (and some day, millions) of free networks that require a click or other process to gain access.

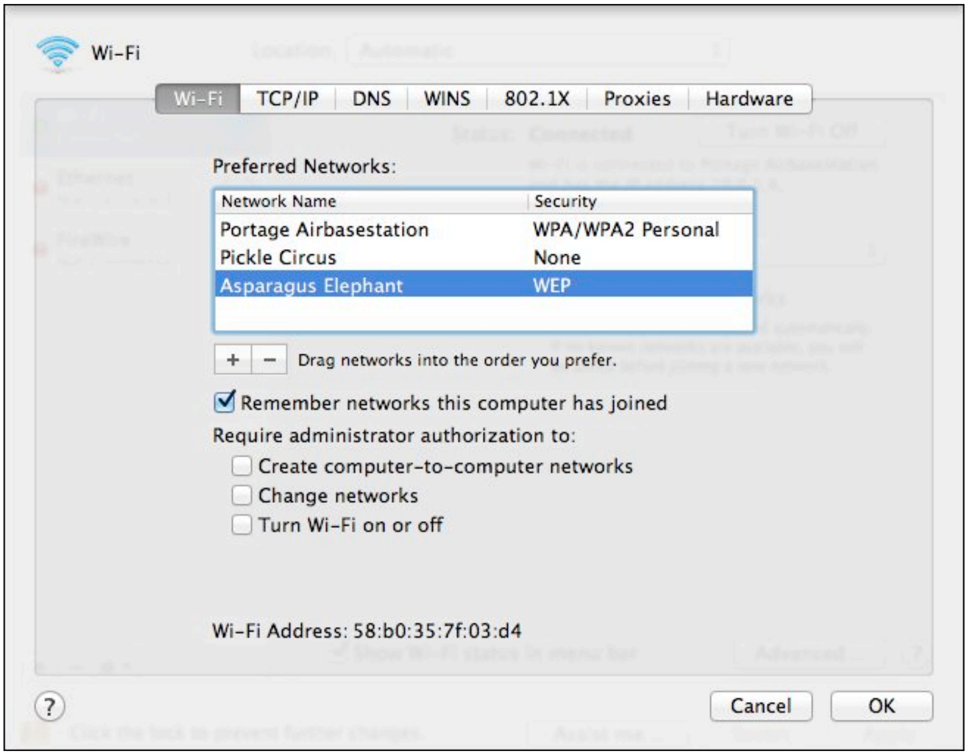


You are online.

Figure 52: *If you are logged in to a Boingo account, Boingo's software will automatically recognize and join a Wi-Fi network that's part of the Boingo plan.*

Manage Network Profiles

Wi-Fi network *profiles* work on Macs running 10.5 Leopard and later. They let you enter and store any needed passphrase, key, or login details to access a network. You can manage Wi-Fi network profiles in the Network system preference pane. Open the pane and select the Wi-Fi adapter; then click the Advanced button to see more configuration options in the Wi-Fi view (**Figure 53**).



Preferred Networks:

Network Name	Security
Portage Airbasestation	WPA/WPA2 Personal
Pickle Circus	None
Asparagus Elephant	WEP

Drag networks into the order you prefer.

☑ Remember networks this computer has joined

Require administrator authorization to:

□ Create computer-to-computer networks

□ Change networks

□ Turn Wi-Fi on or off

Wi-Fi Address: 58:b0:35:7f:03:d4

Figure 53: You can add, delete, and prioritize 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 plus + button.
- Delete a profile you no longer need by selecting it and clicking the minus − 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.

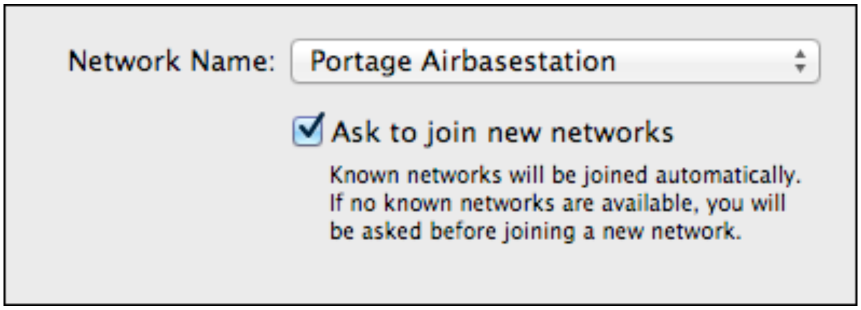
Note: Apple weirdly removed the Edit button in Lion, which in Leopard and Snow Leopard looks like a little pencil. In Lion—as of the 10.7.3 release, at least—if you make an error when creating a profile, or need to change the encryption method or password, you have to delete the profile and create a new one. Silly, really.

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

Refine Your Connection Options

To control some of how a Wi-Fi adapter connects to networks, select the Wi-Fi adapter in the Network system preference pane, and do any of the following:

- 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 54**). (See **Figure 48** for an example of what that alert looks like.)



Network Name: Portage Airbasestation

☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Figure 54: If this checkbox is checked, when Mac OS X spots a new network, you're asked if you want to join.

- Click the Advanced button to reach additional options:
  - 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.
  - The "Require administrator authorization to" checkboxes allow you to override someone's attempt to create computer-to-computer (ad hoc) networks, switch networks, or turn Wi-Fi off.

Learn from the Wi-Fi Menu

Since Leopard, Mac OS X's Wi-Fi menu has been dynamic: the operating system scans for networks after you open the menu, adding more to the list as it finds them (**Figure 55**). 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. Also since Leopard, Mac OS X shows a signal strength indicator to the right of the network name.

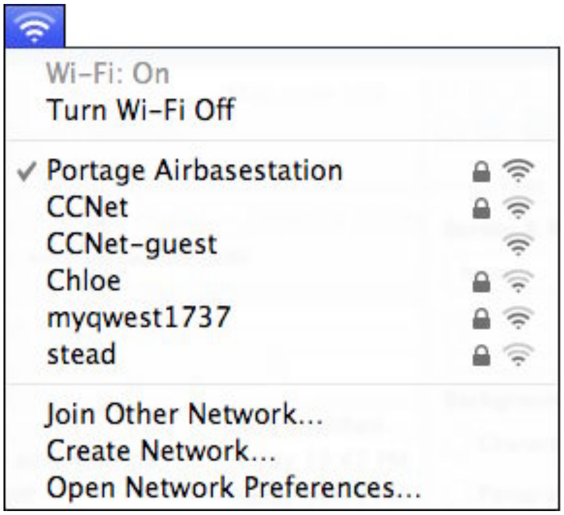


Figure 55: When you first open it, the Wi-Fi menu shows a progress spinner. It then shows the networks that your Mac has found.

In Lion, Apple added two labels in the Wi-Fi menu that may appear below the list of standard Wi-Fi networks and above the Join Other Network item: Devices, which shows any printers or computer-to-computer or *ad hoc* networks (see Ad Hoc Networking), and New AirPort Base Station, which shows any unconfigured devices on the local network available via Bonjour (**Figure 56**) (read Set Up a Network).

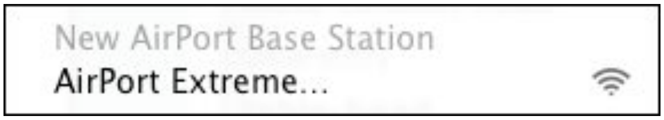


Figure 56: A separate area in the Wi-Fi menu shows any unconfigured base stations by type instead of as before, with an obscure network name.

Devices and New AirPort Base Station appear only if an appropriate device or new base station is available.

To show more network details in the Wi-Fi menu, hold down the Option key while opening the menu (**Figure 57**).

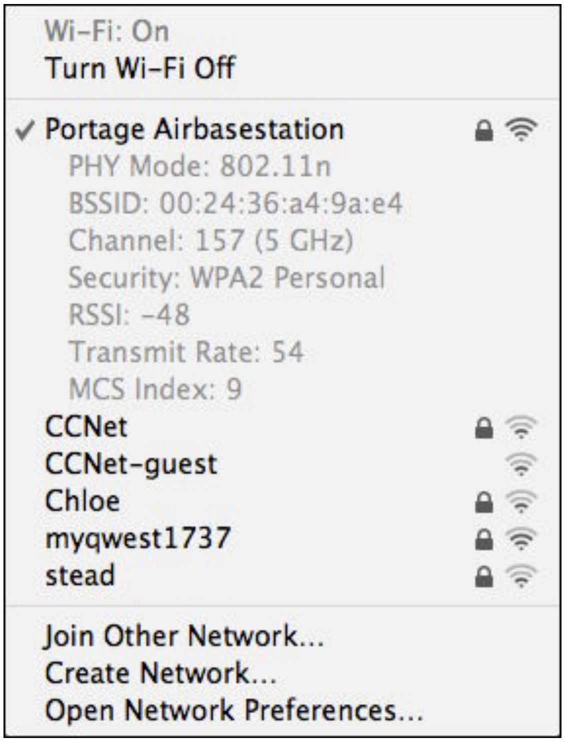


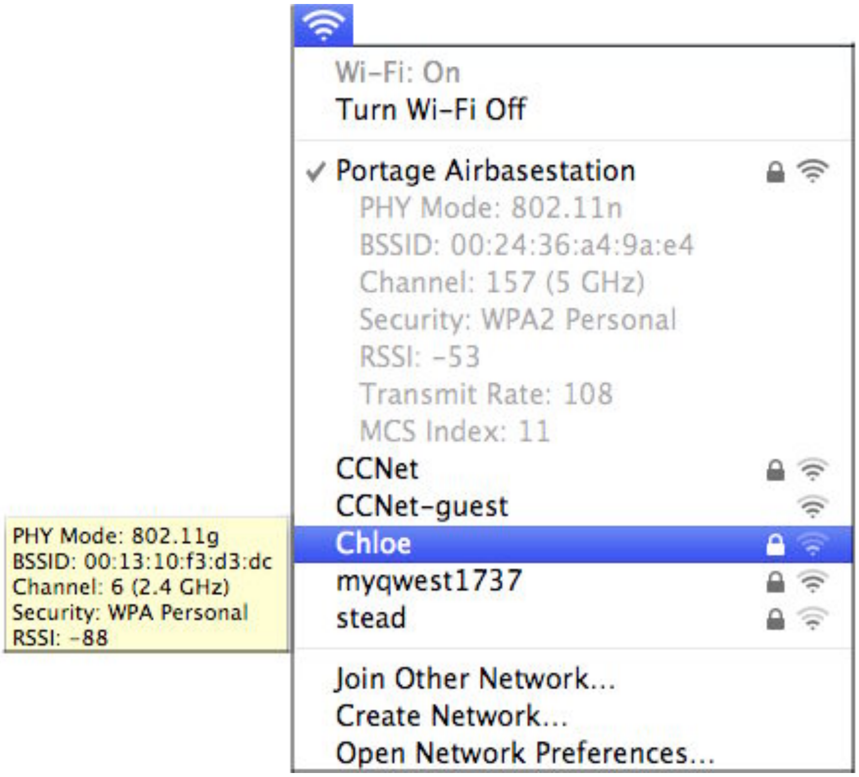
Figure 57: Hold down Option while opening the Wi-Fi menu to see additional details about the network that you're connected to.

The menu offers a plethora of data—you can see seven pieces of information about the network that you've joined:

- The *PHY Mode,* or protocol name in use (e.g., 802.11n)
- The MAC address or Wi-Fi ID of the network (BSSID), a unique address for each base station
- The channel and band in use (e.g., channel 157, 5 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 the encoding method

You can also learn about a network other than the one you're connected to by hovering over the network's name in the menu

(**Figure 58**). In this case, you see the PHY Mode, MAC address, channel and band, security method, and the RSSI (signal strength).



PHY Mode: 802.11n
BSSID: 00:24:36:a4:9a:e4
Channel: 157 (5 GHz)
Security: WPA2 Personal
RSSI: -53
Transmit Rate: 108
MCS Index: 11

PHY Mode: 802.11g
BSSID: 00:13:10:f3:d3:dc
Channel: 6 (2.4 GHz)
Security: WPA Personal
RSSI: -88

Figure 58: 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, flip back to Use the Wi-Fi Menu.

Disconnect

Once a Mac is connected to a standard Wi-Fi network, it's fiendishly hard to disconnect it. (Ad hoc networks can be disconnected with a Wi-Fi menu item.) While still in range, you may:

- Choose Turn Wi-Fi Off from the Wi-Fi menu, which disables your network connection entirely.
- Connect to a different network.
- Remove the network profile:
  1. In the Network system preference pane, select the Wi-Fi adapter in the list at left.
  2. Click Advanced.

3. In the Wi-Fi view, select the network in the Preferred Networks list and click the minus − button.

4. Click OK, and then click Apply.

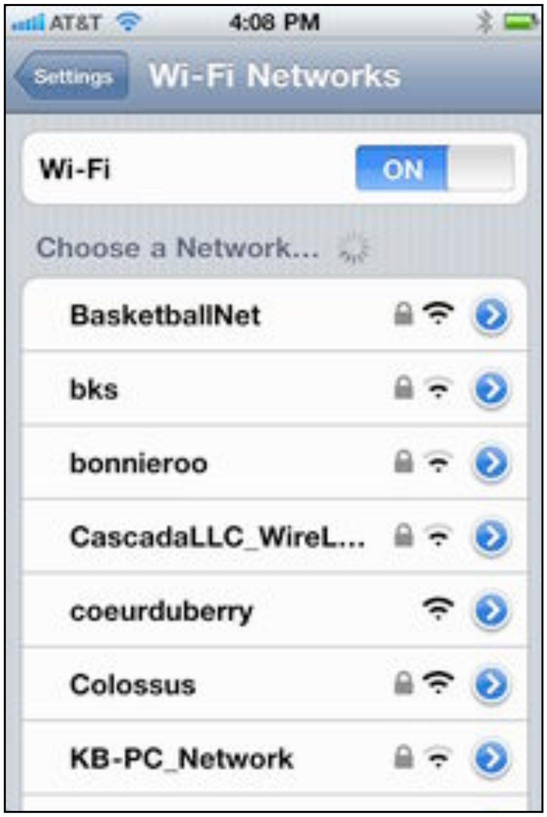
5. You may additionally need to turn the Wi-Fi adapter off and on from the Wi-Fi menu to have it drop the current connection.

Connect in iOS

iOS provides a simple way to join any Wi-Fi network with a few taps. If the Ask to Join Networks option is on in Settings > Wi-Fi, then whenever you're in range of one or more Wi-Fi networks and not already connected to one, iOS pops up a dialog asking if you want to join. Tap the network you want, and you're prompted for a password if one's required.

You can also join a network by tapping its name in a list:

1. In the Settings app, tap Wi-Fi to open the Wi-Fi Networks view (**Figure 59**).



Wi-Fi ON

Figure 59: The Wi-Fi Networks view lets you tap a network to join.

2. Select the network from the Choose a Network list by tapping it. (If the network you're trying to find doesn't appear, tap Other—you may have to slide down to find Other.)

3. Enter a password if prompted.

You're now connected. Tap the blue detail ❯ icon next to the connected network for TCP/IP details, such as the assigned IP address.

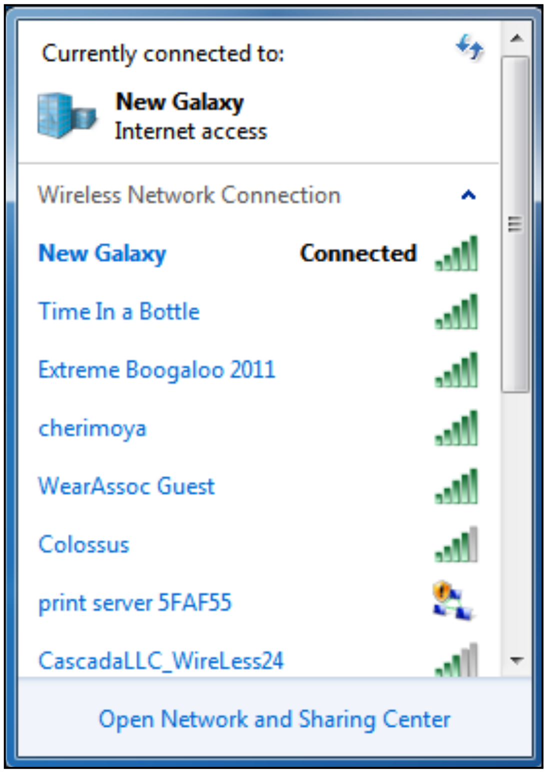
Note: Apple uses a chain-link 🔗 icon to indicate when a Wi-Fi network has been created using the Personal Hotspot feature in iOS, either on an iPhone 4 or 4S or on a third-generation iPad. Personal Hotspot lets the iOS device act like a cellular router for other devices.

To disconnect while still in range of the network, do either of the following:

- Tap Settings > Wi-Fi and turn off the Wi-Fi switch to disable the Wi-Fi adapter. While it remains off, you're disconnected.
- Tap Settings > Wi-Fi, tap the blue detail ❯ icon next to your currently connected network, and tap Forget This Network. This will immediately disconnect you, and you will remain disconnected.

Connect in Windows 7

To see what Wi-Fi networks are available in Windows 7, click the Wireless icon in the System Tray. This reveals a list of available networks (**Figure 60**). The icon for an open network or printer is badged with an exclamation point.



Currently connected to:

New Galaxy
Internet access

Wireless Network Connection

New Galaxy Connected

Time In a Bottle

Extreme Boogaloo 2011

cherimoya

WearAssoc Guest

Colossus

print server 5FAF55

CascadaLLC_WireLess24

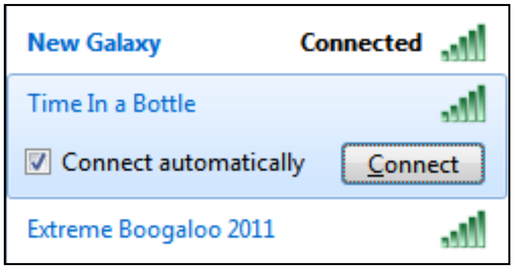
Open Network and Sharing Center

Figure 60: In Windows 7, you can view available Wi-Fi networks and networked printers.

To join a network, follow these steps:

1. From the list of wireless networks, click the network that you want to join.

   Windows 7 opens an area below the network name, with a Connect Automatically checkbox and a Connect button (**Figure 61**).



New Galaxy Connected

Time In a Bottle

☑ Connect automatically

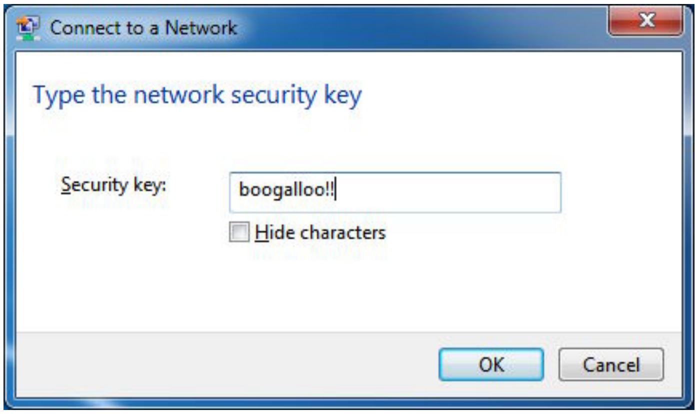
Connect

Extreme Boogaloo 2011

Figure 61: Click the Connect button to proceed.

2. Leave Connect Automatically selected (so that you can connect without a prompt in the future), and click the Connect button.
3. If the network has encryption enabled, you're prompted to enter the network key (**Figure 62**). Like Mac OS X, Windows 7 figures out what kind of key the network needs and translates what you

enter into the format required. Enter the key, and click OK. (Select Hide Characters if you don't want a shoulder surfer to spot what you're typing.)



Connect to a Network

Type the network security key

Security key: boogalloo!!

□ Hide characters

Figure 62: Enter the network's passphrase or key, and click OK.

A dialog box shows Connecting to *Network Name*, concluding when the network has been joined successfully.

4. A Set Network Location dialog box appears and lets you place the network by degree of trust: Home Network, Work Network, or Public Network. Click the appropriate area.

5. Windows 7 completes the connection, showing you a final dialog box with a summary, and links to make changes. Click Close.

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.

Stream Audio with AirPlay

AirPlay is a method of streaming media from a computer or iOS device to an external output device, such as an AirPlay-compatible speaker or an Apple TV, or—most interestingly for our purposes—an AirPort Express.

Historical note: In early 2011, Apple updated and renamed what was AirTunes to AirPlay. AirTunes was available only in the AirPort Express and Apple TV, and it required iTunes on a desktop computer for management.

In the case of the AirPort Express, only audio can be streamed. The Express sends the stream through its audio output port (**Figure 63**) to stereo speakers. You control the settings in AirPort Utility, and then play the audio via iTunes on a desktop computer or via an iOS device.

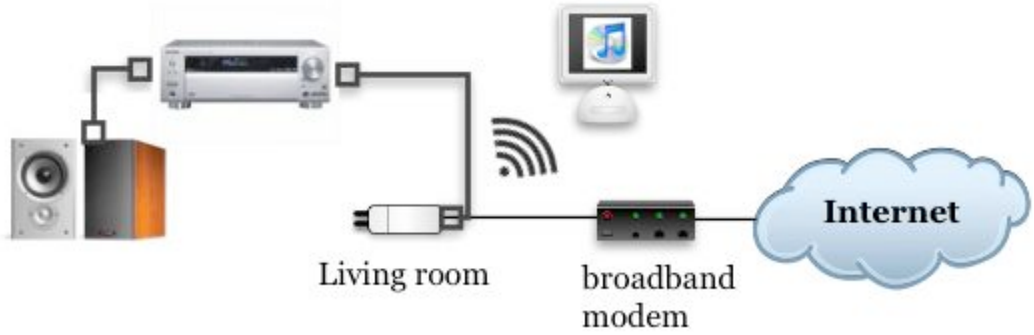
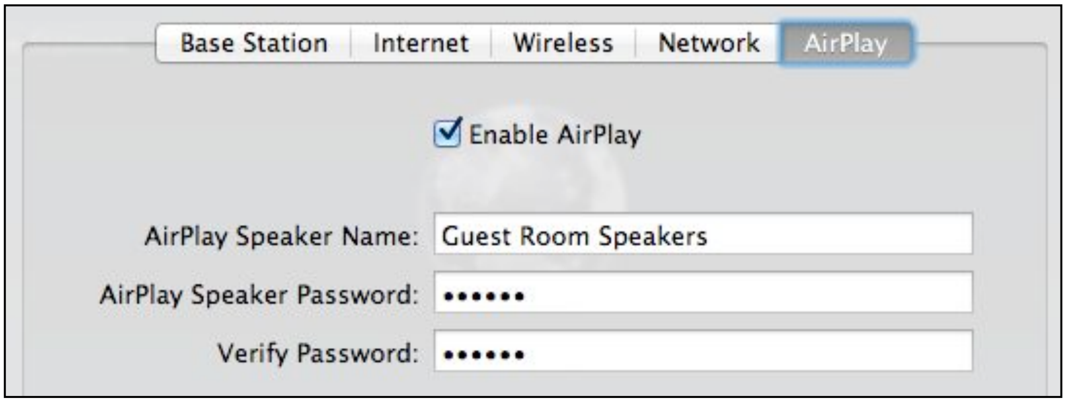


Figure 63: You can stream music from a computer on the network through AirPort Express to a stereo or powered speakers.

Tip: The fine folks at Rogue Amoeba offer Airfoil, a program that lets you play the sound output from any program on a Mac—not just iTunes—over AirPlay. See Share with Airfoil, later in this chapter.

Set Up AirPlay

To set up AirPlay, open AirPort Utility and edit your AirPort Express's configuration. Click or tap the AirPlay button to see the AirPlay view (the Mac version is shown in **Figure 64**).



☑ Enable AirPlay

AirPlay Speaker Name: Guest Room Speakers

AirPlay Speaker Password: ••••••

Verify Password: ••••••

Figure 64: The Music pane lets you set AirTunes options.

The AirPlay Speaker Name (or AirPlay Name) will appear in the iTunes remote speaker list on a desktop computer and in the AirPlay list in iOS.

You can set a password to limit use of this speaker set to people who have the password. The verify field requires you to enter the password a second time to make sure you didn't mistype it. Click Update to apply changes.

Play Music with iTunes

Near the lower right corner of iTunes, look for the AirPlay icon. Click this icon, and you can choose a device to use (**Figure 65**) for audio or video output. An icon next to each device name shows whether the device can play video or just audio (the lock in the audio icon indicates that a password is required).

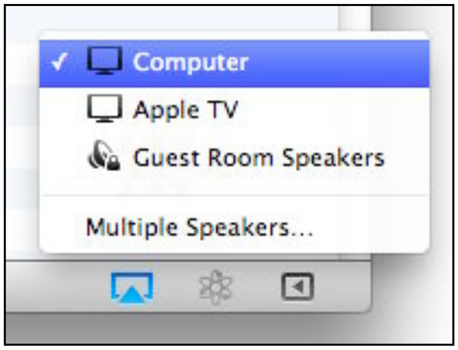
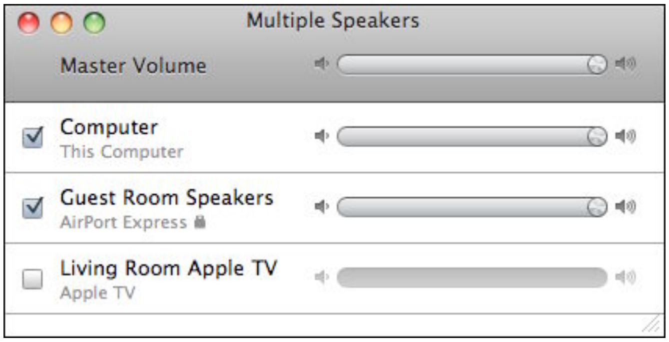


Figure 65: The AirPlay pop-up menu shows all available devices on the network.

Choose Multiple Speakers to see a list of all AirPlay devices that are available on the network (**Figure 66**). Check the box next to the speakers or devices you wish to use. You can use the Master Volume settings to set the overall output volume to all devices, and balance each of them with associated with sliders.



Multiple Speakers

Master Volume

☑ Computer
This Computer

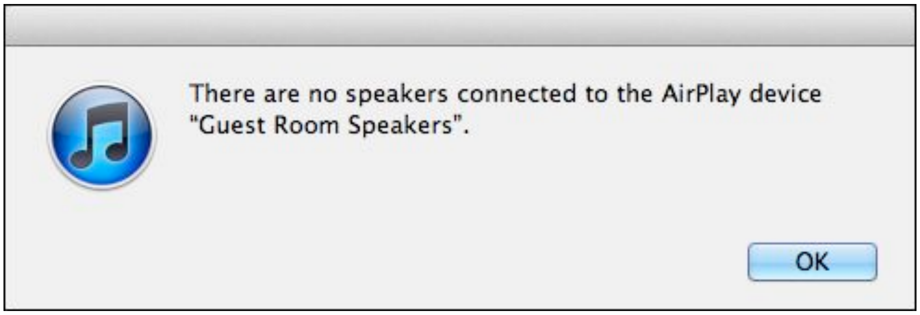
☑ Guest Room Speakers
AirPort Express

□ Living Room Apple TV
Apple TV

Figure 66: Choose the speakers and volume levels from the Multiple Speakers list.

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

- **No speakers connected:** If you select an AirPort Express to which no speakers are connected, iTunes will let you know (**Figure 67**). The AirPort senses whether there's a plug in place.



There are no speakers connected to the AirPlay device "Guest Room Speakers".

Figure 67: You can't play music if there's nothing plugged in!

- **Two people playing music at once:** If you try to play music through an AirPort Express or other device that someone else is actively playing music through, iTunes notifies you when you press Play (**Figure 68**). 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 device.

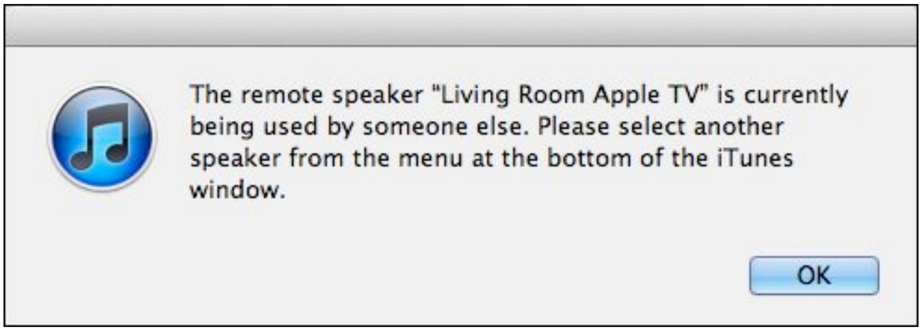

The remote speaker "Living Room Apple TV" is currently being used by someone else. Please select another speaker from the menu at the bottom of the iTunes window.

Figure 68: Only one source can control a set of "remote speakers," whether an Apple TV, powered speakers, or an 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.

Use the Remote App to Control Music

Apple's free Remote app runs on an iPad, iPhone or iPod touch. It can connect over a local network to iTunes running under Mac OS X or Windows. If iTunes is set to output audio via an AirPort Express, then Remote and its volume control can effectively handle whatever's coming out of your AirPort Express audio port.

Tip: A few models of remote speakers can control iTunes remotely when connected via an AirPort Express or as part of a Wi-Fi network. If you care about this behavior, you can check or uncheck Allow iTunes Control from Remote Speakers in the iTunes Devices preference pane.

Play Music in iOS

If you are running iOS 4.2 or later, you can play music from any app to an AirPlay device, including an AirPort Extreme. From any program that offers audio output, tap the AirPlay button and choose the AirPort Express as the destination.

If an AirPlay device doesn't appear when you think it should, try switching into Airplane Mode on the iOS device briefly, and if that doesn't help, try restarting the AirPlay device.

Share with Airfoil

Rogue Amoeba's Airfoil software (http://rogueamoeba.com/airfoil/; $25, downloadable demo version) for Mac OS X and Windows is a tour de force for streaming audio and video among different computers, handhelds, and devices. A free, separate app for Mac and Windows called Airfoil Speakers and an iOS app dubbed Airfoil Speakers Touch, may be used as the "receiver" to enable streaming to those devices.

iTunes by itself can stream music over AirPlay only to an AirPort Express, AirPlay-enabled speaker or other audio device, or Apple TV. iTunes can also stream video to an Apple TV. Airfoil extends your streaming options tremendously:

- Stream audio from iTunes on Mac or Windows to an iOS device using the Airfoil Speakers Touch app as a receiver.
- Stream audio from any program on a Mac or Windows system to any AirPlay device (like an AirPort Express), to another computer, or to an iOS device.
- Airfoil Speakers on a Mac and Airfoil Speakers Touch (version 3) can appear as an AirPlay destination to an iOS device with no special software installed on the iOS device.

The advantage here is that you're not limited to iTunes or an iOS device, nor to playing audio only via AirPlay-enabled hardware.

Tip: Airfoil can also play many kinds of Web video on a remote system, while playing the audio locally or elsewhere and keeping it in sync.

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 69**).

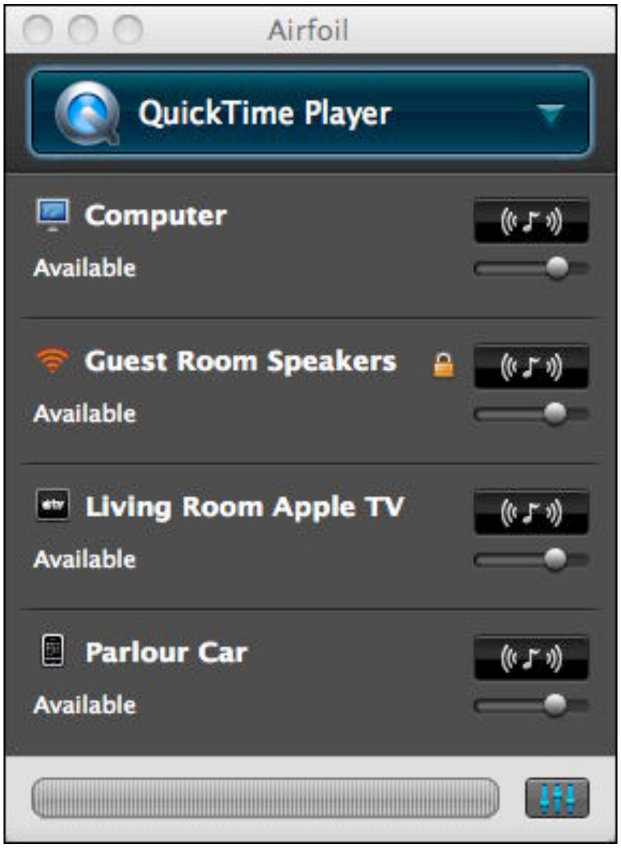


Figure 69: Airfoil showing the audio outputs available on my local network. From top to bottom, that's the computer on which Airfoil is running, an AirPort Express (locked with a password), an Apple TV, and my iPhone running Airfoil Speakers Touch.

2. Click the speaker icon to the right of the AirPort Express; in this example, it's Guest Room Speakers.
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.

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 70**). This mode, called *ProxySTA* by Apple but not mentioned by that name in Apple's documentation, is handy for using the Express in circumstances where you can't control how the network works.

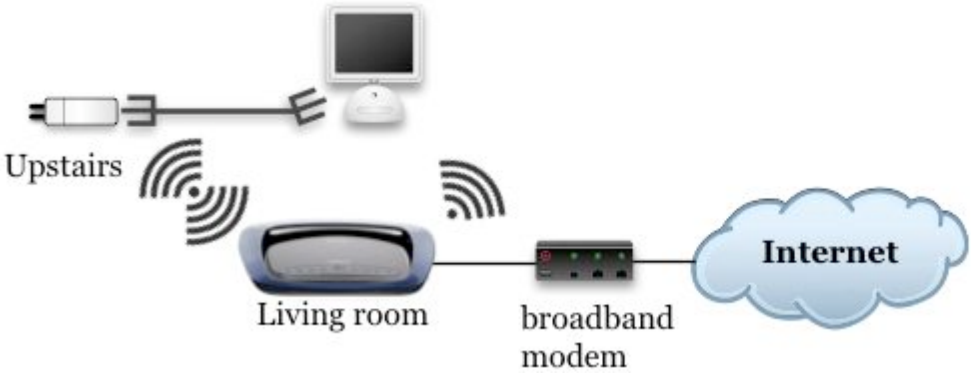


Figure 70: An AirPort Express (located upstairs here) can connect to any Wi-Fi network (such as the one from the living room shown here), and then share that network via its Ethernet port.

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.*

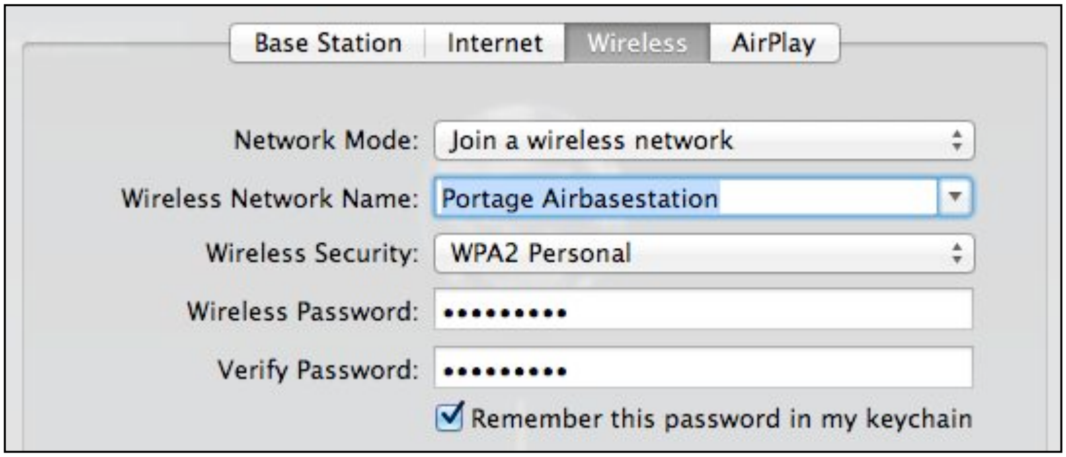
With ProxySTA, Ethernet clients—computers connected directly or multiple computers connected via an Ethernet switch—must obtain a DHCP address through a passthrough connection on the network that the Express has joined.

To use ProxySTA mode, follow these steps:

1. On your Mac, launch AirPort Utility , select the Express, and click Edit.

2. Click the Wireless button.

3. From the Network Mode pop-up menu, choose Join a Wireless Network (**Figure 71**).



Network Mode: Join a wireless network

Wireless Network Name: Portage Airbasestation

Wireless Security: WPA2 Personal

Wireless Password: •••••••••

Verify Password: •••••••••

☑ Remember this password in my keychain

Figure 71: Choose a network and enter its password, if any.

4. Choose the network from the Wireless 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 and chosen to remember on this computer.)

5. Click Update.

Now your Express 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 was once described as reaching “only” about 150 feet, which is a rough estimate of the radius of older B and G devices; with 802.11n, the distance is sometimes cited longer, or just as “farther” because it’s impossible to characterize with any precision how Wi-Fi signals will pass through any arbitrary house, office, café, airport, or store. Also, range measured as a linear dimension misstates the problem of *volume*, the three-dimensional space to fill.

But you can extend the covered volume by adding more base stations with overlapping signals. As a Wi-Fi adapter in a laptop or a handheld device moves across overlapping regions, it can automatically switch base stations while maintaining a network connection.

Know the Basics

When you extend a network, the additional base stations tend to be dumb; that is, they don’t assign addresses or handle other features you think of as belonging to a base station. 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 often called *access points* to distinguish them from gateways.

Because dumb base stations (access points) just pass traffic through, an adapter retains the same IP address as it switches from one base station to another, thus maintaining its 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 in comparison to 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.

Spectrum Differences

Simultaneous dual-band base stations complicate planning a network because the two spectrum bands have different coverage areas. In **Figure 72** you can see a coarse look at the how the 5 GHz and 2.4 GHz ranges compare.

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.

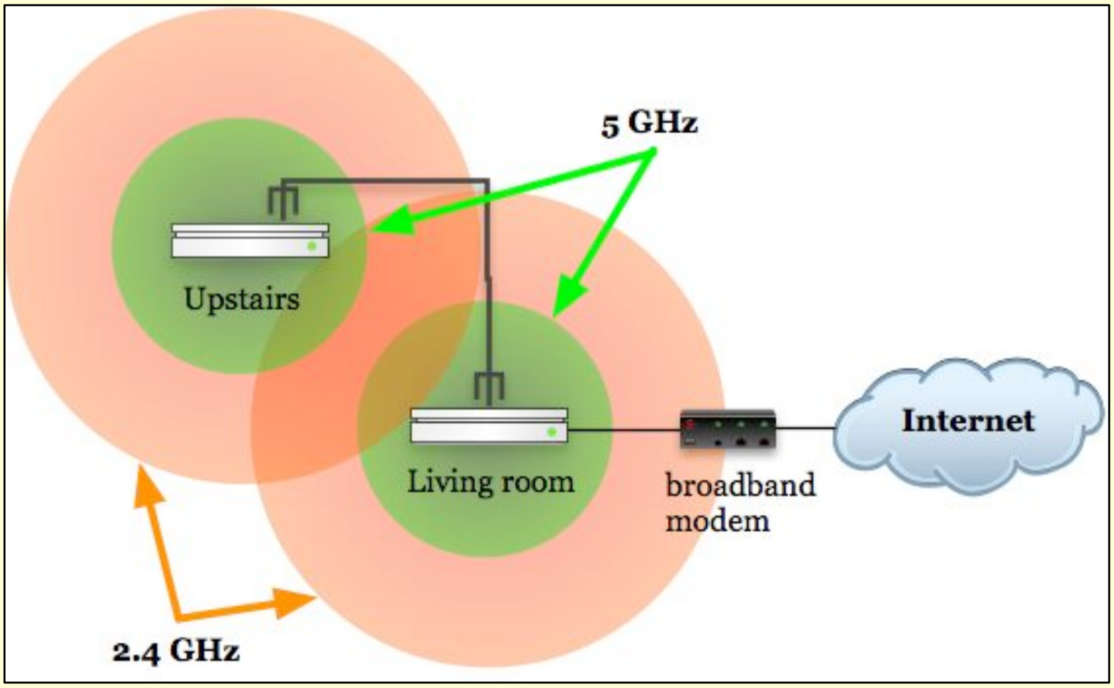


Figure 72: *You can overlap just one band and still gain seamless coverage.*

What about ProxySTA?

The ProxySTA mode of extending an existing Wi-Fi network with an Express is another method, but it has its limits: it works only with an 802.11n 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.

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 73**). 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.

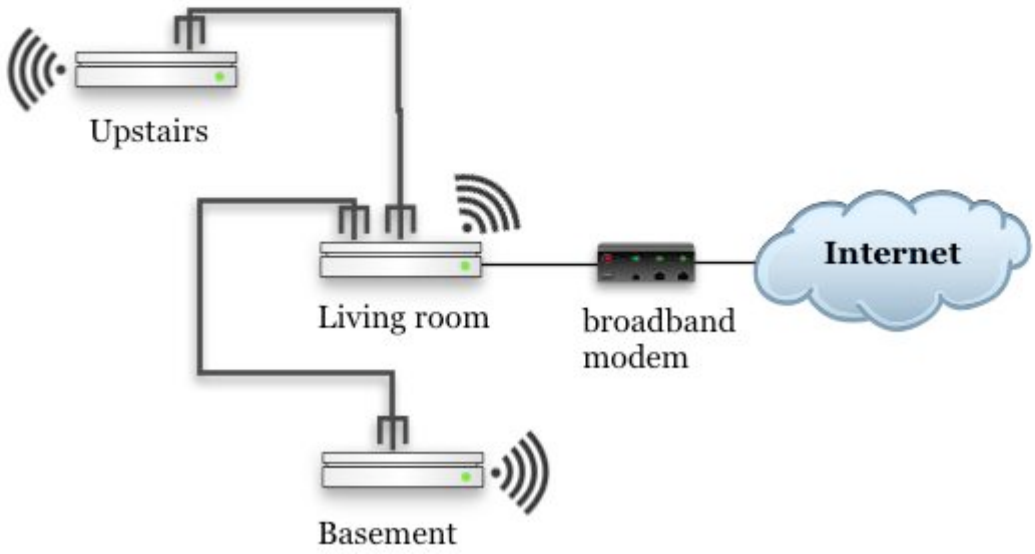


Figure 73: A common Ethernet backbone connects one base station in the living room, another upstairs, and a third in the basement.

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.

In the United States, if you're not getting the range that you want—especially in the 5 GHz band—follow the steps in Pick Compatibility and Set a Channel. As discussed in Channels, you want to choose (in the United States) 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

AirPort Utility automatically configures base stations as discussed in Extend a Network via Ethernet or Wi-Fi. However, if you have an existing base station that you want to reset to use as a wired extension of a network, you can follow these steps:

> **Note:** You can alternatively reset a base station to its factory defaults and use AirPort Utility to add it to a network. See How to Return to the Factory Defaults.

1. On your Mac, launch AirPort Utility, select the additional base station that you want to configure, and click Edit.

2. In the Internet view, choose DHCP from the Connect Using pop-up menu.

3. In the Wireless view, select Create a Wireless Network from the Network Mode pop-up menu. Enter the same wireless network name as the main base station, and choose the same Wi-Fi security option and enter the same passwords.

4. In the Network view, choose Off (Bridge Mode) from the Router Mode pop-up menu.

5. In the Wireless view again, click the Wireless Options button. 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 Set a Channel for specific directions, and choose in this manner:

   - For the 2.4 GHz band (B, G, or N) in the United States, 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. Click Save.

   - In the 5 GHz band (A or N) in the United States, none of the channels 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. Click Save.

Tip: As noted earlier in this chapter, 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. Click Update to restart your base station with the new settings.
7. Plug your additional access point into your main base station via Ethernet, connecting the cable from the WAN port on the additional access point either to a LAN port or to an Ethernet switch connected to a LAN port on the main base station.

Extend with HomePlug

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 500 Mbps—that's a raw rate, not the actual throughput, however.

With powerline networking, you typically use Ethernet wall plugs. Connect a computer or Ethernet switch to 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. Powerline network adapters must be plugged into wall sockets, not power strips, and they're often quite big wall warts. All the adapters must be connected to the same circuit back at your circuit breaker, or on the same power phase, which is a complicated and tricky matter to sort out. Across distant rooms in a house, it might work poorly or perfectly; you need to install equipment to find out. (Make sure what you buy is returnable.)

HomePlug gear costs from $30 for each adapter for the slowest 85 Mbps HomePlug 1.0 Turbo standard up to $80 for each 500 Mbps adapter. You can buy a "kit" with two or more adapters, one of which might also have a built-in Ethernet switch. I recommend purchasing paired or multiple adapters from the same firm. Despite promises of compatibility, there are many different HomePlug flavors on the market, including some newer, faster, proprietary versions.

To extend a wireless network, place your access points in appropriate locations, configure them as described above for an Ethernet network extension, and then plug them into powerline Ethernet bridges.

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's first pass at WDS was a *static* version, in which you had to enter the MAC addresses for every base station you wanted to connect, and reconfigure for minor changes. That was revised when 802.11n models were introduced in 2007 to a *dynamic* flavor that reconfigures itself automatically. It can sometimes work better, sometimes worse, than the static method.

Static Method Is Gone

The static method remained available as a hidden option even in AirPort Utility 5.x, but was removed in AirPort Utility 6.0 and never appeared in the iOS version.

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

How It Works

WDS works much like plugging an Ethernet hub into an Ethernet switch. An Ethernet hub interconnects devices to each other as a single segment, just like wireless clients connecting to a wireless base station. An Ethernet switch, by contrast, isolates each port as a separate segment. A computer connected to a hub connected to a switch's port can reach computers on other ports' hubs because the switch has information about which computers (by MAC address) are on other segments; this info allows the switch to transfer data across segments.

Likewise, WDS allows access points to exchange information about where computers and other devices are located on a physical network. One access point can then route data to another or to a series of other access points to reach the destination computer (**Figure 74**).

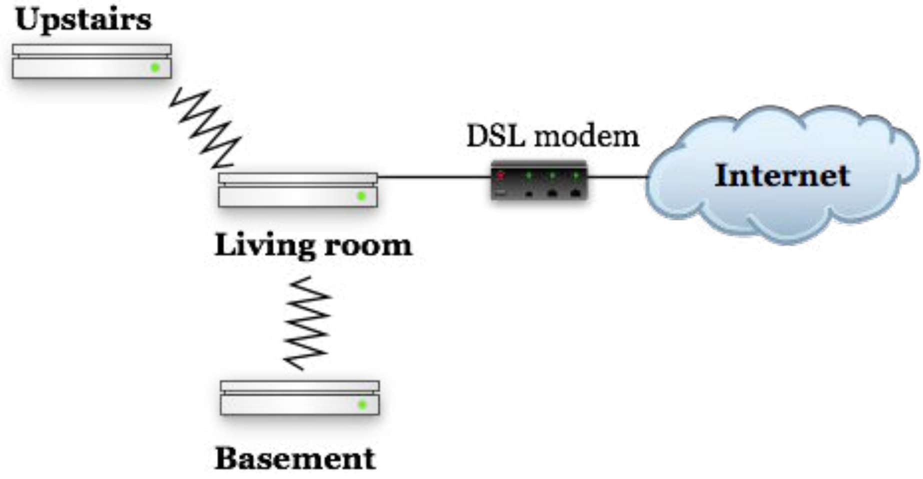


Figure 74: Wirelessly connected base station need to be placed only within Wi-Fi range to spread service around a house or office.

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 if one base station will be able to 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 a WDS connection will work.

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."

This problem is especially bad if you have an 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 while that client is chattering away.

But with an effective network throughput of 100–300 Mbps on a simultaneous dual-band 802.11n network, splitting that into pieces still provides plenty of bandwidth.

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 consider this issue, 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.

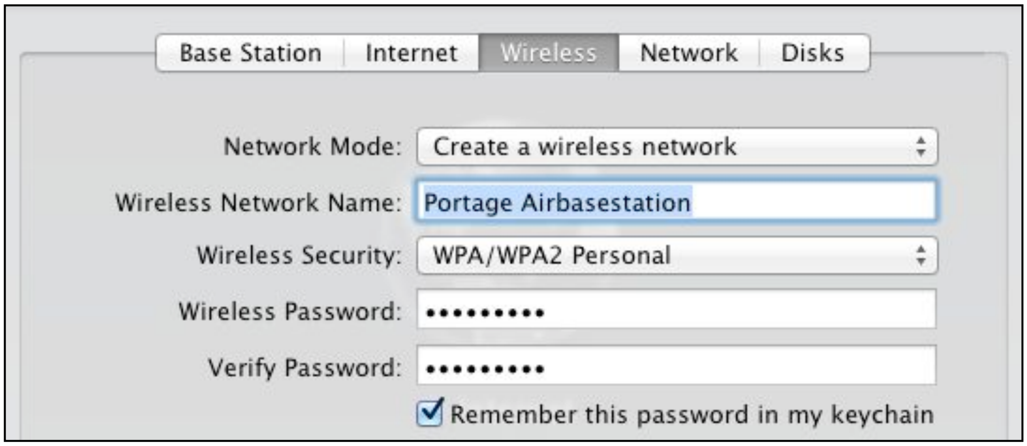
Distribute Wirelessly

AirPort Utility automatically configures new or reset base stations to join existing networks, and that's true for both Ethernet and Wi-Fi. You can follow the steps in Extend a Network via Ethernet or Wi-Fi for an unconfigured base station. However, you can reset a configured base station as a main base station or an extension. The following instructions provide the details.

Configure the main base station:

1. In AirPort Utility on your Mac, select your main base station and click Edit; then in the top of the window, click Wireless.

2. In the Wireless view, from the Network Mode pop-up menu, choose Create a Wireless Network (**Figure 75**).



Network Mode: Create a wireless network

Wireless Network Name: Portage Airbasestation

Wireless Security: WPA/WPA2 Personal

Wireless Password: •••••••••

Verify Password: •••••••••

☑ Remember this password in my keychain

Figure 75: Set up a main base station by letting it create a network and allow its extension.

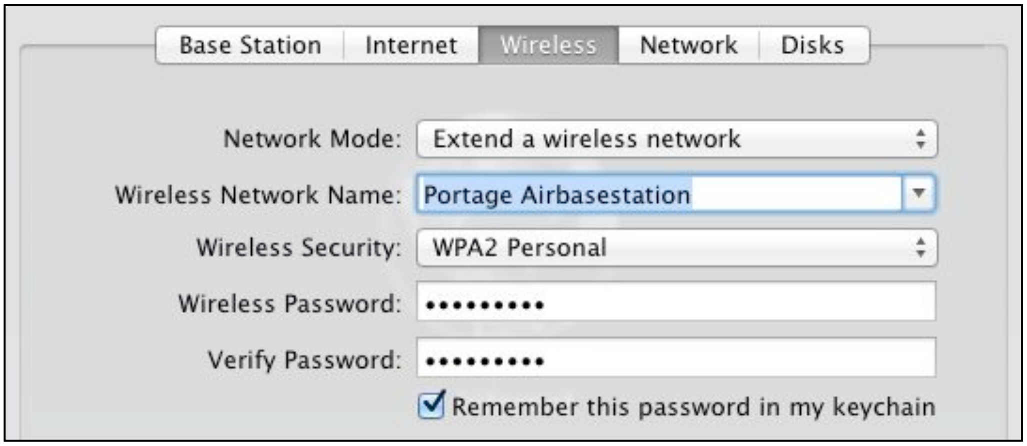
3. Set other base station options, such as wireless security.

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

Configure additional base stations:

1. In AirPort Utility on your Mac, select the appropriate base station and click Edit; then in the top of the window, click Wireless.

2. In the Wireless view, choose Extend a Wireless Network from the Network Mode pop-up menu (**Figure 76**).



Network Mode: Extend a wireless network

Wireless Network Name: Portage Airbasestation

Wireless Security: WPA2 Personal

Wireless Password: •••••••••

Verify Password: •••••••••

☑ Remember this password in my keychain

Figure 76: Other base stations connect 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. Set your Wireless Security choice and Wireless Password to be identical with your main base station.
5. Click Update, and you should be prompted after the base station restarts for the base station password of the main unit. (If the password is the same for the main and additional base station, you may not be prompted.)

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.

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 an iCloud account and Back to My Mac.

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 just ahead in this chapter.

- **Punch through from certain programs:** A protocol from Apple 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 this 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:** If you have an Apple ID account associated with iCloud, you can access your base station remotely via AirPort Utility from a Mac running 10.7 Lion or later. Once you've accessed it, you can reconfigure it or mount any internal (Time Capsule) or USB-attached disks. I provide directions in Access a Base Station via iCloud.

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 slightly ahead.)

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.

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.*

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.

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 77**). In the figure, I show the example of operating a Web server and playing Half Life behind a NAT gateway.

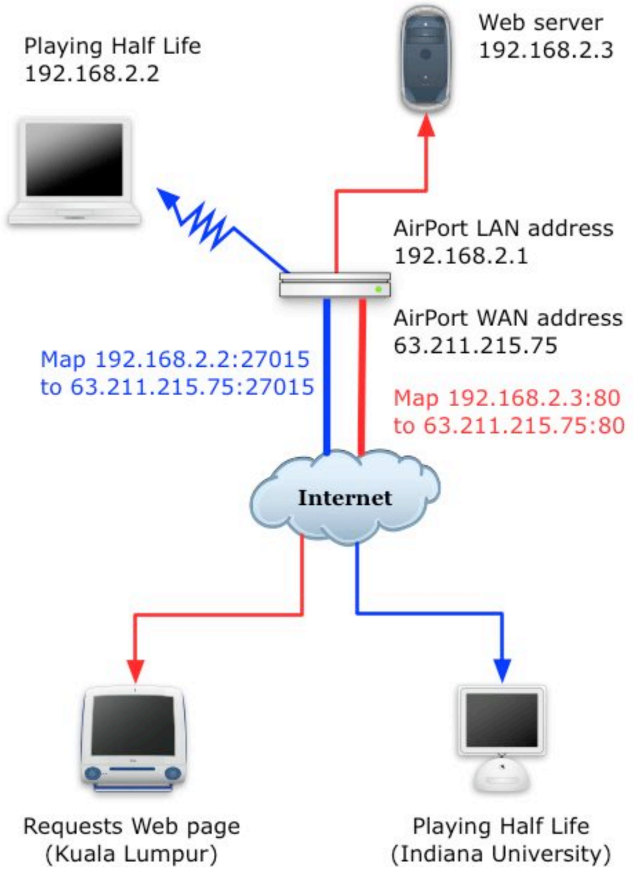


Figure 77: One user on a laptop is playing Half Life over the Internet; another computer on the network is running a Web server. When a user in Kuala Lumpur requests a Web page, the gateway maps the incoming request on port 80, the standard port for Web servers, from its public address to the Web server's 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.

Using port mapping reliably has two parts: set a persistent private ("reserved") 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. In the topics ahead, I explain how to complete both of these tasks.

Set a Reserved Address

For each computer with which you want to use port mapping, you should create a DHCP reservation, which I describe in Reserved Addresses, earlier. As you work, I suggest that you create a text file or other 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.

Warning! *Port mapping works only on a base station that’s distributing addresses. One that’s set to bridging can’t (and doesn’t need to) handle port mapping. Instead, connect to the base station that’s feeding out addresses for the network.*

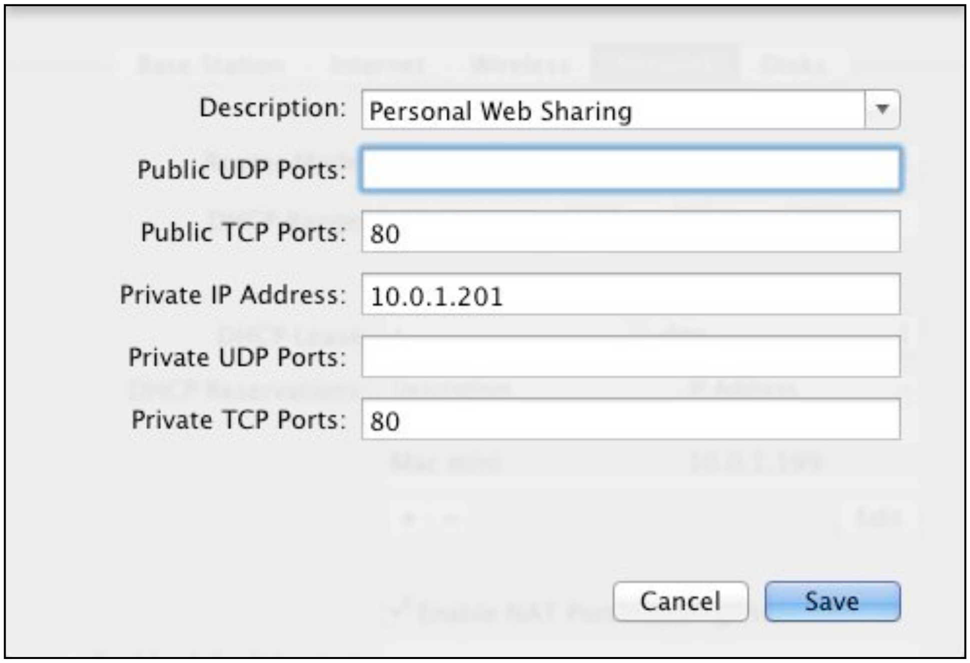
Set Base-Station-to-Computer Port Mapping for a Web Server

With a Web server running on a computer on the network, we need to set up the base station to pass traffic to the newly configured port:

1. Launch AirPort Utility on your Mac, select your base station, and click Edit.

2. Click the Network button.

3. Below the Port Mapping list, click the plus + button to bring up a port-mapping dialog (**Figure 78**).



Description: Personal Web Sharing

Public UDP Ports:

Public TCP Ports: 80

Private IP Address: 10.0.1.201

Private UDP Ports:

Private TCP Ports: 80

Figure 78: After you choose Personal Web Sharing from the Service pop-up menu, the correct ports are entered.

4. From the Description pop-up menu, choose Personal Web Sharing (really, this means any kind of Web server). To a provide a more descriptive name, click in the Description field and type a name. (For a more advanced network setup, described below, enter all of the necessary ports in this step.)
5. In the Private IP Address field, enter the reserved IP address. (You can edit only the last number of the IP address, as the first three numbers are set in DHCP configuration.)
6. Click Save.
7. 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 Web server 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 server 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 alternative-port servers. You should reserve using alternative-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.

Map Other Ports

We won't all run only Web servers on our private networks, however, so let's look at the options in the port-mapping dialog more closely (**Figure 78**, slightly earlier):

- **Description:** The pop-up menu part of this field contains the names of many common services, like FTP Access for file transfer and Apple Remote Desktop. Choosing an item from the pop-up menu fills the port fields with the correct values for that service.

  If what you need isn't in that menu, 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.

  If you like, you can click in the field to edit the preset name.

- **Public and Private UDP and TCP Ports:** 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 that 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 Ports 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 Ports field.

Punch Through with NAT-PMP

Apple has a protocol that helps 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.

To enable this feature, select your base station in AirPort Utility on your Mac, click Edit, click the Network button at the top of the window, and check the box labeled Enable NAT Port Mapping Protocol. Click Update. (It's already checked and available on new base stations or those reverted to factory settings.)

The downside to NAT-PMP is that each program must have built-in support 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 widespread use of NAT-PMP, because it's not found in routers outside Apple's.

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.

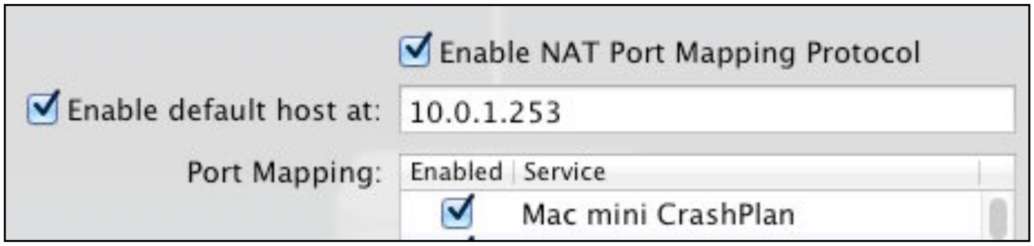
Apple calls this machine the *default host*; other gateway makers call it the *DMZ host*. You must share an IP address over DHCP and NAT for this option to be available.

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 on your Mac, select your base station, and click Edit.
2. Click the Network button.
3. Check the Enable Default Host At box, and enter the last number in the IP address for your default host (**Figure 79**).



☑ Enable NAT Port Mapping Protocol

☑ Enable default host at: 10.0.1.253

Port Mapping:

Enabled	Service
☑	Mac mini CrashPlan

Figure 79: 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 iCloud

There's one more way to gain remote access, but not to computers on your network. Using the Back to My Mac feature of iCloud, you can access your base station from a Mac running Lion or later. Back to My Mac uses iCloud 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 Lion or later system to see a base station in the Finder window's sidebar under Shared or in AirPort Utility.

This option lets you access a hard drive inside a Time Capsule or drives attached via USB to either an Extreme 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.

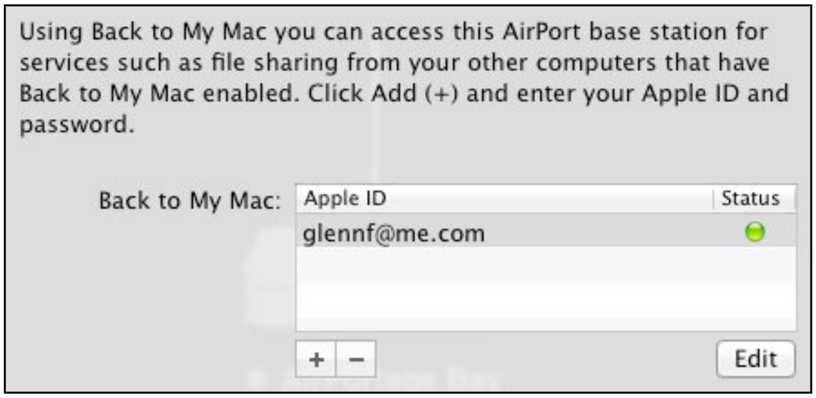
MobileMe and iCloud

Until June 30, 2012, MobileMe subscribers can continue to use Back to My Mac with Apple base stations, but you must stick with AirPort Utility 5. AirPort Utility 6 can't manage MobileMe services.

To enable Back to My Mac access for a base station:

1. Launch AirPort Utility on your Mac, edit the base station's configuration, and then click the Base Station button.

   In the Base Station view, you can enter one or more iCloud-affiliated Apple IDs (**Figure 80**).



Using Back to My Mac you can access this AirPort base station for services such as file sharing from your other computers that have Back to My Mac enabled. Click Add (+) and enter your Apple ID and password.

Back to My Mac:

Apple ID	Status
glennf@me.com	●

Figure 80: Entering an iCloud-associated Apple IDs allows you to use AirPort Utility 6 to configure the base station over the Internet.

2. Click the plus + button, enter your Apple ID username and password, and then click Sign In.

3. 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’s icon.

Now from a remote Lion or later system where you’re logged in to iCloud using one of the Apple IDs set for that base station, 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. The base station should appear in the graphical display. You can select and configure it just as you would any locally connected base station—even (as I did!) updating the firmware remotely.

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.

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 either a single printer or hard drive through its lone USB port. Add a USB hub, and you can connect one or more printers and drives in any combination. (To maximize reliability and performance, I recommend a Hi-Speed powered hub with external AC power.) The AirPort Express is designed to allow only a single USB printer to connect, and it cannot handle an attached hard drive nor a hub.

In this chapter, I explain how to configure a base station for an attached printer, and how to connect 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, Time Capsule). You should not need to reboot your base station for it to recognize the printer.
2. As needed, configure Macintosh computers to connect to the printer. Add a Shared Printer in Mac OS X explains how.
3. As needed, configure Windows machines to connect to the printer; Add a Shared Printer in Windows has instructions.

Note: Earlier versions of AirPort Utility let you view which printers were connected to a base station and modify the Bonjour name that is broadcast on the local network. That feature was removed, which is a shame.

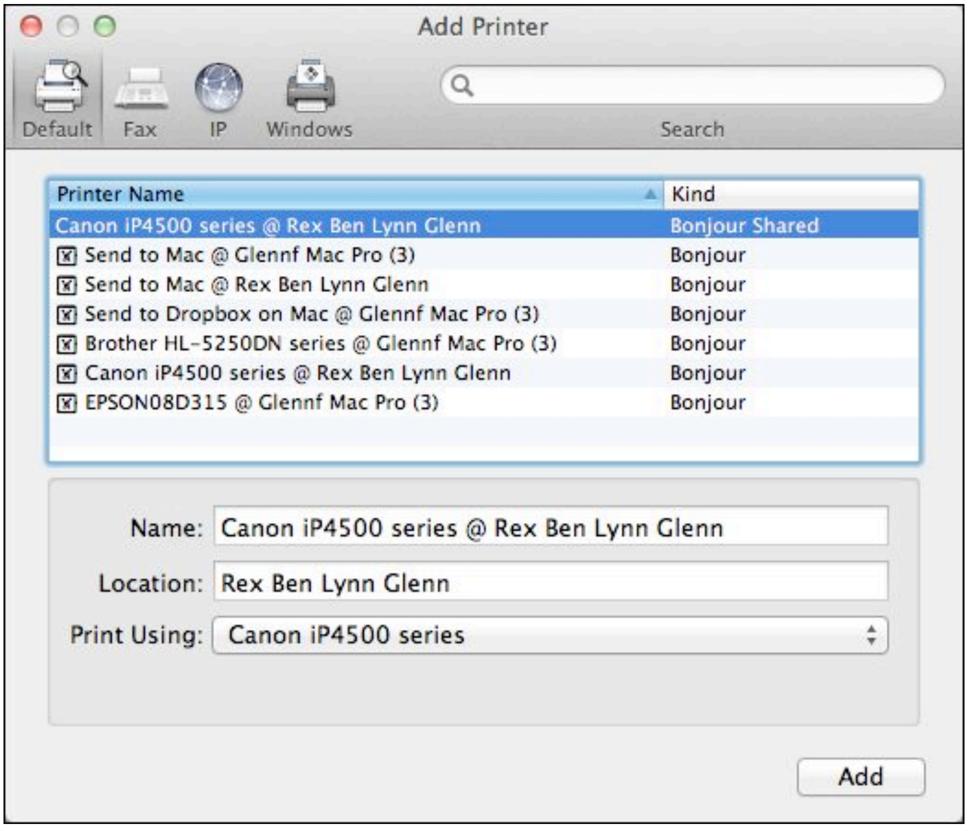
Add a Shared Printer in Mac OS X

To add a shared printer in Leopard and later, make sure the printer is on and not in standby-power mode, and then use these steps:

1. Open the Print & Scan system preference pane (called Print & Fax before Lion).

2. Click the plus + button near the bottom left of the window.

   This launches an Add Printer window. If needed, click the Default icon at the top of the window to see the printers available over Bonjour (**Figure 81**).



Printer Name	Kind
Canon iP4500 series @ Rex Ben Lynn Glenn	Bonjour Shared
☒ Send to Mac @ Glennf Mac Pro (3)	Bonjour
☒ Send to Mac @ Rex Ben Lynn Glenn	Bonjour
☒ Send to Dropbox on Mac @ Glennf Mac Pro (3)	Bonjour
☒ Brother HL-5250DN series @ Glennf Mac Pro (3)	Bonjour
☒ Canon iP4500 series @ Rex Ben Lynn Glenn	Bonjour
☒ EPSON08D315 @ Glennf Mac Pro (3)	Bonjour

Name: Canon iP4500 series @ Rex Ben Lynn Glenn

Location: Rex Ben Lynn Glenn

Print Using: Canon iP4500 series

Figure 81: 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.

3. 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.

4. Click Add. Your Mac may automatically download printer drivers.

The printer should now be available from the Print dialog in your various Mac applications. If not, consult Troubleshoot an Unavailable Shared USB Printer, later in this chapter.

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! (If Bonjour doesn't appeal, see the directions for Windows 7, next.)

Add a Shared Printer Using Bonjour

Apple lets you add Bonjour network resource discovery for Windows XP through Windows 7 with the free Bonjour Print Services for Windows package. You can download it from Apple at http://support.apple.com/kb/DL999.

Once you've installed the package, make sure your printer is turned on and not in standby-power mode 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 7

To add a shared USB printer in Windows 7, 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 Devices and Printers.
2. From the menu bar at the top, click Add a Printer.
3. Click Add a Network, Wireless, or Bluetooth Printer.
4. After a moment, the printer should appear in the list of available printers. Select it and click Next.

(If the printer doesn't appear, read the troubleshooting advice immediately after these steps.)

5. Windows now contacts the printer to obtain the printer's information, such as its name. If all is well, Windows will suggest you use a currently installed driver for the printer. Click Next.

6. If you want the printer to appear in Windows with a different name, enter that name. Click Next.

7. 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've configured everything correctly or try the troubleshooting suggestions just ahead.

Troubleshoot an Unavailable Shared USB Printer

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

- Make certain that the printer is powered up, not in standby-power mode (which sometimes prevents an initial connection), 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 graphical network display with a green dot next to it. If not, use Quick Troubleshooting Guide to discover why.

- Using AirPort Utility on your Mac, select the base station and choose Base Station > Restart. Click Continue. (In AirPort Utility for iOS, edit the base station and then tap Advanced > Restart Base Station.) Once the base station has restarted, 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 and the Time Capsule both add an interesting option to a 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.

Attached hard drives can be accessed over the Internet via AFP using Back to My Mac, too (see Access a Base Station via iCloud).

In this chapter, I cover a handful of procedures for using the Time Capsule and the Extreme to share disks:

- Read Prepare Your Drive, next, to find out about formatting and physically attaching drives.
- Work with Time Capsule 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 and Gain Access 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.*

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 must format attachable disks before you connect 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.)

You can connect a single drive to the USB port on the Extreme 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.

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

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:

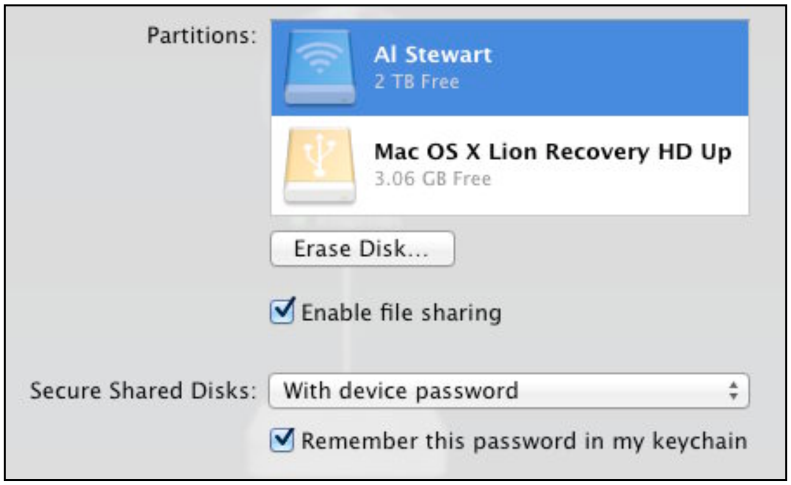
- **Hard disk:** A *hard disk* is a physical piece of hardware that contains data.
- **Partition:** A *partition* is a division of a disk's available storage into a separate logical compartment—part of the physical disk is written with certain kinds of data, and a disk-wide partition map is updated to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

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.*

View and Manage Connected Volumes

In AirPort Utility, select your base station, click Edit, and then click the Disks button. Each disk connected to the base station has its partitions noted in the Partitions list at the top (**Figure 82**). This list includes the name and the available space.



Partitions:

Al Stewart
2 TB Free

Mac OS X Lion Recovery HD Up
3.06 GB Free

☑ Enable file sharing

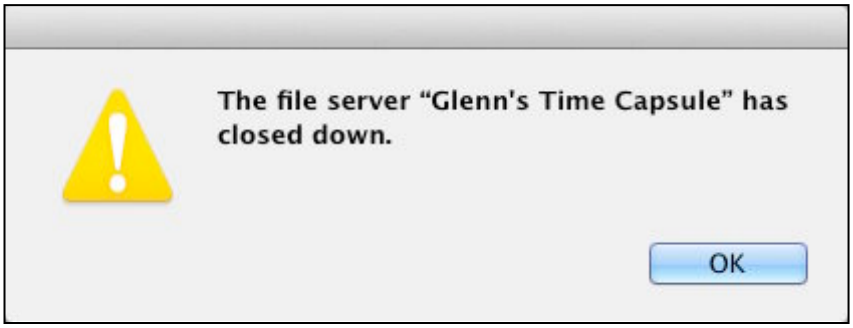
Secure Shared Disks: With device password

☑ Remember this password in my keychain

Figure 82: AirPort utility lists any disks’ partitions that are connected to a base station.

Tip: In AirPort Utility, you can rename a partition for a Time Capsule drive to give it a more descriptive name. Double click the name to make it editable.

If you click Update, choose Base Station > Restart, or unplug a base station, users connected to the base station as a file server will have their connection interrupted (**Figure 83**). Better to have you (and everyone else on the network) unmount the base station’s volumes first, if at all possible.



The file server “Glenn's Time Capsule” has closed down.

Figure 83: Mac OS X complains if you unplug or restart a base station with users connected to a shared disk.

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

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 explain how to Erase a Time Capsule 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

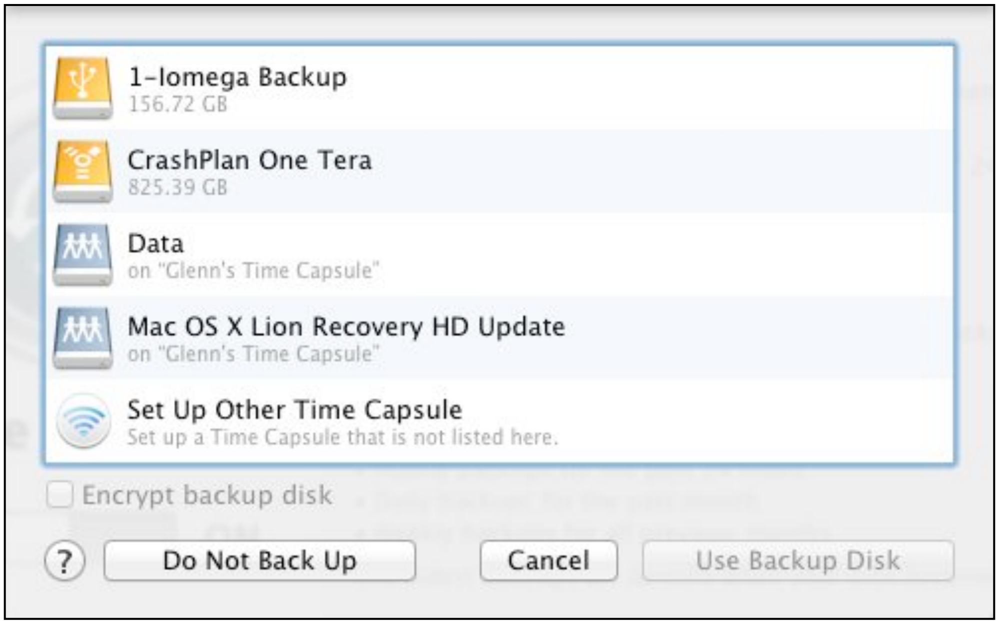
The Time Capsule’s very name indicates that it has something to do with the Time Machine backup feature. Any internal drive or external drive partition on a Time Capsule can be chosen as a Time Machine destination backup by any Mac running 10.5 Leopard or later on the same local network.

Warning! Apple promised that in Leopard, Time Machine would back up to Extreme-connected drives. But when Leopard shipped, Apple had removed the feature.

*The Time Capsule supports Time Machine backups to both its internal drive and any externally connected drives, and after an early Leopard update, that support extended to Extreme external drives. This was apparently an accident: Apple never documented the feature and doesn't officially support it, and the feature can be unreliable—backup images may become corrupted and drives may stop appearing as an option in the Time Machine drive selection dialog (**Figure 84**) after a few days or weeks goes by. Sadly, this situation has been in place for several years without Apple making a move to make it better or remove the option. I still advise not using an Extreme-connected drive for greatest reliability.*

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

1. Open the Time Machine System Preferences pane.
2. Click the Select Disk button.
3. In the dialog that appears, all locally available Time Capsule drives should be listed (**Figure 84**). (Only HFS+ formatted drives, including the Time Capsule internal drive, show up.)



1-Iomega Backup
156.72 GB

CrashPlan One Tera
825.39 GB

Data
on "Glenn's Time Capsule"

Mac OS X Lion Recovery HD Update
on "Glenn's Time Capsule"

Set Up Other Time Capsule
Set up a Time Capsule that is not listed here.

□ Encrypt backup disk

Figure 84: Time Machine shows available disks attached to your computer and over the network.

4. Select the disk and choose Use Backup Disk.

> ***Can't encrypt:*** *Encrypt Backup Disk is not an option for networked volumes, only locally connected drives.*

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. For the first back up, connect a Mac via Ethernet to a Time Capsule overnight.*

Disk Integrity

Every time that a Time Capsule powers up or restarts, it performs a quick integrity check of the internal drive to make sure it's working as expected. Minor errors are automatically fixed, but if the drive can't be repaired, the yellow light on the front of the Time Capsule flashes, and AirPort Utility launches on any computer with which you've configured the base station that can "hear" the Time Capsule over Bonjour.

There's little you can do with the internal drive once it's failed, however, except get a replacement if it's under warranty, or find a third-party firm that can swap 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:

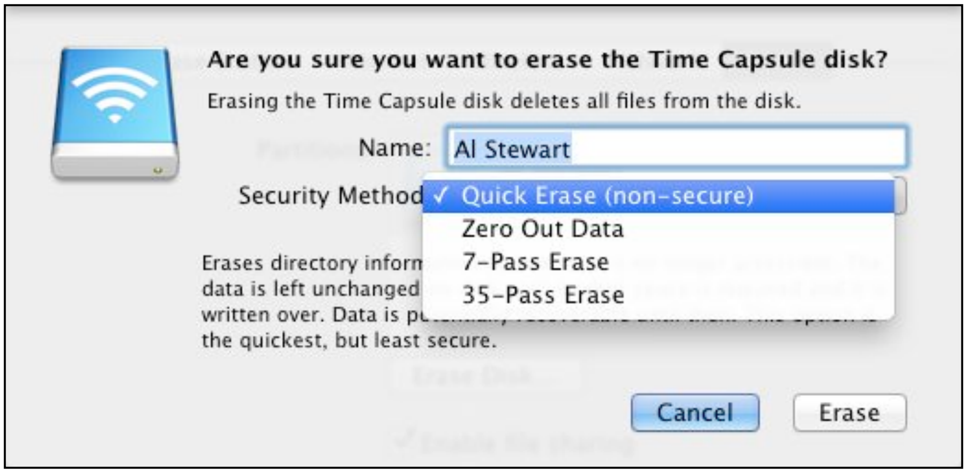
1. In AirPort Utility, select your Time Capsule, click Edit, and click the Disks button.

2. Select the internal hard drive, which appears with a blue icon.

3. Click the Erase Disk button below the Partitions list.

4. In the dialog that appears, optionally rename the sole partition on the drive and/or choose an erasure method. The Security Method 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 85**).

Warning! *Choosing 7 or 35 passes could take many, many, many hours to complete.*



Are you sure you want to erase the Time Capsule disk?

Erasing the Time Capsule disk deletes all files from the disk.

Name: Al Stewart

Security Method: ✓ Quick Erase (non-secure)

Erases directory inform
data is left unchanged
written over. Data is p
the quickest, but least secure.

Figure 85: You can go to rather extreme extremes to secure the erasure of your internal drive.

5. Click Erase.

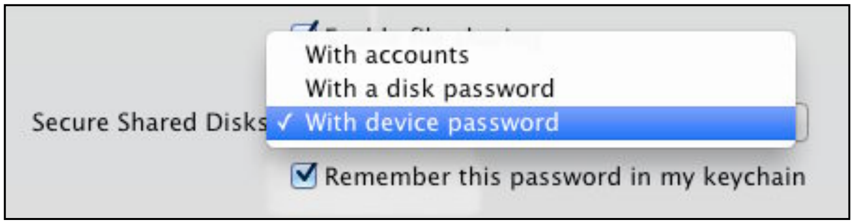
Warning! *While an erase operation is in process, the Time Capsule locks out Time Machine backups and file-server access to any volumes, internal or external.*

6. You're prompted again to make sure you really want to erase the drive. Click Continue 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 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.

AirPort Utility has three ways to grant access, found in the Disks view in the Secure Shared Disks pop-up menu (**Figure 86**).



Secure Shared Disks ✓ With device password

☑ Remember this password in my keychain

Figure 86: AirPort Utility offers three options for securing a shared disk by controlling the level of security.

The three ways to grant access are:

- **With accounts:** On partitions formatted with HFS+, you can set up individual usernames 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 list appears through which you can add, edit, and remove 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.)
- **With a disk password:** This sets a password that controls access to all disks; this password is distinct from the base-station password and network encryption 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 device password (default):** This self-explanatory option 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 who knows the disk-access password also changing the settings on a base station. (If you use the default setup, this password is also the same as the network encryption password for WPA or WPA2.)

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 and Write), read only (Read Only), or no access (Not Allowed).

Gain Access

File sharing with the Extreme and Time Capsule uses standard methods: AFP, commonly known as AppleShare, and Samba, Windows's default method. Users on your network can access base station file servers connected to an Extreme or Time Capsule via normal file-sharing options, such as selecting the server from a Finder window's sidebar in the Shared section.

With a base station or disk password, the contents of all partitions are available when a partition is mounted

With accounts, however, the options vary by partition type:

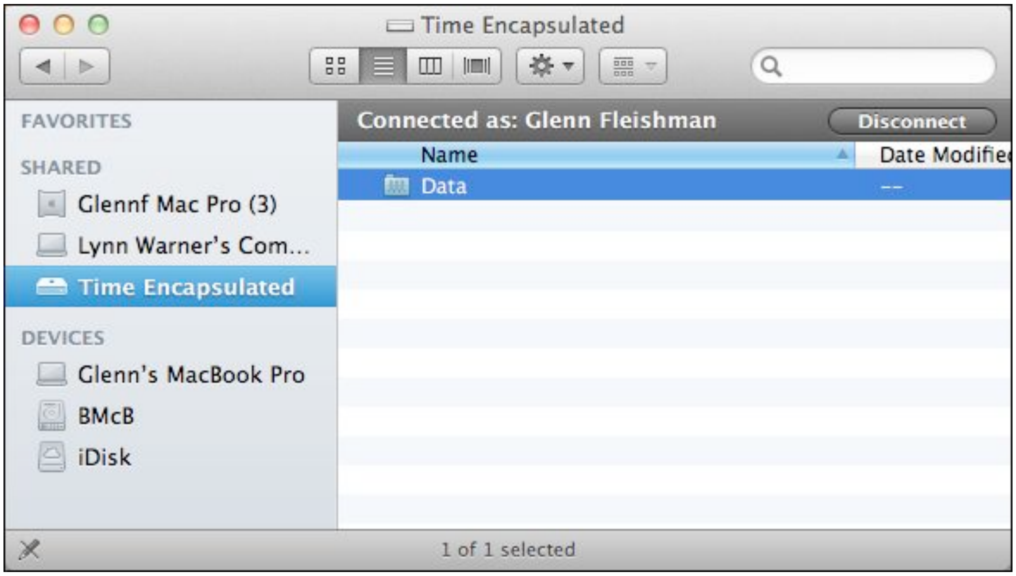
- With an HFS+-formatted partition:
    - A folder named with the account is created on only one partition, no matter how many HFS+ partitions are attached; users mount this folder as a volume having the account name.
    - A folder named Shared is also created on one partition, and users mount it as a volume named with the partition name.
    - Any other partitions are served as volumes named with the partition name.
- With a FAT 16/32-formatted partition:
    - A folder named Shared is served. Users mount it as a volume having the partition name.

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 Mac OS X

Mac OS X 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 87**). 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 iCloud from that Mac, you'll also see any available base station(s) in that list.

Note: This will look slightly different in Leopard and Snow Leopard, but mounting works the same.



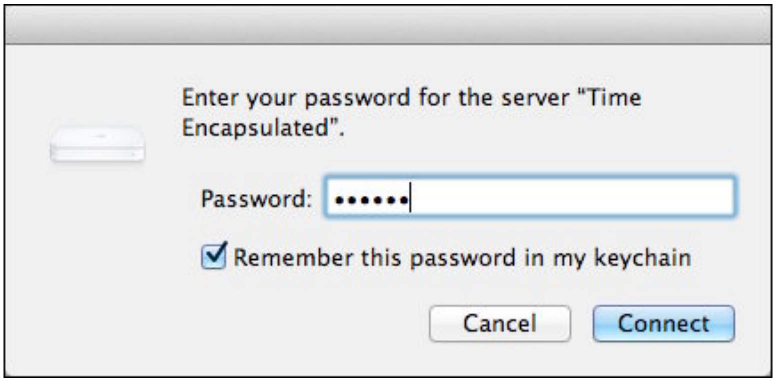
Connected as: Glenn Fleishman

1 of 1 selected

Figure 87: 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 username 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 Shared section of the sidebar.
2. Click the Connect As button in the upper right and enter your credentials. Mac OS X is clever enough that for Extreme and Time Capsule shared drives that use just a password for access—no user accounts—it prompts you just for that password (**Figure 88**).



Enter your password for the server "Time Encapsulated".

Password: ••••••

☑ Remember this password in my keychain

Figure 88: Mac OS X is smart enough to know that just a password is needed to connect to a base station's file-sharing service.

3. Double click a volume that's shown in the mounted server window to mount it on your system.

***Unmounting:** To unmount a network volume, select the volume on the Desktop and press Command-E, or choose File > Eject "volume name." Or, to unmount all volumes associated with a server, in a Finder window sidebar, click the Eject icon next to the server's name, or in the server's Finder window, click Disconnect (**Figure 87**, just a bit earlier).*

In Snow Leopard and later, a disk icon turns gray while Mac OS X is in the process 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 and later tell you which one.

Mount in Windows

With Windows 7, follow these steps:

1. Open the network browser by double-clicking Network on the Desktop.
2. The base station name should appear in the Network browser. Double-click the name, and a login prompt appears.
3. In the Name field:
   - If you don't have a user account because the base station is using a base-station or disk password, 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.

Unmounting: *To unmount a disk, find the volume under My Computers or on the desktop, right-click the volume, and select Disconnect.*

Share Files with AirDrop

Have you ever wanted to swap a file between a couple of your computers without setting up file sharing and mounting a volume? Or pass a file to a friend or colleague without joining a common Wi-Fi network, setting up ad-hoc networking, or emailing it?

AirDrop is the answer to that common task. Added in Lion, the feature lets you find and share files with other users near you, so long as their Macs are running Lion or later. It has a pile of provisos that I discuss below, but it's a remarkably nifty way—when all the right hardware is available—to hand files back and forth.

What Makes AirDrop Tick

AirDrop relies on a special feature in new Wi-Fi adapters that allows a network card to connect simultaneously to a Wi-Fi network and to other devices on a peer-to-peer basis. A Wi-Fi network is typically called an *infrastructure* network, as it provides a hub around which all network activity zooms. In contrast, a peer-to-peer network is known as a *personal area network (PAN)* network; it allows direct communication among devices without a central coordinating switch.

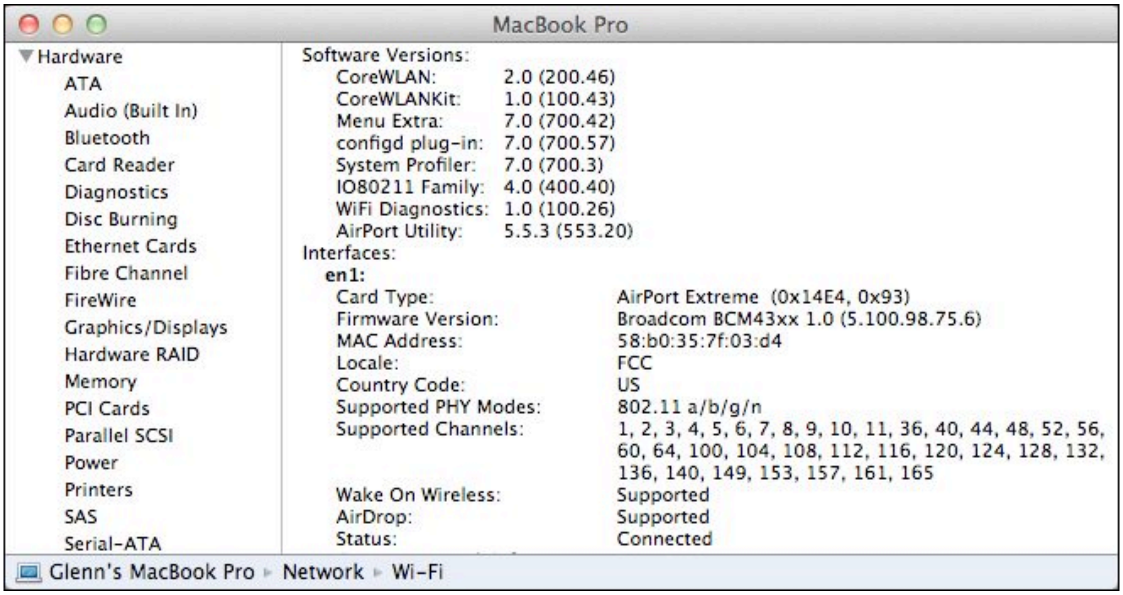
This sounds a lot like Ad Hoc Networking, doesn't it? With *ad hoc* or *computer-to-computer* networking, a set of computers can all connect to one another as peers. However, ad hoc networking has three drawbacks. First, it doesn't include robust security, and even the available security requires each party to type in an encryption key. Second, you can't maintain a connection to an Internet-connected base station network and use ad hoc networking at the same time. And, finally, you still have to establish a file-sharing connection on top of the ad hoc network.

AirDrop eliminates all that. Click a button in the Finder, and an AirDrop window opens showing all available peers in the vicinity. Drag a file or files or receive one or more, and it's done. However, you can use AirDrop only with other computers that are running Lion or later, and those computers must have a fairly recent vintage Wi-Fi chipset. Sadly, an Ethernet connection doesn't help, and iOS doesn't have any interaction with AirDrop.

Apple has posted a list of computers that qualify (https://support.apple.com/kb/HT4783):

- MacBook Pro (late-2008 or newer)
- MacBook Air (late-2010 or newer)
- MacBook (late-2008 or newer)
- iMac (early-2009 or newer)
- Mac mini (mid-2010 or newer)
- Mac Pro (early-2009 with AirPort Extreme card, or mid-2010)

You can also tell whether a given computer has the right circuits by using System Information (formerly called System Profiler): Hold down the Option key and choose Apple > System Information. At the left, under Network, click on the Wi-Fi label. In the main view, you'll see AirDrop as an item (**Figure 89**). If it says Supported, you're good to go; otherwise, that machine doesn't qualify, and I'm sorry to say there's nothing anyone can do about it.



```
Software Versions:
   CoreWLAN:           2.0 (200.46)
   CoreWLANKit:        1.0 (100.43)
   Menu Extra:         7.0 (700.42)
   configd plug-in:    7.0 (700.57)
   System Profiler:    7.0 (700.3)
   IO80211 Family:     4.0 (400.40)
   WiFi Diagnostics:   1.0 (100.26)
   AirPort Utility:    5.5.3 (553.20)
Interfaces:
  en1:
   Card Type:                 AirPort Extreme  (0x14E4, 0x93)
   Firmware Version:          Broadcom BCM43xx 1.0 (5.100.98.75.6)
   MAC Address:               58:b0:35:7f:03:d4
   Locale:                    FCC
   Country Code:              US
   Supported PHY Modes:       802.11 a/b/g/n
   Supported Channels:        1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 36, 40, 44, 48, 52, 56,
                              60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132,
                              136, 140, 149, 153, 157, 161, 165
   Wake On Wireless:          Supported
   AirDrop:                   Supported
   Status:                    Connected
```

Figure 89: The AirDrop capability is shown in System Information, under the Network category in Wi-Fi. It appears in this screenshot in the right pane, second item from the bottom.

Tip: Certain Macs that Apple says cannot use AirDrop, and for which Lion and later doesn't enable AirDrop, can be activated with a Terminal command-line change. See my article at *Macworld* for the steps: https://www.macworld.com/article/1162407/.

Transfer Files with AirDrop

Transferring files with AirDrop is a breeze. In the Finder, in any open window, the AirDrop item appears in the top left of the sidebar under Favorites (**Figure 90**). This item appears only if your system is capable of using AirDrop as noted just above, but if you don't see it, you may have to enable it—choose Finder > Preferences, and then select the AirDrop checkbox.

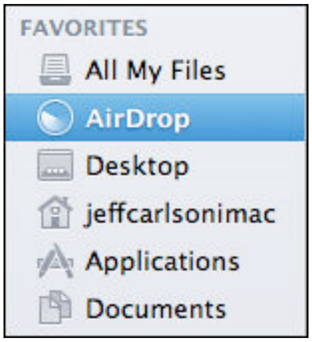
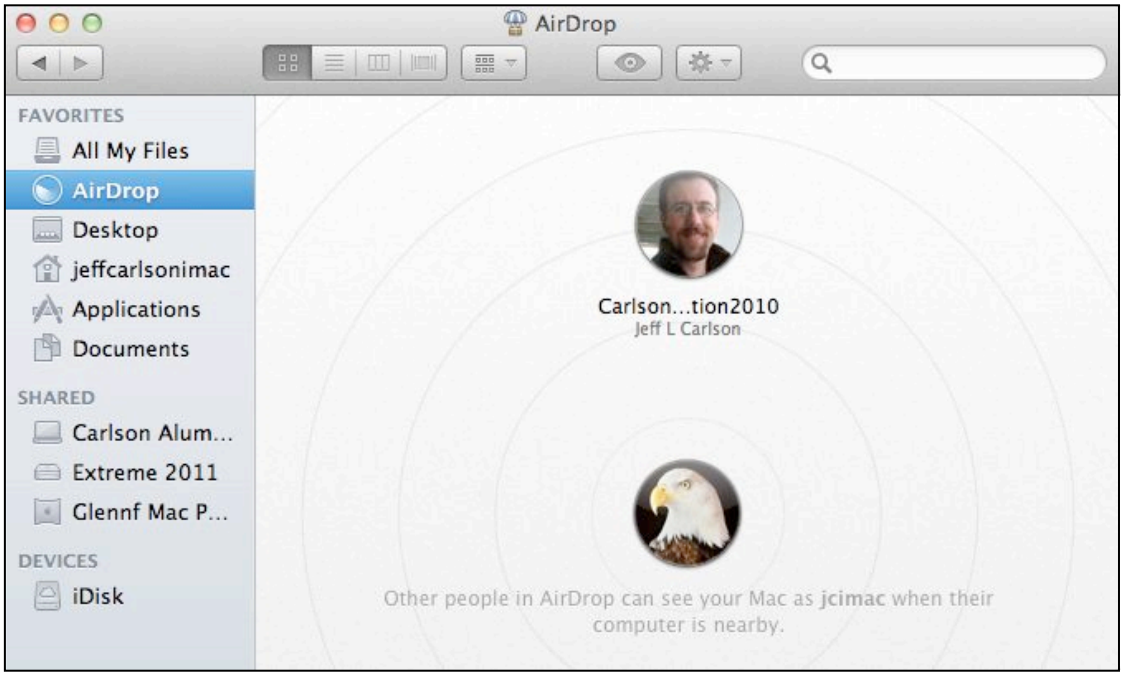


Figure 90: Click AirDrop to trigger the AirDrop mode.

Click AirDrop, and your Wi-Fi adapter begins broadcasting its availability to nearby machines, while the Finder window displays the AirDrop interface (**Figure 91**).



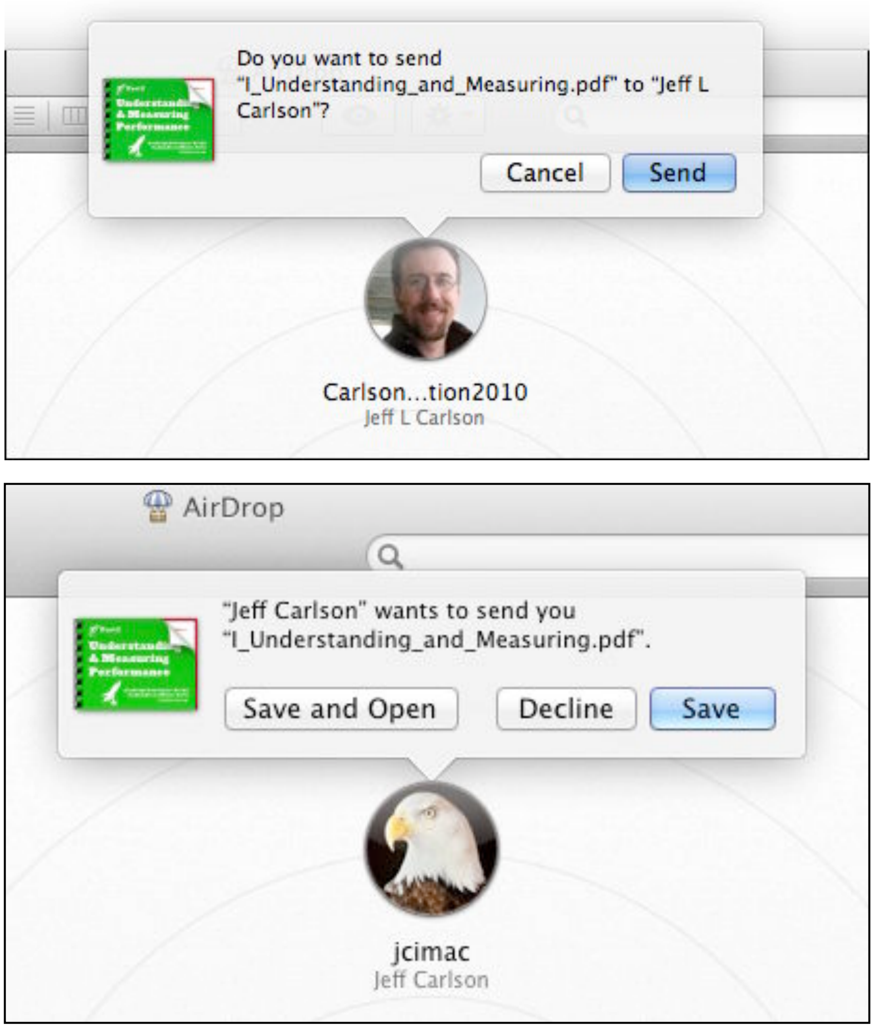
Other people in AirDrop can see your Mac as **jcimac** when their computer is nearby.

Figure 91: The strange AirDrop interface.

Note: The AirDrop feature is rather homely and seems to violate many long-time Apple interface guidelines. It's a weird item that doesn't resemble anything else in Mac OS X.

Your computer appears at the bottom, and Apple helpfully notes how other AirDrop users will see your name listed. Your custom Mac OS X account icon also appears.

To copy files to another user, you drag them in the Finder from any location onto that other user's icon at the top of your AirDrop window. You're asked by Lion to confirm the copy (**Figure 92**, top), and the recipient is asked whether they want to receive the incoming files (**Figure 92**, bottom).

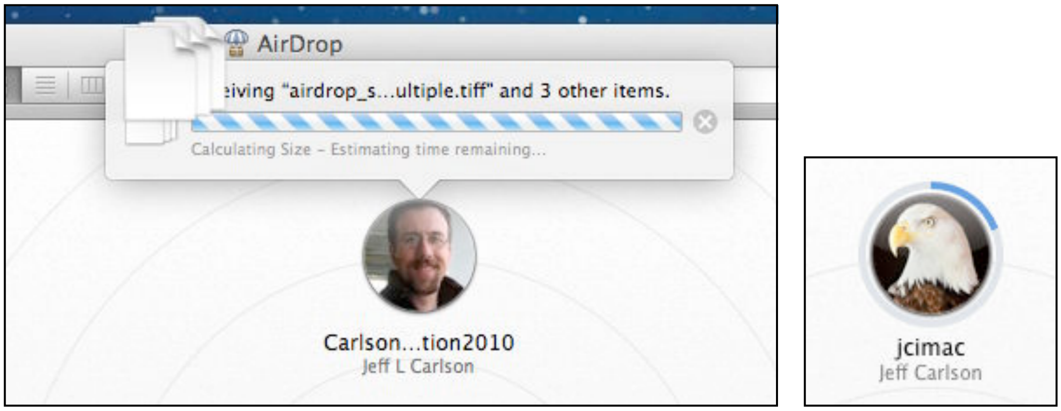


Do you want to send "I_Understanding_and_Measuring.pdf" to "Jeff L Carlson"?

"Jeff Carlson" wants to send you "I_Understanding_and_Measuring.pdf".

Figure 92: You're asked to confirm both sending files (top) and receiving them (bottom).

Once the recipient agrees to receive the files—either to Save or Save and Open them—their computer first shows a progress bar as the size of the files to be transferred is calculated, and then an empty circular border around the sender's icon is filled in with blue to indicate progress (**Figure 93**). I find it rather bizarre, although it resembles the circle fill-in that happens in iChat as files transfer.



eiving "airdrop_s...ultiple.tiff" and 3 other items.

Calculating Size – Estimating time remaining...

Figure 93: File size is first calculated (left), and then progress is shown as a circle being filled in around the sender's icon (right).

AirDrop Is Closely Related to Wi-Fi Direct

Wi-Fi Direct is a technology developed by the Wi-Fi Alliance to allow any device—computer, mobile, printer, or other gizmo—to advertise what kinds of service it offers over a peer-to-peer network. Wi-Fi Direct hasn't yet made inroads because it's not built into any operating systems except Android 4 (Ice Cream Sandwich); it's promised for Windows 8, as well.

AirDrop isn't compatible with Wi-Fi Direct, but it relies on the same hardware features, and is a good glimpse of what Wi-Fi Direct will look like for things like printing, scanning, and even gaming.

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.

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. In practice, this doesn't work.

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 Wi-Fi 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 click Edit.
2. Click the Wireless button and then the Wireless Options button.
3. Select the Create Hidden Network checkbox.
4. Click Done, and then click Update to restart the base station.

Timed Access Control

Apple used to offer a way to limit access to devices by their MAC address, a unique identifier set for every network adapter. While this feature was removed, AirPort Utility does retain Timed Access Control (in the Network view) to limit devices to access the network on specific days of the week during specific hour ranges. You set access for a device by its MAC address (see Appendix E: What and Where Is a MAC Address?).

The feature can be useful if you're trying to keep your kids (or spouse?) from using the Internet except during certain hours, but I find that it is too fussy to recommend, and the same settings must be re-entered on every base station on a network. It also doesn't restrict plugging in via Ethernet.

Use Built-in Encryption

For a real defense, you must use password-protected encryption. 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. The currently useful options are compared in **Table 3**. I look at each option in more detail next.

Table 3: Comparing Wi-Fi Security Methods

Name	What Can Use It?	Difficulties
TKIP (WPA Personal)	Works with original AirPort Card (10.3 or later), and with many early adapters with new firmware.	Requires slightly newer computers and operating systems. Doesn't work in 802.11n mode.
AES-CCMP (WPA2 Personal)	Works only with gear shipped starting in late 2002, including AirPort Extreme.	Older machines can't connect, including those with original AirPort Card.
WPA/WPA2 Enterprise	Supported in 2003 and later mobile and desktop operating systems.	Requires a back-end server to handle account management.

Wait, Where's WEP?!

Once upon a time, boys and girls, there was a big, bad weak encryption standards for Wi-Fi. Don't worry. It's dead. Mostly.

Wired Equivalent Privacy (WEP), part of the original 1999 802.11 specs, was demonstrated to be thoroughly crackable as early as 2003, the same year WPA was released; WPA2 followed a year later. However, WEP persisted because many older base stations and adapters couldn't be updated. Even so, it's long past time to move forward from WEP. A "WEP Transitional" mode is available (but hidden) in AirPort Utility. It isn't reliable enough for me to explain.

802.11n connections require WPA2, and Apple's base stations can use WPA (in WPA/WPA2 modes) to talk to older but updated 802.11b and 802.11g adapters.

You can use plain old WEP in one way: set your Radio Mode to 802.11b/g in 2.4 GHz and 802.11a in 5 GHz. That allows the older, bad method of connections, which I don't recommend. (See Set the Radio Mode for details.)

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 replaces the weaker WEP key with 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 10.3 Panther or later is required to use it.

***Warning!** The original AirPort Card (found in pre-2003 Macs) cannot access WPA2-protected networks.*

The Key to Keys

WPA2 is a more robust version of WPA, which replaced it. WPA supports just one new encryption method that's a repaired version of WEP, known as TKIP (Temporal Key Integrity Protocol). WPA2 instead relies on AES-CCMP (Advanced Encryption System, Counter-mode CBC-MAC Protocol, whew), which incorporates the U.S. government-backed AES method limited to 128 bits.

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. (On 802.11n networks that are set to use only 802.11n, WPA2 is the minimum security level. This makes sense because all 802.11n devices must support WPA2 and can't use earlier encryption methods.)

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 username and password. Apple dropped support in AirPort Utility 6 (and never offered it in the iOS app) for setting up a base station to work with

WPA/WPA2 Enterprise, but Mac OS X and iOS support client connections to WPA/WPA2 Enterprise networks.

Turn On WPA/WPA2 or WPA2 Personal

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

1. Run AirPort Utility, select your base station, and click or tap Edit.
2. Select the Wireless view on the Mac, or tap Network in iOS.
3. From the Wireless Security pop-up menu (Mac) or Wireless item (iOS), choose WPA/WPA2 Personal or WPA2 Personal.

   Warning! *Macs with the original AirPort Card (models from 2003 and earlier) 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 or Password field and the same key again in the Verify Password or Verify field.
5. Click Update on the Mac or tap Done and Done again in iOS, 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 Devices, earlier.

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 feature available only to the simultaneous dual-band models of the Extreme 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.

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.

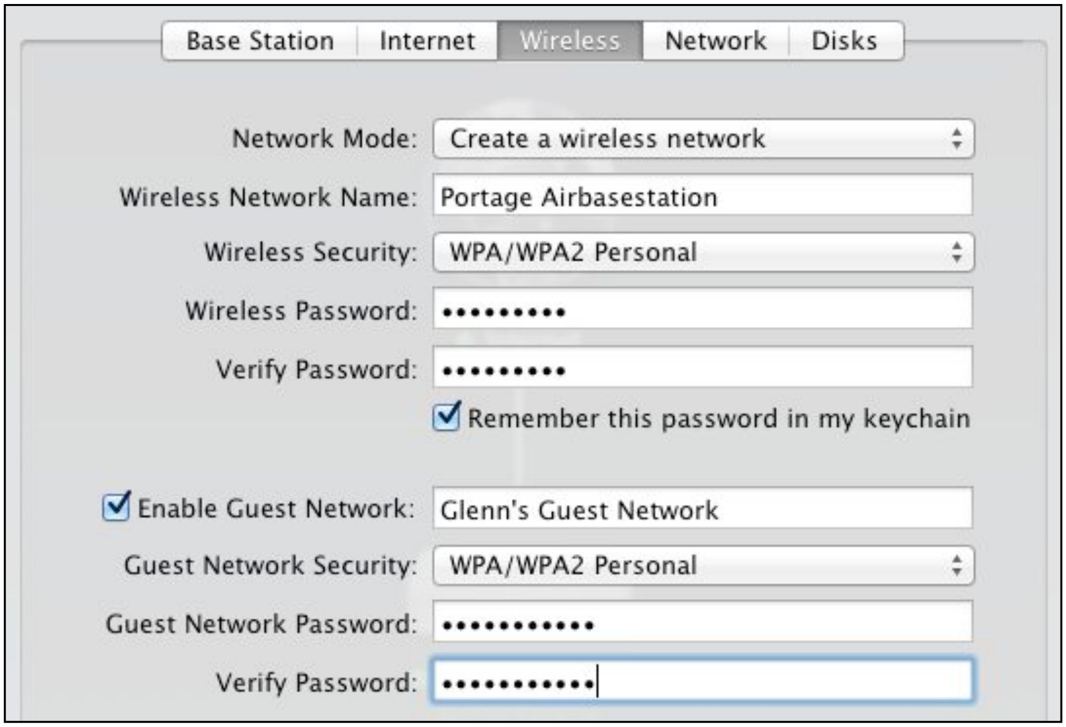
No password, no problem: *If you don't password-protect your guest network, guests can gain wireless Internet access with no hassle, and you've not put other network resources at risk.*

Warning! *Only base stations that are set up to offer both DHCP network assignment and use NAT for sharing a network connection can offer guest networking.*

Note: A guest network always uses both bands, and always has 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.

To set up a guest network, follow these steps:

1. Launch AirPort Utility, and edit the base station's configuration.
2. Click the Wireless button (**Figure 94**) on the Mac, or tap Guest Network in iOS.



Network Mode: Create a wireless network

Wireless Network Name: Portage Airbasestation

Wireless Security: WPA/WPA2 Personal

Wireless Password: •••••••••

Verify Password: •••••••••

☑ Remember this password in my keychain

☑ Enable Guest Network: Glenn's Guest Network

Guest Network Security: WPA/WPA2 Personal

Guest Network Password: •••••••••••

Verify Password: •••••••••••

Figure 94: Guest Network view lets you set options for visitors to use your Internet connection without accessing your main network.

3. Now:

   - On the Mac, select Enable Guest Network and name the network. This name appears in the Wi-Fi menu.

   - In iOS, turn on the Guest Network switch, and tap Guest Network to set a name, which appears in the Wi-Fi menu. Tap Done.

4. Optionally, set a password by choosing either WPA2 Personal or WPA/WPA2 Personal from the Guest Network Security pop-up menu (Mac) or by tapping Security on the Guest Network screen (iOS). Enter a password, and then re-enter it to verify it.

5. Click Update on the Mac, or tap Done and then Done again in iOS.

Overcome Interference

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 or 5 GHz:

- Run iStumbler (http://www.istumbler.com/) to determine whether other networks are running nearby. 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.
- If you're desperate for a solution, check out Wi-Spy, a relatively inexpensive spectrum analyzer that comes in 2.4 GHz only and 2.4 and 5 GHz versions. It can show whether there's interference beyond Wi-Fi. (See Testing from Client to Base Station.)

For 2.4 GHz only:

- Investigate your cordless phones and microwave oven as culprits—they can both create static on the Wi-Fi line. Do you have problems only when talking on the phone or making popcorn? There you go.
- 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.

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. The popular DECT standard finally entered the United States a few years ago in its DECT6 version, which relies on 1.9 GHz signals. You can also find 5.8 GHz cordless phones.
- In 5 GHz, use lower-numbered channels; 5.8 GHz falls within the highest range of channels supported by 802.11n base stations. (This solution also reduces interference from wireless ISPs, firms that use 5 GHz to provide residential Internet service.) Using a lower-numbered channel will reduce the signal strength of your network by 95 percent, but it might be the only solution in extreme cases.

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.

Appendix A: Apple TV and Wi-Fi

The 2nd-generation Apple TV, released in 2010, is a nifty device designed to act as a conduit for streaming content from devices on your network to an HDTV set. You can also use the Apple TV to rent movies and TV shows, stream Netflix movies, watch games from MLB.tv, and access other video sources over the Internet. The 3rd-generation Apple TV works identically, but adds support for 1080p HD video.

In this chapter, I cover how to set up your network for a 2nd- and 3rd- generation Apple TV, which makes it available for use on the network and as a destination for iTunes on a desktop computer and for AirPlay from iOS devices.

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 wirelessly or via Ethernet on an 802.11n network with no problems.*

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 after nearly five years and two product generations, remains 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.

Tip: Like me, you might use Ethernet if your router is anywhere near the Apple TV rather than occupy your Wi-Fi network with streaming data. Wi-Fi is a great second option if Ethernet won't work.

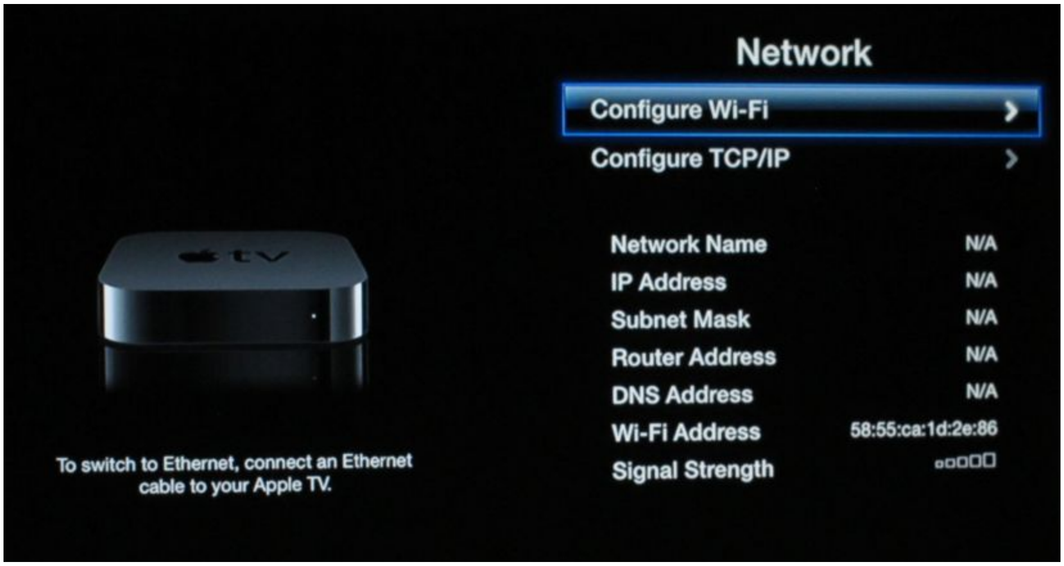
The Apple TV connects to a network in a straightforward way:

- **Ethernet:** 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. With an Ethernet connection, there's zero configuration needed for a network connection.

Tip: The free Remote app for iOS makes it simpler to tap in keyboard entries on your Apple TV.

- **Wi-Fi:** Connect your Apple TV to your TV, power up both devices, grab your Apple Remote or iOS device with the Remote app installed, and follow these steps:

1. On the TV, from the Apple TV main menu, choose Settings > General > Network.
2. On the Network screen, select Configure Wi-Fi (**Figure 95**).

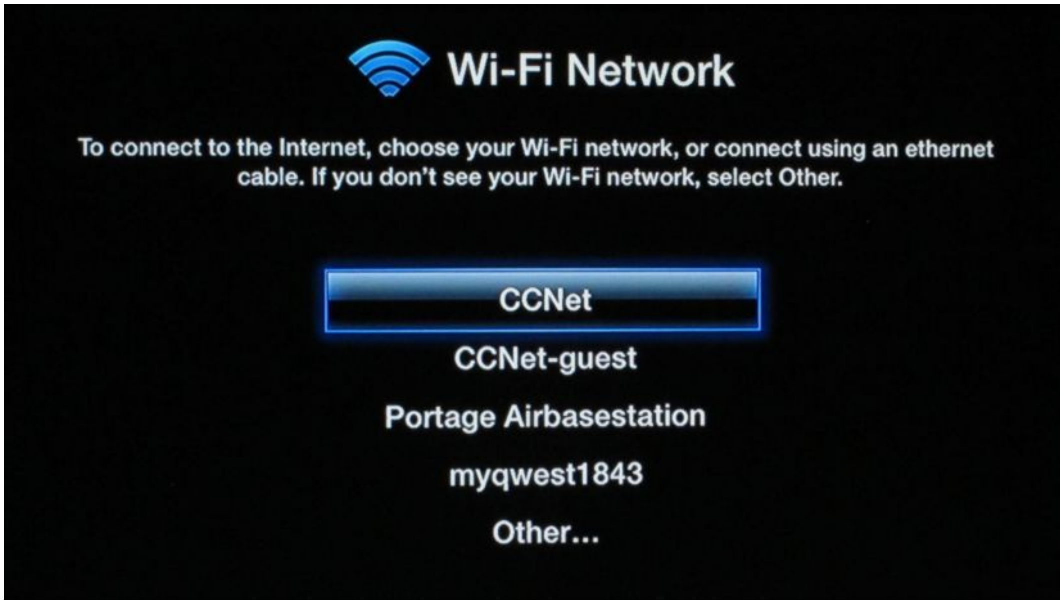


Network Name	N/A
IP Address	N/A
Subnet Mask	N/A
Router Address	N/A
DNS Address	N/A
Wi-Fi Address	58:55:ca:1d:2e:86
Signal Strength	○○○○○

To switch to Ethernet, connect an Ethernet cable to your Apple TV.

Figure 95: The unconfigured Apple TV settings are displayed.

c. On the Wi-Fi Network screen, select your network (**Figure 96**). If you have a closed network, choose Other and enter a network name.

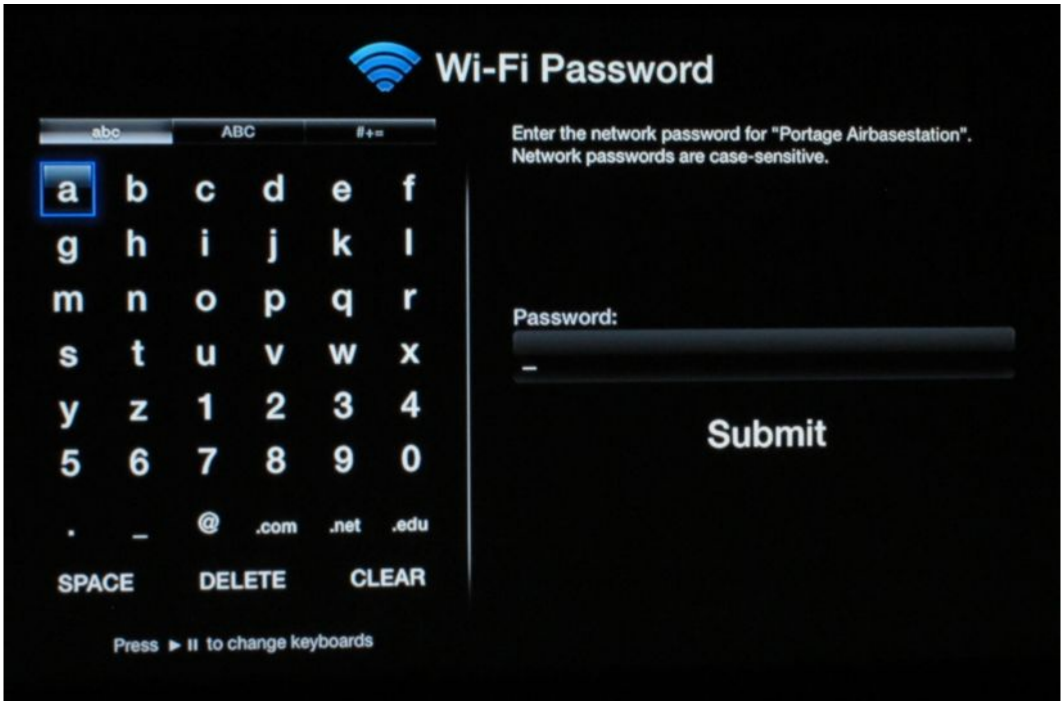


Wi-Fi Network

To connect to the Internet, choose your Wi-Fi network, or connect using an ethernet cable. If you don't see your Wi-Fi network, select Other.

Figure 96: Choose your network from the list.

4. If your network has an encryption key or passphrase, use the Apple Remote or Remote app for iOS to enter it on the Wi-Fi Password screen (**Figure 97**). (Each character is displayed on the TV screen for a moment after you type or tap it.)



Wi-Fi Password

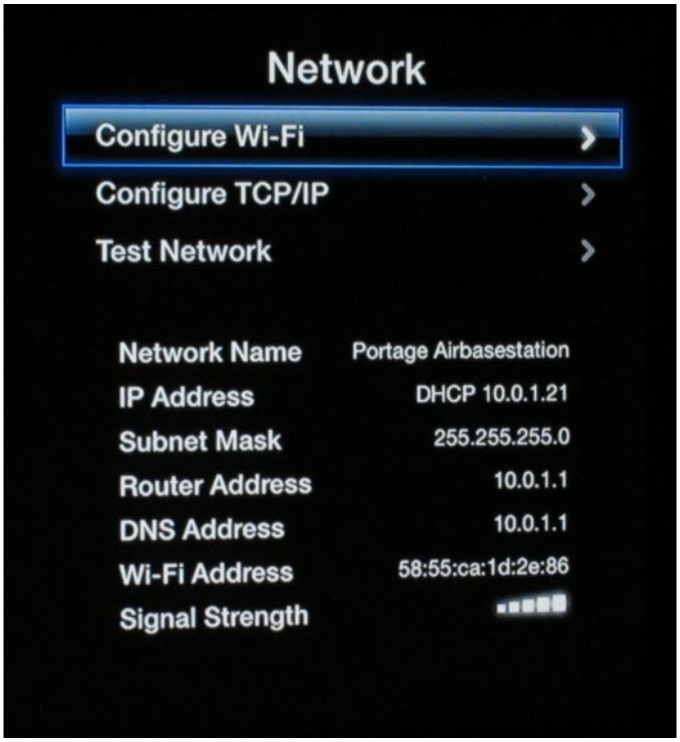
Enter the network password for "Portage Airbasestation". Network passwords are case-sensitive.

Password: _

Figure 97: 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 other details.

The Apple TV is now configured to work on the network (**Figure 98**). It will appear as a destination from any iOS device running iOS 4.2 or later, and from iTunes under Mac OS X and Windows.



Network Name	Portage Airbasestation
IP Address	DHCP 10.0.1.21
Subnet Mask	255.255.255.0
Router Address	10.0.1.1
DNS Address	10.0.1.1
Wi-Fi Address	58:55:ca:1d:2e:86
Signal Strength	▪▪▪▪▪

Figure 98: The Apple TV is on the network.

Appendix B: Configuration Files

You can export the current state of your base station configuration 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.

To export a configuration:

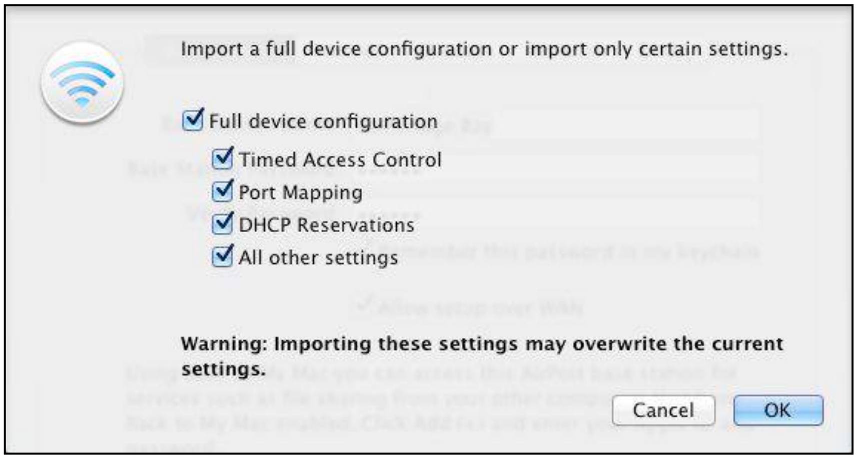
1. In AirPort Utility for Mac, select the base station and click Edit.
2. Choose File > Export Configuration File, and name the file descriptively, as there will be few other clues that help you identify the file.

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 configuration file:

Warning! *Before importing a configuration, you should save a copy of your current active setup using the steps just previously. Importing overwrites your current active base station settings.*

1. In AirPort Utility for Mac, select the base station, and click Edit.
2. Choose File > Import Configuration File.
3. Select the configuration file, and click Open.

   AirPort Utility asks which settings in the configuration file you'd like to import (**Figure 99**). Base stations 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; DHCP reservations for assigning addresses to local computers; and miscellaneous other settings. This list will have a variable number of checkboxes depending on the configuration file. If a type of setting isn't configured, no checkbox shows for that item, logically enough.



Import a full device configuration or import only certain settings.

☑ Full device configuration

- ☑ Timed Access Control
- ☑ Port Mapping
- ☑ DHCP Reservations
- ☑ All other settings

Warning: Importing these settings may overwrite the current settings.

Figure 99: 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 file is imported, the settings replace your current base station settings. 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 after you update them on one base station without resetting the other base stations' names or assigned IP addresses.

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 later, 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: a Wi-Fi adapter plus some other interface, 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 one distinct problem with security and one particular choice for channel selection, which I should address before you turn on the feature.

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. With Lion, Apple once again avoided updating this feature for the appropriate level of security.

Because the software base station uses WEP, enabling security is just the virtual equivalent of posting a “do not enter” sign, rather than providing robust security. You cannot prevent someone from easily breaking the key on your network—all that’s needed is a nearby location, free cracking software, and 1 to 20 minutes.

There’s a second drawback to WEP. If you enable WEP on a Mac running Lion, you lock out Android devices, and potentially other devices as well. Why? Because the Mac incorrectly broadcasts the kind of connection available from the software base station.

Macs that can run Lion all have 802.11n adapters installed (as do many Leopard and Snow Leopard systems, which have the same problem). With Security set to None, these computers advertises that they can communicate using 802.11n, although they can also accept older protocols. (Using a 2.4 GHz channel, that’s 802.11b, g, and n; using a 5 GHz channel, that’s 802.11a or n.) However, when Security is set to either type of WEP key, a mismatch occurs. The Mac continues to claim that it can accept 802.11n connections, but it also says it’s using WEP. 802.11n is incompatible with both WEP and WPA, requiring WPA2 as the only encryption type.

Macs and iOS devices, as well as some devices running other operating systems, drop down to try an 802.11g (in 2.4 GHz) or 802.11a (in 5 GHz) connection, and then send a WEP key. But Android (at least up to version 2.2) tries to use 802.11n to connect. It can’t: it fails. Android doesn’t report an error that describes the situation, either. To use non-Apple gear with the software base station feature, Security must, alas, be set to None.

Frequency

Lion was the first release of Mac OS X that allows you to select either a 2.4 GHz or 5 GHz channel for use with a software base station. You can pick any 2.4 GHz channel, as well as 5 GHz channels 36, 40, 44, and 48. (These channels vary by country.) Apple is offering only 4 of the 8 channels available in its dedicated base stations, which are just 8 of the 23 legal channels in the United States. These lower-numbered channels (36, 40, 44, and 48) broadcast at no more than 5 percent of the maximum legal power of the higher-numbered channels according to U.S. rules. Apple must have thought it better to use lower power and thus not interfere with any nearby networks (see Channels for more details).

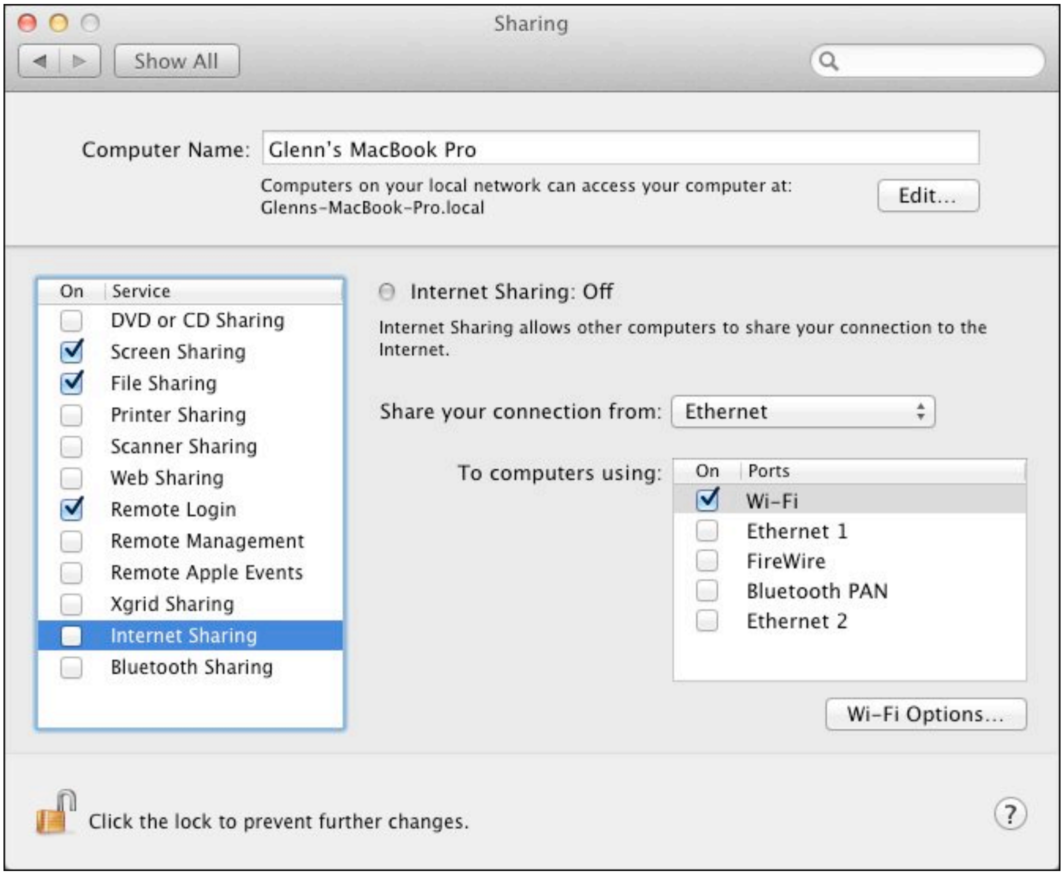
With Security set to None, a software base station set to a 5 GHz channel may accept connections using 802.11a or 802.11n; set to either WEP key, only 802.11a is available. All 5 GHz client adapters that I'm aware of can back off to 802.11a for compatibility's sake.

Starting Up Software Base Station

The Software Base Station feature is found in the Sharing preference pane. Before starting, make sure you have 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 100**).



Computer Name: Glenn's MacBook Pro

Computers on your local network can access your computer at: Glenns-MacBook-Pro.local

On	Service
□	DVD or CD Sharing
☑	Screen Sharing
☑	File Sharing
□	Printer Sharing
□	Scanner Sharing
□	Web Sharing
☑	Remote Login
□	Remote Management
□	Remote Apple Events
□	Xgrid Sharing
□	Internet Sharing
□	Bluetooth Sharing

○ Internet Sharing: Off

Internet Sharing allows other computers to share your connection to the Internet.

Share your connection from: Ethernet

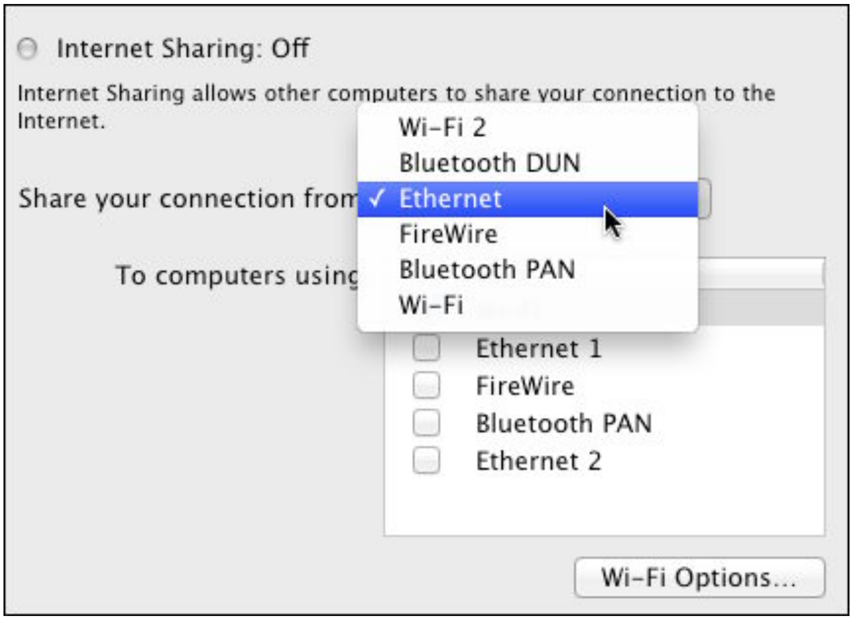
To computers using:

On	Ports
☑	Wi-Fi
□	Ethernet 1
□	FireWire
□	Bluetooth PAN
□	Ethernet 2

Click the lock to prevent further changes.

Figure 100: 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, Ethernet and checking Wi-Fi. (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 Ethernet, and then select the Wi-Fi checkbox in the “To computers using” list (**Figure 101**). (This also works with any other active Internet connection, so long as it’s not Wi-Fi!)



○ Internet Sharing: Off

Internet Sharing allows other computers to share your connection to the Internet.

Share your connection from: ✓ Ethernet

To computers using:

☐ Ethernet 1

☐ FireWire

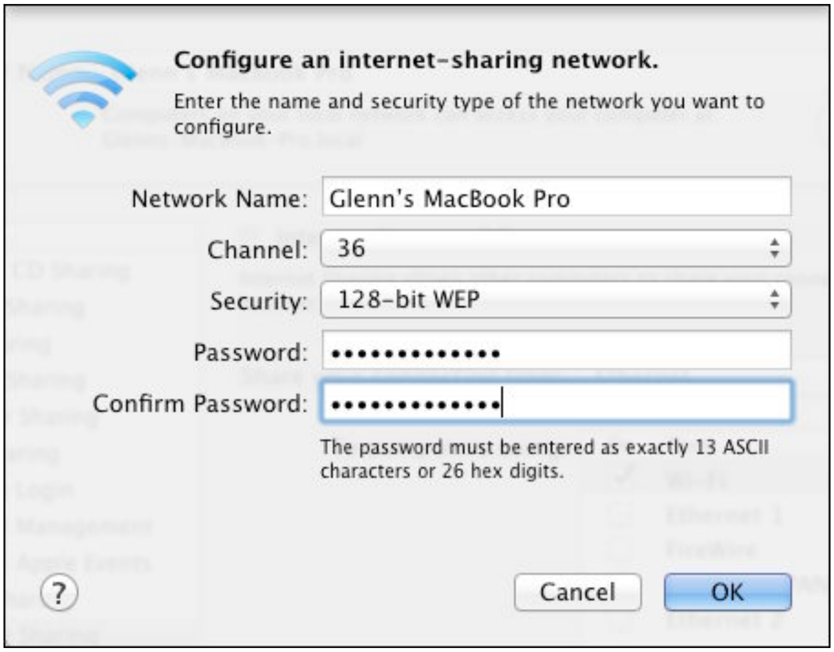
☐ Bluetooth PAN

☐ Ethernet 2

Figure 101: The Share Your Connection From menu lists all active network connections, including some obscure ones, like Bluetooth DUN (dial-up networking). Bluetooth DUN is used for mobile broadband access via Bluetooth.

3. If you want to also share a connection via other active interfaces to other computers or devices connected via your Mac, check any of the additional boxes in the “To computers using” list. For instance, you might have a device connected via a Bluetooth PAN (Personal Area Network) that could then be fed Internet access from your Ethernet connection.

4. Click Wi-Fi Options to set the network name, channel, and, optionally, a WEP key (**Figure 102**). Click OK. (Look back to the start of this section for advice on channel and security options.)



Configure an internet-sharing network.

Enter the name and security type of the network you want to configure.

Network Name: Glenn's MacBook Pro

Channel: 36

Security: 128-bit WEP

Password: •••••••••••••

Confirm Password: •••••••••••••

The password must be entered as exactly 13 ASCII characters or 26 hex digits.

Figure 102: 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 that computers other than Macs with AirPort cards will ever want to access your network, I suggest that 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 the Internet Sharing box to start the service.
6. An alert asks you to confirm that you want to turn on Internet Sharing; click Start.

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.

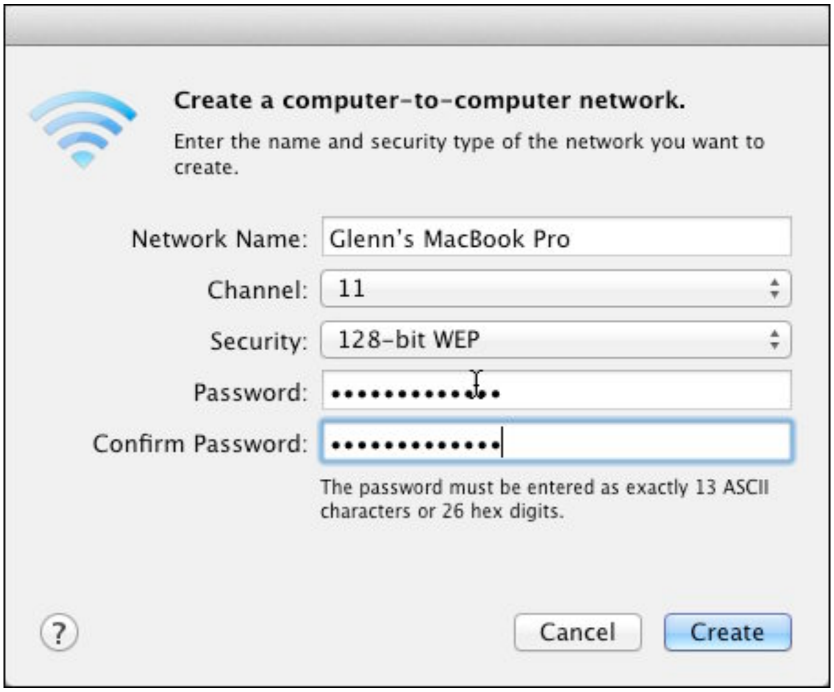
Ad Hoc Networking

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, where x is a number between 1 and 254; 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 Wi-Fi menu, choose Create Network.
2. Enter a network name, choose a channel, and consider security (**Figure 103**). See Secure Your Network for more details about the Security pop-up menu and tradeoffs, and Channels for help in picking a channel. If you select either WEP option from Security, enter the same password twice.



Create a computer-to-computer network.

Enter the name and security type of the network you want to create.

Network Name: Glenn's MacBook Pro

Channel: 11

Security: 128-bit WEP

Password: •••••••••••••

Confirm Password: •••••••••••••

The password must be entered as exactly 13 ASCII characters or 26 hex digits.

Figure 103: Create an ad hoc network by filling in these settings.

3. Click Create to create the network.

Your Wi-Fi menu now shows a computer-in-a-fan icon, which indicates that ad hoc networking is in use.

To turn off an ad hoc network, choose Wi-Fi > Disconnect from *your network name*. You'll find the command under a Devices label, listed in the menu below the names of any regular Wi-Fi networks in the vicinity (**Figure 104**).

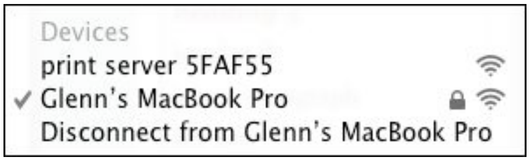


Figure 104: The Devices section of the Wi-Fi menu lets you turn off an ad hoc network by choosing Disconnect.

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 you may be among the more technically inclined readers who want to know more about the technical minutiae of Wi-Fi. In this appendix, you can learn about why the 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 Set a Channel, earlier, 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.

Channel availability varies widely from country to country. 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.

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 log2 of the sum of 1 + signal divided by noise (**Figure 105**).

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

Figure 105: *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 106**). 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.)

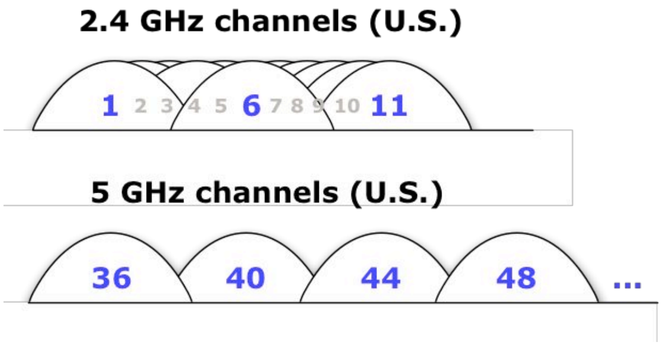


Figure 106: 2.4 GHz 802.11 channels are staggered, with channels 1, 6, and 11 having the least overlap. 5 GHz 802.11 channels have little overlap; only the four lowest channels of 23 are shown.

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: For 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.

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 of 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 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: UNII-1 (4 channels), UNII-2 (4 channels), UNII-2 Extended (11 channels), and UNII-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) has a maximum permitted signal strength that's 5 percent of the strength 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 and 2011 updates to Apple's AirPort gear, Apple has continued to increase the power emitted by the upper 5 GHz channels, too, so that signal strength is closer to the maximum permissible amounts.

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 4 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 would be unable 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.

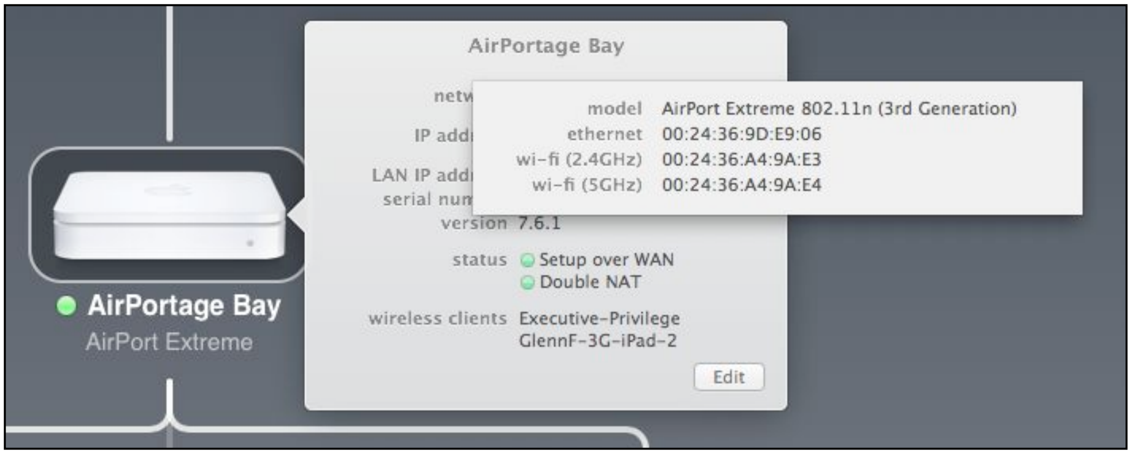
Appendix E: What and Where Is a MAC Address?

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 are various ways to locate Mac addresses:

- **Base station:** Look on the bottom of the base station (Extreme, Time Capsule) or near the plug (Express). Or, in AirPort Utility for the Mac, select a base station and hover over the network's name (**Figure 107**):
  - The *AirPort ID* or *Wi-Fi ID* is the wireless MAC address. Starting with the early 2009 models of the Extreme and Time Capsule, these devices have two AirPort IDs, one for each band's radio, and they are noted by band on the base station itself and in AirPort Utility.
  - The *Ethernet ID* is the WAN port's MAC address.



AirPortage Bay

AirPort Extreme

AirPortage Bay

netw

IP addr

LAN IP addr

serial num

model AirPort Extreme 802.11n (3rd Generation)

ethernet 00:24:36:9D:E9:06

wi-fi (2.4GHz) 00:24:36:A4:9A:E3

wi-fi (5GHz) 00:24:36:A4:9A:E4

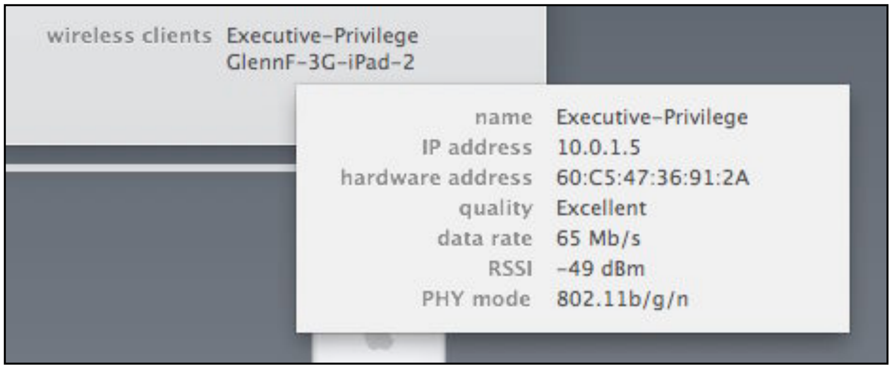
version 7.6.1

status Setup over WAN
Double NAT

wireless clients Executive-Privilege
GlennF-3G-iPad-2

Figure 107: View the base station's MAC addresses by hovering over the name.

- **Computers connected to a base station via Wi-Fi:** In AirPort Utility, select the base station and hover over a connected device's name in the Wireless Clients list at the bottom (**Figure 108**). The Name shows either the value entered in the Network preference pane in Mac OS X or a Bonjour name.



wireless clients Executive-Privilege
GlennF-3G-iPad-2

name Executive-Privilege

IP address 10.0.1.5

hardware address 60:C5:47:36:91:2A

quality Excellent

data rate 65 Mb/s

RSSI -49 dBm

PHY mode 802.11b/g/n

Figure 108: Wireless Clients reveal information about connected devices when you hover over a name in the list.

- **Wi-Fi adapter in a Mac:** In Mac OS X, open the Network System Preferences pane. Click Wi-Fi in the adapter list, and click the Advanced button. The MAC number is the Wi-Fi Address. (Leopard and Snow Leopard call this the AirPort ID.)
- **Wi-Fi adapter under Windows 7:** View the connection status of the adapter, and click Details below the Connection Status section. The Physical Address is the MAC address.

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.

Ebook Extras

You can access extras related to this ebook on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and—usually—Mobipocket. (Learn about reading this ebook on handheld devices at http://www.takecontrolbooks.com/device-advice.)
- Read postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.
- Get a discount when you order a print copy of the ebook.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the "access extras…" link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the "access extras…" link above. Then, once you are logged in to your new account, add your ebook by clicking the "access extras…" link a second time.

Note: If you try the directions above and find that the device you're reading on is incompatible with the Take Control Web site, contact us at tc-comments@tidbits.com.

About the Author

Glenn Fleishman is a senior editor at *Macworld,* and one of the writers of the *Economist's* Babbage blog where he is also a regular contributor to the print edition. He's the Macintosh columnist for the *Seattle Times,* and a contributing editor at *TidBITS*, where he built the content management software and handles programming tasks. He also writes for *Ars Technica, BoingBoing,* and *TechHive,* among other publications. He can be heard regularly on public radio in Seattle and nationwide.

He lives in Seattle in a bungalow with his wife and two sons. His older child's first word was "book," not "Mac."

Author's Acknowledgments

This book has gone through many, many changes since its first edition in 2005, when 802.11n was still a pipe dream, and networks were simpler beasts, even though quite challenging.

I want to thank Tonya Engst for her continued work in developing this book through now its fourth major overhaul, 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.

About the Publisher

Publishers Adam and Tonya Engst have been creating Apple-related content since they started the online newsletter *TidBITS,* in 1990. In *TidBITS*, you can find the latest Apple news, plus read reviews, opinions, and more (http://tidbits.com/). Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.

Production credits:

- Take Control logo: Jeff Tolbert
- Cover design: Jon Hersh
- Production Assistants: Michael E. Cohen, Oliver Habicht
- Editor in Chief: Tonya Engst
- Publisher: Adam Engst

Thanks to reader Bill Boyd for reminding us about the difference between a variable and a function!

Copyright and Fine Print

Take Control of Your 802.11n AirPort Network, Third Edition
ISBN: 978-1-61542-405-4
Copyright © 2012, 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

Click any book title below or visit our Web catalog to add more ebooks to your Take Control collection!

Take Control of BBEdit (Glenn Fleishman): Learn how to take full advantage of BBEdit's text-processing power!

Take Control of CrashPlan Backups (Joe Kissell): Join backup expert Joe Kissell as he shares real-world advice about protecting your data with CrashPlan’s onsite, offsite, and cloud backups.

Take Control of Getting Started with DEVONthink 2 (Joe Kissell): Store, organize, and locate your PDFs, paper documents, email messages, and scribbled notes with DEVONthink 2.

Take Control of iTunes 10: The FAQ (Kirk McElhearn): This FAQ-style ebook helps you wrap iTunes around your little finger and enjoy your media more.

Take Control of Screen Sharing in Lion (Glenn Fleishman): Figure out which type of screen sharing to use when and how to get the most out of screen sharing.

Take Control of Spotlight for Finding Anything on Your Mac (Sharon Zardetto): Whether by mouse or by menu, or by typing a complex query, you’ll learn how to find files, contacts, images, and much more.

Take Control of the Mac Command Line with Terminal (Joe Kissell): Learn the basics of the Unix command line that underlies Mac OS X, and get comfortable and confident when working in Terminal.

Take Control of Troubleshooting Your Mac (Joe Kissell): Learn basic troubleshooting procedures, solve common problems, and gain confidence in solving any Mac problem.

Take Control of Your iPad (Tonya Engst): Optimize your iPad experience—make important customizations, sync media and data, and get tips on making the most of core iPad apps.

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!