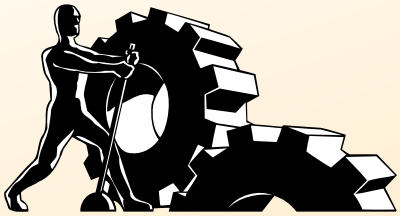
Check for Updates
Make sure you have the latest information!



TidBITS Publishing Inc.

Take Control of v1.2

Back to My Mac

Glenn Fleishman

$10

Help Catalog Feedback Order Print Copy

Table of Contents

Read Me First

Welcome to *Take Control of Back to My Mac,* version 1.2, published in February 2010 by TidBITS Publishing Inc. This book was written by Glenn Fleishman, and it was edited by Dan Frakes and Tonya Engst.

This book will help you master Back to My Mac, a feature introduced in Mac OS X 10.5 Leopard that lets you remotely access files and remotely control the screens of multiple Macs that you manage or own.

UPDATES

We may offer free minor updates to this book. To read any available new information, click the Check for Updates link on the cover or click here. If you own only the print version of the book or have some other version where the Check for Updates link doesn't work, contact us at tc-comments@tidbits.com to find out about obtaining the PDF.

LINKS

As a rule of thumb, cross-references and URLs (Web links) in this ebook are *hot,* meaning you can click them to open their associated pages. Two caveats:

- In Snow Leopard's Preview, longer URLs may appear to be broken. To avoid this Preview bug, try clicking the last character in the URL.

- In an iPhone app, the convention for following a link is that you *touch* the link (meaning you hold down on it for several seconds) until it highlights. Once a highlight shows, release your finger and the page will load. If your iPhone app does not support hot links, or if certain links are not working, please contact us at tc-comments@tidbits.com for advice.

BASICS

In reading this book, you may get stuck if you don't know certain facts or if you don't understand Take Control syntax for things like working with menus or finding items in the Finder. Please note the following:

- **Path syntax:** I occasionally use a *path* to show the location of a file or folder in your file system. Path text is colored in purple type. For example, Mac OS X stores most utilities in the Utilities folder. The path to the Utilities folder is: /Applications/Utilities.
- **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 brings up the Finder's preferences dialog is Finder > Preferences.
- **Finding preference panes:** To open System Preferences, click its icon in the Dock or choose System Preferences from the menu. When that window opens, click the icon of the pane whose settings you want to adjust. I refer to these panes using an abbreviated notation such as "the Sharing preference pane."
- **Network primer:** This book is loaded with network jargon and concepts. If you need a boost to understand those basics, please see Appendix A: Understand Network Terms.
- **Screen sharing:** *Screen sharing* is a catchall term for remote control of a computer with a display that simulates being directly in front of that remote computer. In Leopard and Snow Leopard, you can set up the Screen Sharing service (in the Sharing preference pane), use the Screen Sharing application (hidden in the System folder), and generically use screen sharing as a concept.
- **Bonjour:** *Bonjour* is an Apple technology that computers, printers, and various services can use to announce their availability on a local

network, so that other devices can find and access them without knowing their names in advance. This may be all you need to know to get started with this ebook, but read the sidebar Bonjour, Everybody (p. 13) if you want more details.

WHAT'S NEW IN VERSION 1.2

This version contains updates for Mac OS X 10.6 Snow Leopard (but still covers 10.5 Leopard), and it documents the addition of Back to My Mac support for drives inside or attached to Apple base stations:

- Snow Leopard didn't change how Back to My Mac works, but many cosmetic details in the interface are different. This version makes those changes clear.
- Back to My Mac was added as a so-called MobileMe feature in the AirPort Extreme Base Station and Time Capsule so you can Access Base Station Hard Drives (p. 38).
- In Snow Leopard, Apple added a new Wake on Demand feature, which—if you have the right hardware—makes it easy to wake up a sleeping Mac for remote access. See Enable Wake on Demand in Snow Leopard (p. 67) for details.
- I've enhanced my discussion of how to Revoke Certificates via Me.com (p. 53).

WHAT WAS NEW IN VERSION 1.1

Here is a list of the most important changes:

- The book now refers only to MobileMe, the service from Apple that replaced .Mac in July 2008.
- I added brief information about revoking digital certificates.
- Version 1.0 claimed you could make Back to My Mac work with manual port mapping or default host exposure. Unfortunately, despite some success in testing, I've been unable to make these techniques work consistently, and Apple doesn't officially support anything but public IP addresses and automatic port mapping. I removed all references to these options.

Introduction

If you thought this book title was interesting, then you probably own more than one computer, and your computers are likely located in different places—whether just down the hall or halfway around the world from each other.

I'm no mind reader, and you can easily determine how I predicted your computer ownership. It's increasingly the case that when we're on one computer, we find that we need files from or need control of another computer. Fortunately, starting with Mac OS X 10.5 Leopard, Apple added a significant tool to our arsenal that can reach out over a local network or the Internet: Back to My Mac.

Back to My Mac uses a host of industry standards and Apple-developed protocols to create an intertwined web (as in a woven web, not the World Wide Web) of services. It uses these services to create a connection between Macs for the purposes of extending the power and convenience of a local Bonjour network to any other computers under your control—even if those computers are located across the Internet. This includes file sharing and screen control. The "key" to this connection, so to speak, is a shared MobileMe account.

Mac OS X uses MobileMe as a way to figure out where on the Internet computers are without requiring manual router configuration or knowing fixed names or IP addresses for those devices. MobileMe "tunnels" can reach through home and office wireless and broadband gateways and past network obstructions.

Apple would like to say that one or two clicks turns on these services. However, as with any set of tools that relies on the Internet, there's more beneath the surface.

In this book, I show you not only how to set up your network and your connected Macintoshes for the best results with Back to My Mac, but also how to troubleshoot problems, determine whether Back to My Mac can even work for you, and overcome stumbling blocks.

Back to My Mac Quick Start

This book shows you how to use Back to My Mac, including configuring your router, and it teaches you to troubleshoot problems that prevent the service from working reliably.

Learn background that will help you configure like a pro:

- Read Why Use Back to My Mac? to get a better sense of how Back to My Mac addresses your needs (p. 10).
- Take a quick whirl through how Back to My Mac actually makes its way over the Internet or a local network for a connection, noting whether your networks are set up as Back to My Mac expects. See Learn How It All Works (p. 15).
- Learn networking terminology and concepts in Appendix A: Understand Network Terms (p. 73).

Configure and use Back to My Mac:

- Read Configure Your Router or Gateway to first see if you need to make any changes to allow remote access, and, if so, what settings to modify (p. 25).
- Enable remote file sharing and screen sharing with Back to My Mac. Consult Turn On Back to My Mac (p. 32), Set Up File Sharing (p. 35), and Set Up Screen Sharing (p. 37).
- Add Back to My Mac support to Apple base stations. See Access Base Station Hard Drives (p. 38).
- Learn how to connect to remote computers in Connect to a Back to My Mac System (p. 40).
- Help friends and relatives troubleshoot problems via Back to My Mac. See Overcome the Same MobileMe Account Limit (p. 57).

Deal with Back to My Mac security issues:

- Avoid security pitfalls that make Back to My Mac less safe. See Secure Back to My Mac (p. 42).
- Did you use Back to My Mac on a computer that's not yours? Erase Back to My Mac's Traces (p. 51) on that Mac.

Solve problems:

- Diagnose and solve commons problems that prevent Back to My Mac from working. See MobileMe Preference Pane Troubleshooting Messages (p. 60) and Back to My Mac Stops Working or Doesn't Work (p. 63).
- Figure out if your ISP is keeping Back to My Mac from making a connection. Refer to Double NAT (p. 61).
- Keep your computer from falling asleep and being unreachable remotely. See Sleep Causes Lack of Access (p. 66).

Why Use Back to My Mac?

Back to My Mac is one of the most powerful remote-services features ever built into in an operating system. Back to My Mac lets you easily connect two computers, even ones separated by the Internet and intermediate network hardware, and then share files or the remote screen between them without entering additional passwords. It's not just about file and screen sharing, though: any Bonjour services can be used over the connection, although other services are of less interest to most people.

Back to My Mac is designed primarily to meet the needs of one person with two or more computers that are not located on the same local network.

The key phrase in that description is "one person": everything is tied to a single person's MobileMe account. The advantage of using just one account is that because the service is designed securely, you needn't set up multiple accounts, nor install special software, nor manage connections. Back to My Mac assumes you own all the computers you're connecting to, and it lets you use them with the same kind of permission that you have on the computer you're in front of.

Back to My Mac Workarounds and Alternatives

To manage a bunch of computers that you aren't the primary user of, or that can't share the same MobileMe account, see Overcome the Same MobileMe Account Limit for a limited workaround. Alternately, look into LogMeIn, Timbuktu Pro, or Apple Remote Desktop, which I cover briefly in Appendix B: Other Remote Access Solutions. Also note that running Mac OS X's Screen Sharing feature via iChat, Bonjour, or a direct connection could be an excellent alternative if all you want to do is view and control a remote Mac's screen.

REMOTE ACCESS TO FILES

The most common use of remote access is to copy files from one computer to another. In other words, while using a *local* computer—one that you are sitting at—you can download to that local computer files stored on a *remote* computer (that is, one located elsewhere), and copy files from your local computer to the remote one.

Some people solve the problem of needing to use the same files on more than one computer by carrying around external drives; however, for smaller files—or a small number of files—remote access can be more convenient. With Back to My Mac, you have the same options as with any file server that you have full access to: you can create and delete folders and files on the remote computer, copy files to and from it, and rearrange things. You can also remotely access hard drives in and attached to Apple's Wi-Fi base stations.

REMOTE ACCESS TO A SCREEN

Instead of transferring files, it's sometimes useful to work with files by accessing a program running on a remote computer. If you need to interact with software, then screen sharing is the way to go. *Screen sharing* literally gives you a window into a remote computer, allowing you to see and interact with that computer as if you were sitting in front of it. The window on your system may be part of an application, or it may fill your local screen.

For example, I find screen sharing useful when I'm trying to find an old piece of email and I'm away from my office. My email folder is gigabytes in size, and it changes whenever I send, receive, or file email; syncing isn't a good option, because it would involve transferring too much data back and forth. Screen sharing lets me keep the email on my main machine (my cake) and still be able to search it from anywhere (eat it, too).

Tip: Starting with 10.5 Leopard, you can use Spotlight to find files across computers on a network, or even over the Internet. When network volumes are mounted, Finder search windows include a Shared item in the Search header. Select that item to search remote Macs.

Screen sharing is also useful if you have a computer dedicated to slow or CPU-intensive processes such as encoding video. You can use screen sharing to view the screen of the computer doing the work to check on the progress. Or, you might use screen sharing to control servers that aren't in your vicinity or that lack displays altogether.

Screen sharing as a concept is not new to Mac OS X; however, screen sharing coupled with Back to My Mac is trivially easy to use, requiring no additional passwords or configuration beyond what you've already done in setting up accounts on your Mac and in MobileMe. With screen sharing, you have instant access to the screens of all computers you've set up with Back to My Mac.

What can you do with screen sharing?

- **Remotely control the pointer on the other computer:** You can click, drag, and move the pointer as if your mouse was plugged into the other computer.
- **Remotely type on the other system using a keyboard:** Anything you type locally in the screen-sharing window shows on the remote system as if your keyboard was connected to the other computer.
- **Copy the contents of the Clipboard back and forth:** Anything that you can copy onto the Clipboard can be transferred between a remote and local computer.

What can't you do with screen sharing?

- **Drag files between the local and remote computers:** While some advanced remote access software, such as Timbuktu Pro, allows you to use a copy file dialog and even drag files to and from a remote system, screen sharing in Leopard and Snow Leopard is limited to remote control.
- **Use peripherals:** The system you're remotely controlling can't use an iSight camera, a hard drive, a scanner, and whatever other peripherals you might have attached to your local computer. However, you can use any peripherals on the remote computer *from* the remote computer. That is, you can print a file from a program running on the remote computer to a printer that the remote system can reach.

Leopard and Snow Leopard support two general kinds of screen sharing: one in which iChat facilitates a connection with user-granted permission to link two computers over a local network or over the Internet; the other, in which you set up a remote computer to allow access and then connect to it using an IP address, host name, or Bonjour (see the sidebar below, "Bonjour, Everybody"). The latter option includes Back to My Mac, and is thus the method I focus on in this book; it is appropriate for a single user controlling multiple Macs. Consult the sidebar, Other Forms of Screen Sharing vs. Back to My Mac, next page, for more details on the different sub-categories of screen sharing that fall under these two types, and to make certain that Back to My Mac is the right kind of screen sharing for you.

Note: As mentioned earlier, Back to My Mac isn't limited to file and screen sharing. Nearly any Mac OS X program or service that supports Bonjour should work over a Back to My Mac connection. However, Apple blocks its own iTunes and iPhoto sharing from working over Back to My Mac.

Bonjour, Everybody

Bonjour is a "network discovery" protocol that allows services on a computer to advertise their availability through a special form of broadcast—essentially, an electronic "announcement" to the rest of the local network.

Without Bonjour, computers on the same network using private IP addresses can access services from one another, but each user must know the IP address of a given machine in order to access a given service. Bonjour gets rid of this recordkeeping.

You take advantage of Bonjour whenever you use the Network browser in Leopard or Snow Leopard, look for local Web sites in Safari (if Include Bonjour is enabled under Bookmarks in Safari's Bookmarks preference pane), or add a local printer. Back to My Mac uses Bonjour over local networks and over the Internet as a component of how it ties different computers together.

For more details on how Bonjour fits into Mac OS X's overall networking, see Appendix A: Understand Network Terms.

Other Forms of Screen Sharing vs. Back to My Mac

Besides Back to My Mac, there are several other types of screen sharing. (I cover them in the companion volume to this book, *Take Control of Screen Sharing in Snow Leopard*.) They are:

- **iChat:** Two Macs both running iChat in Leopard or Snow Leopard can share a screen when a person on one Mac asks to share the other's screen or offers to share theirs. iChat works over the Internet and over a local network.
- **Bonjour:** You can use Bonjour on a local network without iChat, using a password to restrict access, rather than requiring that another person approve access. Bonjour is also useful for accessing a server that lacks a monitor. Bonjour requires less configuration and overhead than Back to My Mac.
- **IP address or host name:** If Bonjour is not an option, or a computer you want to control is outside the local network, you can set up a direct connection using the remote computer's IP address or host name along with a password.
- **VNC:** Virtual Network Computing is a widely used remote-access tool on which Leopard-and-later's screen sharing feature is based. VNC can even be used between computers running different operating systems. This means you can use VNC when some computers involved don't have Leopard or Snow Leopard installed, because VNC is the best common denominator.
- **Skype:** Recent versions of Skype for Mac OS X and Windows include free person-to-person screen sharing very much like iChat's screen-sharing option in Leopard and Snow Leopard, but without remote control.

Learn How It All Works

Back to My Mac uses a combination of network controls in Mac OS X and underlying networking protocols to pull off the trick of connecting two remote computers in a secure fashion, even when those computers are "hidden"—located behind gateways that typically prevent direct access. Let's look at a few important aspects of how Back to My Mac works:

- In Requirements and An Intricate Web you'll learn how a connection is made. This will make it easier to pinpoint the cause of anything that might go wrong. As you read along, take notes on aspects of the configuration that might require special attention in your particular case. (I provide setup steps in the next section, Configure Your Router or Gateway.)
- In Security, you'll learn what goes on behind the scenes with certificates, tickets, tunnels, and more to ensure a secure connection.

If You Need an Even More Basic Introduction

If you start reading this section and find that it's too complex or that you don't know enough of the jargon, make sure you've read Why Use Back to My Mac? (just previously) and read Appendix A: Understand Network Terms, which will give you a leg up on the topics discussed here.

REQUIREMENTS

Before we start down the path of how the pieces of Back to My Mac fit together, let's note the requirements for using the service:

- **Leopard or Snow Leopard:** Leopard or later must be installed on each computer you use with Back to My Mac; in this ebook I assume that you are running at least Mac OS X 10.5.4, which is the Leopard version that added MobileMe support, or any version of 10.6 Snow Leopard. Back to My Mac works fine among a mix of Leopard and Snow Leopard systems.

- **MobileMe:** A MobileMe account, either a stand-alone account or part of a family pack. An email-only MobileMe account will not work because it lacks the part of MobileMe that Back to My Mac uses to track network settings among supported computers.
- **Remote access:** For remote access (connecting between Macs located on different local networks), *either:*
  - A publicly reachable IP address for each remote computer

    or
  - A router with a publicly reachable IP address that you can configure to use NAT-PMP (Network Address Translation-Port Mapping Protocol) or UPnP (Universal Plug and Play).

    Warning! *Back to My Mac requires a public IP address on a router that's acting as a NAT server for the computer on which Back to My Mac is running. Some ISPs assign a private address to their router, or provide an address that a router you supply uses, but then the ISP maps that private address to a publicly reachable IP address. That works fine, too.*

    While Skype, LogMeIn, GoToMyPC, and other services can work around this public IP address problem, Back to My Mac cannot. To remedy the situation, you could ask your Internet service provider if they offer a router with UPnP support; change your router if it's one you bought separately; or look into a different ISP that can give you either automatic port mapping or a range of publicly reachable addresses.

Warning! *You can't use Back to My Mac with manual port mapping, where you configure a router to pass traffic to a specific computer on the local network. Back to My Mac only works with public IP addresses or with automated port mapping via NAT-PMP or UPnP.*

Note: NAT-PMP and UPnP are described in great detail in Appendix A: Understand Network Terms.

AN INTRICATE WEB

Back to My Mac uses MobileMe as glue to bind together different Macs on the Internet. To use it, you must set up each Mac with the same MobileMe account. Then, each computer stores connection information on MobileMe where the other Macs can access it.

Here's the roadmap for how the service works:

1. The Router: If the computer is connected to the Internet via a router that assigns network addresses, Back to My Mac asks the router for configuration information.
2. Back to My Mac Sends Information to MobileMe: Back to My Mac tells MobileMe where the computer is located and how to reach it on the network or via the Internet (including any information necessary to access the computer through the router). This information is stored on MobileMe's servers.
3. Each Computer Sees the Others: When connecting to a remote computer, your copy of Back to My Mac creates a secure connection with the other computer, using the information about that computer's location and configuration stored on MobileMe. Assuming everything goes right, that is.

To understand this set of steps, we have to look at the router first, which may seem out of order. But it's the router that determines how Back to My Mac ultimately sets itself up. We then look at Back to My Mac's process of communication, and conclude with how the connection is created between computers.

What about Using Back to My Mac with a Local Connection?
On a local network where all the Macs share the same set of network addresses, you can use Back to My Mac for regular file sharing and screen sharing, but it's is often just as effective to use Apple's Bonjour technology. Back to My Mac's specialty is in helping you reach machines outside the local network, and that's where using the service gets complex.

The Router

A Mac with Back to My Mac enabled can be accessed via Back to My Mac only if another similarly configured Mac can connect to it.

This seems logical, of course. But whether a connection can be established depends primarily on the configuration of the target Mac's local network, starting with the ISP that provides the connection to the Internet, on through the router, and down to the individual computer.

There are two ways to set up the target computer's local network, which vary in how easy they are to configure for remote access:

- **Private IP addresses are assigned by a router that uses automatic port mapping:** In this common situation, locally connected computers can request a continuously available incoming connection, which the router provides with NAT-PMP or UPnP.

  (Configure Your Router or Gateway covers how configure the automatic port-mapping protocols NAT-PMP or UPnP. Not sure what those are? See Appendix A: Understand Network Terms.)

  Any number of Macs on the local network can have remote access enabled using this option.

- **Publicly reachable (or routable) IP address is used on the target computer:** In this simplest case, which you'll hardly ever see, the remote (target) computer has an IP address that can be reached from anywhere on the Internet: the IP address is public, and the computer is not behind any gateway that prevents access. (A firewall could restrict access by unauthorized networks and to closed services, but that's a different issue.)

  Every computer on a network with its own public IP address can have remote access enabled with no additional configuration.

Alternatives for Connecting Two Macs

If the remote computer has a public IP address, you could use ShareTool from Yazsoft instead of Back to My Mac. ShareTool doesn't require a MobileMe subscription, and it connects many different services between two Macs, making it more broadly useful (http://yazsoft.com/products/sharetool/information/; $20 each, $35 for two licenses, $75 for five).

The program works with routers that support NAT-PMP or UPnP to expose services from the computer running the software. Older versions of ShareTool lacked encryption, but Yazsoft added SSH-based security in a recent update.

When you turn on Back to My Mac, the feature tries to set up port mapping on your network router using automatic port mapping (NAT-PMP or UPnP), and then it keeps track of the information the router responds with, including whether the router understood its request for ports. (This doesn't apply to computers that use Back to My Mac with each other within a local area network, as connections are made without passing through the router.)

What's provided by the router to Back to My Mac depends on what port-mapping protocol is available on the router that sits between the computer and MobileMe:

- **If either NAT-PMP or UPnP is enabled:** For a router that uses one of these automatic port-mapping protocols to assign a private address to the computer that's being set up, the Back to My Mac service asks the router to assign it arbitrary public ports. If all goes well, the router then provides Back to My Mac with the port number(s) and the router's public IP address. (Troubleshooting feedback will alert you if neither protocol is enabled or available. See MobileMe Preference Pane Troubleshooting Messages, p. 60)
- **If NAT is disabled and a public, routable IP address is used:** With a publicly reachable IP address, Back to My Mac registers the actual address of the computer, which exposes the correct ports. As noted earlier, this is a rare case; Back to My Mac isn't needed for remote file access in this circumstance, although it does provide additional security.

Reachable router: *A router may have a publicly routable IP address or be hidden behind an ISP's own NAT gateway, which might prevent remote access altogether (see Troubleshooting). For Back to My Mac to work, the router's IP address has to, in some fashion, be reachable remotely.*

Back to My Mac Sends Information to MobileMe

Once Back to My Mac determines the port-mapping information, it talks to MobileMe, registering the information about the ports used for the computer and the IP address of the router or computer. These details are updated in a special set of *DNS* (domain name service) entries for Back to My Mac (**Figure 1**). The information is stored

separately in your MobileMe account so that all Back to My Mac computers using your account can retrieve the details.

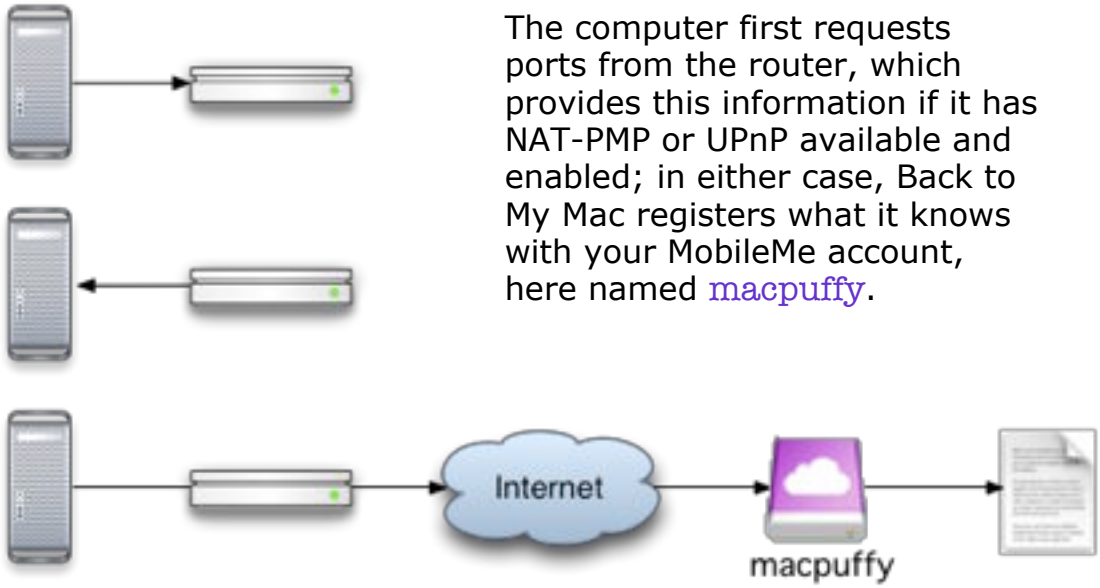


Figure 1: This diagram shows how Back to My Mac works behind the scenes with a router that supports automatic port mapping with NAT-PMP or UPnP. In your MobileMe account, your Mac registers itself in a list of all your computers set to use Back to My Mac.

DNS and Back to My Mac

The DNS entries for Back to My Mac are made using the *wide-area Bonjour* protocol, an Apple-devised (but not proprietary) way of publishing local networking resource information to DNS. Whenever the details of your Back to My Mac connection—such as the public ports or public IP address (with a dynamic address assigned by an ISP, for instance)—change, Back to My Mac updates the DNS record with those new details.

Consult Appendix A: Understand Network Terms for the background on how dynamic DNS and MobileMe work together with Back to My Mac.

Each Computer Sees the Others

When a computer with your MobileMe credentials has Back to My Mac active, that computer automatically retrieves a list of all other computers that have registered themselves with your MobileMe account and that have Back to My Mac enabled (**Figure 2**). (See Set Up Back to My Mac for more on the Shared list.)

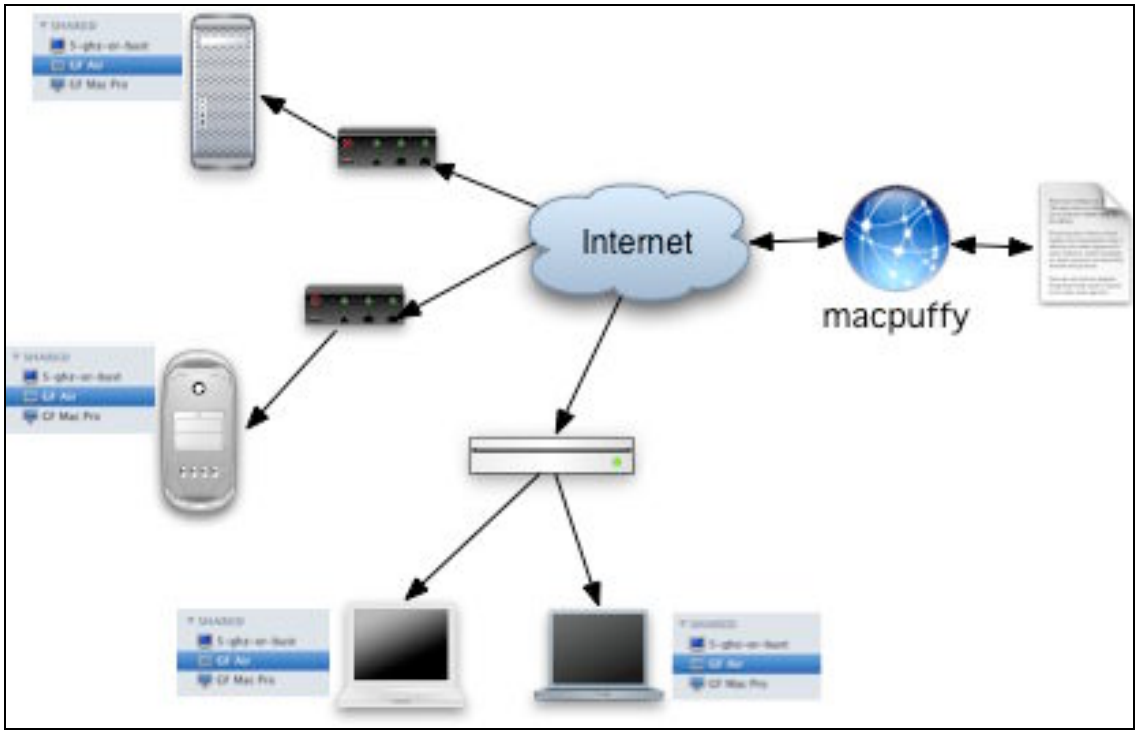


Figure 2: Each computer connected to Back to My Mac retrieves a list of all computers registered with the service through your MobileMe account.

Don't sync keychains! *While you can use MobileMe to sync your keychains (collections of passwords and certificates) to let multiple Macs under your control have the same data in their keychains, I don't recommend it. In my testing, unique information that should be stored on a single computer often winds up synchronized among multiple machines, confusing software as to the local identity. Further, in a recent test between two computers, MobileMe continuously deleted and added the same set of entries in an endless loop.*

If you have been synchronizing keychains without trouble, and have Back to My Mac problems, see *Don't Synchronize Keychains via MobileMe (p. 64)* *for how to set this up correctly.*

You can see icons for these active computers in the Shared portion of the Finder window sidebar, just as if they were on the local network with File Sharing (AFP or Samba) or Screen Sharing enabled.

Each active computer can retrieve details about how to reach all the other active computers. That means that computers that themselves turn out to be unreachable due to network configuration issues may still be able to connect to other Back to My Mac machines. For

example, even if a Mac lacks the router magic to allow inbound access, that Mac can still pull details from MobileMe that allow it to access another computer via Back to My Mac (assuming, of course, that the other computer is behind a properly configured router).

Short Delays in Updating Remote Systems

If one of your computers isn't reachable via Back to My Mac but *can* reach other machines, it may also experience a delay of up to 15 minutes in showing which other Back to My Mac computers are currently or no longer available. Back to My Mac gets that updated list immediately only if it's running on a computer with a publicly routable address or on a network using a router with automatic port mapping.

SECURITY

When you make a screen sharing or file sharing connection via Back to My Mac, you needn't worry about security: Apple protects Back to My Mac connections with a method of encryption that is well known for its security. When your Mac connects to MobileMe, Mac OS X retrieves (if it hasn't already) a certificate relating to sharing: the MobileMe Sharing Certificate. This cryptographic document, itself secured on your Mac by your account password, is found only on Macs running Leopard and Snow Leopard that have successfully logged in to MobileMe. The certificate is used to confirm your identity when you start services such as file sharing. A separate Back to My Mac session key is used as the basis of an encrypted tunnel between any two computers that connect via Back to My Mac (**Figure 3**).

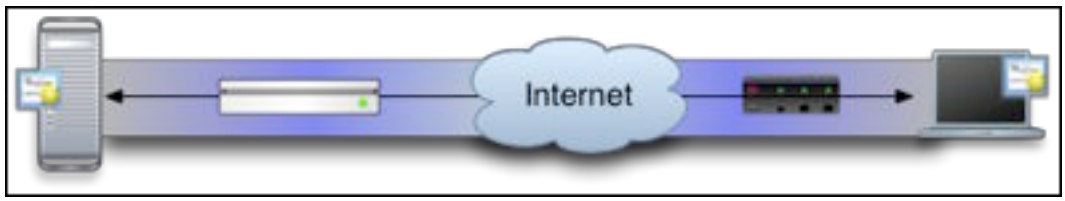


Figure 3: An encryption key shared between two computers allows for an encrypted tunnel across the Internet, protecting data at all points in between.

What's a Certificate?
A *certificate* is a combination of an encryption key, used to scramble data, with a digital signature that verifies the identity, integrity, and validity of the key. The signature can be separately verified based on information that's pre-installed in an operating system. Thus the certificate can't be compromised and replaced with a fake one without breaking the whole system.

What's a Tunnel?
A *tunnel* is a network connection between two endpoints within which all network traffic passes, and which is wrapped up with encryption. The tunnel metaphor implies, accurately, that you can access the tunnel's contents only from the ends, and since the two endpoints are secured, a tunnel is a safe connection. Tunnels can pass between two user computers (as with Back to My Mac), between a user computer and a server, or between two servers.

If your Mac is stolen! *If you believe that one of your computers with Back to My Mac running has been compromised—stolen, for example—Me.com lets you log in and revoke the associated certificate. This doesn't destroy existing sessions, but existing sessions will expire within hours, and it prevents new sessions from being created. For more on this process, see* *Revoke Certificates via Me.com*.

Warning! *Apple did a great job in securing both the initial connections between Back to My Mac computers and the subsequent data exchanges. But your MobileMe password and the physical security of your machine are still issues of concern. See* *Secure Back to My Mac* *for the full scoop.*

With the encrypted tunnel in place, the security for using sharing services over the Internet is the same as if the two computers were directly connected to each other with an Ethernet cable—except even more secure, because the encryption defeats any interception.

Mac OS X has another security element for service connections—such as file or screen sharing—made over Back to My Mac (or Bonjour). Instead of just handing over and confirming an accurate password, the operating system uses public-key cryptography to ensure that

both parties have the same password. In those cases, Leopard and Snow Leopard use a technology called Kerberos (invented at MIT and still developed there) to issue a *ticket,* which is a secure, time-limited stub for permission to use a given resource. The ticket is set by Apple to expire after 10 hours, at which point authentication must happen again. This Kerberos ticket makes it easy to reconnect to network resources that you've recently disconnected from or unmounted without the overhead of another round of authentication, but with a greater level of security than that of Mac OS X 10.4 Tiger and earlier versions of Mac OS X.

Configure Your Router or Gateway

Whether or not Back to My Mac can successfully provide access to a target Mac, and how much configuration you'll need to do, depends on your network router or gateway—the box that connects a target Mac and other computers to your network—and your ISP's network, the conduit from your broadband modem out to the larger Internet. (See "Router or Gateway, or Both?", below, for more explanation.)

In the ideal case, your gateway is directly connected to a broadband modem (or perhaps even integrated in the same box with it) and your ISP has a simple *topology*—network architecture. When you configure the gateway in this situation, you directly affect its remote accessibility over the public Internet. In the worst case, your ISP has multiple layers of NAT in place that essentially render Back to My Mac unworkable.

In this section, I explain how to configure common and generic routers; if you run into a problem, see the Router Disrupts Connection subsection in Troubleshooting, later, where I help you identify what's not working and discuss whether it can be overcome.

Router or Gateway, or Both?

I use the terms *router* and *gateway* interchangeably; both connect different networks, passing traffic between them. In homes and offices, the device sits between a broadband network and a local network, and figures out which data needs to pass between those networks. At one time, there was a more strict distinction between gateways (which translated among different network protocols) and routers (which connected different networks), but those distinctions have been erased. Home routers are usually called "gateways" for no particular reason except common usage.

DO YOU NEED TO CONFIGURE YOUR ROUTER?

You may not need to configure your router at all. Check this list to see if you need to configure your router or not:

- **All public IPs:** Every computer you're connecting has a publicly routable IP address (static or dynamic). This is a rare case. But if it's so, you needn't make any changes to your router.
- **No public IP on your router:** If your ISP doesn't offer either a publicly reachable IP address for your gateway or for a gateway that they provide to you, you can't use automatic or manual port mapping, and Back to My Mac will not work. Some ISPs map a private address they assign to your gateway with a public address on the Internet—Qwest, for one, does that—and that works, too.

  If you don't have a publicly reachable IP address, no amount of port mapping will work for you with Back to My Mac. I suggest looking at a solution from LogMeIn for remote screen sharing that works around this constraint; see Appendix B: Other Remote Access Solutions.
- **Try it first and see if it works:**
  - If, at the end of the setup process, you can access each computer from the other—with any computer being local and another remote—you needn't make any router changes.
  - If you can't access other computers, or the MobileMe system preference pane displays a yellow or red dot with a trouble-shooting message, read on (and consult MobileMe Preference Pane Troubleshooting Messages, p. 60).

However, if any of your Macs are on a network that uses NAT, you will almost certainly have to make a few changes to your setup.

DETERMINE WHICH ADVICE TO FOLLOW

To proceed, determine which of the following descriptions matches your target Mac's router and then follow the corresponding cross-reference. You may have different brands or models of routers at the various places where your computers are located, so you may need to follow separate configuration steps on each network where you have a target Mac.

In each of the following cases, the router allows multiple computers, using private addressing, to be reachable for remote access through automatic port assignment:

- An Apple AirPort Extreme Base Station, AirPort Express Base Station, or Time Capsule: A single checkbox enables NAT-PMP on these routers. See Set Up an AirPort Base Station, next page.

  Warning! *Pre-2003 AirPort Base Stations don't offer NAT-PMP.*

- Any modern Linksys router: Any Linksys router that's not labeled an "access point" sold in the last 3 to 5 years is almost certain to have UPnP built in. Refer to Set Up a Linksys Router with UPnP (p. 29).

- Any other router that has UPnP built in: Read Set Up Non-Linksys Routers with UPNP (p. 31). You need to consult your manual to determine whether your router offers UPnP.

If none of those three cases matches, you cannot make Back to My Mac work with your current network setup, because it requires either a publicly reachable address on each computer or NAT-PMP or UPnP. To remedy the situation, you could ask your Internet service provider if they offer a router with UPnP support; change your router if it's one you bought separately; or look into a different ISP that can give you either automatic port mapping or a range of publicly reachable addresses.

Note: In my case, I changed my ISP when I found I could get neither the broadband speed nor the remote access I needed.

SET UP AN AIRPORT BASE STATION

Apple makes it easy to use Back to My Mac (and iChat) with 2007-and-later Apple hardware, naturally. But NAT- PMP is also available for 2003 through 2006 model Apple base stations.

To turn on NAT-PMP, follow these steps:

1. Launch AirPort Utility (found in Applications/Utilities/).
2. From the list at the left, select your base station. Then choose Base Station > Manual Setup.
3. Click the Internet icon in the toolbar, and in the resulting pane, click the NAT button. Then check the Enable NAT Port Mapping Protocol box (**Figure 4**). (If you don't have a NAT button, see the next page for help.)

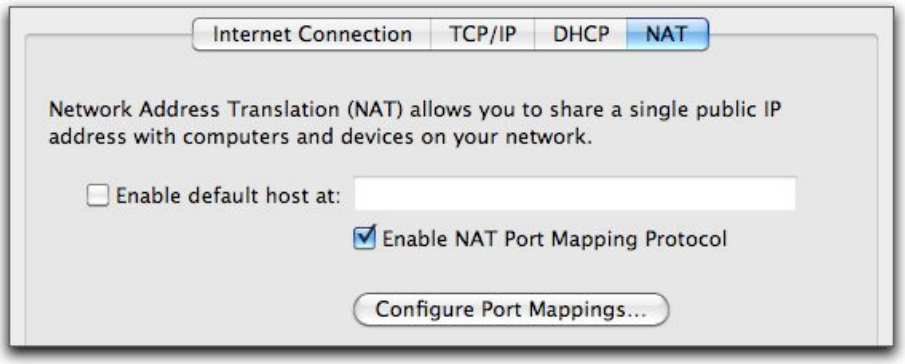


Figure 4: Turn on NAT-PMP with a single click.

4. Click Update.

With NAT-PMP configured and your AirPort base station ready to go, you can proceed to the next section, Set Up Back to My Mac.

If the NAT Button Is Missing

If you don't see a NAT sub-pane in the Internet pane, be sure that you're using NAT. In the Internet pane, click the Internet Connection button to open the Internet Connection sub-pane and ensure that Connection Sharing is set to Share a Public IP Address (**Figure 5**).

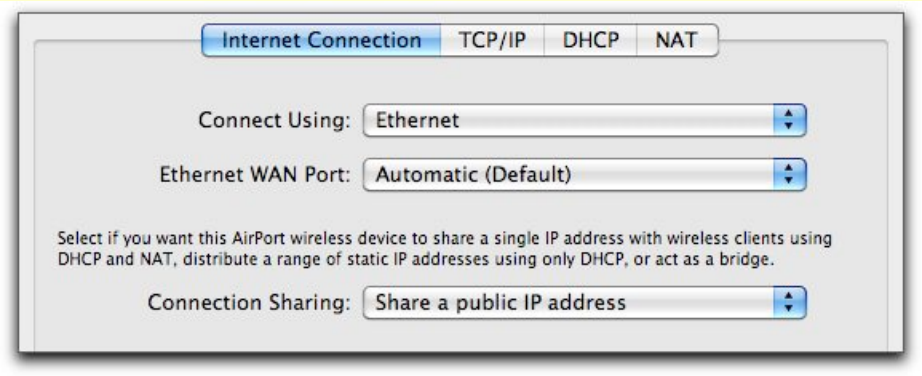


Figure 5: To use NAT-PMP, make sure that Connection Sharing is set to Share a Public IP Address.

SET UP A LINKSYS ROUTER WITH UPNP

Except for certain router-specific features, most Linksys routers have similar configuration interfaces. This means that the UPnP settings should be easy to find and turn on, regardless of which Linksys router you are working with.

The first task is to connect to your Linksys router. Follow these steps:

1. In any browser window's Location field, enter the Linksys router's local network IP address, if you know it. If you don't know the address, try 192.168.1.1 or 192.168.2.1, which are typically what the Linksys presets (also see the tip, next paragraph). Enter the IP address in this format: http://192.168.1.1/

Finding the IP address: *If neither of the typical preset IP addresses brings up a request for a password or a configuration window, you may have an older or non-standard router, or one for which the IP address has been changed. You can find the router's address by opening the Network System Preference pane and selecting your network's active connection in the list of network interfaces to the left. As long as you're using DHCP, the router's address appears next to the word Router on the main screen for Ethernet, or, after you click the Advanced button, on the TCP/IP screen for AirPort. Enter that address in your browser, and you should be in business.*

2. When prompted, enter the router's password and click OK. If you haven't changed the password, it will be admin. The user name can be left blank for older models; newer models require admin entered in both the user and password fields (again, assuming you haven't changed the latter).

Tip: Always change the administrative password that you use for making configuration changes to your router. Standard passwords such as admin and public are well known, and havoc can be wreaked if the wrong person accesses your router.

3. On most Linksys routers, you now select the Administration tab in the top navigation window, and then click the Management link that's one of several links beneath Administration.

Can't find the tab? *If you can't find this tab and link on your router, visit http://www.linksys.com/, click the Support link, and follow the prompts to download the manual for your router. Search for "UPNP" in the PDF, and follow those instructions.*

4. Next to the UPnP label, click the Enable button if it's not already selected, and click Save Settings. This should restart the router with the UPnP enabled.

With your Linksys router configured, you can skip to Set Up Back to My Mac, two pages ahead.

SET UP NON-LINKSYS ROUTERS WITH UPNP

The location of the checkbox or settings for turning on UPnP is likely slightly different in each router-configuration program, so I can't give you exact advice on how to configure every possible router. I suggest that you download the manual for the router from the maker's Web site, search for UPnP, and follow the instructions. (I know that sounds obvious, but it's worth stating that manuals can be useful: some folks spend hours looking for a setting that doesn't exist or is named incorrectly when it's clearly noted in the manual.)

With your UPnP router configured, proceed to Set Up Back to My Mac, next page.

Tip: If you enable UPnP on a router, and you're having trouble, make sure you have the latest firmware (internal software) for the router. Go the manufacturer's Web site, click the Support link, and navigate through to find downloads for your model. Some downloads may require Windows to install, unfortunately.

Set Up Back to My Mac

In the previous section, Configure Your Router or Gateway, I talked about how to set up your routers so that Back to My Mac connections can be made between a local Mac that you're sitting at and a remote Mac that you've set up. I suggest that you work through that section (or at least skim it) before you follow the steps here.

In this section, I assume that you have all Requirements for Back to My Mac in place.

TURN ON BACK TO MY MAC

You can enable Back to My Mac in the MobileMe preference pane:

1. In System Preferences, select the MobileMe preference pane.
2. Enter your account name in the Member Name field and password in the Password field.
3. Click Sign In:
   - If the login fails, visit http://www.me.com/ and confirm that your password is correct. If you can't log in there, use the Forgot Password link on the login screen to reset your password, and then try clicking Sign In again.
   - If the login succeeds, you'll see "Signed into MobileMe" and your account status (**Figure 6**).
4. Click the Back to My Mac button.
5. If you see the status message "Back to My Mac: Off" in bold below the bar of buttons, click the Start button. The message changes from "Off" to "On."

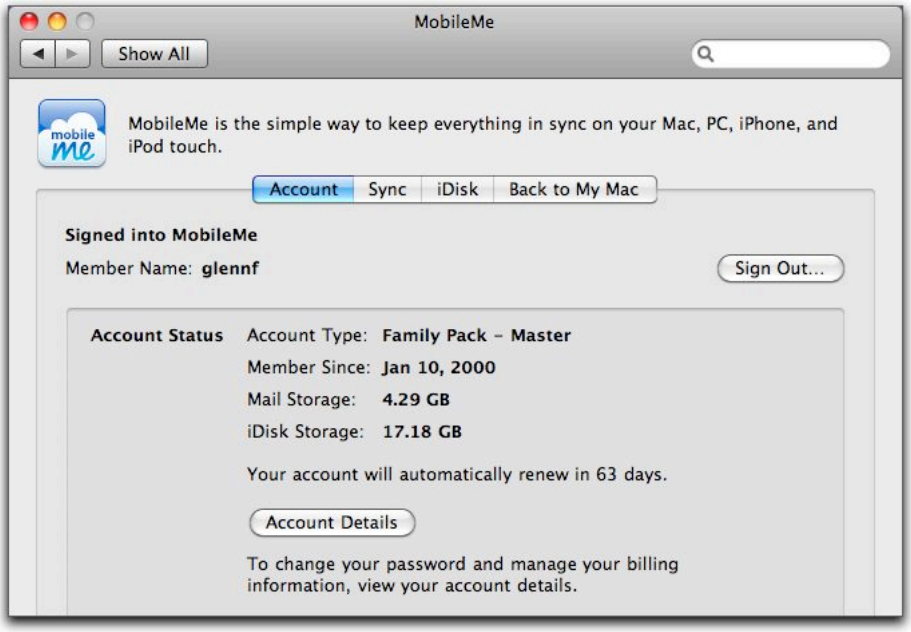


Figure 6: A successful login shows your account status and a Sign Out button.

6. Evaluate the status message (added in Mac OS X 10.5.3):

   - If you see a green dot (**Figure 7**), skip to the next step.

Figure 7: The Back to My Mac sub-pane lets you turn remote access on and off.

   - If you see a yellow or red dot, read MobileMe Preference Pane Troubleshooting Messages (p. 60) to figure out what's wrong with your attempt to start Back to My Mac.

7. Click the Open Sharing Preferences button to switch to the Sharing preference pane. In that pane's Computer Name field, name your computer something distinctive; whatever you enter here is the name that will appear in the Shared list in the Finder-window sidebar on your other Back to My Mac–enabled Macs (and on other locally-connected Macs).

Warning! *Make sure the Computer Name and the associated Local Hostname used for Bonjour aren't the same for any two computers in your Back to My Mac set. (Change the Local Hostname by clicking the Edit button beneath the Computer Name field.) Apple warns that you might not be able to connect from one such computer to another if either the Computer Name or the Local Hostname are the same.*

8. Verify that your other Back to My Mac–enabled computers appear in the Shared list in the sidebar of Finder windows (**Figure 8**); local computers will also be in the list.

Figure 8: The sidebar's Shared list shows locally accessible networked computers as well as Back to My Mac systems. In this case, *Glennf Mac Pro* is a remote Mac listed via Back to My Mac, while *Rex Ben Lynn Glenn* and *Lynn Warner's Computer* are systems on the same network as the computer on which this view was captured.

If you don't see your Back to My Mac machines: *This could be because your sidebar isn't configured to show them—see* *Displaying Shared Computers in the Sidebar, next page,* *or it could be because you are connected to more than seven servers—read the next paragraph.*

You can also view your other Back to My Mac computers in a list of servers in a Finder window by choosing Go > Network. When using List view, the Kind column identifies each server by platform, but labels Back to My Mac machines with My Mac (**Figure 9**). This list is also useful when you have more than seven computers available in the Shared list, as only the first seven are displayed in the Shared list in the sidebar. (Mac OS X adds an All link below the first seven machines which, when clicked, brings up the server view in **Figure 9**.)

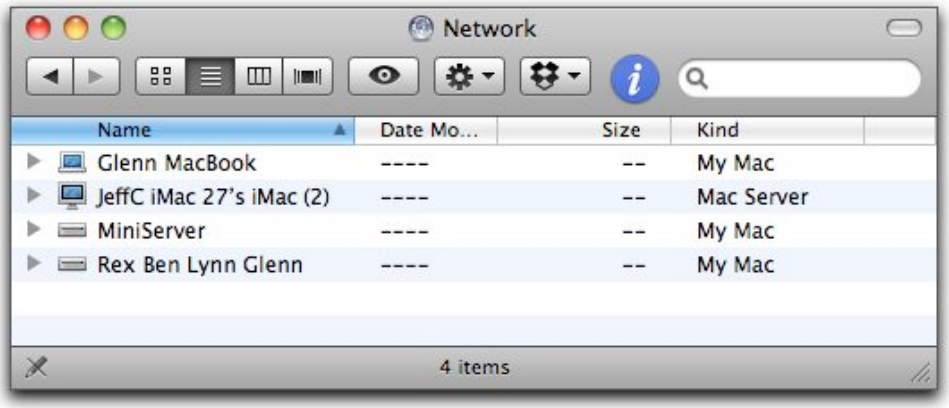


Figure 9: The server list in a Finder window labels servers by kind.

Computers that crash or are removed from a network unexpectedly—for example, if an AirPort connection disappears or a network cable is unplugged—aren't immediately removed from the Back to My Mac list. There can be a lengthy delay before they disappear.

Mac OS X alerts you to problems that might cause a computer to be remotely unreachable. See MobileMe Preference Pane Troubleshooting Messages (p. 60).

Displaying Shared Computers in the Sidebar

If you don't see your Back to My Mac counterpart computers in the Shared list, you (or someone else) may have disabled their display. To enable the display:

1. Click the Finder icon in the Dock.
2. Choose Finder > Preferences.
3. Click the Sidebar icon.
4. Check the Back to My Mac box.

SET UP FILE SHARING

To gain remote access to files on this Mac from the other Macs in your Back to My Mac "network," you need to set up file sharing; you set up file sharing within Back to My Mac the same way you set it up for local networks. Any volume that is accessible via Bonjour locally or by an IP address on the local or a remote network is also reachable via Back to My Mac.

Follow these steps to set up file sharing:

1. Open System Preferences, and select the Sharing preference pane.
2. At the left, select the File Sharing service (**Figure 10**).

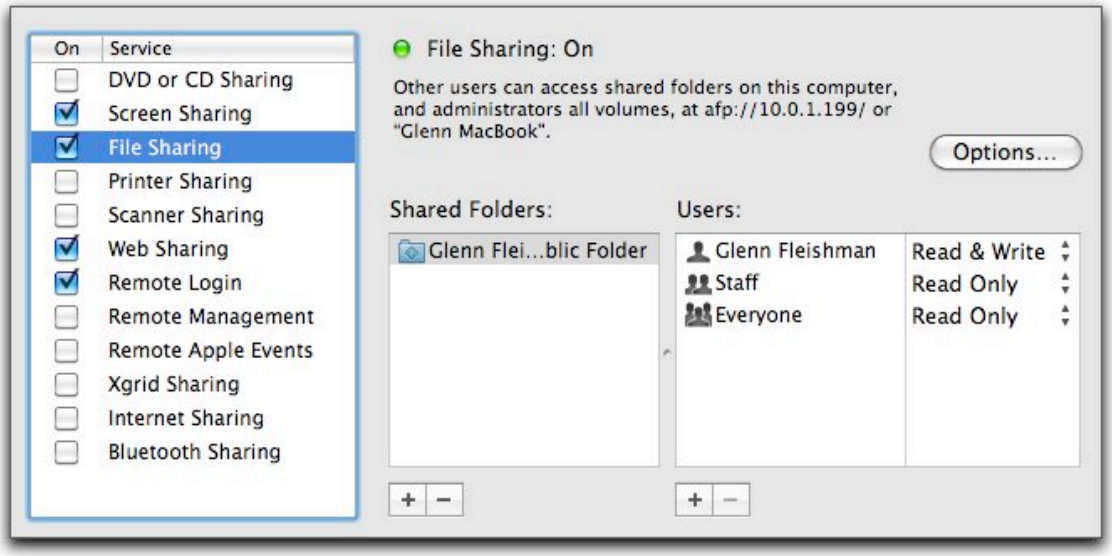


Figure 10: File Sharing allows you to choose which folders or volumes to share with which users and groups, and how they can modify or view the contents of what's shared.

3. For each folder or volume you want to share:

    a. Drag the item from a Finder window into the Shared Folders list, or click that list's + button to navigate to the item, select it, and then click Add.

    b. With the item selected in the Shared Folders list, configure the Users list to set which users have access to the item: click the list's + button and then select users from the list that appears; remove one by selecting it and clicking the − button.

    To enable remote access for file sharing via Back to My Mac, the users list must include one (or both) of the following:

    - The name of the Mac OS X user account in which you've configured Back to My Mac.
    - The Administrators group, but only if the user account in which you've configured Back to My Mac is an administrative account; you can see if administrative access is enabled in the Accounts System Preferences pane.

c. Use the pop-up menu to the right of a user or group name to choose Read & Write access privileges for that item.

4. Click Options, check Share Files and Folders Using AFP (which stands for Apple Filing Protocol), and click Done.

You're finished, and you should be able to access the folder or volume you've shared from the Macs that are connected via Back to My Mac.

Note: Samba isn't supported over Back to My Mac; FTP works but requires special client software.

Tip: If you need more than the plain-vanilla details supplied in these steps, check out my book *Take Control of Sharing Files in Snow Leopard*. It provides vastly more detail about file sharing. For most purposes with Back to My Mac, you're sharing files among computers you control, and won't need many complicated options for access—because you probably trust yourself.

SET UP SCREEN SHARING

The steps for setting up screen sharing with Back to My Mac are laughably simple:

1. Open System Preferences, and select the Sharing preference pane.
2. Check the box next to Screen Sharing.

None of the other options for the Screen Sharing service make sense with Back to My Mac, because you're connecting as yourself and using Apple's technology.

Access Base Station Hard Drives

All 2007 and later models of AirPort Extreme and Time Capsule base stations allow remote hard-disk access over Back to My Mac.

By entering, via AirPort Utility, one or more MobileMe account/password combinations for a given base station, any internal (Time Capsule) or external (AirPort or Time Capsule) hard drive can be reached from any computer, local or over the Internet, that matches any of the base station's credentials.

Before Apple added this option to Back to My Mac, Apple base stations that supported external hard drives, as well as Time Capsule models, could share those drives over the Internet, but only if you were willing to expose the drives such that anyone could attempt to access them.

Two models: *This feature works with any model of the AirPort Extreme Base Station (2007 or later) and Time Capsule (2008 or later). Any drives connected via USB, as well as the internal drive in the Time Capsule, can be reached in this manner. The feature is not available with any AirPort Express, which does not allow a drive to be connected via its USB port.*

Tip: Back to My Mac also lets you remotely administer any Apple base station, including the AirPort Express, released in 2007 or later. Remote base stations appear in the base station list in AirPort Utility on any computer in a MobileMe set.

Back to My Mac lets you layer the security in this system with the simplicity of accessing a drive via Bonjour.

To get started, follow these steps:

1. Launch AirPort Utility (found in the /Applications/Utilities folder).

2. Select your base station in the list at left, and then click Manual Setup at the bottom of the screen (or press Command-L).
3. Click the Advanced icon, and then the MobileMe button.
4. Depending on the firmware release of your base station, you can either enter just one MobileMe account or you can enter one or more MobileMe accounts in this pane:

Which version? *In AirPort Utility, select your base station, and the firmware version is shown in the pane at the right, such as 7.4.2 or 7.5.1.*

Why two versions? *Apple shipped new models of the AirPort Extreme Base Station and Time Capsule in October 2009 with firmware 7.5.0. Bafflingly, as I write this three months later, Apple hasn't released firmware 7.5.1 as expected for all 802.11n AirPort Extreme and Time Capsule base stations released starting in 2007. I have all indications that Apple will provide this update, just as the firm has for other similar features that don't rely on hardware updates for that range of models.*

   - **Firmware 7.4.2:** Enter a MobileMe user name and password.
   - **Firmware 7.5.0 or later:** Click the plus sign, enter a MobileMe user name and password, and click OK.
5. Click Update to restart the base station with the MobileMe account(s) active.

After the base station restarts, any hard drives it hosts will appear in the Shared section of Finder window sidebars on any computer with the same MobileMe login information that has been assigned to the base station.

How you remove an account from your base station depends on the firmware release:

- **Firmware 7.4.2:** Delete the contents of the user name and password fields, then click Update.
- **Firmware 7.5.0 or later:** Select the MobileMe account and click the minus sign. Then click Update.

Connect to a Back to My Mac System

Once everything is properly configured, it's just as easy to connect to a Mac via Back to My Mac as it is to connect via Apple's Bonjour technology to one that's sharing resources on a local network. In fact, on a local network, the only difference between a Bonjour-advertised computer and one that's using Back to My Mac is that you needn't enter a password for Back to My Mac.

To connect via Back to My Mac to a target Mac, follow these steps:

1. Open a Finder window, and from the sidebar's Shared list, select the computer.

   Can't find the target Mac in the Shared list? *See Step 8, p. 34, in "Turn On Back to My Mac."*

   The Finder window displays "Connecting" in a gray bar, and, in the upper right corner one or two buttons, depending on whether you have enabled File Sharing, Screen Sharing, or both (**Figure 11**).

2. Now:

   - **To connect via Screen Sharing:** Click the Share Screen button. You have full control of the remote system, which fills the Screen Sharing application window.
   - **To connect to shared volumes:** No further action should be needed to connect to shared remote volumes, even though the Connect As button appears in the upper-right corner. When you select the server, all its shared volumes appear after a moment. Double click any volume on the remote system to mount that volume, after which you can copy files to and from it based on the permissions you set while following the steps in Set Up File Sharing.

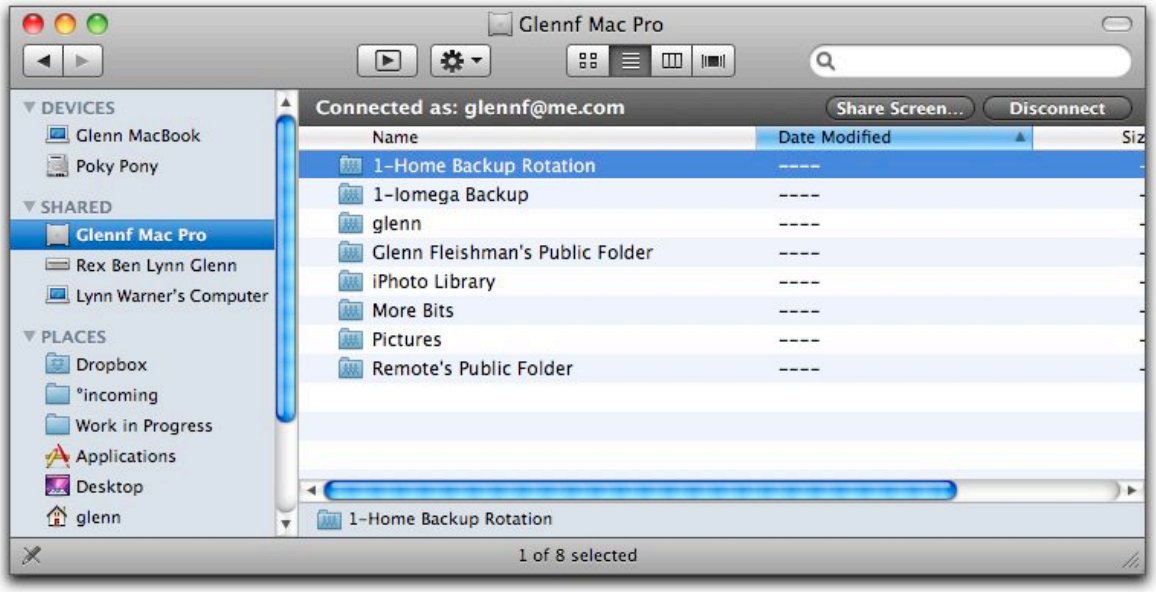


Figure 11: After I selected Glennf Mac Pro in the Shared list, my Mac connected to that computer and displayed all the *shares*—shared folders and volumes—available from Glennf Mac Pro.

Notice that the gray bar near the top of the window says that I'm connected as glennf@me.com—my MobileMe address. But that's not an account on the remote machine; that's just Apple's way to confirm that I'm using Back to My Mac. (Mac OS X shows the MobileMe address if your Mac OS X account information is identical on the two computers.) Mac OS X can also retrieve login information you stored in the keychain, or prompt you to log in.

If you can't connect successfully, skip ahead to Troubleshooting. Otherwise, move on to the next section where you can make sure that you've set up an appropriate level of security for all your Back to My Mac computers.

Note: Because you're ostensibly the owner of all the Macs that you've set to the same MobileMe account, as long as you have identical Mac OS X user account logins on these computers, file and screen sharing will now bypass the normal login protection and instead use a certificate to validate your identity (described in Security, earlier).

Secure Back to My Mac

Back to My Mac is unusual in that it's an extremely secure service, designed with encryption, identity, and validation in mind from the get-go. Most services of this kind start unprotected—and without much foresight about these issues—and then layer them up later.

But there are two serious worries about MobileMe, both more related to you than to the underlying technology: picking a good password and keeping it secret, and Physical Security for a Back to My Mac Computer. I cover these concerns in this section.

MOBILEME PASSWORDS AS A WEAK LINK

While all the elements of MobileMe connections are secure, your MobileMe password is plain text that you enter directly. In contrast, many remote-access systems offer the capability to use a digital certificate or two-factor authentication (where a password is combined with a physical device, usually the size of a key fob, that generates a unique code). But Back to My Mac is designed for everyone to use, so it's simpler, and that puts you at more risk. If someone possesses your MobileMe password, no matter where they are in the world, they can connect to any of your Back to My Mac systems remotely without you even knowing about it—there's no monitoring system for Back to My Mac that lets you know if other computers are currently connected to yours or what they're up to, nor is there a straightforward log of Back to My Mac connections or actions by remote users. (Although Screen Sharing, when in use, adds a special menu in the menu bar.)

The three key pieces of advice for a MobileMe password are:

- **Choose a good one:** Don't use your name, a family member's name, a pet's name, your street's name, and so forth. A *strong* password—meaning one that would be difficult to guess—has a combination of letters (both upper and lower case), numbers, and punctuation. So, since my dad's name is Charlie, `charlie` would be a bad password. But `%cHArl5!6` would be essentially unbreakable.

- **Don't write it down in an obvious way in an obvious place:** Unless you live alone and never have guests, keeping your password written down where someone else can come across it is a bad idea. It's not about trust as much as opportunity. I'm not accusing your family or friends of being thieves, but the one time a friend brings a friend over, or your daughter's boyfriend spots the password—there goes your personal security (and credit rating?) out the door. My editor, Tonya, uses a simple cipher so she can leave her passwords out, all *Purloined Letter*-like, without giving away anything if they're seen or lifted by others.
- **Don't share it:** Keep the password to yourself and to only those who may need access if you're not around—or incapacitated! If you give access to someone who is less trustworthy than your inner circle, change the password after they've finished whatever they need to do.
- **Change it occasionally:** Part of password security is not using the same password indefinitely. (If you change your MobileMe password via the service's Web site, you need to open the MobileMe preference pane, click Sign Out, and then sign back in with your new password.)

Tip: For much more advice on passwords, read Joe Kissell's in-depth book, *Take Control of Passwords in Mac OS X*.

PHYSICAL SECURITY FOR A BACK TO MY MAC COMPUTER

I've never considered physical access to my computers a problem because I don't have any desktop computers in places where others I don't know can gain access, and I keep almost no information on my laptop that I'm worried about losing if it were stolen.

But Back to My Mac ups the ante, because anyone who can gain access to a Mac OS X admin account on any computer on which the service is enabled can gain access to not just the files on that computer, but also to files on—and the screen of—all other computers you've enabled Back to My Mac on. If your laptop is stolen, that becomes an issue. It's

also a concern if you share an office and someone who shouldn't sits down in front of your Mac.

In many situations, this means you need to secure the computer against physical access. Fortunately, Mac OS X has a host of methods to prevent unwanted access without disabling your use.

To fully protect your computer, you need to change four settings. I cover each in turn, next.

Track Your Stolen Mac

Most advice ahead is applicable for protecting and securing your Mac generally, not just for Back to My Mac. If you're concerned about tracking your Mac if it were to be stolen, check out one of several theft-monitoring and recovery-assistance programs:

- I use Orbicule's Undercover, which handles reports of theft through a central monitoring server. http://www.orbicule.com/undercover/mac/ ($49 for one computer or $59 for a family pack of five, no recurring fee)
- I also recommend GadgetTrak's MacTrak for Mac OS X, which puts all the information gathered into your hands, so you can work directly with law enforcement. http://www.gadgettrak.com/products/mac/ ($24.95 for 1 year or $59.95 for 3 years, per computer)

Both services can snap pictures via a Web cam, capture IP-address information, and use the Skyhook Wireless Wi-Fi positioning system to come up with rough geographic coordinates.

You might also like to read a *TidBITS* article that I wrote, "Help! I'm Being Held Captive, and All I Have Is a Wi-Fi Network!," at http://db.tidbits.com/article/9627, as well as subsequent updates referenced in the Related Articles sidebar.

Keychain and Screen Lock

By locking your keychain on the remote Mac, you prevent someone from accessing that system or its stored passwords. Apple suggests that before you disconnect from a Screen Sharing session via Back to My Mac, that you enable the Keychain lock on the remote machine.

Warning! *Locking your keychain makes sense only for computers under your control that someone else might be able to gain physical access to when you're not connected for remote screen sharing. However, locking your keychain is not necessary after a session with a headless server in a locked server room, nor when you're done helping your mother with remote technical support.*

To enable the lock, follow these steps:

1. On the remote Mac, launch Keychain Access (found in Applications/Utilities/).

2. Choose Keychain Access > Preferences, and check Show Status in Menu Bar.

   The Keychain status menu appears in the menu bar (**Figure 12**).

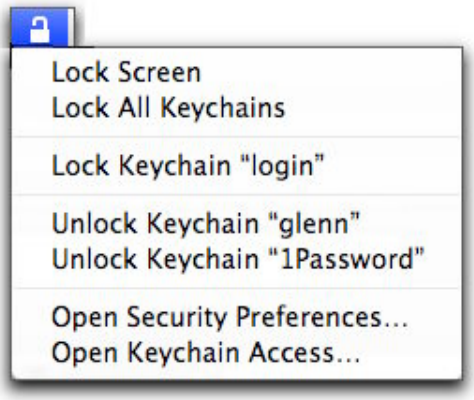


Figure 12: The Lock menu allows you to prevent access to items in a computer's keychain or keychains when you're not sitting in front of that computer.

3. Before you're done with a remote screen-sharing session, choose Lock All Keychains from the Keychain menu on the remote Mac. You can then choose Lock Screen to disable local access.

This locks out any users who are in front of that computer unless they have that account's password or an administrative account; it also locks out any remote access from someone who might be using another Back to My Mac linked machine without your permission.

Screen Saver and Sleep Lock Plus More

You can lock your computer's screen when it's unattended or put to sleep:

1. Open System Preferences, and select the Security pane.
2. In the General sub-pane, check "Require password *time period* after sleep or screen saver begins." Choose a reasonable period based on how long you typically are away from your computer for brief stints; or Immediately for instant protection.
3. If you want to further restrict access, click the Lock () button and enter an administrative password. For example, you can force a logout after a period of inactivity and not allow automatic login at startup (see next item).

You will now have to enter your password in order to use your Mac after it's been sleeping or running the screensaver. More important, so will everyone else, which means someone trying to access your system for the wrong reasons will have to work a bit harder to break in.

Don't Store Password for Login

If you allow automatic login, someone could access your account and settings—even if you've enabled screen-saver and sleep lock—by force-restarting the computer (using the power button or by cycling power). If you're the only user of your Mac, it's likely that you've set your Mac up for automatic login—in fact, it's the default Mac OS X configuration when there's only a single account.

Follow these steps to disable automatic login:

1. Open System Preferences, and select Accounts.
2. Click the Lock () button in the lower left, and enter your administrative user name and password.
3. Click Login Options.
4. From the Automatic Login pop-up menu, choose Off.

You will now have to enter your password during startup. Of course, everyone else who is trying to casually break into your Mac will also have to enter a password, and this extra hurdle should help keep honest people honest.

Firmware Password

This last change sounds a bit nutty, but bear with me. Because anyone with a Mac OS X installation disc and physical access to a Mac can boot the computer and change the main administrative password, if you're especially concerned about someone gaining physical access to your computer, you need to set a firmware password, too.

With the firmware password set, your Mac disables a host of typical administrative and startup options. You can't, for instance, hold down any of the special keyboard keys to boot from a separate disc or reset parameter RAM. (Apple has a full list of what behavior the firmware password restricts at http://support.apple.com/kb/HT1352.)

Warning! *Note that if you forget a firmware password or if you enter it incorrectly twice, you'll be restricted from changing your startup volume, upgrading your operating system, and other activities.*

The firmware password does *not* prevent a Mac from being restarted by someone who has physical access. However, that person can't prevent the Mac from using the startup disk you've previously selected.

Warning! *Fellow Take Control author Joe Kissell told me that firmware password security is ignored if someone changes the amount of RAM in a computer and then resets the PRAM on the next restart. A sophisticated user who wants to gain access to your system could thus open up the Mac, remove, add, or swap RAM, and then restart to bypass this password.*

If you need particularly high security or have a particularly high level of paranoia, your solution could be to use a lock on the security slot on a desktop machine; a padlock works just fine, or you can get a keyed or numbered security lock that anchors a computer. Laptops can't be easily protected from memory swaps, however, but you're also less likely to leave a laptop where someone could crack it open (and if you do leave a laptop unsecured, someone could just walk away with the laptop and then remove the hard drive for access).

Accessing Firmware Password Utility

There are two ways to launch the Firmware Password Utility on a Mac running Leopard or Snow Leopard:

- Boot your computer from the installation DVD.
- Copy the Firmware Password Utility from the DVD to the Mac. If you use this method, you won't have to find your DVD the next time that you want to run Firmware Password Utility.

I cover each option next.

Boot method:

This method must be followed each time you want to use the utility.

1. Insert the Leopard or Snow Leopard installation DVD.
2. From the DVD's window, double-click Install Mac OS X (for a Snow Leopard disc) or Install Mac OS X and Bundled Software (for a Leopard disc).
3. *Snow Leopard only:* Click the Utilities button in the lower-left corner of the window that appears.
4. Click the Restart button.
5. Enter your administrative password.
6. When the computer restarts, select English as the installation language in order to proceed.
7. From the Utilities menu, choose Firmware Password Utility.

Copy method:

1. Insert the Leopard or Snow Leopard installation DVD.
2. In the Finder, choose Go > Go To Folder to open the Go To Folder dialog.
3. Type /Volumes/Mac OS X Install DVD/Applications/Utilities

   In the Finder, the hidden Utilities folder on the installation disc appears.
4. Copy Firmware Password Utility to your /Applications/Utilities folder.

5. Launch Firmware Password Utility from your hard drive.

Note that you need to copy the software only once; subsequently, just launch it from /Applications/Utilities.

Using Firmware Password Utility

With the program launched either from the disc or from your hard drive, follow these steps:

1. Click the New button.
2. Check the "Require password" box, and enter your desired firmware password in both the Password and the Verify field (**Figure 13**).

Figure 13: This is your last chance to get it right. Once you change the password, if you later forget it, or, if you enter it incorrectly twice, you'll be restricted from changing your startup volume, upgrading your operating system, and other activities.

3. Because forgetting this password could cause you to incur significant expense and trouble, you may wish to record it in some way, however cryptic or protected, while it is still fresh in your mind.
4. Click OK.
5. When prompted, enter an administrative account name and password. Click OK.

   If the change succeeds, Mac OS X informs you with a dialog that says the settings will be active after the next restart (**Figure 14**).

Figure 14: Your computer is now protected from restarting from another volume.

6. Click Quit.

With those changes in place, you and your computer can rest safely, knowing that an intruder can only restart the computer, not take control of it.

Now that you've set up a good MobileMe password and considered the physical security of your Back to My Mac computers, keep reading to learn how to remove all traces of your Back to My Mac usage from a computer. This might be important if you've used Back to My Mac on a public computer or a borrowed machine, or if your computer were stolen.

Erase Back to My Mac's Traces

You may want to remove all traces of your use of Back to My Mac on a computers where you've enabled it to avoid other people having the slightest chance of remote access to your other computer or computers. This could be important if you've borrowed a computer or used a shared computer in a lab or café. I recommend the procedures in this section in order of increasing paranoia; the farther you go, the less likely anyone could gain access from that computer to other Macs that you operate.

Don't Read This Tip to Criminals

In May 2008, an Apple Store employee in White Plains, New York, recovered her stolen Mac laptop with some help from Back to My Mac. A few days after her laptop was stolen, a friend spotted her on iChat, and called to congratulate her on recovering her laptop. Since she had not, and her appearance on iChat meant that her Mac was fired up and logged into MobileMe, she had an idea. She used Back to My Mac screen sharing from another Mac to grab an iSight photo of one of the alleged thieves, and used file sharing to transfer images apparently of the other alleged burglar. The two men were identified by friends of one of her roommates, and were subsequently found with the stolen gear and charged.

The thieves should have read this section, so please—keep it away from them.

Tip: For a clean approach to using Back to My Mac from someone else's Macintosh, use the Guest account. All of your settings are wiped out when you log out of the account, and you needn't follow the procedures in this section. Just choose > Log Out.

Warning! *A bug in 10.6.0 and 10.6.1 can delete regular user accounts when someone logs in to and out of the Guest account! Be sure to update to Mac OS X 10.6.2 or later, which fixes the problem.*

LOG OUT OF MOBILEME

To log out of MobileMe, open System Preferences, select MobileMe, and click Sign Out. This signs this computer out of Back to My Mac and the preference pane forgets your MobileMe password.

DELETE RELATED CERTIFICATES AND PASSWORDS

To delete all certificates and passwords related to Back to My Mac, follow these steps:

1. Launch Keychain Access (located in /Applications/Utilities/), and examine the list of entries. You'll likely be surprised at how many items are tagged with your account name (**Figure 15**).

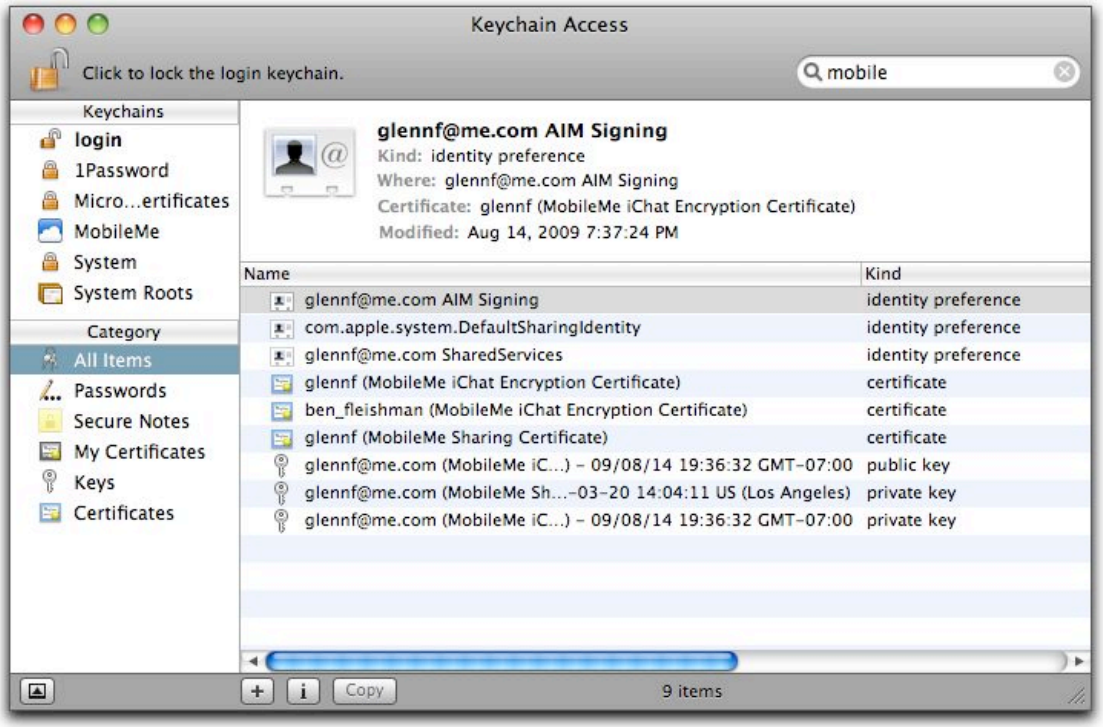


Figure 15: In this screenshot, you can see the plethora of items tagged with something related to MobileMe. Deleting these relevant items on a Mac I'm visiting provides additional peace of mind.

2. Select all of the following entries and delete them. You can select each item individually and then Press Delete (or choose Edit > Delete). Or, you can Command-click multiple items to select them together and then press Delete:

Warning! *Take care when deleting items, because your MobileMe account name could be the same as the name of other important items in the keychain. (Your MobileMe account name is the part before @me.com, like the glennf in glennf@me.com). If you delete an item for another program or a subsystem of Mac OS X that uses the same account name, you might have to re-enter a password when launching a program or using a service. Or, it could be even worse: you might have to reinstall a certificate or go through more hoops to restore access. If you're not using your own Mac OS X user account, then take extra care to avoid deleting entries needed for access to that account. On the flip side, if you're the only user with that name and you aren't using your own Mac, there's likely no good reason to leave anything behind with your name on it.*

- A certificate with your MobileMe account name in the Name field. To quickly find these, select My Certificates from the Category option in the left column.
- Any item that says MobileMe or (for legacy reasons) .Mac in its description. These are tedious to find if you have many entries, as they are not organized or labeled consistently.
- Your MobileMe account's stored password.

Other users most likely can't use these certificates and passwords to their advantage—except the MobileMe password entry. If you've stored that entry in the keychain and not deleted it, then the owner of the account you just used would be able to decrypt it and access your MobileMe password.

REVOKE CERTIFICATES VIA ME.COM

A few months after launching MobileMe, Apple provided access to a powerful certificate-revocation security feature for iChat and Back to My Mac. You'll want to use this feature if your computer is compromised or stolen—or if you're security-minded enough that you want to update your certificate on demand.

The reason for this revocation feature is that Back to My Mac and iChat both use certificates as a tool to create secure connections. Over those secure connections Bonjour sessions flow with Back to My Mac just as

if you were on the same local network. (With iChat, text and other chats are encrypted to prevent snooping.)

Thus, if someone has one of your computers, and it's logged in to your MobileMe account with Back to My Mac active, that person may have access to shared services on your other Back to My Mac computers. For instance, the compromised computer could mount shared drives and copy files, or remotely control a system via screen sharing.

This means that if one of your Back to My Mac computers is stolen or lost, you should immediately change your MobileMe password via the Me.com site; revoke the certificate used for Back to My Mac; and then log out and back in to MobileMe on each computer. This prevents the missing computer from gaining access to your other machines.

Tip: You could be brave and try to connect to the remote Mac via Screen Sharing using Back to My Mac, and then snap pictures or transfer files first, like the intrepid Apple Store employee noted at the start of this section, in Don't Read This Tip to Criminals.

Here are the complete steps for revoking your Back to My Mac certificate:

1. Log in to MobileMe at Me.com and change your password.
2. In the Sharing system preference pane on each remote computer, uncheck any active services, such as File Sharing and Screen Sharing. (If there are mounted remote volumes, you will be prompted to disconnect and optionally send a message to remotely connected users. Choose 0 minutes and click OK.)
3. Log out of MobileMe on each system via the MobileMe system preference pane. This will immediately disconnect you from Back to My Mac on each system, too.
4. At Me.com, revoke your iChat and Back to My Mac certificates:
   a. Click the Account () button at the top of the window.
   b. Click Security Certificates in the list at left.
   c. Click Revoke Certificate next to each active certification (**Figure 16**). You may see two for each category (iChat and Back to My Mac) if your user name was originally a .Mac login.

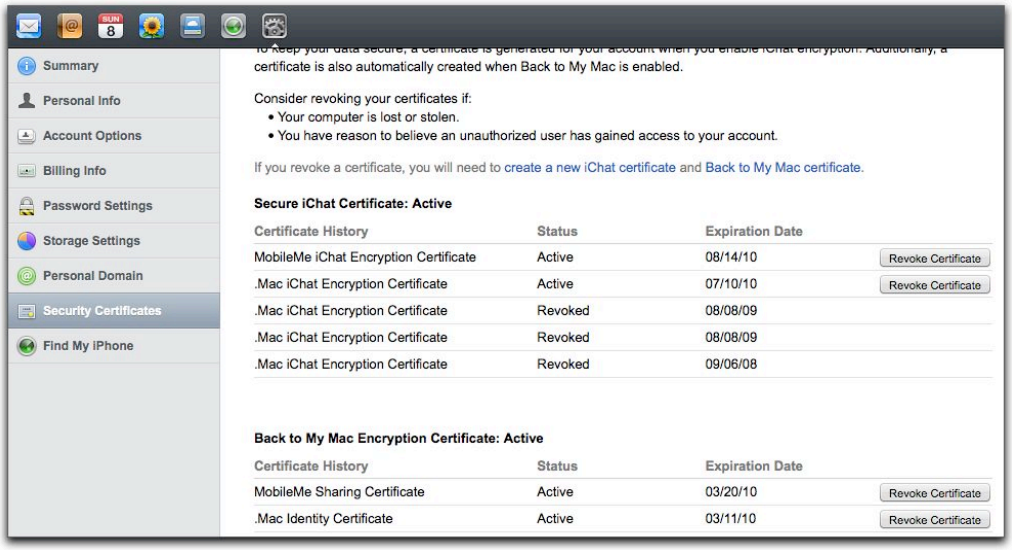


Figure 16: The Security Certificates portion of Account Settings lets you revoke certificates.

5. Log in to MobileMe on each Mac (via the MobileMe system preference pane); this creates a new connection and loads new certificate data for MobileMe. Then switch to the Back to My Mac sub-pane and click Start; this loads the new certificate for Back to My Mac.

6. In iChat:

   a. Choose iChat > Preferences, click Accounts, and select your MobileMe account.

   b. In the Account Information sub-pane, enter your new password.

   c. Click the Security button, and then click Enable, next to the iChat Encryption label, to create a new certificate.

You can reload the Security Certificates pane at Me.com to see that the new certificates are available.

Warning! *If a remotely compromised system is logged in to iChat, it's possible that any active iChat session and any active chats will remain active for a period of time. If you have iChat set to allow multiple sessions at a time, log in to iChat, and then follow the prompts to log other users out.*

REVOKE KERBEROS TICKETS

You may be thinking I'm totally insane to go to this level, but if you're interested in removing any vestigial chance of someone reconnecting to your remote computer's files or screen, this step is necessary.

Kerberos tickets assigned for sharing services last 10 hours. During this time, someone on a computer from which you have, say, un-mounted a shared volume could, under very specific circumstances, reconnect to that volume.

To delete tickets before 10 hours elapses, open Keychain Access and choose Keychain Access > Ticket Viewer (Kerberos Ticket Viewer in Leopard). This launches a separate program. Select any items in the Ticket Viewer, and then click Destroy Ticket (**Figure 17**). This doesn't delete passwords, but it does prevent automatically authenticated reconnections within the remaining time.

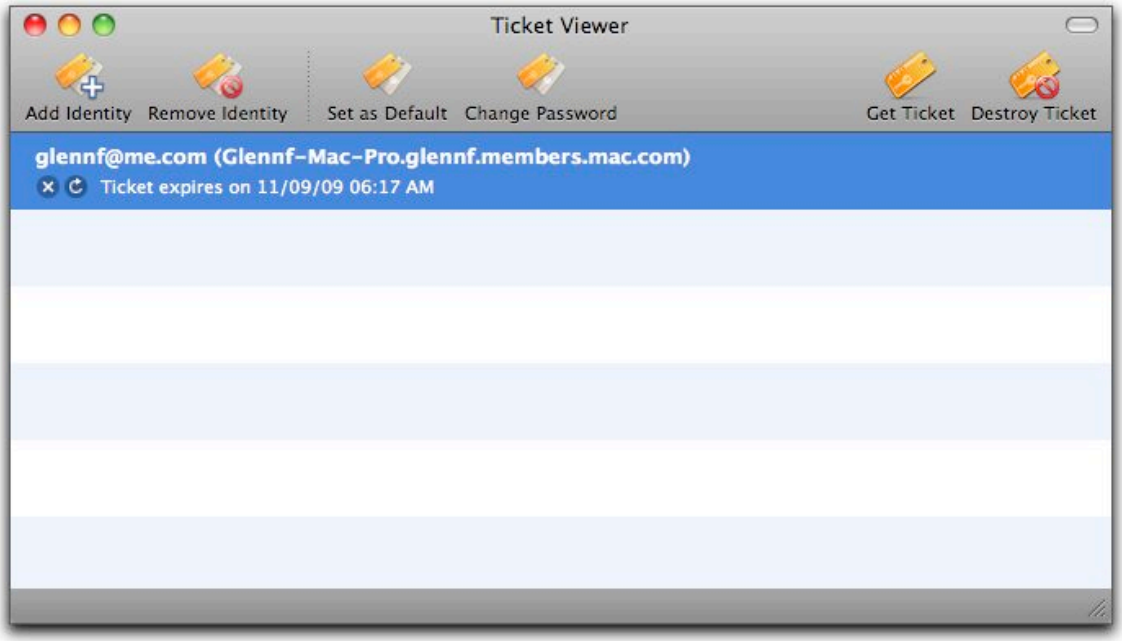


Figure 17: The Kerberos Ticket Viewer shows when a given authorization will expire and lets you destroy tickets. Destroying the ticket revokes any current access, but doesn't delete passwords. (While the entry shown here is readable by humans, entries can be obscure, comprising just hexadecimal digits.)

Overcome the Same MobileMe Account Limit

The biggest limitation of Back to My Mac is that it requires you to use the same MobileMe account for each computer that you want to share. A situation in which this could be a problem is if you want to use Back to My Mac as a neat shortcut for providing technical support to others.

Screen sharing via iChat might be a worthwhile option for working around this problem, but I have a strategy that could also work if you want to keep your personal MobileMe account private:

1. Sign up for a MobileMe Family Pack, which costs an additional $50 per year compared to a regular account, but provides *four* extra full accounts, each valid for Back to My Mac. (Email-only accounts, while cheaper, are not sufficient.)

   Now you can keep the primary MobileMe account for yourself while using one or more of the extra ones for technical support. For example, if you often provide technical support for your college-aged daughter, you could give her one of those accounts.

2. Set up the remote user to use one of the extra MobileMe accounts (either as that user's only MobileMe account, or only when you want to provide tech support).

3. Pick one of the following options for providing remote tech support:

   - **Switch MobileMe accounts:** Open the MobileMe preference pane on your Mac using your regular Mac OS X account, click Logout, and then log in with the appropriate MobileMe account information. Especially if you use MobileMe for backups or syncing, be sure to log back in to your account when you finish.

   - **In Snow Leopard only, switch Mac OS X accounts:** Set up another Mac OS X user on your Mac and configure that user with the appropriate MobileMe account. You can then keep that separate account logged in at the same time as you use your regular Mac OS X account, and when you want to start a screen-sharing

session, you can then switch to that account via Fast User Switching (see the sidebar just below).

Tip: You could use iChat-based screen sharing to set most of this up for the other user. See *Take Control of Screen Sharing in Snow Leopard* for how to use that option to its best advantage.

Setting up a Mac OS X Account and Fast User Switching

To create a unique Mac OS X account, follow these steps:

1. Open System Preferences, and select Accounts.
2. Click the Lock button ( ) in the lower left, enter an administrative user name and password, and click OK.
3. Click the plus ( ) button.
4. From the New Account pop-up menu, choose Standard; configure the account's settings and click Create Account (**Figure 18**).

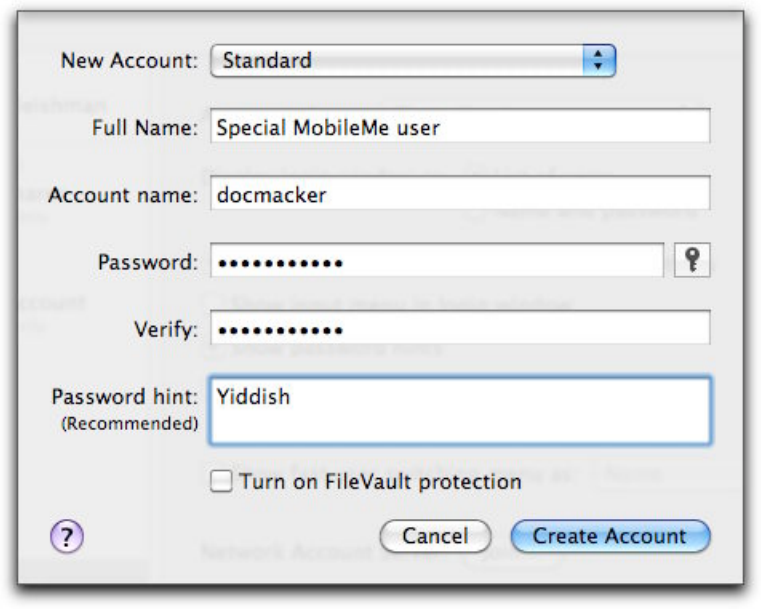


Figure 18: Create a Standard user account that can act as a Back to My Mac conduit to a friend or family member.

5. Back in the main Accounts pane, click Login Options and check the Show Fast User Switch Menu As box.

Now that you've set up the new account and turned on Fast User Switching, choose the account name from the far right of the menu bar to switch to the new account.

Troubleshooting

While Back to My Mac can often be set up without a hitch, you may run into setup or connection difficulties. How can you tell which kind of problem you're facing? Here's a quick lay of the land:

- Does the MobileMe system preference pane's Back to My Mac sub-pane show a yellow or red dot with a troubleshooting message? Or does the Start button, when clicked, stall and never change to read Stop? Take a look at MobileMe Preference Pane Troubleshooting Messages (next page).
- Does the Mac you're trying to connect to appear in the Finder's sidebar under the Sharing head? If not, then consult Back to My Mac Stops Working or Doesn't Work (p. 63). You should also read Sleep Causes Lack of Access (p. 66); your remote computer may simply be in standby mode!
- Does the computer you want to reach appear in the list, but you can't connect to it? Try Router Disrupts Connection (p. 71).
- Is the router connected to a remote Mac crashing or restarting itself regularly after you start using Back to My Mac? See Router Disrupts Connection (p. 71).

Local Connections

While all the services in this book can be used over a local network as well as remotely over the Internet, I haven't come across any particular problems for local networks. As long as two computers are on the same network segment—connected to the same router or using the same range of IP addresses—you should have no problems. If you encounter difficulties, let me know, so I can help troubleshoot them and document them.

MOBILEME PREFERENCE PANE TROUBLESHOOTING MESSAGES

In the 10.5.3 update to Leopard, Apple added status messages to the MobileMe preference pane's Back to My Mac sub-pane. These messages help you troubleshoot what's wrong with your network if Back to My Mac can't exchange the appropriate data with MobileMe to enable remote connections to other computers.

In the Back to My Mac sub-pane:

- If you see a green dot, you can skip the rest of this section; everything's copacetic (**Figure 19**).

Figure 19: When Back to My Mac is working as Mac OS X expects, a green dot confirms its status in the MobileMe preference pane.

- If you see a yellow dot and a status message:
  - **NAT-PMP or UPnP not enabled on the router:** The correct router protocol isn't turned on or available. I explain this issue at length in NAT-PMP and UPnP Not Enabled or Available, next page.
  - **Double NAT:** (The error message explains that you have "more than one device on your network providing Network Address Translation.") In this case, the router to which your Mac is attached is plugged in to another router, and each is providing its own NAT gateway. See Double NAT, next page.
  - **Connection error to MobileMe:** A problem at your ISP, the networks between you and Apple, or at Apple's end is preventing a connection. See MobileMe Can't Be Reached, a few pages ahead.

- If you see a red dot, Mac OS X believes that you have no Internet connection.

Note: Apple documents this sub-pane's messages at http://support.apple.com/kb/TS1626.

NAT-PMP and UPnP Not Enabled or Available

In Configure Your Router or Gateway and in Appendix A: Understand Network Terms, I explain how Back to My Mac relies on automatic port mapping. If Mac OS X talks to the router to ask for the ports it needs and gets no response using either NAT-PMP or UPnP, the preference pane explains that fact (**Figure 20**).

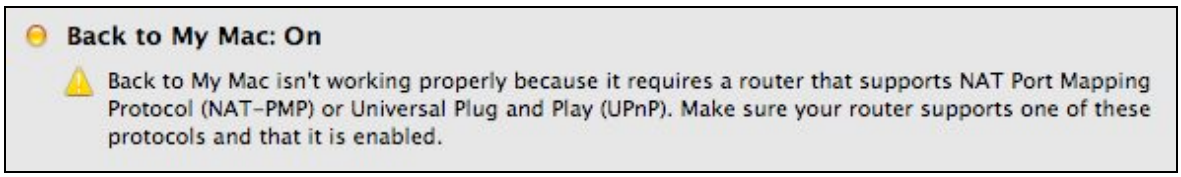


Figure 20: Back to My Mac recognizes when a router can't engage automatic port mapping.

If you believe that your router has NAT-PMP or UPnP available and turned on, consult Configure Your Router or Gateway to double-check. Failing that, upgrade your router's firmware, if an update is available, since having too-old firmware is a common problem. And if none of that works, you might consider buying a more recent router.

Note: All Apple base stations models released starting in 2003 support NAT-PMP.

You can avoid using NAT-PMP or UPnP if you have public IP addresses on each computer, but otherwise, you're out of luck for using Back to My Mac.

Double NAT

A *double NAT* occurs when you have one NAT nested inside another: that is, your computer is connected to a router that is creating a set of private network addresses, but that router is itself connected to another router—such as a broadband modem—that is also assigning private addresses.

This scenario often occurs when an ISP chooses to use NAT on its broadband modem, and you can't obtain additional IP addresses from the ISP. This forces you to share the ISP's network address through private addressing and NAT, but that's an insurmountable barrier for Back to My Mac, which tries to punch through an outgoing connection past the NAT gateway, but which requires a publicly routable IP address on the router that connects to your computer.

Apple's explanation, at this writing, is somewhat incorrect when it detects a double NAT (**Figure 21**). It talks about multiple devices on the network using NAT, when it's actually a very specific layered situation. Your computer is connected via Wi-Fi or Ethernet on a router's LAN side, and the router's WAN port is plugged into a LAN port of the router that's one step closer to the Internet.

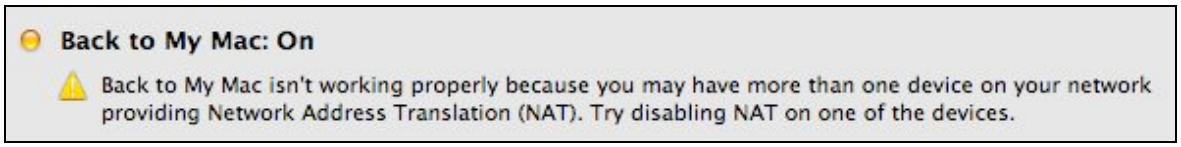


Figure 21: Although Back to My Mac correctly recognizes a double NAT, Apple's explanation is imprecise and technically inaccurate.

The solution to this problem is to turn on bridging or passthrough mode on the router your computer connects to. In this mode, your router passes through automatic address assignment from the next-higher-level router, and is more or less transparent to that router.

On any Apple Wi-Fi gear introduced in 2003 or later, you can enable bridging by following these steps:

1. Launch AirPort Utility (from /Applications/Utilities), select your router in the list at left, and click the Manual Setup button.
2. Choose the Internet pane.
3. From the Connection Sharing menu, choose Off (Bridge Mode).
4. Click Update to restart the router with the new settings.

Tip: You can read more about these configuration options in my book, *Take Control of Your 802.11n AirPort Network*.

MobileMe Can't Be Reached

There's one final diagnostic message. You'll see "Back to My Mac isn't working properly because there's a problem with your connection to MobileMe" if your Internet connection is working, but there's no response from the MobileMe service.

I've found that simply clicking Stop, waiting for the service to stop, and then clicking Start often clears this state. However, you might find this a more intransigent problem. Apple notes in its technical support note that this could occur when a firewall—particularly a corporate one—blocks outgoing traffic on port 5354, or if you're using a DNS proxy that doesn't allow certain kinds of record lookups. Consult Apple's note—at http://support.apple.com/kb/TS1626—for more detail.

BACK TO MY MAC STOPS WORKING OR DOESN'T WORK

For what appears to be a variety of unexplained reasons, Back to My Mac can stop working on certain machines. I expect that Apple, which says it's continually working to improve the service, will keep improving its reliability. I characterize Back to My Mac as "not working" when you can't access a remote computer in your Shared list in a Finder window's sidebar, even though on the unreachable remote computer, in the Back to My Mac sub-pane of the MobileMe system preference pane, you have a green dot in the status message.

To solve this problem, skim the tips ahead, and try them as desired. Such a lack of access can even happen if Back to My Mac was previously working without a hitch. If none of the tips help, or even if they may have helped, you may also have to reconfigure your router once again; see Configure Your Router or Gateway.

Turn Back to My Mac Off, and Then Back On

If it appears that your computer should be remotely accessible via Back to My Mac, but it isn't, you can turn the feature off and back on again, which would certainly reset the IP address stored with your MobileMe account. (Open the MobileMe preference pane, click the Back to My Mac button, click Stop, wait, and then click Start.)

Same Name May Prevent Connection

In a technical note, Apple warns against using the same name for any two Macs in a Back to My Mac set, because that might prevent each of those Macs from contacting the other. Each computer has two distinct names, both set in the Sharing system preference pane:

- At the top of that pane, you can set the *Computer Name,* the label used to identify machines over a network and the name that appears in Finder window sidebars in the Sharing list.
- The *Local Hostname* is used with Bonjour to identify computers to other computer and resources. To change the Local Hostname, click the Edit button beneath the Computer Name field. You're limited generally to letters, numbers, and dashes, and Mac OS X will keep you from using characters that aren't permitted.

Don't Synchronize Keychains via MobileMe

A *TidBITS* reader provided me with a terrific tip, and an explanation as to why Back to My Mac *and* iChat text encryption was failing to work on some systems, and why it worked and then failed in a later attempt on other systems. (My fellow Take Control author Joe Kissell, author of *Take Control of MobileMe,* hasn't seen this happen often.)

Leopard allows you to sync a bunch of different items using the MobileMe preference pane's Sync sub-pane. If you have multiple computers on which you enter calendar, address book, and bookmark information, it may make sense to sync that data to keep the computers consistent. Keychains, however, are a different matter.

At first glance, you might think, "Why not have all my passwords securely distributed among all the computers I use?" But that means that anything unique—which includes certificates assigned for Back to My Mac sharing and iChat's encryption of text messaging—is also replicated across all machines. This may cause failures.

If you have Keychain synchronization turned on, follow these steps to disable that option:

1. Open System Preferences, and click the MobileMe preference pane; then click the Sync button.
2. Uncheck Keychains (**Figure 22**).

Figure 22: Uncheck Keychains to avoid certificate conflicts on multiple Macs that could prevent Back to My Mac from working properly.

3. Repeat on each computer with the same settings.

Firewall Blocks Access

Firewalls are the enemy of many network services: they're trying to prevent precisely what you want to achieve. If you have a firewall installed on your computer or have enabled Leopard's built-in firewall (but not Snow Leopard's), or you are using one built into your router or gateway, you may need to change its settings to ensure that you aren't accidentally blocking remote access.

Snow Leopard's firewall is different: *Snow Leopard uses a very different approach to creating a firewall on your computer than Leopard and Tiger did. In Snow Leopard, when the firewall is enabled, each application or service is set to allow or disallow incoming access. Services that rely on Back to My Mac, like Screen Sharing, create their own entries as needed in an enabled firewall.*

To use Back to My Mac, outgoing access to ports 443 (TCP) and 5354 (TCP), and both incoming and outgoing access to 4500 (UDP) must be enabled. Most third-party Mac firewalls focus on incoming access, and they won't block attempts to use the outgoing 443 and 5354 ports. Leopard doesn't block those ports, for instance, and Snow Leopard won't interfere when Back to My Mac is turned on.

You should track the firewall changes you make, or test Back to My Mac after making changes, because you might unintentionally break remote access, not realizing that it's not working until after you've forgotten the change you put in place.

Little Snitch

Little Snitch is a great piece of application-firewall software from Objective Development that alerts you whenever any program attempts to connect over any network (http://www.obdev.at/products/littlesnitch/, $29.95). You can train it to block certain traffic, and allow other traffic, on a program-by-program basis. It can be useful here because it lets you see what ports you might need to tweak on a firewall to ensure that remote access works.

Delete Everything and Start Over

In Erase Back to My Mac's Traces, I explain how to delete everything associated with Back to My Mac on a computer. In some cases when I've had trouble with Back to My Mac, following those steps, and then setting up Back to My Mac from scratch, was the only way I could get it working again. It's worth a shot, and it doesn't take long to try.

SLEEP CAUSES LACK OF ACCESS

It used to be that a sleeping Mac would slumber through any attempts to stir it from afar. These days, there are two discrete ways to wake a remote Mac. Wake on Demand is new to Snow Leopard, and works only in particular cases; an older method—Wake on LAN—works with previous systems, but requires that a sleeping computer be connected via Ethernet.

You can also simply Disable Sleep mode to make certain that a Mac never nods off.

Enable Wake on Demand in Snow Leopard

In Snow Leopard, Apple added an extremely cool feature that lets you simultaneously benefit from the reduced wear, electrical cost, and heat of having your computer sleep when not in use, while retaining continuous access to services, such as screen sharing, available from that Mac.

This Snow Leopard feature, Wake on Demand, requires either an AirPort Extreme Base Station or a Time Capsule; either model needs firmware version 7.4.2 or later. The base station acts as a kind of proxy whenever your computer goes to sleep, rebroadcasting any Bonjour messages that your computer had sent just before it went to sleep. When another computer wants to access those services, the base station triggers the computer, which wakes up and responds.

Tip: While this method might only seem to be useful over a local network, a computer can be woken remotely via a Back to My Mac linkage.

For a Snow Leopard Mac to be woken via Wake on Demand, the Mac must meet several criteria:

- **Compatibility and connections:** Certain 2008 and every 2009 Mac model may be roused by Wake on Demand whether connected via Wi-Fi *or* Ethernet; for other Snow Leopard-compatible models, only Ethernet works. (Apple hasn't released a list of compatible 2008 systems and explained to me that the feature requires a combination of chipset and internal modules standard in all Macs released in 2009 but present in only some 2008 systems.)
- **Special WPA Personal detail:** If WPA Personal or WPA2 Personal encryption is enabled, a Mac that can be woken via Wi-Fi must be connected to the main base station on the network—the one that's providing IP addresses and is directly connected to the broadband modem. I'm not sure why this is a requirement, but Apple says it is. (In other words, if a base station is set up to *bridge*—pass through—DHCP messages, it apparently doesn't qualify.)
- **Wake on Demand must be enabled:** Snow Leopard enables the Wake on Demand feature by default. You can set it in the Energy

Saver preference pane, in the sole view on a desktop machine or in the Power Adapter view on a laptop (**Figure 23**).

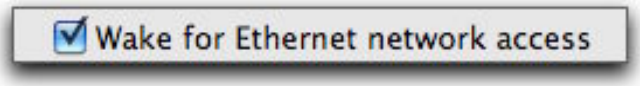


Figure 23: The checkbox that enables and disables Wake on Demand. The option has different names in different cases—look for Wake on Network Access, Wake on Ethernet Access, or Wake on AirPort.

Enable Wake on LAN

Mac OS X (and Windows) can be woken from a slumber through a bit of Sleeping Beauty magic commonly known as Wake on LAN, which works only over Ethernet. Rather than a prince's kiss, a specially formed bit of network data—the *magic packet*—is sent to the right network port, whether over a local network or remotely, to awaken the computer.

Tip: The "magic packet" method works over Ethernet in Snow Leopard, too, regardless of what kind of router is in use.

Over the local network, any Ethernet-connected computer with this feature enabled can be directly addressed by its IP address on that network. However, if you want to wake a computer from outside the local network on which it resides, the computer must either have a publicly reachable IP address, or you must set up port mapping on your router so that the special magic packet port that's used can be reached remotely.

To allow this kind of remote wake-up call, follow these steps:

1. Open the Energy Saver system preference pane.
2. In Leopard, if you don't see the Sleep and Options buttons, click the Show Details button. Click Options. In Snow Leopard, these options are shown by default.
3. In Leopard, check the box for Wake for Ethernet Network Administrator Access (**Figure 24**). In Snow Leopard, the option reads Wake on Network Access or Wake on Ethernet Network Access.

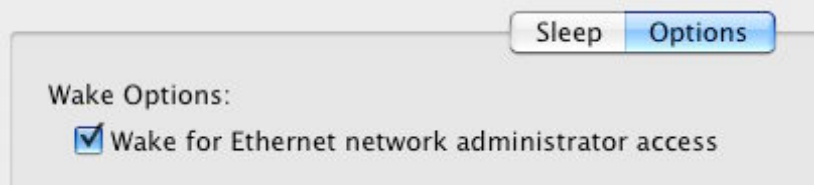


Figure 24: This Leopard checkbox allows remote wake-up of the computer in question.

Now, you need a way to wake that Mac up. Download WakeOnLan (http://www.readpixel.com/wakeonlan/), a free package that scans a local network, shows available computers, and lets you select them and tell them to Wake Up! (as the button's label reads, **Figure 25**).

Scan first: *Run WakeOnLan while computers you might want to wake up are actually still awake; otherwise, the program can't spot the computers when they're asleep—and, thus, won't display them as options for waking.*

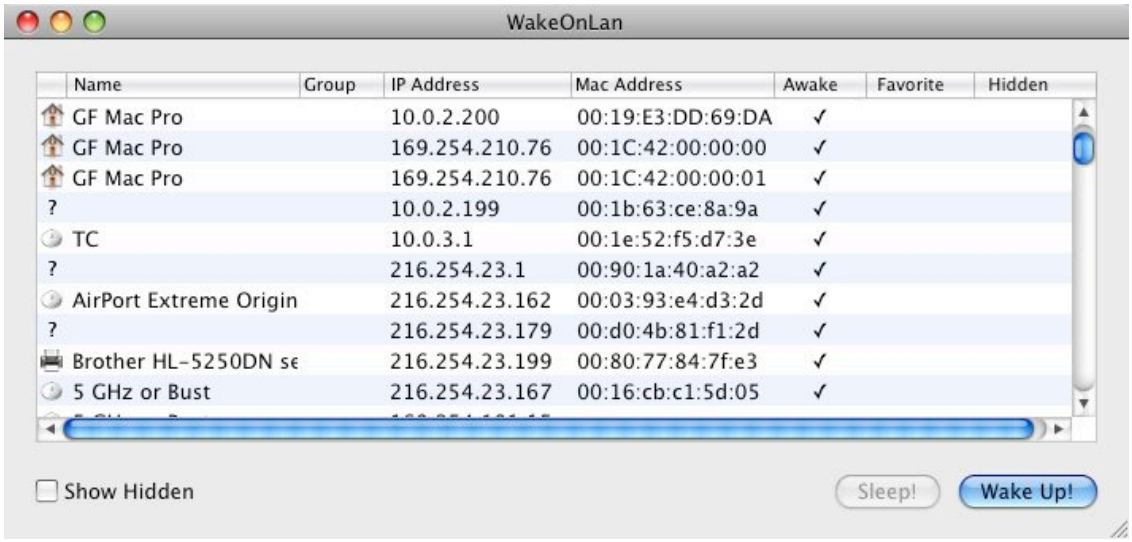


Figure 25: WakeOnLan scans the local network to find computers and other devices. I've never seen Sleep! light up, but Wake Up! is an option for any device, even when already "awake."

WakeOnLan also works remotely for:

- Any computer that has a publicly routable IP address; or
- A computer with a private IP address that has its port 9 mapped to a gateway's port 9, where the gateway has a publicly routable IP address

You need to know both the public IP address and the *MAC address* of the computer—its unique Ethernet adapter address—for remote wake-ups to work.

Finding a MAC address: *You can find the MAC address for the Ethernet connection that links a computer to the local network in one of two ways. While that computer is awake, launch WakeOnLan on the same network, and all the MAC addresses are exposed; that's pretty straightforward. Or, launch System Preferences, open the Network preference pane, and choose Ethernet in the list to the left; click the Advanced button, and you'll find the Ethernet MAC address—called* Ethernet ID*—at the top of the Ethernet sub-pane.*

In WakeOnLan, to add a remote Macintosh to the list, choose Hosts > Add, and enter the name, publicly reachable IP address, and MAC address of the computer in question. That computer then appears in the WakeOnLan list, and you can select its entry in the future to wake it up.

Disable Sleep

If you don't want a Mac to ever fall asleep, follow these steps to keep it awake:

1. Open System Preferences, and select Energy Saver.
2. Expose the sleep option:
    - In Leopard, if you see a Show Details button at the lower left, click it. Otherwise, the details are already showing as in **Figure 26**, top.
    - In Snow Leopard, the option is found in the main view for a desktop computer or the Power Adapter sub-pane for a laptop computer (**Figure 26**, bottom).
3. In the Sleep pane, drag the "Put the computer to sleep when it's inactive for" slider (Leopard) or Computer Sleep slider (Snow Leopard) all the way to the right, to Never.

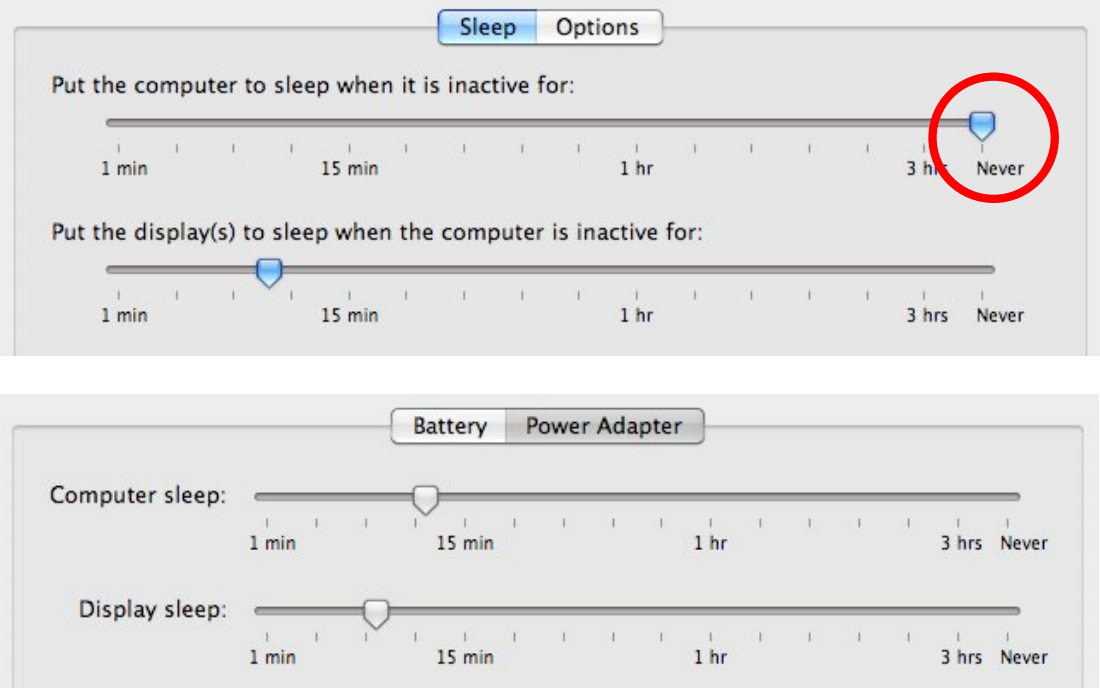


Figure 26: The sleep settings in Leopard (top) and Snow Leopard (bottom). If Wake on Demand or the "Magic Packet" isn't an option, drag the sleep slider to Never to ensure the Mac is always awake.

ROUTER DISRUPTS CONNECTION

Routers, the devices that handle interaction between the local network and the Internet, are the root (not route) of most troubles.

Can't find NAT-PMP or UPnP Setting

This isn't exactly a bug, but some routers don't offer automatic port mapping using NAT-PMP or UPnP; as noted earlier in this section, the MobileMe system preference pane will alert you to the absence of NAT-PMP or UPnP when you try to turn on Back to My Mac.

You can remedy this by buying a new router, as long as your ISP doesn't provide you with a broadband modem that has router features built in; the 2Wire series of routers used by DSL providers lack automatic port mapping. For most cable-modem customers and many who subscribe to DSL services, you won't be barred by the modem.

A router with UPnP can be had for $30 to $100 from Linksys, NetGear, D-Link, and many others, with the price depending on features, and sometimes even less with rebates; Apple's $99 AirPort Express and $179 AirPort Extreme Base Station both include NAT-PMP, too. (You

should also check for new firmware on your existing hardware; see "Back to My Mac Works Inconsistently," below.)

UPnP Should Work, But Doesn't

Not all routers are created equal; some are more reliable than others. Some readers have already told me that when they can't get UPnP to work, restarting their router fixes the problem.

Back to My Mac Works Inconsistently

You might see inconsistent performance where older routers drop Back to My Mac connections. But that might be fixable—many routers have their firmware (the software that runs the hardware) updated regularly.

Make sure you have the latest firmware for your router installed by visiting the manufacturer's Web site, clicking their support link, finding your model, and seeing what's available. In some cases, you may need to use Windows XP—newer versions of Windows may not launch the software—to install firmware using special software provided by the maker.

Appendix A: Understand Network Terms

Back to My Mac works over the Internet and local networks, and thus relies on protocols and principles that can be baffling without a bit of background. I've put these background details in this appendix so you can understand the numbers and terms you need to make a connection work reliably.

As explained in Learn How It All Works, Back to My Mac connects two computers over the Internet using a variety of technologies. But the two machines find each other by using Back to My Mac, and then register themselves with the MobileMe service, thus providing the details needed for each computer to connect to any of the others in the set.

You'll learn in this appendix about the unique address assigned to each computer; the way in which each computer interacts with its network router to register i

tself with MobileMe; and what limits Back to My Mac from working everywhere.

IP ADDRESS

The Internet works with a minimum of centralized authority. Instead, it relies on an overarching principle of delegation, in which a few top-level authorities hand out power in the form of chunks of IP addresses to organizations and individuals.

Internet Protocol (IP) addresses uniquely define a device's location on the Internet, both logically (via data connections) and, ultimately, physically (via wires or wireless). An IP address comprises four 8-bit numbers (ranging from 0 to 255) separated by dots, such as 127.0.0.1. IP addresses always include those dots.

Each and every device on the Internet has an IP address. (Some devices appear to share the same IP address, but each device has

its own address, nonetheless, as I explain in a moment.) In order to connect to a target Mac for a purpose like Back to My Mac, the target Mac's IP address must be known, if not to you, then to the software that creates the connection.

Smaller networks with only a few IP addresses assigned to them are connected to bigger networks, which are in turn interconnected to huge networks. For instance, I once ran a network with only eight IP addresses; these were supplied to me by my ISP (Internet Service Provider). My ISP in turn controlled part of a range of hundreds of thousands of addresses, which in turn was mapped to other, higher networks which controlled millions of addresses.

When browsing the Web, you rarely have to enter or know an IP address. For example, when you connect to the Take Control Books Web site via "takecontrolbooks.com," you needn't know the Web server's actual IP address, even though your operating system uses that IP address, 216.168.61.78, to open connections between your computer and the site.

An entire system, called the *domain name system,* or *DNS,* ensures that you rarely need to know or enter an IP address. DNS lets you access a Web site, for instance, by entering the Web site's name in a Web browser's URL field, like www.takecontrolbooks.com, without having any idea of the corresponding IP address. Behind the scenes, DNS converts the name into the correct number. In this way, DNS makes the Internet friendly and more flexible; however, IP addresses still underlay every connection.

Every time a computer needs to interact with another one over the Internet, and often even over a local network, the local computer's operating system uses the target computer's IP address—obtained via DNS or directly entered by a person—to let the target computer know it wants to communicate. The target computer, if it wants to reply, opens a connection back. Pairs of these connections, called *sockets,* form the basis of all Internet services, such as Web browsing, video streaming, and email.

When making a remote-access connection to a target Mac, the operating system may have to navigate some interesting virtual twists, depending on two properties of the target computer's IP addresses:

- Public or private
- Static or dynamic

Let's look at these two sets of properties in turn.

The remote computer's address is most important: *For the purposes of Back to My Mac, it's the target (remote) Mac's IP address and the router that controls the assignment of that address that are most crucial. Routers don't limit most outgoing connections, and thus the machine initiating the connection isn't blocked; the remote machine's router, however, or its ISP's configuration, may limit incoming connections to the Back to My Mac service.*

Public or Private

Each computer that uses the Internet must have an IP address in order to both issue requests to and receive responses from other computers. But that address can be public, and thus easily—and directly—reached from anywhere on the Internet, or private, which restricts its use to *behind* a router or gateway.

Although there's no *behind* in real terms, it's useful to think of the Internet as a series of branches; routers are nodes that have terminal branches, each of which is a computer. Thus the computers are below or behind the router, in relation to the rest of the Internet (see the diagram in **Figure 27**).

A *public address,* often called a *publicly routable address,* is directly "visible" to other computers on the Internet. This type of address is part of the hierarchy, where higher-level networks that comprise the Internet can directly communicate with devices on branches that occupy lower levels. Each router knows the pool of addresses that are part of the branches beneath them; data traverses down nodes, a branch at a time through this succession of routers, until the final router is reached that contains, within its network, the target computer or device.

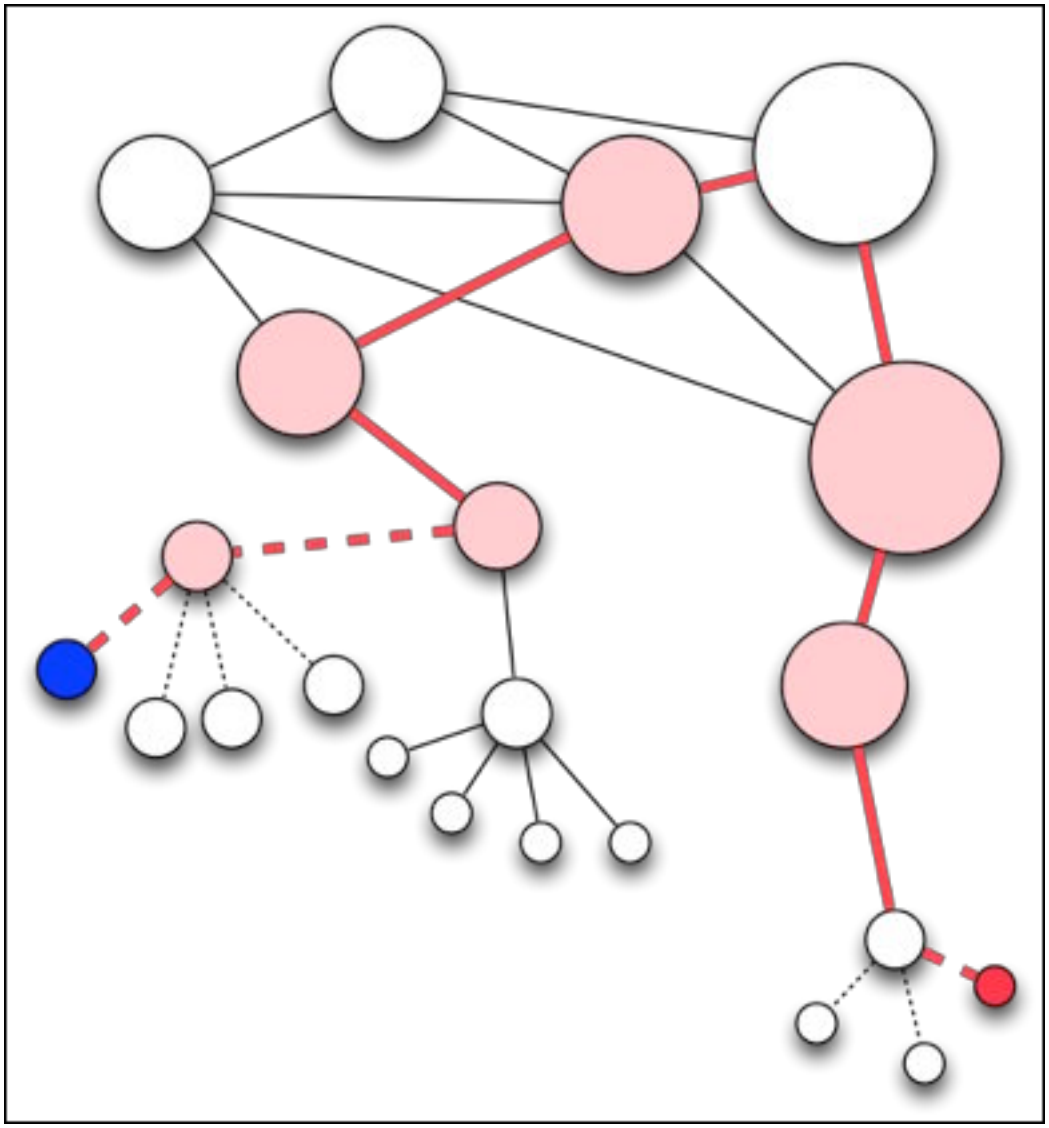


Figure 27: Communication between two computers on the Internet bubbles up from branches of a hierarchical tree: the blue dot at the left middle represents a computer trying to connect to the computer shown as a red dot at the lower right.

The red line indicates the path (one of many) through the larger routers that make up the Internet *backbone*—a kind of top layer used to interconnect the largest networks with many paths among them—to reach the destination computer. Dotted lines show private IP addresses; solid lines public IP addresses.

In contrast, a *private address* is one that belongs to one of several reserved ranges of IP addresses that are used only on local—i.e., private—networks. In **Figure 27**, previous page, note that the dotted lines representing private networks are always at the bottom of the branching hierarchy. (Note that *local* doesn't necessarily mean *small*—

a local network can comprise a single computer plugged into a Wi-Fi base station, but it can also span an entire corporation.)

Because IP addresses in a private range can't be used on—and can't ever be reached directly from—the public Internet, this means that the same ranges can be used on many different private networks without conflicts. Conversely, because these private IP addresses are not unique, they are guaranteed to be unreachable from outside their local network. Computers that have private addresses usually get those addresses from a network router; that router will generally use Network Address Translation (NAT), described ahead in this section, to allow the computer to receive communications from the Internet.

A public IP address is easy to reach from anywhere on the Internet, and thus it's easy to set up remote-access connections to a computer that has a public IP address. However, private addresses are a little more tricky, because the connection—or, more specifically, the router that handles the connection—must be set up to use NAT to make the private address externally accessible. (How do you know if you have a private address? See "Private Network Ranges," below, and Double NAT, p. 61)

Private Network Ranges

When the Internet's current numbering system for IP addresses was set up, three ranges of numbers were put aside for use as private network addresses. (A few other address ranges can be used, but you'll never see them in common usage.)

In the list below, *x* is any number between 0 and 254, while *y* is any number between 1 and 254. (The number 255 in all positions, and 0 in the farthest right position, are reserved for special network purposes.)

Here are the three private address ranges:

- 192.168.x.y (64,770 addresses): most commonly used.
- 10.x.x.y (16.5 million addresses): Apple has always liked this range, possibly to be different.
- 172.16.x.y through 172.31.x.y (1 million addresses): rarely used, for no particular reason.

Static or Dynamic

Although a computer's or a router's IP address can be permanent (as permanent goes in the age of the Internet), it can also last for only days, hours, or even seconds. If it changes, an address is called *dynamic*.

A dynamic IP address might change every few hours or days, or only when a computer is restarted or a router is rebooted. Dynamic addresses are usually assigned automatically by a router; for example, your ISP's router may assign a temporary, publicly accessible IP address to your cable or DSL modem, and your personal router (perhaps an AirPort Extreme Base Station) may assign private IP addresses to the computers on your local network.

A *static* IP address, by contrast, remains the same until you change it.

Back to My Mac is designed to track dynamic address changes by rewriting the registration information for a given Mac OS X system in your MobileMe account whenever the service notices the address has changed. (This is a fancy way of saying, "Back to My Mac stores information about your computers.")

UPnP Doesn't Pick Up Changes Instantly

Back to My Mac immediately picks up any change to your public IP address if you're using NAT-PMP (available only with Apple base stations); with UPnP, you may need to turn Back to My Mac off and back on to register the new IP address. (Open the MobileMe preference pane, click the Back to My Mac button, click Stop, wait, and then click Start.)

It's worth noting that public and private IP addresses can each be static or dynamic, and you can have any combination of static and dynamic public and private addresses, depending on the network configurations used by your Internet provider and your local network.

On a local network, dynamic addresses are assigned to computers via a *DHCP* (Dynamic Host Configuration Protocol) server, which is built into all home routers. A network interface in each computer—for example, Ethernet or AirPort—can be set to use a DHCP client (part of the networking software in a computer's operating system) that requests and accepts an IP address from a DHCP server. The software then configures the network interface with that address. This system

provides a simple—and largely automatic—way for computers on the local network to obtain an IP address, and then to use that address to have a full network connection, thus solving what would otherwise be a chicken-and-egg problem of how to have an IP address in order to get an IP address.

To configure either type of address—static or dynamic—in Leopard or Snow Leopard, you use the Network pane of System Preferences: select a network interface in the list at left, click the Advanced button in the bottom-right, and then click TCP/IP.

With a static public IP address, neither Back to My Mac nor any other remote access systems have difficulty directly contacting your computer. Where it gets stickier is when either dynamic or private addresses are involved. Because it's typical that most home broadband connections and many office networks have both dynamic *and* private addresses, I next explain ports (addresses within IP addresses, of a sort), and how they relate to remote access with Back to My Mac.

Dynamic DNS

There's an interesting way to overcome the limitation of having a dynamic public IP address assigned to your computer or router that makes the address reachable with a consistent name: using dynamic DNS, you can have a domain name like remote.glennf.com always point to the current IP address used by a router or a computer.

Back to My Mac uses dynamic DNS behind the scenes to keep your dynamic address in sync with your MobileMe account, but if you need dynamic DNS for some other purpose, you can use various domain hosting services that offer dynamic DNS. This requires a special, but simple, piece of software for a computer, or built-in support in a router, to notify the domain host whenever the IP address changes. If you want to use dynamic DNS for your own purposes, consult this list of available software: http://directory.google.com/Top/Computers/Software/Internet/Clients/Dynamic_DNS/.

PORTS WITHIN ADDRESSES

A potentially confusing part of Internet networking is an extension of IP addresses called *ports*; each is a unique number that identifies the type of service—email, Web, file sharing, and so on—to which a particular connection pertains. When explaining ports, I often find it useful to describe a port as a cubbyhole on a server that is intended for holding communication about a particular service, such as outgoing email, Web browsing, or a remote-access connection. On an ordinary computer—technically called a *client*—a port works like an "ear" that's waiting to hear a response from a *particular* service or type of communication.

All outgoing and incoming Internet data has a set of IP addresses attached to it, uniquely identifying the sending computer and the destination router or computer. But each IP address also indicates the number of the originating and destination port, too.

Ports were designed to let the same computer handle lots of different network-related tasks without lots of overhead. By providing many slots, many services can run at the same time using a single IP address.

Well-known services—like the Web, FTP, email sending, and so forth—all have reserved ports that are the same on every server by default. For example, email clients always expect to send unsecured email via port 25 unless told otherwise. Back to My Mac uses ports 443 and 4500 for its incoming connections.

Here's a more detailed example. Say you enter http://www.me.com/ in the address field of your Web browser. Now, your computer needs to retrieve the Web page for that URL. Your computer and the server performs a series of steps of which you are usually blissfully unaware:

1. Your computer looks up the IP address of www.me.com.
2. Your computer initiates a connection to that IP address from a port number of its own that it picks randomly (but above 1024, since ports below 1024 are reserved for other purposes).
3. Your computer sends the connection to port 80 at the IP address of www.me.com. (All Web browsers assume that 80 is the Web server port.) Your computer requests me.com's home page.

4. In response, me.com sends the home page via a connection that originates on its port 80 and is targeted at your computer's IP address and originating port.

Note: Web servers of any scale use a form of private addressing themselves, so that a few, a few hundred, or even hundreds of thousands of servers (in Google's case) appear to have the same IP address. Internal networking software and hardware shuffles requests among the servers to keep the load on any one machine from rising too high. So when I say "me.com," I really mean, "one of hundreds or thousands of computers that act as if they're a single monolithic Web site at www.me.com."

Another way to think about ports is to take an analogy to how email is delivered from your computer to a mail server. Outgoing email uses port 25 or port 995; port 995 is used for secured email, in which the account login, password, and email contents are encrypted.

Consider a city that contains only buildings full of offices or apartments (each building is a computer with an IP address). Everyone in the city has agreed, without any law being passed, that each building will have dedicated rooms for common purposes—all unsecured mail will be received in room 25, for instance (these rooms are ports). With this agreement, a hired messenger could easily determine where to deliver a message:

- If you had a regular letter to send, you'd hand the messenger the envelope; then he would find the desired building, enter the building, and go to room 25, where he would be expected.
- To send a message so that it's received securely, you might hire a bonded and insured messenger (the equivalent of an encrypted connection), and provide that messenger with a special key that lets her, when she arrives at the destination building, unlock the door to room 995 to deliver the envelope.

The analogy for Back to My Mac is more complex. Because it's a continuous connection, it's as if you built a private pipeline between two rooms you rent in different buildings: a pneumatic tube inside the pipeline carries documents (file sharing) back and forth, while a cable TV wire with a camera on either end carries a picture (screen sharing).

Two Port Types

Ports come in two flavors; you can have one of each type with the same port number carrying separate data:

- **TCP:** TCP (Transmission Control Protocol) is a *reliable* protocol, meaning that data that's dropped in transmission is automatically transmitted again by the sending computer when the receiving computer lets it know there's a missing packet.
- **UDP:** UDP (User Datagram Protocol) is *unreliable*, which means that the protocol doesn't notice if packets are lost. UDP doesn't rely on the network part of the operating system to retransmit lost packets, but rather on a program using UDP to notice a missing packet and care that it's missing.

TCP is typically used for things like email, where every bit is important; UDP is typically used for things like streaming media, where some data can be dropped without harm, but the media server and player negotiate how missing pieces are re-sent.

With an explanation of ports in hand, we can next talk about how ports are assigned on private networks, where IP addresses—and, thus, ports—aren't directly reachable from the rest of the Internet.

NETWORK ADDRESS TRANSLATION (NAT)

Early Internet users, such as academic institutions, received enormous allotments of IP addresses, with some getting a 16.7-million chunk (all addresses with a similar first number; for example, 15.x.x.y, per the explanation of private address ranges earlier in this appendix), even though they use only tens of thousands of addresses.

Back in the late 1990s, with millions of people poised to gain access via new broadband cable and DSL services, it was thought that this uneven distribution of IP addresses would lead to *address space exhaustion,* meaning that there would be no more addresses left to assign to new networks and computers. This is when *NAT* became prominent. NAT lets a gateway act as an arbiter between the public Internet and private addresses on a local network. NAT is the superhero that has prevented the collapse of the Internet since IP addresses started to run scarce.

Note: NAT as generally implemented includes *PAT* (port address translation), so that both ports and addresses are involved in being *translated* from outside to inside networks. It's called NAT for simplicity's sake.

NAT also handles *port mapping* or *port forwarding*: assigning a specific port on the router's wide area network (WAN) IP address—typically the address used to communicate with an ISP's network and the Internet at large—to a corresponding port on a specific computer on the local network. In other words, *all* Internet traffic aimed at that port on the local network's public IP address gets *forwarded* to the designated computer on the local network. Port mapping allows Back to My Mac and many other services to work.

If you're wondering about the difference between NAT and port mapping, NAT affects IP addresses, while port mapping handles ports at those addresses. NAT also uses temporary ports to handle whatever traffic is passing from the local network to the larger network, where IP addresses tend to be fixed over periods of time, even when they're dynamically assigned.

A *NAT gateway* is software that's built into a router. A NAT gateway examines every piece of inbound and outbound network traffic. It has two functions:

- **Incoming to outgoing:** The NAT gateway acts as a proxy between computers on a network and the next-up larger network. For every outgoing connection request the router receives from one of those local computers, the NAT gateway rewrites the request to appear to come from the network's public address (the wide area network—WAN—IP address of the router) and from a port that the gateway makes up.

  For example, if a computer on a local network needs to send email, that computer tries to open a connection to a mail server on the Internet. The NAT gateway in between rewrites the local computer's private IP address and port in the packets of the data stream. To the mail server, the request appears to come from the router's (public) IP address, not the computer on the private network.

When a response to a request comes back, it's received by the NAT gateway, which re-routes the response to the private IP address and appropriate port of the computer on the local network.

- **Outgoing to incoming:** When a request initiated from the outside world arrives at the router, the router checks to see whether the specific port specified in the request is listed in a port mapping entry. If so, the NAT server rewrites the request to direct it to the local computer—and the port on that computer—specified by the port mapping entry.

  For example, this lets you run a Web server on a computer on the local network by simply mapping its Web-hosting port (80) to the same port on the router's WAN IP address.

NAT is a critical component in remote services, as you'll see next when I wrap up this overview.

NAT doesn't affect local networks: *NAT affects only connections between computers within a local network and those on the "other side" of the router. The other side includes any network, anywhere on the public Internet, that can connect to the router's WAN port. Within a local network that uses NAT, all resources and services remain available unless a firewall on an individual computer has been configured to disallow a particular service or port, or has been set to reject connections from other local computers, whether specific local IP addresses or all local IP addresses.*

THE ROLE OF NAT-PMP AND UPNP

You now have all the pieces to understand the role of *automatic port mapping*, used by Back to My Mac to handle multiple computers using the same network.

As you read this appendix, you might have been struck by the fact—covered just previously—that with a router and regular port mapping, it would seem that you could map the ports needed for Back to My Mac only to a single computer. And you'd be right. With *static port mapping*, each incoming port on the router is mapped to a single IP address and port on the local network. That's why Back to My Mac and other services need *automatic port mapping*.

Using two common protocols—NAT-PMP (NAT Port Mapping Protocol), and UPnP (Universal Plug and Play)—Back to My Mac can request special ports for its own purposes that are unique for each computer on the local network. This allows multiple computers to each receive incoming Back to My Mac connections.

The port number or numbers that the router assigns and informs the requesting software about can then be published in various ways—preferably automatically if and when the port changes—so that a server running on a particular machine is reachable in a reliable fashion, and you have a connection that behaves in a persistent manner.

Back to My Mac uses dynamic DNS and a special form of Bonjour called *wide-area Bonjour* to publish to MobileMe both the public IP address and the particular ports assigned to each computer for which Back to My Mac is enabled.

Nat-PMP and UPnP Backgrounder

NAT-PMP and *UPnP* are router protocols that allow software on a computer on the network to request ports; the router fulfills that request and provides the software with a response that lets it know which ports were assigned.

NAT-PMP is an Apple-derived protocol, but part of an IETF (Internet Engineering Task Force) draft; UPnP is an industry standard maintained and certified by a trade group. NAT-PMP is specifically tailored for one purpose; UPnP's public port portion is a piece of a larger set of multimedia and networking tools.

Manage NAT-PMP with a Utility

Lighthouse, from Codelaide Software, lets you control NAT-PMP and UPnP on a router directly from the computer. This is nifty, because for services other than Back to My Mac, you could use Lighthouse to set up remote access on specific ports that you could write down and use to access certain services remotely (http://www.codelaide.com/blog/products/lighthouse/, $13).

With normal NAT, a port on the WAN IP address is assigned and used only for the duration of a given connection; it doesn't remain open and listening indefinitely. For example, if a local computer with a private address asks for a Web page from a public Internet server, the request

and response constitute the connection, and after a *Keep Alive* time that the Web server allows (to make sending multiple images and other data more efficient) expires, the connection is shut down.

However, for Back to My Mac, the connection must be *persistent,* which means a static port must be open on the WAN IP address, so NAT by itself isn't enough. Instead, you need to enable NAT-PMP or UPnP to make the target Mac available for a remote connection.

BACK INTO THE FRAY

With this grounding, you can learn how Back to My Mac works, how to enable and disable it, and, crucially, how to troubleshoot it when Back to My Mac doesn't seem to function. Start with Configure Your Router or Gateway.

Appendix B: Other Remote Access Solutions

Back to My Mac is just one way to gain remote control of your Mac. If you want only to view and control a remote computer, running Mac OS X's built-in Screen Sharing feature via iChat, Bonjour, or a direct connection may be an good alternative. However, if you need more features—or different features—Timbuktu Pro, LogMeIn, and Apple Remote Desktop are three others I recommend for particular purposes. In this section, I look at each of these products in turn.

Citrix's GoToMyPC, one of the oldest software/service combinations, released a Mac-compatible version of its software just as this edition was being completed. I explain it briefly at the end.

LOGMEIN

LogMeIn, which is both the company and software's name, offers browser- and mobile-device-based remote access to computers (https://secure.logmein.com/US/home.aspx). On the Mac, LogMeIn offers a free service that includes just screen control—you don't get file sharing or other features found in certain of the company's Windows releases. (A Pro version with a monthly fee that adds file transfer and other options was in beta testing as I finished this book.)

LogMeIn uses a Web-browser plug-in combined with Java or other Web technology to display the remote screen within a browser window. (iPhone and iPod touch users can gain similar access using the Ignition app.) The same account can control Windows and Mac systems. I've even set up LogMeIn to control virtual machines running on remote computers!

The software uses robust security (there's no option to turn it off, even), and it handles multiple monitors with aplomb.

Why use LogMeIn instead of Back to My Mac or other forms of Mac OS X Screen Sharing? Because LogMeIn works when:

- A remote machine doesn't have a remotely reachable IP address.
- A network barrier trips up Back to My Mac.
- You are controlling a mix of Mac and Windows systems.
- You need remote access via an iPhone or iPod touch.

Note: I describe several options for remote access from an iPhone or iPod touch—including LogMeIn's Ignition app—in *Take Control of Screen Sharing in Snow Leopard*.

TIMBUKTU PRO

Netopia's Timbuktu Pro (often abbreviated as TB2 by those in the know) is a full-featured remote control and administrative tool (**Figure 28**). TB2 is widely used across Windows and Mac OS X systems in corporations and academia (http://www.netopia.com/software/products/tb2/).

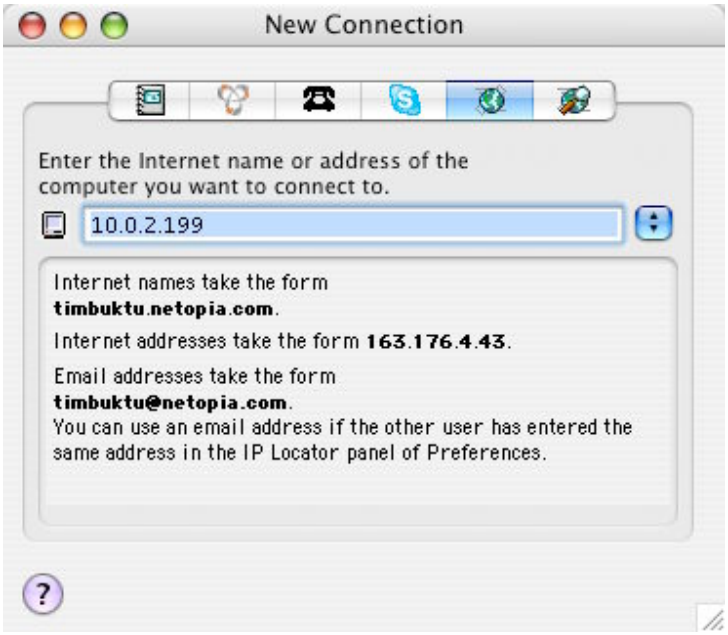


Figure 28: Timbuktu's New Connection window shows its range of support for stored entries, Bonjour-linked computers, dial-up (!), Skype, direct IP connections, and its own form of network discovery.

The software combines both client and server features in one package. You need at least two copies of TB2 to make a connection: one on a target machine, running as a server; the other on the connecting computer, using the client interface (shown in **Figure 28**, previous page). You can choose not to enable incoming access on a computer that you want to use only as a client (to connect to other remote systems).

TB2 has two substantial flaws for use outside large organizations:

- **High cost:** It's expensive. The downloadable version starts at $94.95 for a single license, but you need at least two copies to make a connection. A two-system license is $179.95; volume discounts are available for larger numbers of licenses.
- **No NAT:** TB2 can't reach through NAT on its own. The NAT problem is more substantial than the cost problem. Timbuktu Pro, even in its 8.7 version for Leopard or 8.8 for Snow Leopard, doesn't talk to NAT-PMP or UPNP, so even if you have a publicly routable IP address on your router, you can't use TB2. But, see The Skype Workaround, next page, for a possible solution.

Timbuktu Pro does, however, have a host of advantages:

- Support for both Mac and Windows computers.
- Multiple accounts (both using built-in Mac and Windows user accounts and Timbutku Pro accounts) with actions limited by user.
- A wide array of transfer and communications options, including file transfer and intercom (chat).

The Skype Workaround

Netopia added a way around Timbuktu's NAT limitation that I've found useful, but not perfect in practice: the company takes advantage of Skype's awesome NAT traversal, which seems to allow Skype to work nearly everywhere, even when firewalls should prevent it.

This Timbuktu feature, which first appeared in TB2 8.6 for the Macintosh, requires a logged-in Skype user at each location. The controls allow each remote user to grant automatic remote access to Skype users with the proper account credentials. In typical use, because of the number of network workarounds that are required to connect two computers over Skype, TB2 remote access can be very sluggish compared to a direct connection between the same two computers. But it does work. Skype, at least, is free.

For more details, see http://www.netopia.com/software/products/tb2/tb2_skype.html.

(Skype's own screen-sharing feature allows you to view another machine only if a user of that computer specifically shares his or her screen with you. It's not useful for unattended remote access to a headless server or to idle computers under your control.)

APPLE REMOTE DESKTOP

Designed mostly for academic and corporate environments, Apple Remote Desktop 3 (often called ARD) lets an administrator control several or dozens of computers (http://www.apple.com/remotedesktop/). You can see all the screens in a group at once, control a screen to provide support, or push your screen to one or more members of the group. It's also used for installing software remotely and limiting how a computer can be used.

ARD's problem, like Timbuktu Pro's, is cost: $299 per controlling computer for ten clients or $499 for unlimited clients. This is a system-administrator model, not a solution for casual use. ARD is compatible with Screen Sharing in Leopard and later, as they both use the same underlying VNC technology. However, you must check a box in either of two places to allow remote VNC access in Leopard or Snow Leopard.

To set up Mac OS X for ARD, open the Sharing preference pane, check either the Remote Management service or the Screen Sharing service, and then click Computer Settings. Whichever service you enabled, you'll then see a dialog that includes an option that reads "VNC viewers may control screen with password"; check that box (**Figure 29**). ARD users on any platform (as well as VNC users) can now gain access.

If Screen Sharing is dimmed: *The Screen Sharing service is dimmed if you've enabled the Remote Management service. The Remote Management service overrides any Screen Sharing settings.*

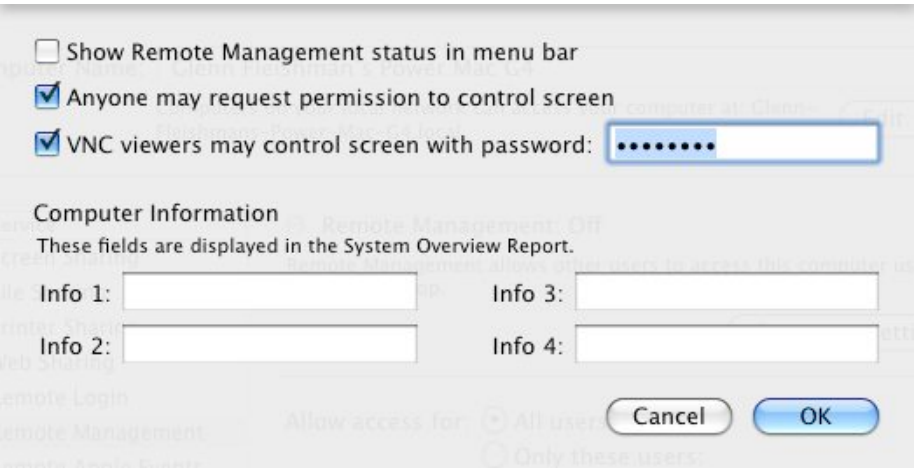


Figure 29: The Remote Management service in the Sharing preference pane.

GOTOMYPC

The folks at Citrix released GoToMyPC (http://gotomypc.com/) way back when it was often impossible to connect two computers on office and home networks to each other because of firewalls, network address translation, and other factors. GoToMyPC just worked.

Long years later, in January 2010, Citrix released a Mac-compatible version of GoToMyPC, which also works under Linux, Unix, Solaris, and some mobile platforms (but not yet iPhone OS).

Citrix charges either $19.95 per month or $179.40 per year for each computer with the server installed for remote access; any Web browser with a free plug-in can access GoToMyPC systems.

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

ABOUT THE AUTHOR

Glenn Fleishman is a technology journalist based in Seattle, where he lives with his wife and two sons, both of whom are adept at accidentally pressing the Power button on his laptop. He's a contributing editor at *TidBITS,* responsible for much of their Web and publishing infrastructure; a columnist for the *Seattle Times* on all things Mac related; and a regular contributor to the *Economist*, *Macworld,* and *Ars Technica*. He appears regularly on public radio, including his local station, KUOW-FM.

AUTHOR'S ACKNOWLEDGMENTS

I would like to thank Tonya for her extensive development work on this book, and Dan for his patience in persisting through drafts while also awaiting his second child's arrival during this book's first version! This book originally began as a larger tome comprising both screen sharing and Back to My Mac, but it became clear that the two topics, though intertwined, had so many differences that we needed to de-intertwingle them. Thanks, then, Tonya and Dan, for your work in birthing two books, and revising this one through its various versions so far.

SHAMELESS PLUGS

I write daily about Wi-Fi networking at my own Wi-Fi Networking News (http://wifinetnews.com/), a site that I've edited since 2001; and all things Mac at *TidBITS* (http://www.tidbits.com/). I'm also the author or co-author of several other Take Control books, most recently *Take Control of Sharing Files in Snow Leopard*, *Take Control of Your 802.11n AirPort Network*, and *Take Control of Your Wi-Fi Security*.

ABOUT THE PUBLISHER

Publishers Adam and Tonya Engst have been creating Macintosh-related content since they started the online newsletter *TidBITS,* in 1990. In *TidBITS*, you can find the latest Macintosh news, plus read reviews, opinions, and more (http://www.tidbits.com/).

Adam and Tonya are known in the Mac world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.

PRODUCTION CREDITS

Take Control logo: Jeff Tolbert

Cover: Jon Hersh

Technical Editor: Dan Frakes

Editor in Chief: Tonya Engst

Publisher: Adam Engst

Production Assistants: Shelly Goldhar, Morgen Jahnke

Thanks to Lorna and Andrew for chocolate cake. And, very special thanks to the folks at Earth Arts for taking care of Tristan!

Copyright and Fine Print

Take Control of Back to My Mac

ISBN: 978-1-933671-46-8

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 the trademarks or the registered trademarks of Apple Inc.; to view a complete list of the trademarks and of the registered trademarks of Apple Inc., you can visit http://www.apple.com/legal/trademark/appletmlist.html.

Featured Titles

Now that you've seen this book, you know that Take Control books have an easy-to-read layout, clickable links if you read online, and real-world info that puts you in control. Click any book title below or visit our Web catalog to add to your Take Control collection!

Take Control of Mac OS X Backups (Joe Kissell): Set up a rock-solid backup strategy so that you can restore quickly and completely, no matter what catastrophe arises. $15

Take Control of MobileMe (Joe Kissell): This ebook helps you make the most of the oodles of features provided by a $99-per-year MobileMe subscription. $10

Take Control of Permissions in Snow Leopard (Brian Tanaka): Solve quirky problems, increase privacy, and share files better. $10

Take Control of Running Windows on a Mac (Joe Kissell): With Intel-based Macs, it has become possible to run Windows software on a Mac, and with Joe's advice, it's easy! $10

Take Control of Screen Sharing in Snow Leopard (Glenn Fleishman): Learn about the many screen-sharing options and get going with the right one for your situation! $10

Take Control of Sharing Files in Snow Leopard (Glenn Fleishman): Share files the smart way! Get help with picking hardware and software, set up, sharing with Windows users, and more. $10

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. $10

Take Control of Your 802.11n AirPort Network (Glenn Fleishman): Make your AirPort network fly—get help with buying the best gear, set up, security, and more. $15

Take Control of Your Wi-Fi Security (Engst & Fleishman): Learn how to keep intruders out of your wireless network and protect your sensitive communications! $10