NOTE ▶ Most third-party applications will not honor parental controls' content filters and account limit settings. Examples of unsupported applications include the Firefox browser and Entourage email client. This is, however, ~~is~~ easily remedied by using the aforementioned parental controls application restriction list.

[delete]

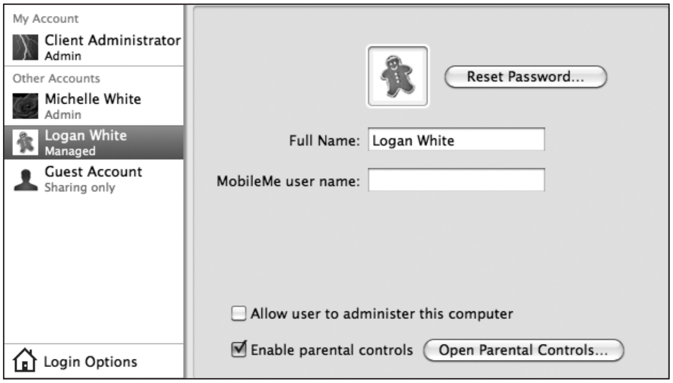
To enable and configure parental controls:

1. Open the Accounts preferences and authenticate as an administrative user to unlock its settings.

2. Select the user from the accounts list you wish to manage with parental controls.

3. Ensure that the Enable parental controls checkbox is enabled.

   If not, Click the Enable parental controls checkbox and you will see the user's account type change from Standard to Managed in the accounts list.



Full Name: Logan White

MobileMe user name:

□ Allow user to administer this computer

☑ Enable parental controls

4. Click the Open Parental Controls button. You can also access the Parental Controls preferences directly from the main System Preferences window.

5. Select the user you wish to manage from the accounts list and use the tabs to navigate through all the options.

TIP ▶ You can use the `mkdir` command to quickly create temporary folders for command-line testing. You can also use the `touch` command followed by a filename to quickly create temporary files for command-line testing. While the original purpose of the `touch` command is to update the modification date of the specified item, it will also create an empty file if it doesn't already exist.

cp

Short for "copy," this command will copy items from one location to another. The syntax is `cp` followed by the path to the original item, and ending with the destination path for the copy. In the following example, Michelle uses the `cp` command to create a copy of testfile located at the root of her home folder and place the copy, testfile2, in her Desktop folder.

NOTE ▶ Remember, if you want to copy a folder and its entire contents you must tell the `cp` command to run recursively by adding the `-R` option.

```
MyMac:~ michelle$ ls
Desktop Library Pictures testfile
Documents Movies Public
Downloads Music Sites
MyMac:~ michelle$ cp testfile Desktop/testfile2
MyMac:~ michelle$ ls Desktop/
testfile2
```

When working with the `cd` command, specifying a destination folder but no filename will make a copy with the same name as the original. Specifying a destination filename but not a destination folder will make a copy in your current working folder. Further, unlike copying with the Finder, the `cp` command will not warn you if your copy will replace an existing file. It will simply delete the existing file and replace it with the copy you told it to create. This behavior is true of most commands.

TIP ▶ You can use the secure copy command `scp` to copy files between networked Macs via SSH remote login. Enabling SSH remote login is covered in Chapter 8, "Network Services."

Alternately you can manage the sudo configuration file /etc/sudoers. This file contains the rules by which the sudo command determines allowable actions. As an administrative user you can read this configuration file using the cat or less commands. In the following example, Michelle uses cat to read the sudo configuration file. Note that she must preface the cat command with sudo because the sudoers file is protected by root access. Also, the output of the less command has been truncated to show only the most interesting bits of the sudoers file.

```
MyMac:~ michelle$ sudo cat /etc/suders
Password:
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
# Failure to use 'visudo' may result in syntax or file permission errors
# that prevent sudo from running.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
...
# User privilege specification
root         ALL=(ALL) ALL
%admin       ALL=(ALL) ALL
...
```

As you can see from the “User privilege specification” section of this file, the root user or anyone in the admin group is allowed unrestricted sudo access to all commands. You can edit this file, but note that the document states you must use a special version of the vi command known as visudo. Using vi to edit text files is covered earlier in this chapter.

Once you are familiar with vi usage, editing the sudoers file with visudo is quite easy. To disable administrative user sudo access, simply add a hash mark (#) to the beginning of the %admin line, and the sudo command will ignore that line. You can add additional users or groups for sudo access by duplicating the existing user privilege lines with alternate account names. Just remember to use only the account’s “short” name and to use the percent symbol (%) to specify any group names.

Command-Line “Helpers”

Before you begin command-line scripting proper, there are a few special characters and commands that help facilitate automation at the command line. Examples include `grep`, | (pipe), and > (redirect).

grep

This command, short for Global Regular Expression Print, searches for patterns (using regular expressions) in text and outputs only the lines that match. This is not only useful for filtering out specific information in an existing large file; it’s also useful to filter the output of other commands, as you’ll see in the description of pipe later in this section. To filter through an existing file enter `grep`, followed by the search expression, and then the path to the file.

MORE INFO ▶ The `grep` command uses regular expressions as filter criteria, which are similar to the wildcard characters covered previously in this chapter. You can find out more about regular expressions by entering `man re_format` at the command line.

In the following example Michelle uses `grep` to filter for the phrase “afp” in the /etc/services file. This file lists all the common network ports and services, but it’s over 14,000 lines long. The `grep` command finds the two requested lines almost instantly, which is obviously much faster than a human could.

```
MyMac:~ michelle$ grep "afp" /etc/services
afpovertcp      548/udp     # AFP over TCP
afpovertcp      548/tcp     # AFP over TCP
```

| (pipe)

The special character “|”, entered via Shift-Backslash on U.S. keyboards, is called a pipe. As its name implies, it pipes the output of one command to the input of another command.

[delete "is"]

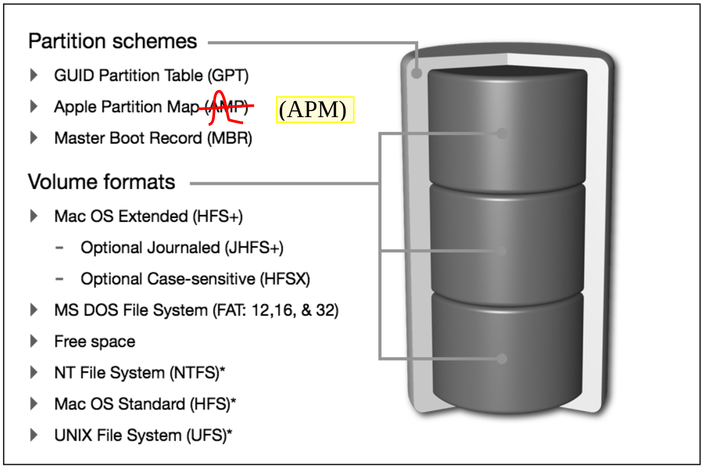
This ~~is~~ can be used to great effect when combining command features. For example the `system_profiler` command is equivalent to the System Profiler application, but instead it defaults to outputting the information as plain text to the Terminal window. This makes it extremely inconvenient to read the output from this command, much less find exactly what you’re looking for.

File System Components

Before you begin managing storage on Mac OS X, it is important to understand the distinction between storage, partitions, and volumes. Traditionally, computer storage has been defined by disk drive hardware. After all these years, disk drive hardware still maintains the storage lead, as it has moved from removable floppy disks to enclosed hard disks. However, other more convenient removable formats have become extremely popular as they have increased in capacity. This includes optical media like CDs and DVDs and solid-state storage like SSD, USB key drives, and CompactFlash cards. All are equally viable storage destinations for Mac OS X.

Without proper formatting, though, any storage technology is nothing more than a big empty bucket of ones and zeros, and consequently not very useful to the Mac. Formatting is the process of applying logic to storage in the form of partitions and volumes. Partitions are used to define boundaries on a storage device. You can define multiple partitions if you want the physical storage to appear as multiple separate storage destinations. Even if you want to use the entire space available on a device as a single contiguous storage location, the area must still be defined by a partition.

Once partitions have been established, the system can create usable volumes inside the partition areas. Volumes define how the files and folders are actually stored on the hardware. In fact, it's the volume that is ultimately mounted by the file system and then represented as a usable storage icon in the Finder. Obviously, a storage device with several partitions, each containing a separate volume, will appear as several storage location icons in the Finder.



Volume formats supported as read/write in Mac OS X:

- Mac OS Standard (HFS)—This is the legacy volume format used by the classic Mac OS. This format, though a precursor to HFS+, is not supported as a startup volume for Mac OS X.
- File Allocation Table (FAT)—FAT is the legacy volume format used by Windows PCs and still used by many peripherals. This format has evolved over the years, with each progressive version supporting larger volumes; FAT12, FAT16, FAT32. Apple's Boot Camp supports running Windows from a FAT32 volume, but Mac OS X itself cannot start up from such a volume. Boot Camp is covered in Chapter 6, "Applications and Boot Camp."
- UNIX File System (UFS)—UFS is the legacy native volume format supported by Mac OS X. UFS served as the default UNIX file system for decades. Starting with Mac OS X v10.5, though, UFS volumes are no longer supported as startup volumes. Further, Disk Utility does not support the creation of UFS volumes.

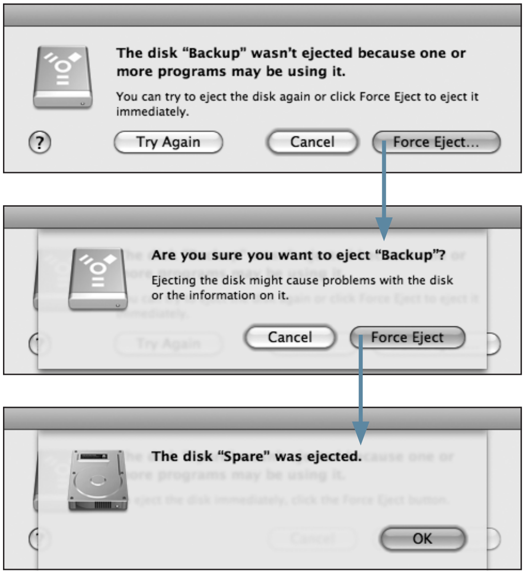
Volume formats supported as read-only in Mac OS X:

- NT File System (NTFS)—Windows 7, Windows Vista, Windows XP, and Windows Server all use this as their native volume format. Once again Boot Camp supports running Windows from an NTFS volume, but Mac OS X itself cannot write to or start up from such a volume. Further, Disk Utility does not support the creation of NTFS volumes.

  TIP You can add NTFS volume write support to Mac OS X by installing the free and open source NTFS-3G and MacFUSE software bundle: http://macntfs-3g.blogspot.com.

- ISO 9660 or Compact Disk File System (CDFS)—This is a common standard for read-only CD media. Note, however, that "Mac formatted" CD media can contain HFS-formatted volumes.
- Universal Disk Format (UDF)—This is a common standard for read-only DVD media. Again, note that "Mac formatted" DVD media can contain HFS-formatted volumes.

  MORE INFO ▸ A wide variety of file systems are out there. Wikipedia has a great comparison of all file systems: http://en.wikipedia.org/wiki/Comparison_of_file_systems.



The disk "Backup" wasn't ejected because one or more programs may be using it.

You can try to eject the disk again or click Force Eject to eject it immediately.

Are you sure you want to eject "Backup"?

Ejecting the disk might cause problems with the disk or the information on it.

The disk "Spare" was ejected.

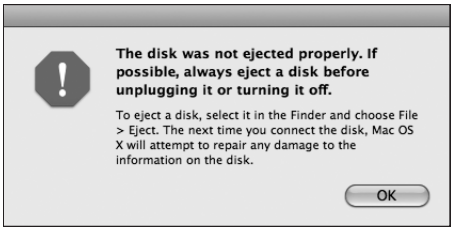
If this doesn't work or the Finder doesn't tell you which application is suspect, you can always log out the current user to quit all their processes and re-log in, or fully restart the Mac to clear the issue. While this may seem excessive, it is not advisable to physically disconnect a volume without first unmounting it, as covered in the next section.

If a volume still refuses to unmount after you've tried the previous troubleshooting steps, or you are unable to restart the computer, you can force a volume to unmount using the `diskutil` command. Again, it's not advisable to force the system to unmount a volume, but if you need to unmount the volume, this method is better than physically disconnecting the drive from the Mac. The following command-line example shows how to forcibly unmount a volume named "ExternalDrive"; further, using this technique also requires administrator authentication:

```
MyMac:~ michelle$ sudo diskutil unmount force /Volumes/Backup
```

Improperly Unmounting or Ejecting

Disconnecting a volume from the Mac that you did not first unmount can lead to data corruption. If you forcibly eject a drive by physically disconnecting it before you unmount it, or if the system loses contact with the drive due to power failure, the Mac will warn you with a Device Removal dialog. You should immediately reconnect the device so the Mac can attempt to verify or repair its contents.



The disk was not ejected properly. If possible, always eject a disk before unplugging it or turning it off.

To eject a disk, select it in the Finder and choose File > Eject. The next time you connect the disk, Mac OS X will attempt to repair any damage to the information on the disk.

Any time you reconnect a drive that was improperly unmounted, the Mac will automatically run a file system diagnostic on the drive before it remounts any volumes. Depending on the format and size of the drive, it may take anywhere from a few seconds to several hours for the system to verify the contents of the drive. Again, journeyed volumes like JHFS+ should verify quite quickly. So if you connect a drive and notice there is a fair amount of drive activity but the volumes have not mounted yet, the system is probably running a diagnostic on the drive. You can verify that the system is diagnosing a volume by opening the /Applications/Utilities/Activity Monitor application and looking for a background process with `fsck` in its name. Monitoring processes is covered in Chapter 6, “Applications and Boot Camp.”

Using Software RAID

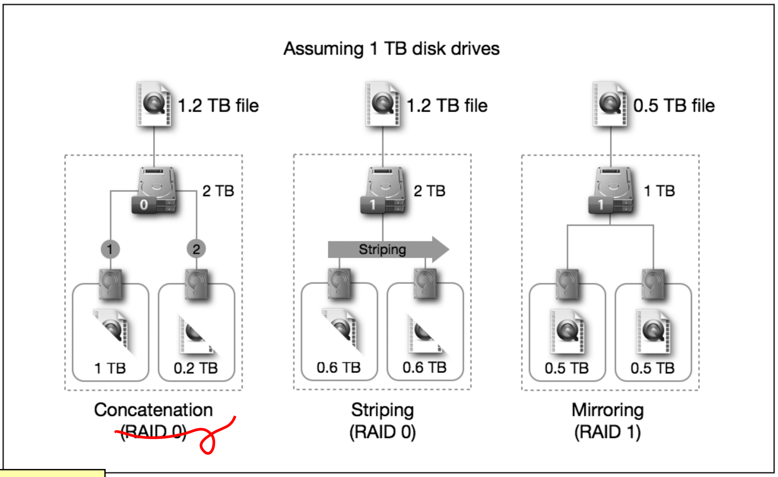
The idea behind RAID (Redundant Array of Independent Disks) is that you can combine similar drives together to form large volumes with increased performance or reliability. The downside is that you have to have special hardware or software to manage the RAID. Hardware-based RAID solutions are often external to the computer because they contain many drives and include specialized hardware to manage the RAID. Conversely, software-based RAID solutions don’t require any special hardware as they use software running from the computer’s processor to manage the RAID.

remember that mirroring is not a backup solution. Backup solutions create an archive of the data frozen in time and save it to another storage device. If hardware failure occurs, you can recover from a previous backup version of the data. With a mirrored RAID set, all file system changes are applied immediately to all drives in the set and no archival history is maintained.

NOTE ▸ Keep in mind that with a RAID 1 set, if a drive fails your Mac may keep running without warning you. This may leave you with only a single drive in your RAID set, effectively disabling the redundancy. You should periodically check the status of a RAID 1 set from the Disk Utility application.

- ▸ Nested RAID, 1+0 or 0+1—Because RAID 0 and RAID 1 offer opposed feature sets, nesting one type inside of the other can provide the features of both. In other words, you can stripe data between two mirrors, or you can mirror data on two stripes. These nested configurations are certainly more complicated and require a minimum of four separate drives. However, when you combine their features you get increased performance and redundancy.
- ▸ Concatenated disk set—This isn't what most would consider a true RAID configuration, as not all drives are being used simultaneously. With a concatenated disk set, the system will simply continue on to the next drive once the previous drive is filled. The only advantage here is that the user will see one large volume instead of several separate drives.

MORE INFO ▸ You can find out more about all the different RAID types by visiting Wikipedia's RAID entry, http://en.wikipedia.org/wiki/RAID.



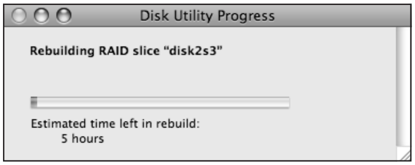
[Please remove or hide "(RAID O)" in leftmost label, if possible.]

3 Depending on the failure mode of the RAID set, you will need to choose one of two resolutions:

- **Inconsistent data.** The system has discovered that one of the drives does not have the same data as the others. You will see the word “Failed” next to the drive with inconsistent data. Simply click the Rebuild button to repair the RAID set.

- **Bad or missing drive.** The system can no longer access one of the drives. You will see the word “Offline” next to the missing drive. Select the missing drive from the RAID dialog, and then click the small minus button below the RAID dialog to delete the missing drive. Drag the replacement drive from the column on the left to replace the missing drive from the RAID diagram. Click the Rebuild button to repair the RAID set.

Depending on the size and performance of the RAID set, the rebuild process can take anywhere from seconds to days. Disk Utility will open a progress dialog with the estimated time required to complete the rebuild task.



Rebuilding RAID slice “disk2s3”

Estimated time left in rebuild:
5 hours

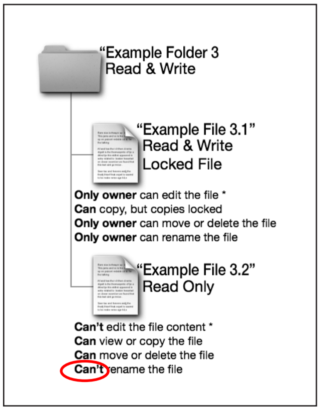
Using Optical Media

Over a decade ago, Apple made headlines by introducing the iMac with only an optical drive, choosing to banish the traditional floppy disk drive from the new computer’s revolutionary design. It should come as no surprise, then, that every Mac sold today (except for the super-thin MacBook Air, which has no room for an internal optical drive) includes a CD/DVD writer.

TIP You can easily identify the capabilities of your Mac’s optical drive by opening /Applications/Utilities/System Profiler and viewing the Disc Burning information section.

Example 2: You have read-only permission to Example Folder 2. You can edit the content of Example File 2.1 because you have read and write access to it, but you can't move, delete, or rename it because you have read-only access to the folder's contents. On the other hand, you can effectively delete the file by erasing its contents. Example File 2.2 is the only truly secure file, as you're only allowed to view or copy the file. Granted, you can make changes to the contents of a copied file, but you still can't replace the original.

NOTE ▶ Many applications cannot save changes to files inside read-only folders, because these applications attempt to replace the original file during the save process, instead of revising the file's content. In other words, you may need read and write access to both the file and the folder it's inside of to save changes to the file.


"Example Folder 3
Read & Write
"Example File 3.1"
Read & Write
Locked File
Only owner can edit the file *
Can copy, but copies locked
Only owner can move or delete the file
Only owner can rename the file
"Example File 3.2"
Read Only
Can't edit the file content *
Can view or copy the file
Can move or delete the file
Can't rename the file

[replace "Can't" with "Can" if possible]

Example 3: Your permissions are identical to the first example, with one significant change. The owner of Example File 3.1 has enabled the locked attribute. Even though you have read and write access to Example Folder 3 and File 3.1, the locked attribute prevents all users who aren't the file's owner from modifying, moving, deleting, or renaming the file. From most applications, only the owner is allowed to change the file's content or delete it, but the owner can also disable the locked attribute to return the file to normal. You can still make a copy of the locked file, but the copy will be locked as well. However, you will own the copy, so you can disable the locked attribute on the copy, but you still can't delete the original locked file unless you're the owner.

MORE INFO ▶ The locked attribute is covered in the "Managing Locked Items via Finder" section later in this chapter.

Answers

1. Disk drives are the actual storage hardware, partitions are logical divisions of a disk drive used to define the storage space, and volumes, contained inside partitions, are used to define how the individual files and folders are saved to the storage.

2. GUID Partition Table is the default partition scheme on Intel-based Macs, and Apple Partition Map is the default partition scheme on PowerPC-based Macs.

3. The volume formats supported as startup volumes for Mac OS X are Mac OS X Extended, the native volume format supported by all Macintosh computers; Mac OS X Extended, Journaled, the default volume format for Mac OS X drives; and Mac OS X Extended, Journaled, Case-Sensitive, the default volume format for Mac OS X Server drives. Volume formats supported as read/write are Mac OS Standard (HFS), a legacy Mac OS volume format; UNIX File System (UFS), a legacy volume format supported by many other UNIX-based systems; and File Allocation Table (FAT32), the volume format used by many peripherals and older Windows-based PCs. Volume formats supported as read-only: NT File System (NTFS), the native volume format used by modern Windows-based operating systems; ISO 9660, a common format for CD media; and Universal Disk Format (UDF), a common format for DVD media.

4. File system journaling records what file operations are in progress at any given moment. This way, if a power failure or system crash occurs, after the system restarts it will be able to quickly verify the integrity of the volume by "replaying" the journal.

5. The four erase options in Disk Utility are Don't Erase Data, which simply replaces the volume's directory structure; Zero Out Data, which provides good security by writing zeros on top of all the previous drive data; 7-Pass Erase, which provides even better security by writing seven separate passes of random information on top of all the previous drive data; and 35-Pass Erase, which provides the best security by writing 35 separate passes of random information on top of all the previous drive data.

6. The Finder's Secure Empty Trash will perform a 7-pass erase on the contents of the Trash folder.

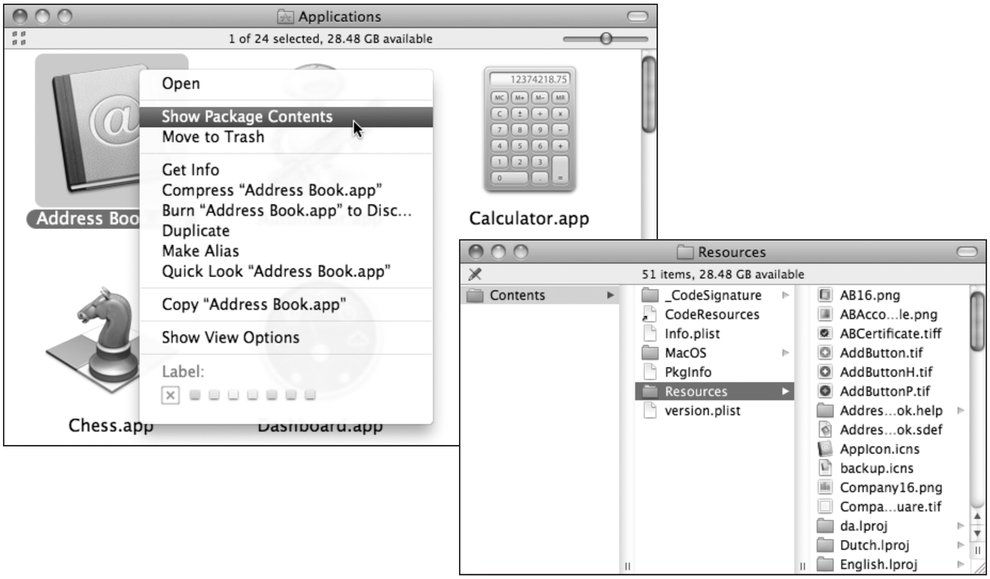
7. The three methods used to eject a volume or drive from the Finder are press and hold the Eject key for a few moments to unmount and eject optical media; select the volume you wish to unmount and eject from the Finder and choose File > Eject from the menu bar; and finally, in the Finder's sidebar, click the small eject button next to the volume you wish to unmount and eject.

application. Other software bundles and packages, on the other hand, are often much more complex as they contain all the resources necessary for the application or software.

Software bundles or packages often include:

- Executable code for multiple platforms
- Document description files
- Media resources such as images and sounds
- User interface description files
- Text resources
- Resource forks
- Resources localized for specific languages
- Private software libraries and frameworks
- Plug-ins or other software to expand capability

Although the Finder default is to hide the contents of a package, you can view the contents of a package from the Finder. To access the content of a package in the Finder, simply right-click or Control-click on the item you wish to explore, and then choose View Package Contents from the shortcut menu.



Mac OS X Process Features

Mac OS X is a desirable platform for running applications and other processes because it combines a rock-solid UNIX foundation with an advanced graphical user interface. Users will most likely recognize the graphical interface elements right away, but it's the underlying foundation that keeps things running so smoothly. Specifically, a few fundamental features of Mac OS X are responsible for providing a high level of performance and reliability.

Mac OS X Process Performance Features

- Preemptive multitasking—This gives Mac OS X the ability to balance computing resources without letting any single process take over. It allows the system to maintain dozens of background processes without significantly slowing down user applications.
- Symmetric multiprocessing—Whenever possible the system will use all available computing resources to provide the best performance. This is a key feature since every currently shipping Mac includes at least two processor cores. Mac OS X v10.6 introduces two new unique multiprocessing features, Grand Central Dispatch and OpenCL, which provide for even greater performance than previous versions of Mac OS X. Grand Central Dispatch makes it much easier for application developers to take full advantage of not just multiprocessor systems, but also multicore processors. OpenCL takes this even further by allowing applications to use your Mac's powerful graphics processor to accelerate general computing tasks.
- Simultaneous 32-bit and 64-bit support—Mac OS X is one of the few operating systems that supports both 32-bit and 64-bit modes simultaneously. A process running in 64-bit mode has the ability to individually access more than 4 GB of system memory, can perform higher-precision computational functions much faster, and can take advantage of Intel's updated x86-64 architecture for improved performance and security. Only Macs featuring 64 bit–capable processors can take advantage of 64-bit system features. Currently, Macs with Intel Core2Duo or Intel Xenon processors include 64-bit support. Mac OS X v10.5 improved 64-bit support by allowing both command-line and graphical interface applications to access 64-bit resources. With Mac OS X v10.6, Apple updated nearly all included software to take advantage of 64-bit resources, including the core of Mac OS X, the system kernel.

  NOTE ▶ Mac OS X always defaults to a 32-bit kernel for compatibility with older kernel extensions. More about the 64-bit kernel is covered in Chapter 10, "System Startup."

Carbon

The Carbon application environment is a streamlined and updated version of the previous Mac OS 9 environment. Developers can update their legacy Mac applications, often with little work, to run natively in Mac OS X. Carbon is based on the industry-standard C and C++ programming languages. On the surface, it's hard to identify any differences between Carbon and Cocoa applications. With every new version of Mac OS X, Apple has further blurred the lines between Cocoa and Carbon. In fact, many modern applications contain code that takes advantage of both environments.

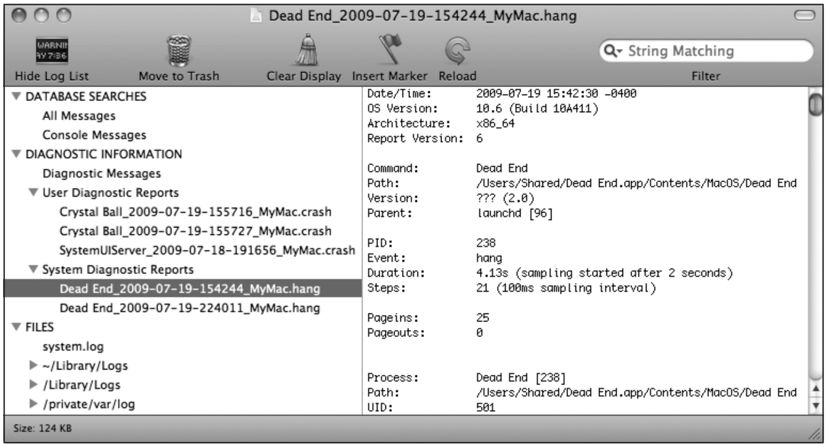
MORE INFO ▶ To learn more about Carbon, see Apple's development resources, http://developer.apple.com/carbon.

Java

Java is an application environment developed by Sun Microsystems with the goal of creating non-platform-specific applications. This means a developer can create software code once and it can run on many different environments. Mac OS X includes both 32-bit and 64-bit Java SE 6 (Standard Edition). This implementation supports Java in two ways: Java applets and full Java applications.

Most full Java applications are also delivered via a web download from a small Java Web Start (.jnlp) file. Double-clicking on a .jnlp file opens /System/Library/CoreServices/Java Web Start, which downloads the remainder of the Java application to ~/Library/Caches/Java/cache. Once the download is complete, the Java application runs in its own environment alongside your other Mac applications. When you open a Java application the second time, the Java Web Start application automatically converts the small .jnlp file to a stand-alone Java application. You can further adjust Java applications by opening the /Utilities/Java Preferences application.

with the name of the application followed by ".hung" is saved in the local /Library/Logs/DiagnosticReports folder. The easiest way to view these reports is to open the /Applications/Utilities/Console application, and then click the Show Log List button in the toolbar. The problem reports will be chronologically listed in the Diagnostic Information section.



```
Date/Time:       2009-07-19 15:42:30 -0400
OS Version:      10.6 (Build 10A411)
Architecture:    x86_64
Report Version:  6

Command:         Dead End
Path:            /Users/Shared/Dead End.app/Contents/MacOS/Dead End
Version:         ??? (2.0)
Parent:          launchd [96]

PID:             238
Event:           hang
Duration:        4.13s (sampling started after 2 seconds)
Steps:           21 (100ms sampling interval)

Pageins:         25
Pageouts:        0


Process:         Dead End [238]
Path:            /Users/Shared/Dead End.app/Contents/MacOS/Dead End
UID:             501
```

These problem report logs include highly technical information that most will not understand, but they also include key pieces of information that may help the average troubleshooter diagnose the issue. For example, diagnostic reports often indicate which files were being used by the application at the time. One of the reported files could be the source of the problem due to corruption.

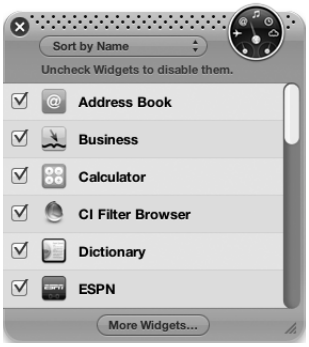
Preference Troubleshooting

Applications primarily access two types of often-changing files during their use: the documents that the application is responsible for viewing or editing and the preference files that contain all the application's settings. From an administration perspective, preference files are often more important, as they may contain important settings that are required for an application to work properly. For instance, an application's serial number or registration information is often stored in a preference file.

Preference files can be found in any Library folder, but most application preferences end up in the user's Library, specifically in the ~/Library/Preferences folder. This is because the local Library should only be used for system preferences. More important, it enables each user to have his own application settings that do not interfere with other users' applica-

3 With the widget bar open, click the Manage Widgets button or the Widgets icon in the bottom right corner of the screen.

This will open the widget manager that allows you to disable installed widgets or download new widgets from Apple's website.



Sort by Name

Uncheck Widgets to disable them.

☑ Address Book
☑ Business
☑ Calculator
☑ CI Filter Browser
☑ Dictionary
☑ ESPN

More Widgets...

4 From the widget manager click the More Widgets button, and it will automatically open the default web browser and take you to Apple's online widget repository.

At this point you can browse and download any additional widgets that strike your fancy. Alternately you can acquire widgets using any method you like including other websites or file sharing.

TIP You can also create your own custom widgets from web pages in Safari by selecting File > Open in Dashboard from the menu bar.

5 If you downloaded the widget with Safari, it will automatically prompt for installation. However, if you acquired the widget through other means you will have to double-click on the widget file in the Finder to start the widget installer.

- 2 GB or more of RAM when running Windows Vista on a Mac Pro—Windows Vista is a notorious resource hog. Mac Pros require more memory when used by Windows Vista because they use Intel Xeon processors.
- Boot Camp Assistant—Included with Mac OS X, Boot Camp Assistant is located at /Applications/Utilities/Boot Camp Assistant.
- A single full-install Windows install disc—At the time of this writing, Boot Camp supports full installations of Windows XP Home Edition or Professional with Service Pack 2 or later, or Windows Vista Home Basic, Home Premium, Business, and Ultimate including both 32-bit and 64-bit versions.

Boot Camp Caveats

Before installing Windows using Boot Camp, be aware of its known limitations:

- The Boot Camp Assistant cannot be used on drives containing more than one partition.

  TIP You can dynamically repartition your Mac's internal hard drive to restore it to a single partition using Disk Utility, as covered in Chapter 4, "File Systems."

  TIP Though not supported by Apple, as an alternative you can set as many partitions as you want using Disk Utility as covered in Chapter 4, "File Systems." However, Boot Camp will only work from the last Windows-formatted partition of the drive.

- Boot Camp does not work with external hard drives.
- If you are installing Windows on a portable computer, always connect the power adapter to ensure that the laptop remains on during the entire Windows installation process.
- Do not use Windows-based tools to create or modify partitions on drives containing Mac volumes. Doing so may delete Mac-formatted volumes or render your system drive unbootable. However, you can use Windows-based tools to modify individual volume formatting.
- Mac OS X includes support for mounting NTFS volumes as read only. So, while using Mac OS X you'll be able to view and copy the contents of Windows volumes, but you won't be able to write changes.

use packet-switching technology to route and transmit data. Almost all digital networking technologies are packet-based because this provides efficient transport for network connections that aren't always reliable. Remember, the TCP/IP protocol was originally designed with the military in mind, so packet-based network technology is ideal because it's designed to work around communications link failure. This is why sophisticated routing hardware was originally developed for TCP/IP networks, so data could be literally rerouted and re-sent should a network link go down.

A lesser-used protocol known as User Datagram Protocol (UDP) is also attached to the TCP/IP suite. UDP is a simpler protocol that does not guarantee the reliability or ordering of data sent across networks. This may seem like a poor choice for networking, but in some cases UDP is preferred because it provides better performance than TCP. Examples of network services that use UDP include the Domain Name System (DNS), media streaming, voice over IP (VoIP), and online gaming. These services have been designed to tolerate lost or out-of-order data so they can benefit from UDP's increased performance.

MORE INFO ▶ For more information regarding the Internet protocol suite, refer to this Wikipedia entry: http://en.wikipedia.org/wiki/internet_protocol_suite.

Networks in Action

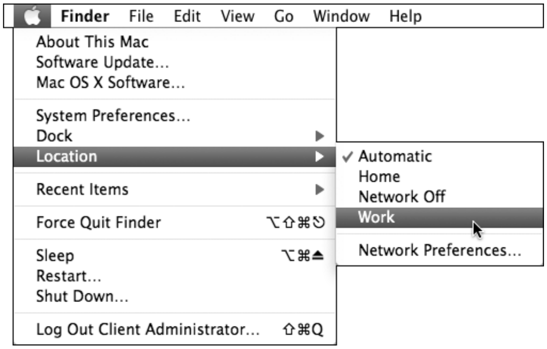
Manually assigning an IP address, a subnet mask, and a router address is technically all that is needed to configure a computer to use TCP/IP-based networking on both local area networks (LANs) and wide area networks (WANs). Yet there are two other network services that are almost always involved in basic network functionality: Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS). These two services, combined with TCP/IP, characterize core network functionality that provides the foundation for nearly any network service.

You may have noticed that the Network preferences is different from all the other system preferences in that you must click the Apply button to activate the new settings. This allows you to easily prepare new network locations and settings without disrupting the current network configuration.

Changing Network Locations

Though you can certainly choose and apply a different network location from the Network preferences, only administrative users have this ability, as normal users do not have access to the Network preferences. Conversely, all users who can log in to the Mac OS X graphical user interface can quickly and easily change the network location by choosing Apple menu > Locations > *location name* from the menu bar. This will apply the selected network location. Keep in mind that changing locations may interrupt network connections. Once a network location is selected, it will remain active until another location is selected. Even as other users log in to the Mac, or the Mac is restarted, the selected network location will remain active.

[replace:]
Location



Using Hardware Network Interfaces

Mac hardware has a long history of providing built-in network connectivity. Apple started including Ethernet on Macs as early as 1991 and was the first manufacturer to have wireless as a built-in option when it introduced the iBook in 1999. Mac models have varied over the years as network technologies have grown increasingly faster and more affordable. You can identify the hardware network interfaces and services available to your Mac from the /Applications/Utilities/System Profiler application. Detecting network

If you configure multiple WINS servers, the system will attempt to access those resources in the order they appear in the list. To edit a server address, double-click its entry in the list, or you can delete a server by selecting it and clicking the minus button at the bottom of the list.

6 When you have entered all the appropriate NetBIOS and WINS settings, click the OK button to dismiss the advanced network options dialog, and then click the Apply button in the bottom-right corner of the Network preferences to save and activate the changes.

If your network requires it, configuring specific NetBIOS and WINS settings will allow your Mac to interact with other Windows-compatible network clients as if you were running Windows natively. Accessing and sharing network services using these two protocols is covered in Chapter 8, "Network Services."

Configuring 802.1X

The 802.1X protocol is used to secure wired and wireless (AirPort) Ethernet networks by only allowing properly authenticated network clients to join the LAN. Networks using 802.1X will not allow any traffic until the network client properly authenticates to the network.

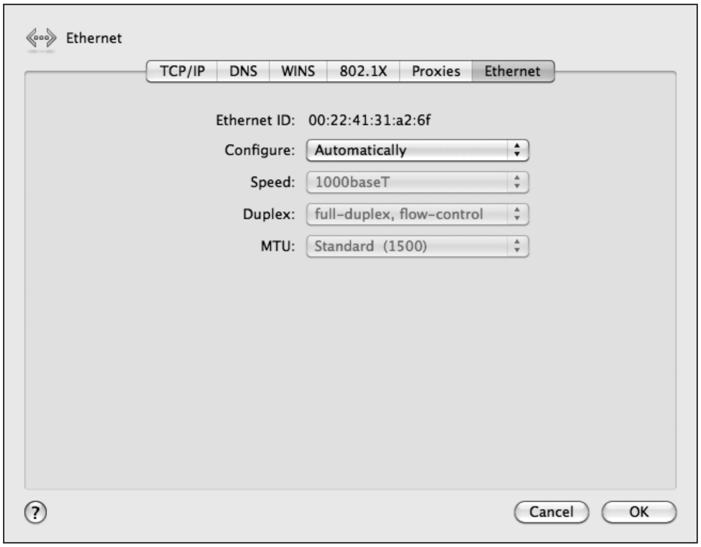
To facilitate 802.1X authentication, Mac OS X provides three types of authentication profiles:

- User Profile—With this configuration the user must manually choose to authenticate to the 802.1X network using account information you've configured. This method requires that users be logged in to the computer with a local account before they can join the 802.1X network. Also, this type of profile is automatically created if you join and authenticate to a wireless network that uses WAP or WAP2 Enterprise. Finally, it's important to note that user profiles are tied to a user's account but not to a network location or interface. Therefore, you can have multiple network locations that can take advantage of a single user 802.1X profile.
- Login Window Profile—Many larger networks use the same usernames and passwords for access to the computers and to their networks. Creating a login window profile allows the system to pass to the network the same credentials that are used to log in the user account to the Mac.
- System Profile—If you want the Mac to always have access to the 802.1X network, you can set a single 802.1X account for the computer as a whole. The account information is saved to the system keychain, and the system will automatically join the network on startup.

2 Select the wired Ethernet service you wish to configure from the network services list, and then click the Advanced button in the bottom-right corner of the Network preferences.

This will reveal the advanced settings dialog.

3 Click the Ethernet tab at the top to view the current automatically configured Ethernet settings.

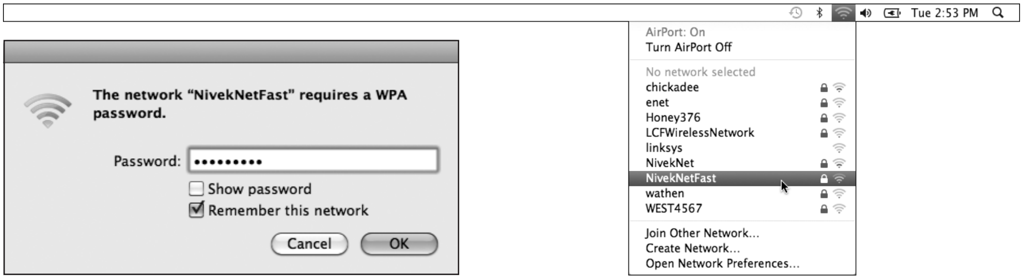


Ethernet ID: 00:22:41:31:a2:6f
Configure: Automatically
Speed: 1000baseT
Duplex: full-duplex, flow-control
MTU: Standard (1500)

4 To manually configure Ethernet options, choose Manually from the Configure pop-up menu. The system will cache the current automatically configured Ethernet settings so you will not have to change all the settings.

The system will prepopulate the Speed, Duplex, and MTU Ethernet options based on your Mac’s network hardwire. Make your custom selections from these pop-up menus.

If you select an open wireless network, the Mac will immediately connect, but if you select a secure wireless network, as indicated by the small lock icon, you will have to enter the network password. By default, the system will automatically remember secure networks by saving the passwords to the system keychain so all users can access the wireless network.



The network "NivekNetFast" requires a WPA password.

Password: •••••••••

☐ Show password

☑ Remember this network

NOTE ▶ If you join and authenticate to a wireless network that uses WAP or WAP2 Enterprise, it's implied that the authentication is handled via 802.1X. Thus, joining this type of network will automatically create an 802.1X User Profile. Conversely, the system does not automatically recognize WEP networks with 802.1X authentication, so you will have to configure this manually as covered in the "Configuring 802.1X" section earlier in this chapter.

To increase security, some wireless networks do not advertise their availability. You can connect to these hidden wireless networks (also called closed networks) as long as you know their network name (or Service Set Identifier, aka SSID) by choosing Join Other Network from the AirPort menu item. This will reveal a dialog where you can enter all the appropriate information to join the hidden wireless network. Again, the system will save this information to the system keychain by default.

Answers

1. An *interface* is any channel through which network data can flow. Hardware network interfaces are defined by physical network connections, while virtual network interfaces are logical network connections that ride on top of hardware network connections. A *protocol* is a set of rules used to describe a specific type of network communication. Protocols are necessary for separate network devices to communicate properly. Finally, a network *service* (as it pertains to the Network preferences) is the collection of settings that define a network connection.

2. The Internet Protocol (IP) address identifies the location of a specific network device. IP addresses are the primary identification used by the Internet protocol suite TCP/IP for both local and wide area networks. Subnet masks are used by network devices to identify their local network range and to determine if outgoing data is destined for a network device on the LAN. Most common IP addresses and subnet masks share the same IPv4 formatting. IPv4 addresses are a 32-bit number represented in four groups of four-digit numbers, known as octets, separated by periods. Each octet has a value between 0 and 255.

3. If a network device needs to send data to another network device on the same LAN, it will address the outgoing packets based on the destination device's MAC address.

4. A network client uses the subnet mask to determine if the destination IP address is on the LAN. If the destination IP address is not on the LAN, then it's assumed the destination address is on another network and it will send the data to the IP address of the local network router. The network router will then send the data, via a WAN connection, on to another router that it thinks is closer to the destination. This will continue across WAN connections from router to router until the data reaches its destination.

5. The DNS service is used to translate host names to IP addresses via forward lookups and translate IP addresses to host names via reverse lookups. DNS is architected as a hierarchy of worldwide domain servers. Local DNS servers provide name resolution and possibly host names for local clients. These local DNS servers connect to DNS servers higher in the DNS hierarchy to resolve both unknown host names and host local domain names.

6. If DHCP is specified as the configuration for a TCP/IP connection and no DHCP service is available, the computer will automatically select a random IP address in the 169.254.xxx.xxx range. It will check the local network to ensure that no other network device is using the randomly generated IP address before it applies the IP address.

7. Mac OS X supports the following network interfaces and protocols:

   Wired Ethernet IEEE 802.3 family of hardware network interface standards

   Wireless (AirPort) IEEE 802.11 family of hardware network interface standards

   FireWire IEEE 1394 hardware network interface

   Analog modem hardware network interface

   Bluetooth wireless hardware network interface

   Virtual private network (VPN) virtual network interface via the Point-to-Point Tunneling Protocol (PPTP)

   VPN virtual network interface via the Layer 2 Tunneling Protocol (L2TP) over Internet Protocol security (IPsec)

   Point-to-Point Protocol over Ethernet (PPPoE) virtual network interface

   6 to 4 virtual network interface

   Virtual local area network (VLAN) virtual network interface via the IEEE 802.1Q standard

   Link Aggregation virtual network interface via the IEEE 802.3ad standard

   Transmission Control Protocol/Internet Protocol (TCP/IP), also known as the Internet protocol suite

   Dynamic Host Configuration Protocol (DHCP)

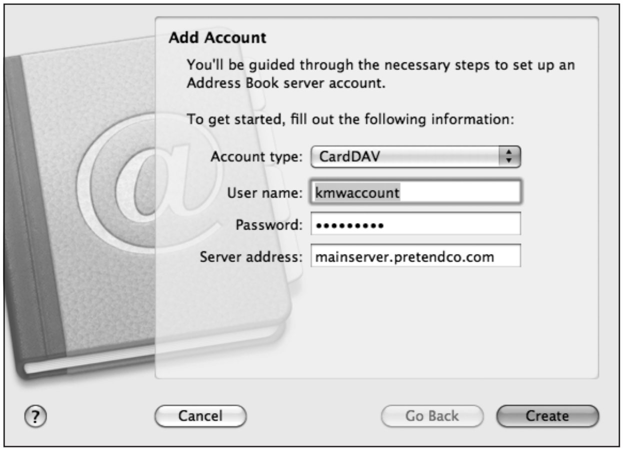
   Domain Name Service (DNS) protocol

   Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) protocols

   Authenticated Ethernet via the 802.1X protocol

   Point-to-Point Protocol (PPP)

8. The network service order list is used to determine the primary network interface if there is more than one active interface. All network traffic that isn't better handled via local connection to an active network interface is sent to the primary network interface. Thus, all Internet traffic is sent through the primary network interface.



Add Account

You'll be guided through the necessary steps to set up an Address Book server account.

To get started, fill out the following information:

Account type: CardDAV

User name: kmwaccount

Password: •••••••••

Server address: mainserver.pretendco.com

Address Book 5 supports the following network contact services:

- Local synchronized contacts—Contacts that are managed locally can be synchronized via the Internet to MobileMe, Yahoo, and Google contact services. All three of these services use the encrypted HTTPS protocol over TCP port 443.
- Directory service contacts—Address Book can search against contact databases via the standard for network directory services, the Lightweight Directory Access Protocol (LDAP). Address Book can be configured for LDAP services either directly from the setup assistant or via integration with Mac OS X's system-wide directory service, as covered later in this chapter.
- CardDAV contact sharing—Address Book supports an emerging calendar collaboration standard known as CardDAV. Again, as the name implies, this standard uses WebDAV as a transport mechanism on TCP port 8800 or 8843 for encrypted, but CardDAV adds the administrative processes required to facilitate contact sharing. Mac OS X Server's Address Book service is based on CardDAV. Furthermore, CardDAV is being developed as an open standard so any vendor can create software that provides or connects to CardDAV services.
- Exchange 2007 contact sharing—With the latest version of Address Book, Apple included support for this popular contact sharing service. Again, Mac OS X's Exchange integration relies on EWA, which uses TCP port 80 for standard transport and TCP port 443 for secure transport.

configured based on those settings. Otherwise, you will have to manually enter Jabber server and account information. Jabber servers are based on the eXtensible Messaging and Presence Protocol (XMPP) that uses TCP port 5222 or 8223 for encrypted.

- Ad hoc messaging—iChat will use the Bonjour network discovery protocol to automatically find other iChat users. No configuration is necessary to access Bonjour messaging. Bonjour details are covered previously in the "Dynamic Network Service Discovery" section of this chapter.

iChat supports a wide variety of messaging features and instant messaging protocols—which means it uses far too many TCP and UDP ports to list here. However, Knowledge Base document HT1507, "Using iChat with a firewall or NAT router," lists all the possible ports iChat may attempt to use.

Using File-Sharing Services

There are many protocols for transferring files across networks and the Internet, but the most efficient are those designed specifically to share file systems. Network file servers can make entire file systems available to your client computer across the network. The key distinction is that client software built into Mac OS X's Finder can mount a network file service similar to mounting a locally connected storage volume. Once a network file service is mounted to the Mac, you will be able to read, write, and manipulate files and folders as if you were accessing a local file system. Additionally, access privileges to network file services are defined by the same ownership and permissions architecture used by local file systems. Details regarding file systems, ownership, and permissions are covered in Chapter 4, "File Systems."

Mac OS X provides built-in support for these network file service protocols:

- Apple Filing Protocol (AFP) version 3 on TCP port 548 or encrypted on TCP port 22—This is Apple's native network file service. The current version of AFP supports all the features of Apple's native file system, Mac OS ~~X~~ Extended.

[should read:]
Mac OS
Extended.

- Server Message Block (SMB) on TCP ports 139 and 445—This network file service is mainly used by Windows systems, but many other platforms have adopted support for this protocol. SMB also supports many of the advanced file system features used by Mac OS X.

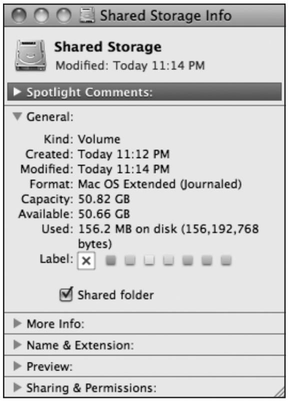
Ultimately, all file-sharing access is controlled by Mac OS X's file system permissions settings. When you enable a folder or volume as a shared item, the file permissions settings dictate which users can access the shared item. For example, the Public folders' Everyone permission setting is what grants all users, including guest and sharing-only users, local and file-sharing access to the Public folders contents. So, if you want to properly configure custom file-sharing access, you must be familiar with the file system permissions architecture, as detailed in Chapter 4, "File Systems."

Custom File Sharing via Finder

To configure custom file-sharing settings from the Finder:

1 If you're setting up a new shared item, prepare the folder or volume to be shared. If you're sharing a new folder, create and name the folder with the Finder. If you're sharing a volume, be sure the volume is properly mounted and formatted as Mac OS Extended (Journeyed), as outlined in Chapter 4, "File Systems."

2 In the Finder, select the folder or volume for which you wish to configure the sharing settings, and then open the Get Info window (choose File > Get Info or press Command-I). You may have to click the General disclosure triangle to reveal the general information section.



Shared Storage Info

Shared Storage
Modified: Today 11:14 PM

▶ Spotlight Comments:

▼ General:

Kind: Volume
Created: Today 11:12 PM
Modified: Today 11:14 PM
Format: Mac OS Extended (Journaled)
Capacity: 50.82 GB
Available: 50.66 GB
Used: 156.2 MB on disk (156,192,768 bytes)
Label: ☒

☑ Shared folder

▶ More Info:
▶ Name & Extension:
▶ Preview:
▶ Sharing & Permissions:

3 Select the "Shared folder" checkbox to share the selected folder or volume.

Deselecting this checkbox will stop sharing the item.

Understanding Remote Login

Mac OS X includes support for command line remote login via the Secure Shell (SSH) protocol, which by default runs on TCP port 22. Apple's implementation of remote login is based on the popular OpenSSH project, and defaults to the more secure SSH version 2 standard. OpenSSH provides a robust and secure environment for remotely accessing the command line of another network host.

With graphical interface screen sharing so readily accessible in Mac OS X, you may wonder why the ability to remotely log in to the command line is still relevant. After all, if you need to remotely access another Mac's command line you can always use screen sharing to open and control the Terminal application on the remote Mac. Well, aside from screen sharing being a bandwidth hog, there are many uses for remote login and SSH that remote screen sharing does not provide.

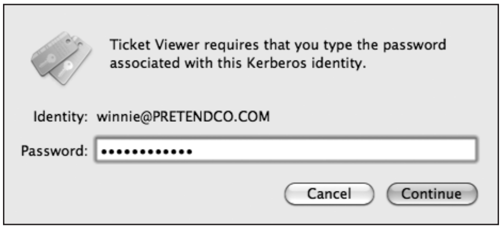
For starters, using remote login is much more efficient than screen sharing because only text is transmitted. Often, remote login is so fast that it's indistinguishable from using the command line on a local computer. From an administration standpoint, remote login is a much more subtle approach for remote management, as users logged in to the graphical interface can't tell that someone has remotely logged in to their Mac's command line. So as an administrative user, you can remotely log in to a Mac and resolve an issue from the command line without the user even knowing you were there. Even if the Mac is sitting idle at the login window, you can still remotely log in to the command line and take care of business.

Aside from providing a secure network connection for remote login, the SSH protocol can also provide secure connections for any other network protocol. You can use SSH to create an encrypted tunnel between two SSH-enabled network devices and then pipe any other TCP- or UDP-based network protocol through the SSH connection. Further, SSH remote login allows you to securely transfer files using Secure File Transfer Protocol (SFTP) or the secure copy command `scp`.

Finally, because SSH is a network standard, it's compatible across many platforms. In other words, your Mac can securely log in remotely via the command line to any compatible network host with SHH enabled. Conversely, any systems with a command line prompt and SSH client software can securely log in remotely to your Mac.

MORE INFO ► As with any command-line tool, you can learn more about SSH by reading the `ssh` manual page.

▶ If a user identity is present but there is no ticket, select the user in the list, and click the Get Ticket button in the toolbar to test Kerberos authentication. In the dialog that appears, enter the user's password and then click the Continue button. Skip to step 5.


Ticket Viewer requires that you type the password associated with this Kerberos identity.

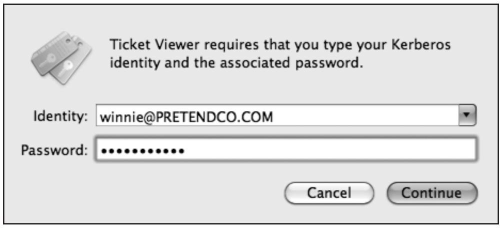
Identity: winnie@PRETENDCO.COM

Password: ••••••••••••

4 If the Ticket Viewer application opens with no Kerberos user identities listed, click the Add Identities button.

From the dialog that appears enter the user's fully qualified Kerberos identity. This usually includes the user's name, followed by the @ symbol, followed by the Kerberos realm in all capital letters.

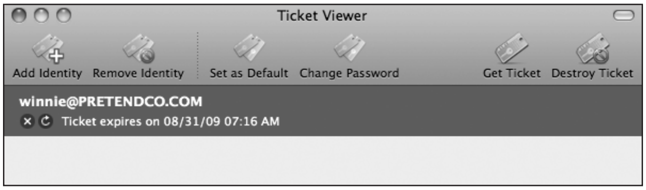
Also enter the user's password, and then click the Continue button.


Ticket Viewer requires that you type your Kerberos identity and the associated password.

Identity: winnie@PRETENDCO.COM

Password: •••••••••••

5 If authentication was successful, then the user's identity in the list will show the date and time when the TGT expires.



winnie@PRETENDCO.COM

Ticket expires on 08/31/09 07:16 AM

Exploring the details of the CUPS web interface is beyond the scope of this guide, but the page is well documented and is the best place to start digging deeper into CUPS. A few of the web interface highlights include the ability to enable remote CUPS administration, essentially allowing you to access the Mac's CUPS web interface from another computer. Also new in CUPS with Mac OS X v10.6 is the ability to create web RSS feeds with print accounting information. This allows you to use an RSS aggregator application to keep tabs on printing statistics.

NOTE ▶ If you aren't already comfortable with navigation in the UNIX command line, it's strongly recommended that you study the command line concepts in Chapter 3, "Command Line and Automation," before reading the remainder of section.

Modifying Printer Administration Rights

As stated previously, by default, you must be an administrative user to make changes to printer and fax settings. However, you can change this default and give any number of specific users and groups the ability to administrate printer and fax settings. With CUPS, only those belonging to the system group "_lpadmin" can do this. You can't edit this group using the Accounts preferences, so if you want to grant additional administration rights for printing and faxing you will have to use the command line group editor `dseditgroup`.

In the following example, Michelle, as an administrative user, adds the Logan user account to the _lpadmin group using the `dseditgroup` command. Thus, Michelle is giving Logan the ability to manage printing and fax settings. Note that Michelle has to put her account name in the `dsedigroup` command arguments and then provider her password.

[change to:] provide

```
MyMac:~ michelle$ dseditgroup -o edit -u michelle -a logan _lpadmin
```

Here is a different example in which Michelle uses the same command, but this time adds the staff group to the _lpadmin group. As covered in Chapter 2, "User Accounts," all local users are in the staff group. Thus, Michelle is effectively giving local users the ability to manage printing and fax settings.

```
MyMac:~ michelle$ dseditgroup -o edit -u michelle -t group -a staff _lpadmin
```

drawing the Mac OS X user interface, but it's still a good indication that things are progressing through the system startup process.

The `launchd` process is designed to expedite system initialization by starting multiple system processes simultaneously whenever possible and starting only essential system processes at startup. After startup, the system `launchd` process automatically starts and stops additional system processes as needed. By dynamically managing system processes, `launchd` keeps your Mac responsive and running as efficiently as possible.

> **MORE INFO ▶** `launchd` is an extremely powerful open source system for managing services. Learn more about `launchd` at Apple's developer website, http://developer.apple.com/macosx/launchd.html.

System launchd Items

As covered in Chapter 5, "Data Management and Backup," `launchd` manages system processes as described by `launchd` preference files in the /System/Library/LaunchDaemons folder. Third-party processes can also be managed when described by `launchd` preference files in the /Library/LaunchDaemons folder.

Apple strongly encourages all developers to adopt the `launchd` system for all automatically started processes. But the system `launchd` process also supports legacy startup routines. This includes support for running the traditional UNIX /etc/rc.local script during system initialization if present, though this script is not included on Mac OS X v10.6 by default. The system `launchd` process also starts the /sbin/SystemStarter process, which manages system processes as described by legacy Mac OS X startup items. Mac OS X v10.6 does not include any built-in startup items, but `SystemStarter` will still look in the /System/Library/StartupItems and /Library/StartupItems folders for third-party startup items.

Viewing the launchd Hierarchy

The /Applications/Utilities/System Profiler application lists all processes along with their identification numbers and parent/child relationships. In the System Profiler, you can sort the process list by clicking on the title of the Process ID column, and you can view a process's parent process by double-clicking on its name in the list. You will find it beneficial to open the System Profiler and examine the process listing as you learn about how Mac OS X starts up the user environment. Detailed information about using the System Profiler application is covered in Chapter 5, "Applications and Boot Camp."

[replace "System Profiler" with
"Activity Manager" x4]