

Tips & Tricks for Macintosh Management

X

April, 2003

Contents

Introduction	p. 1-3
Overview of Client Management	1-4
Section 1	System Preparation
	1.a. Client workstation setup..... 1-5
	1.a.1. Out-of-the-box experiences..... 1-5
	1.a.1.a Optimizing for MacOS X..... 1-5
	1.a.1.b Optimizing for MacOS 9..... 1-5
	1.a.1.c. Optimizing for a 'pure' Classic setup..... 1-6
	1.a.2. Give the machine an identity..... 1-8
	1.a.3. Update to the latest extensions and fixes..... 1-10
	1.a.4. Printing Setup..... 1-11
	1.a.5. What time is it?..... 1-12
	1.a.6. Saving energy..... 1-12
	1.a.7. Extension Management 1-13
	1.a.8. Quicktime settings. 1-13
	1.a.9. Network / TCP/IP settings..... 1-14
	1.a.10. Application setup and testing. 1-15
	1.b. Server basics tips..... 1-16
	1.b.1. Plan for enough server(s)..... 1-16
	1.b.2. Server setup tips..... 1-16
	1.b.3. Sharepoint and home directory planning..... 1-17
	1.b.3.a. Basic 'automount' home directories..... 1-18
	1.b.3.b. Advanced home directories..... 1-19
	1.b.3.c. Customizing the Home Directory template..... 1-20
	1.c. Network tips..... 1-21
	1.d. Additional information..... 1-23
Section 2	Users, Groups, and Open Directory
Section 3	Managed Client for X tips
Section 4	Macintosh Manager tips
Section 5	NetBoot and NetInstall tips
Section 6	Odds and Ends

Introduction

This is the latest of the incarnations of the Tips and Tricks series for client management, finished in April, 2003. The series began in 1992 with a plan to provide the Apple Education sales force a document for demoing At Ease for Workgroups and the other parts of the now-defunct ANAT kit. It grew from there to be sort of a 'missing manual' thing containing hints, tips, and guidelines for practical application of the tools Apple produces for managing Macintoshes. **Note - if you are using MMv2.1.1 and MacOS X server 10.1.4 - you need to use T&Tv7.1.1 for reference. This doc is for 10.2 server and MMv2.2 and higher!**

As with the other versions, this document is not meant to replace the various admin guides and documentation provided with the shipping software; but it does fill in some gaps and/or omissions in the corporate produced material. Reading the Admin Guide, or at least referring to it, is still a requirement. As to the question - 'Is this document official Apple documentation?' The answer to that is yes - in as far as being an Apple employee, anything I publish to the public sector is considered as legally, officially, Apple-produced material. At the same time, I also caveat this statement with the fact that I try to provide a field perspective on much of the corporate-produced items. That is all I can hope for - to help provide a practical application approach to otherwise functional documentation.

The software used in this doc is based on an upgrade to the initial release of MacOS X Jaguar (10.2). I am using v10.2.5 server and core OS code, with all of the updated parts provided with that set. Some of the operations in this document would not work if not for the items in that build of the OS. This doc had to wait for that material to be released to the public sector due to the reliance on 10.2.5. If I miss something, or as a result of following only this guide and not the server admin manual or other support material, you find yourself lost - contact Apple technical support. I used all of the material available as of the date of this document to test and validate the procedures in here. These are my approaches to client management, and as such, may not be the way you want to work out your setups or configurations. I do know that what I present works.

The MacOS core and server teams worked hard to bring about the code used in this doc. They deserve a lot of credit for pushing the limits of what we can accomplish as Mac users and admins. While many sites are still dependent on MacOS 9 and earlier, it is the mission of the Apple software engineers to evolve the OS and I am sure you'll agree that MacOS X v10.2.5, both client and server are quite the accomplishment.

Finally, I have a full time chore of working in the Education Division spreading the word about Macintosh and client management tools. I just don't have the time to provide technical support on the side - sorry, just no bandwidth for that. If you have a problem with your operation, contact Apple Tech Support or your local Apple SE, Professional Services Manager, or Genius Bar. This doc will grow as I get new material, and I am also working to get much of this published in Kbase or LBN (Late Breaking News).

Enjoy, and hopefully, this version of the T&T will help make your life a little easier.

John DeTroye, Sr CE, Apple Education, johnd@apple.com April, 2003
Homepage: <http://homepage.mac.com/johnd/>

Overview of Client Management

Client Management is the art of establishing control over computers and users in such a way as to enhance both the user's ability to perform required functions and the computer's usefulness in that environment. In Education, the computers placed into operation are generally owned by the school and are managed by professionals, even if that professional is also a full time Algebra teacher. The computers are seldom, if ever, the personal property of the end user. In that context, being able to configure, deploy, and manage the computers becomes a required task for the technology administrators. Managed tends to mean controlled, commonly configured, and restricted. Unmanaged tends to mean open, variably configured, and chaotic. As we move toward SY2003/4, Apple's client management strategy has evolved to include two primary OS streams - MacOS X (with and without Classic) and pre-X (MacOS 9.2.2 and below).

Under MacOS X, control happens under the domain of Managed Client for MacOS X, or **MCX** for short. The major change since the last T&T doc (v7.1.1) was the introduction of Jaguar, MacOS X v10.2, and it's updates bringing it to 10.2.5. In this environment, the user account information is maintained at the Directory Services level - in other words, the user's name, password, and home directory information are all maintained in an abstracted database away from the rest of the server processes and especially away from Macintosh Manager. The user database can be stored in NetInfo (the default and easiest to use) or in an LDAP (Lightweight Directory Access Protocol) database on the server. MCX, using the application 'Workgroup Manager' allows Macintosh Manager - like control of application access, group folders, and Finder appearance. A key new capability is the establishment of controlled settings that are cached to the local hard drive, allowing complete client management even for standalone, 1-1 deployed systems. Workgroup Manager and MCX rely heavily on user home directories. If a user account is to be managed, it must have either a local or network home directory. Workgroups are enhanced MacOS X groups that contain managed preference settings.

New to the client management space is NetBoot for MacOS X and Network Install, or NetInstall. These two capabilities supplement the NetBoot for MacOS 9 functions to expand the toolkit for a network admin. Using NetBoot for X, an administrator can test an OSX setup against their workstations without actually installing OSX on the machines. If an install is needed, or desired, NetInstall provides the capability of building custom installation images with all of the components an administrator may need on their workstations using both X and Classic. NetInstall will not install a pure MacOS 9 configuration.

Macintosh Manager is Apple's client management software for MacOS 8&9 workstations. It is designed to provide secure desktops, managed application access, and network accessible home directories. Macintosh Manager is workgroup-based management. Users are assigned to one or more workgroups that contain specific sets of approved items for them to use within that workgroup. A user logs into Macintosh Manager and selects the workgroup they need for that work period. User-specific documents and other items are stored on a network-based home directory. Workgroup shared items, such as clipart or homework assignments, are stored on a workgroup document sharepoint. When a user logs in, all of these items are brought together at their Desktop.

Together these tools, and a few others discussed, provide a wide range of management capabilities for the Macintosh network administrator. Read on for more details...

Section 1. System Preparation - setting up client workstations

There are a few things that need to be done at the workstation level in order to make a Macintosh a well behaved managed client. Over the past few years, changes to the core operating system and updates to certain key components have reduced the amount of work needed; but there is still a need to clean up the workstations you get before turning them over to the students. Face it - the Macintosh as it comes out of the box is designed to go on your kitchen table - not a school lab. It is, by default, loaded with software and extensions meant to improve your productivity at home. There aren't too many schools that need to have fax, personal checkbook, or remote dial-up software enabled on their systems in the writing lab.

1.a. Client workstation setup - clearing the kitchen table

Setting up workstations for the first time may seem like a real chore, unless you are netbooting (see section 5!); but unless you pay attention to a few key configuration items up front, you will have many days of annoyance and trouble ahead. Key here is to determine which OS, or OS'es you are going to be using, which applications you need, and setup the workstations right the first time - before you turn on any management software.

1.a.1. Out-of-the-box experiences. Unless ordered with special CDM (customer driven manufacturing) installations, the current Macintosh comes with both MacOS 9 and MacOS X installed, with the systems set to boot into MacOSX by default. If you are going to be running OSX in your environment, this is a good thing. If you aren't, then you might consider reformatting and re-installing with either a pure MacOS X or a pure 9.2.2 setup. The advantage of leaving the system as dual boot machine is the ability to switch between operating systems without going back through an install process. The advantage of 'going clean' with either MacOS X or MacOS 9 is that you can create a clean master system with only the items you need for your unique environment. Once the master system is created, you can use ARD, ANA, NetInstall, or ASR to clone that master onto the rest of the systems. On the other hand, if you are going to be using both MacOS X and 9 in your setup, then by all means, leave the systems as they come - or perform a completely clean install of both OS's. This includes running either 9 as Classic or as the boot system.

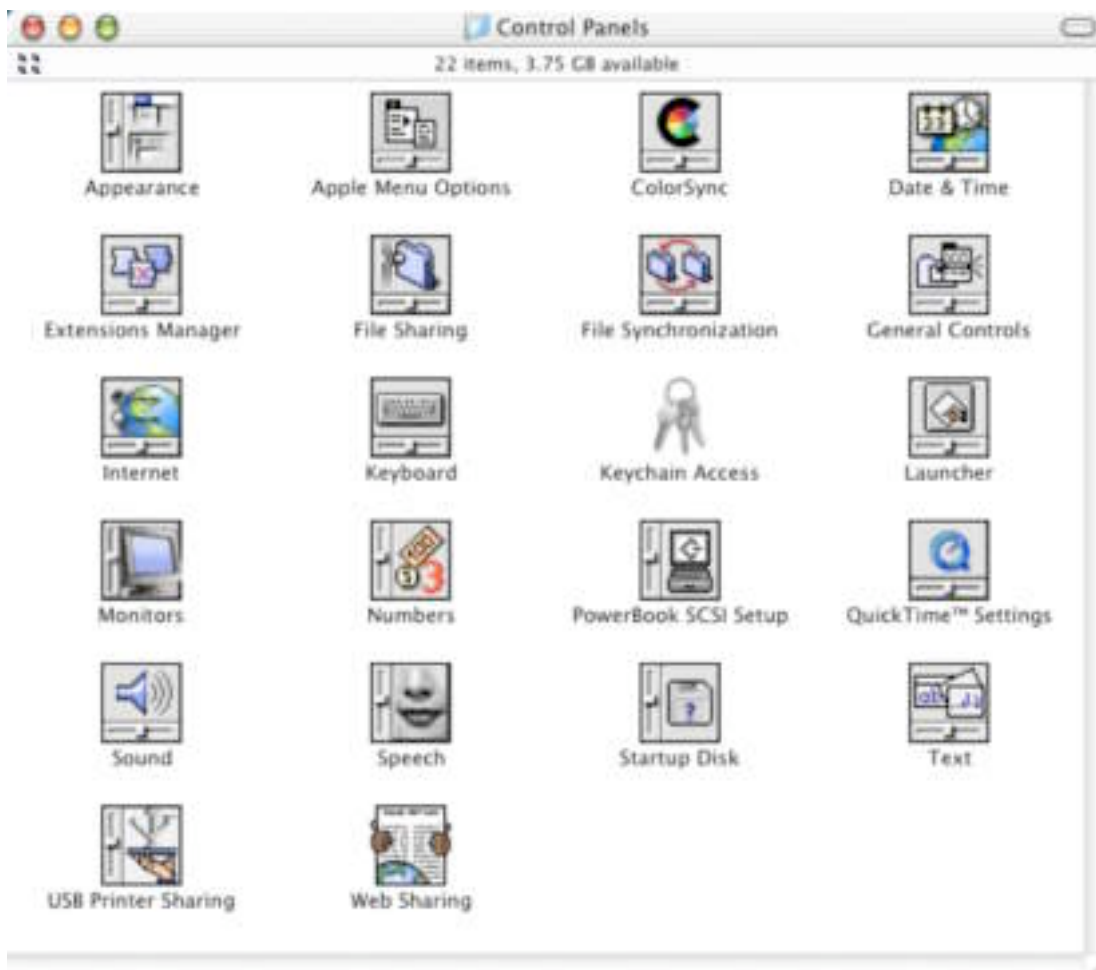
1.a.1.a Optimizing for MacOS X. When first creating your 'perfect' system, you should focus on the key software packages needed, as well as making sure all drivers and updates are in place. It is really annoying to create a master system, clone it, then see all of your workstations pop up with the 'Software Updates' window at first launch. One idea is to turn off automatic updates on the master before cloning. Another is to run Software Updates as often as you need to before locking the image down to avoid the problem. Of course, if you leave the updater offline, it is then up to you to manage a mechanism for updating all of your workstations once they are deployed. Fortunately, Apple Remote Desktop (ARD) is really great for this with the new 'Install Packages' function in v1.2. Unlike MacOS 9, MacOS X doesn't require (or really support), the administrator going in and turning off extensions and items in order to optimize performance. There are some key things that need to be done, such as naming the workstation and providing a local admin account. Otherwise, the system will tend to run what it needs. Advanced workstation 'tweaking' is something for a another chapter.

1.a.1.b Optimizing for MacOS 9. MacOS 9.2.2 is the final version of the venerable 'classic OS' for use by

Mac users. The advantage of it being the 'last one' is that we can finally focus on just this version for optimal configuration. Key in setting up OS9 for best practice is turning off unneeded extensions and making sure the latest versions of all items are in place. If this is also going to be used for running Classic under MacOS X, then you should make sure that you launch it at least once before locking down the desktop. A first run of Classic usually forces installation of additional items used in the Classic environment. If you are going to be using Macintosh Manager, then make sure you have installed and tested **all** of the applications and printers that that workstation will use before installing and running MM client. If you do not perform this simple 'prep' task, odds are many of your workgroups will drastically misbehave.

1.a.1.c. Optimizing for a 'pure' Classic setup. If the goal is to run MacOS X as the only desktop OS (or if you are using a newer Mac that won't boot to 9) and runs some apps in Classic mode, you need to take a different approach to modifying your non-X components. Classic doesn't need all of the 'stuff' running that MacOS 9 needs; therefore, you can streamline Classic by disabling/removing several items.

A default Classic setup contains several control panels that cannot be accessed by the Classic user, and some that shouldn't be accessed. Here's all of the Classic control panels that are accessible:



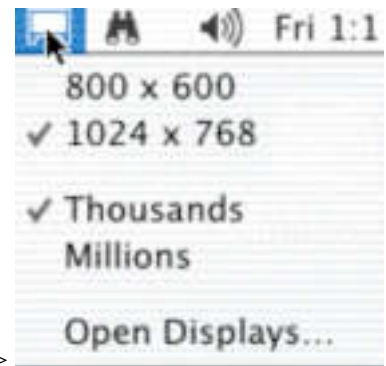
Classic control panels that work.

Turning off the control panels that you do not want users to casually access might be a good idea.

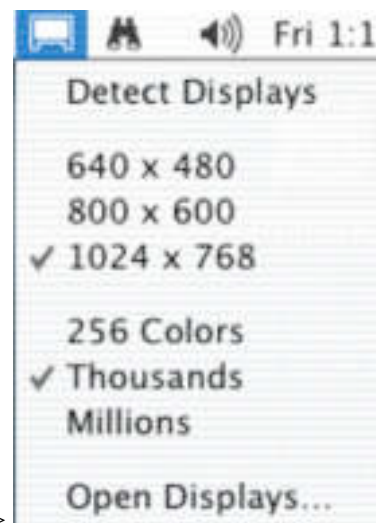
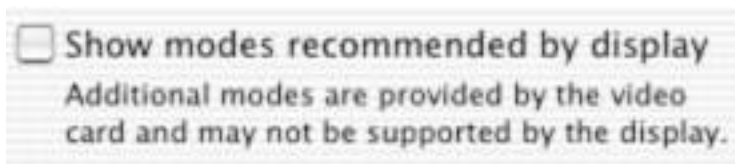
For further access control, you might want to delete a few of the more dangerous ones, such as Web Sharing or File Synchronization. The rest of the configuration for Classic remains the same as for MacOS 9. This includes testing your software and printers, make sure you have the ability make it all work together. Trying to access control panels not supported by Classic will only give you:



Note: Classic and MacOS X displays. There is an issue where, by default, the display settings in MacOS X cannot get to 256 colors. Since there is so much cool K-12 software that needs to change to 256 colors, you need to alter the default settings of your workstation to support this. The process is pretty simple. Under System Preferences/Displays, select the checkbox that turns off recommended modes:



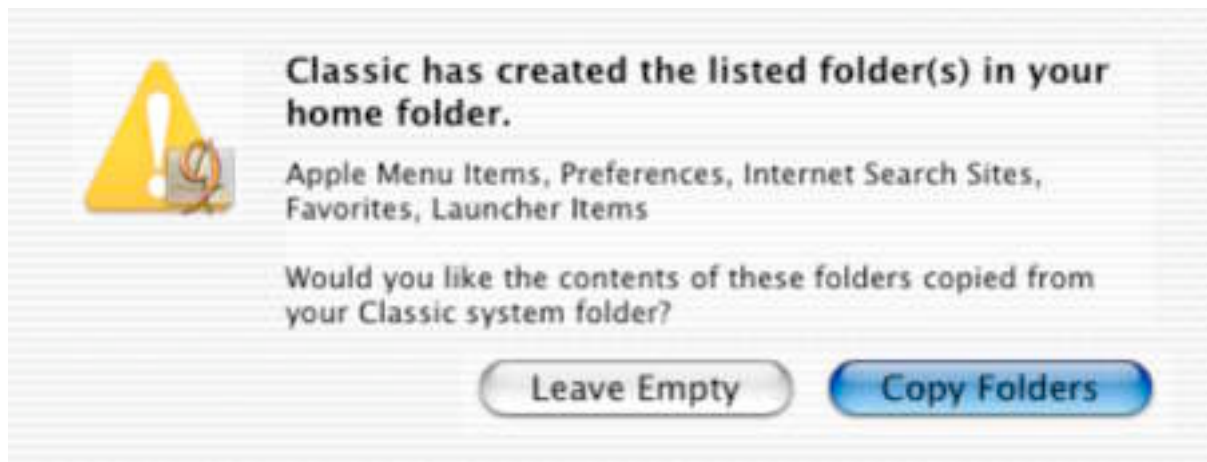
gives you >



gives you >

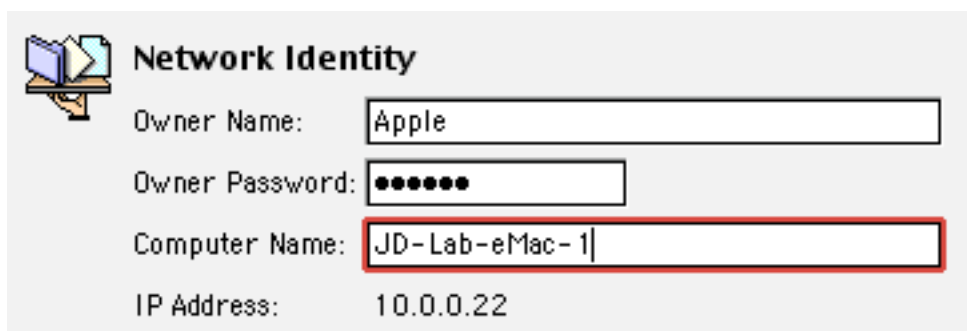
And that makes a difference in being able to run any app that needs to get to 256 colors under Classic.

You also have to decide if you want the ability to redirect Classic items into the new location set up under 10.2.x for Classic preferences, etc. We will discuss this in more detail in the MCX section; but you need to know that the first time you launch Classic as a user you'll see:



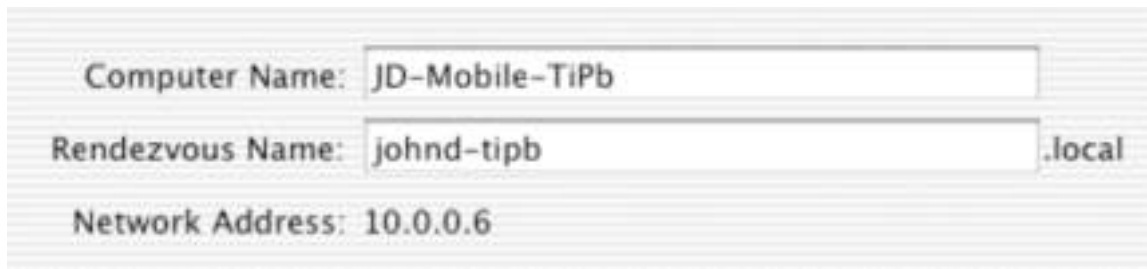
This dialog is saying that the items sitting in the System Folder on your machine will get copied into your own home directory. If you are upgrading from MacOS 9 and have customized all of the items, you definitely want to do this. Otherwise, you can build up those items as you see fit. See the discussion on managing Classic under MacOS X for more information.

1.a.2. Give the machine an identity. You must establish unique computer names for all of the client systems. Inside the File Sharing control panel (9.2.2), you must set a unique name to each computer on the network. You should also set up an owner name and password. This can be the same across all of your computers, or just a subset. The computer name identifies the machine to Macintosh Manager in its Computer lists, as well as to ANA and ARD.



File Sharing Control Panel (MacOS 9.2.2)

Under MacOS X, you will normally go through the Setup Assistant once per workstation to establish owner name and password info. If you use NetInstall or clone from a known good system, still make sure you have a unique computer name and non-trivial password to work with. With Jaguar, you will also have Rendezvous to work with, therefore, you need to also have a unique Rendezvous name for your workstation. Computer names are set under the 'Sharing' system preference; user account info is set under 'My Account' and 'Accounts'.



Computer Name: JD-Mobile-TiPb

Rendezvous Name: johnd-tipb.local

Network Address: 10.0.0.6

Sharing system preference under 10.2.2

The Rendezvous name must be an Internet, or URL, compliant name. The computer name can be pretty much anything; but Rendezvous is actually using the name within URL's provided to other systems, such as during iChat. This means no spaces, so 'Tim's Wookie Holding Zone' is out. You'll actually see the text block fight back if you try to enter a non-compliant name. Hint - use a good, proper name for both blocks to avoid any problems later on.



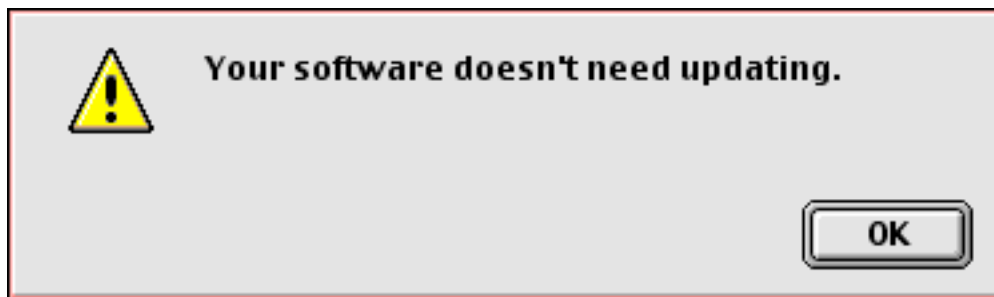
My Account system preference with cute picture

If the workstation is going to be deployed into a 1-1 environment where a non-admin user is going to be using the machine, you need to also create at least one non-admin user accounts in the 'Accounts' system preference. This account will be the primary user. The reason for not allowing the main account to be used all the time is for security and maintenance. Creating one or more local accounts allows the administrator to manage the systems both locally and remotely (using ARD); but also keeps the day-to-day users out of the more dangerous parts of the system.



Local admin and non-admin user accounts for 1-1 deployment

1.a.3. Update to the latest extensions and fixes. I can't count the number of times I've heard 'Why doesn't Apple fix this?' followed by 'I don't have time to update my systems.' A great many of the problems people have experienced in the past have been due to things that were fixed in core OS or application updates. For this paper, I updated my workstations and my NetBoot images to MacOS 10.2.4 and 9.2.2 with the addition of the new Airport drivers, and everything else I saw in Software Updates. I also checked as many 3rd party application sites as possible for updates to any application I was going to use. The goal was to get the following message from the Software Updates control panel:



This is a Good Thing™



I also made sure my MacOS 8.6 workstations were using the latest CarbonLib, and the Ethernet extension v2.4.3 - which can be found in the Ethernet Update 2.0 package. Those two items specifically help provide better stability to the OS. Now - you might ask - why am I only talking about 9.2.2 and 8.6? Well, I do that because those are the two most stable builds of Mac OS 8&9. There were issues with 9.0.4 and 9.1 which were resolved with 9.2.2. If you must run anything below 9.2.2, I would stick with 9.1 - there was a change in the format for several system files between 9.0.4 and 9.1 that can cause problems going between the two OS'es in a managed environment.

With MacOS X workstations, you want to follow the same guidelines. Run Software Update as often as possible until it cries uncle. A tip for Software Updates under X - you can select to download any item that shows up in the Software Updates window to the Desktop, then install it later. You can also select any item and 'hide' it, so it won't keep popping up for install. Keeping a set of downloaded updates will come in handy later on if you want to create a NetInstall updater set, or use it with ARD's new 'Install Package' function.

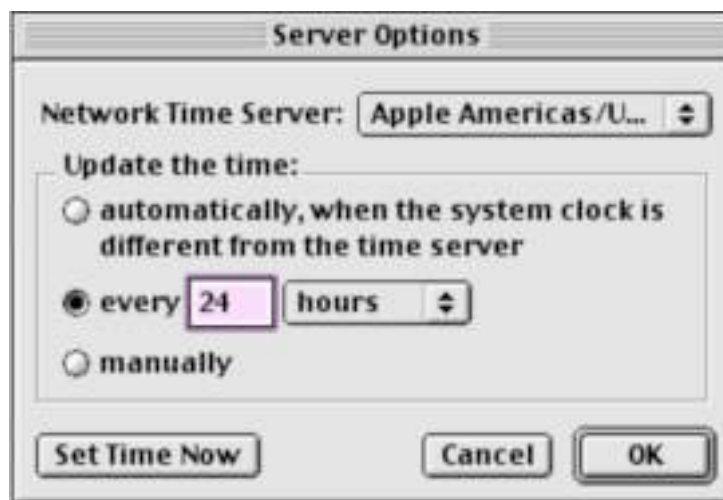
1.a.4. Printing Setup. For MacOS 9 workstations, setting up the client systems for printing must be done before activating MMv2. While the systems are at the Finder, load all of the needed printer drivers, and set up the required printers for that computer. There are two types of printers available - Desktop and non-Desktop printers. The easiest to manage are Desktop printers - they can be controlled and have quotas established in MMv2. Non-desktop printers tend to have non-standard drivers. Under Macintosh Manager, you can have access to either a single (**one**) non-desktop printer, or a set of desktop printers, depending on settings. You cannot establish quotas for non-desktop printers. More on this in the printer management section.

The key is to have all of your printers set up and tested before activating MM. Under MacOS X, you have much more leeway - the printer settings are kept in a file that can be set up with Workgroup Manager for networked systems. If you are going to run with just NetBoot or standalone security, you still need to set up whatever default printer(s) you need from within Print Center.

MacOS X is much more lenient with printing. Basically, you need to have the correct drivers available for the printers you will use, period. The actual link to the printer will be provided in a property list that can come from the server in a managed client setup. Just make sure you are able to print to any of the printers you will be using in your environment from your workstation first.

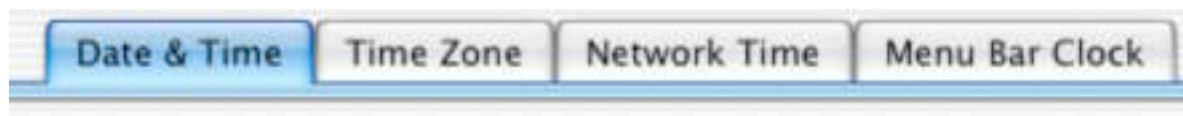
No matter which way you go - test your printer setup before you finalize your configuration. If the machine has a problem printing before you activate either MCX or MM, it will definitely not work later.

1.a.5. What time is it? For MacOS9, settings in the Date and Time control panel are saved in p-ram on the client. Therefore, these settings must be made at each workstation - they cannot be sent over the network. The most important setting is making sure you have established a time zone. You might also want to set the clients to get their time updated from one of the master ntp servers - assuming your network firewall will allow it. If you do so, just use the '..every 24 hours ..' setting, not the '..every time it gets out of whack ..' setting. That setting relies on you having perfect 60 Hz power to keep the clock on track. 'Nuff said there.



Keeping the clock running right.

Under MacOS X, there is a p-list (property list) holding many of the settings for date and time; but you still need to use the Date & Time system preference to establish these settings (this is not counting the CLI way of doing things). Just establish the settings you desire, and make sure you are using the correct time zone. Turn on access to a Network Time Server only if you know that one will be reachable from your network. Otherwise, network traffic will be generated as the workstations try and fail to connect to the NTP server.

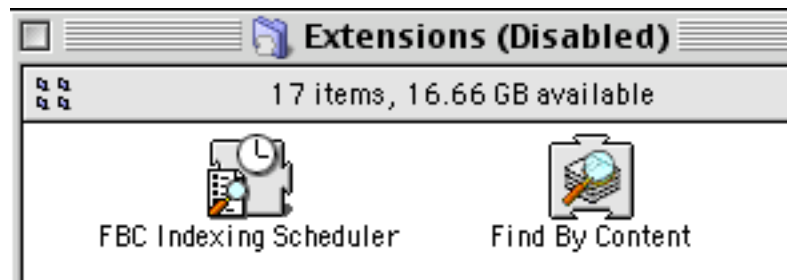


MacOS X Date and Time system preference pane

1.a.6. Saving energy. The Energy Saver control panel lets you establish a sleep schedule for your clients. I say sleep schedule because you don't really need to shut down the clients - just let them sleep. With the new Macs, the systems use less power sleeping than they do starting up and restarting every day. In order to keep the managed clients humming along, I recommend setting only the screen to sleep, and keep the system and

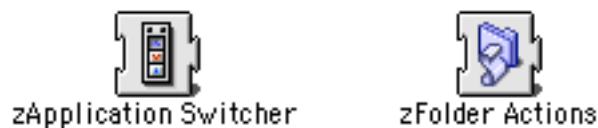
hard drive awake during the day. For MacOS9, you could then set the timer to have the entire machine go to sleep at 6pm and wake up at 6am. Under Options, setting the machine to be woken by admin access is for ANA/ARD control. For those of you who need 'wake on LAN' capability, this is how we implement it.

1.a.7. Extension Management . Under MacOS 9, when you first configure your client, you may have several items in the Extensions folder that you don't really need to be active in a managed client setting. These would include unused print drivers, personal web sharing, and portions of the Sherlock items. In order to avoid problems when clients are logged in overnight, I turn off the 'Find by Content' and 'FBC Scheduling Indexer' extensions. This keeps Sherlock from trying to index the mounted MMv2 sharepoints.



Turning these off may avoid problems.

I have also found that changing the load order for a couple extensions makes a huge difference. The two extensions that need to be renamed are the 'Application Switcher' and 'Folder Actions' extensions. Add a 'z' in front of these two, and it will fix a problem where the Login window locks up or crashes under certain conditions. If you update the system software later on, make sure you toss the older versions and rename the newer ones.

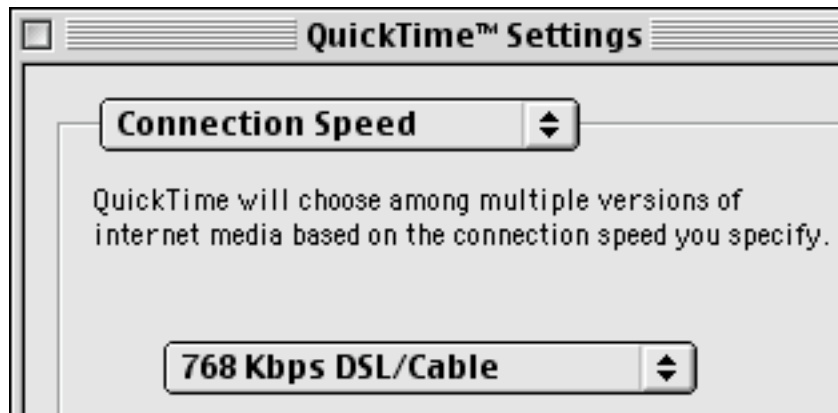


Renaming these two makes a difference.

Under MacOS X, there is no 'Extensions Manager' as we have under MacOS 9. However, the operating system is much more intelligent than it was before. Many of the processes that are available do not load or run until needed, so if you have a core install of all of the different items you need, you can be pretty comfortable with knowing that the OS won't use up excess cpu time running extra items. To check to see if the system is behaving, you can run either 'Process Viewer' from the Utility folder, or the **top - w** command from Terminal. There are ways to reduce the number of processes running; but that is a subject best left to the advanced MacOS X cert course.

1.a.8. Quicktime settings. There are only two QT settings I concern myself with during basic setup. First, make sure you set a connection speed. Second, make sure you have turned off the autostart settings for CD autoplay and autoloading. If the connection speed isn't set, the QT control panel will pop up the first time any network playback is requested - giving little Joey a chance to do something he shouldn't. If the autoplay feature is on, any Audio CD inserted into a client system - even at the Login screen - will just start playing. Consider this a sanity check. The autostart setting for certain applications can allow a certain virus/worm to

establish itself on your system.



By default, this is set to 56k - but the CP will open anyhow first time out.

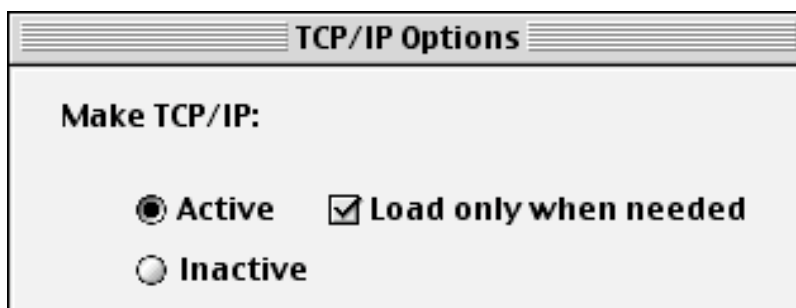


MacOS X QT settings

Quicktime 6.x stores its 'Pro' setting in a per-user control now, which breaks the concept of having a machine license (which is what you paid for). The QTP settings are stored in the user's home directory, and if you need to have all of your workstations set to use Pro, you'll need to make sure the license settings are created in each user's folder. Hopefully, enough calls to tech support will get this issue resolved...

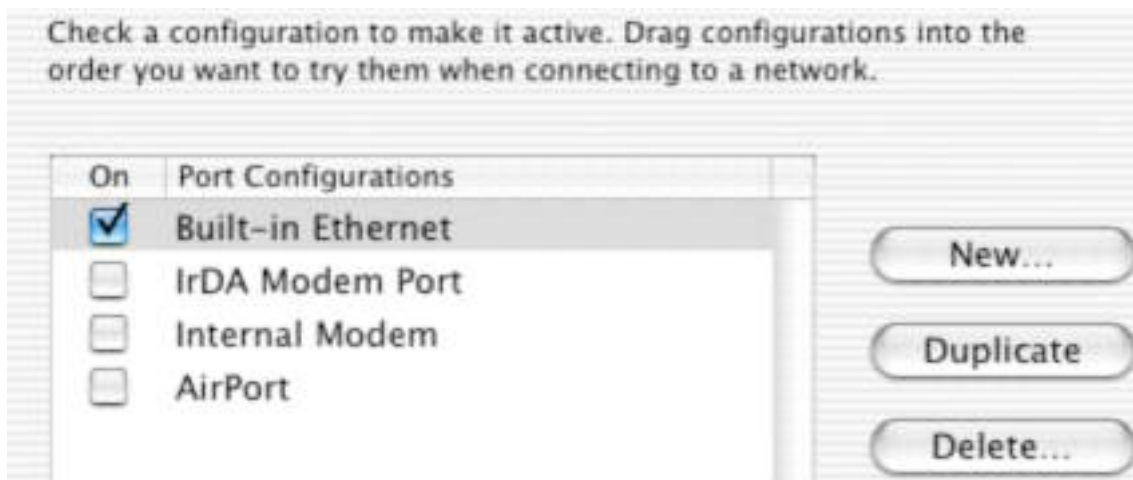
1.a.9. Network / TCP/IP settings. Properly configuring your network is critical, especially the TCP/IP settings. Whereas you used to be able to get away with not having a tightly managed network before, the current MMv2/OSXS combo requires a clean environment. If you are going to use fixed IP addresses, make sure you don't duplicate any anywhere on the network. If you set up VLANs, make sure you don't overlap

any of the address/mask ranges. A good thing to do is set TCP/IP to load at system startup, and stay loaded. You do this by setting the User Mode in the TCP/IP control panel to Advanced, then under the Option button, turning off the 'Load only when needed' checkbox.



Turn off the checkbox when on a LAN

For MacOS X workstations, it is a very good idea to create specific Network locations for where these units will function. For example, if the workstation is going to always be part of a wired LAN, then turn off the other ports. If you are going to be distributing iBooks into a 1-1 deployment, then set up a location each for on the LAN at school, on Airport, and offline - at home. When you manage these computers, you can keep the user from changing the specifics of the settings; but they will be able to switch locations as needed.



Use only the port needed for a specific location

1.a.10. Application setup and testing. This step is crucial (aren't they all?) to having clean logins. make sure all of the applications you are going to use work on the client systems you are going to use. Many applications need registration or initial run data created in order to function properly. Test your applications before locking down the workstations. We'll work through the specifics of preference handling and dealing with oddball applications in the MMv2-specific section.

1.b. Server basics tips

Establishing a decent server setup is essential to making the rest of the client management pieces functional. There are tons of things that need to be done; but here are just a few of the key tips for both planning and configuration.

1.b.1. Plan for enough server(s). The choice is often split between 'how much server can I get' and 'how many servers can I get'. I would follow a couple simple guidelines:

- Home directory servers, NetBoot servers, and web/mail servers should be unique entities. Each of these functions is high load, and dedicating a server to each of these functions can alleviate a lot of pain later on. After all, what are racks for?

- Plan for one server per 150 simultaneous connections, if possible. If you are going to have any leeway at all in your server budget, having a lower number of concurrent connections is way better than having a bigger, badder server.

- Plan for 30-50MB of storage per user. When planning for user quotas and storage, the entire home directory is measured. Browser caches are also automatically stored in the home directory - and under MacOS X, there is no mechanism for redirecting them without writing a special script, so allow for at least an extra 10Mb.

- Split the load as often as possible. If you can spread out your workgroups and home directories, do so. There will be more on this in the section on user and group management.

1.b.2. Server setup tips. There are only a few key tips I have found that should be followed to avoid problems when setting up MacOS X servers. Most of the issues can be dealt with while in the Server Setup Assistant.

- Make sure your Computer name, hostname, and DNS name are all the same. They should be simple, yet unique, and follow normal url guidelines. Avoid spaces in the names, and stick to lower case for ease of management.

- Use **only** fixed IP addresses on your servers.

- Make sure you have a DNS inside your network. Unless you are familiar with setting up machine names and NetInfo Manager, you should have a domain name server inside your network with your server names in its database.

- **Special Note!** If you are not familiar with DNS and its setup, make sure you pick up a copy of O'Reilly's book - DNS & Bind. It will save you a lot of trouble later on. If the powers that be tell you that you cannot have a DNS server inside your network, make sure they understand the requirements of name lookup and server address resolution. A simple packet trace during a machine startup should demonstrate the lunacy of the attitude 'We don't need DNS inside our NAT environment.'

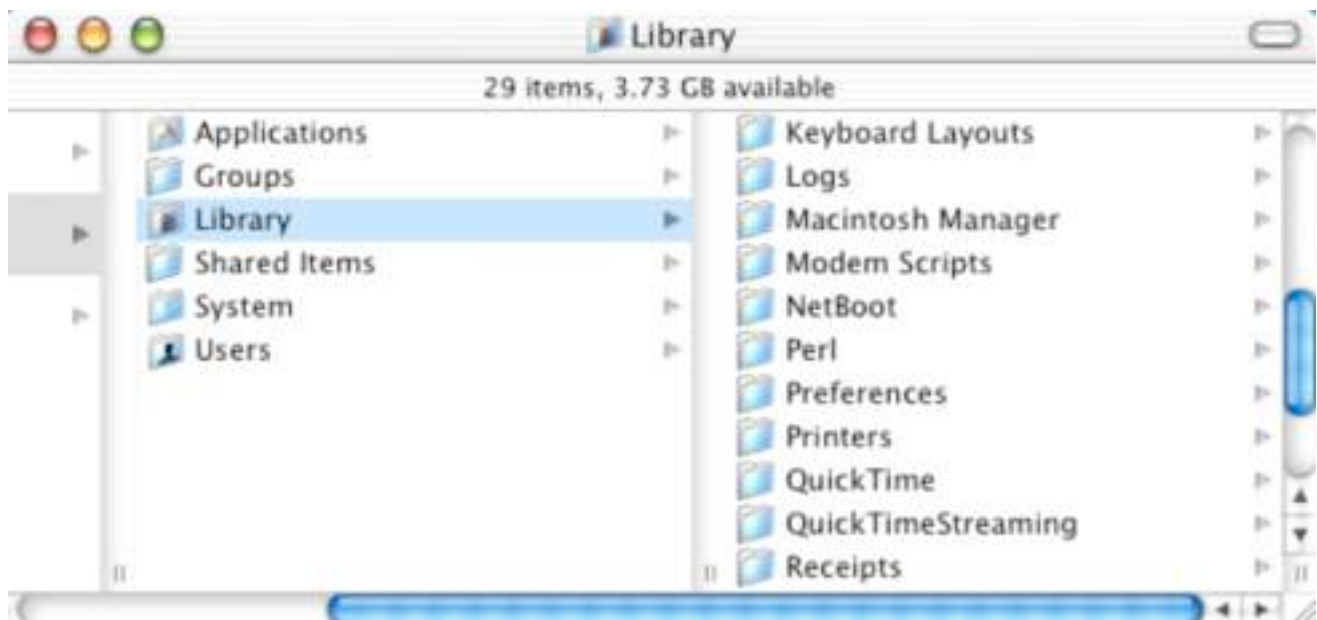
- MacOS X server likes lots of ram - the more the merrier; but at least 256Mb. Try for 3Mb per concurrent workstation connection.

- Don't use the second EN port on an Xserve for anything unless you know how it works. It does **not** support trunking.

- Make sure Energy Saver on the server is set to maximum performance. Sleep is a bad thing for a server. Just turn off the monitor or use a KVM box.

1.b.3. Sharepoint and home directory planning. One factor that always affects users on a network is how well the final chokepoint in the equation works for them - their home directory. Under MacOS X server, setting up home directories is an absolute pass/fail test. I'll go into details on home directory-specific issues in the next section; but sharepoints that hold them must be set up first.

When a server is configured, you always have the option of setting up multiple partitions as well as multiple drives. There will always be a boot drive - whether it is a partition of a larger drive, or its own drive is up to you. It is impossible under the current version of the server software to isolate only the server boot code onto its own drive. Certain items will always show up on the main drive - here's an example:



The Macintosh Manager and NetBoot directories always sit on the boot partition.

Currently, there is no mechanism for moving the MM and NB folders to any other area. However, there is no requirement for you to place your user home directories, group directories, MM workgroup document sharepoints, or ARD scheduled sharepoints on the boot drives (in the default locations). Here's a few tips on setting up the various sharepoints...

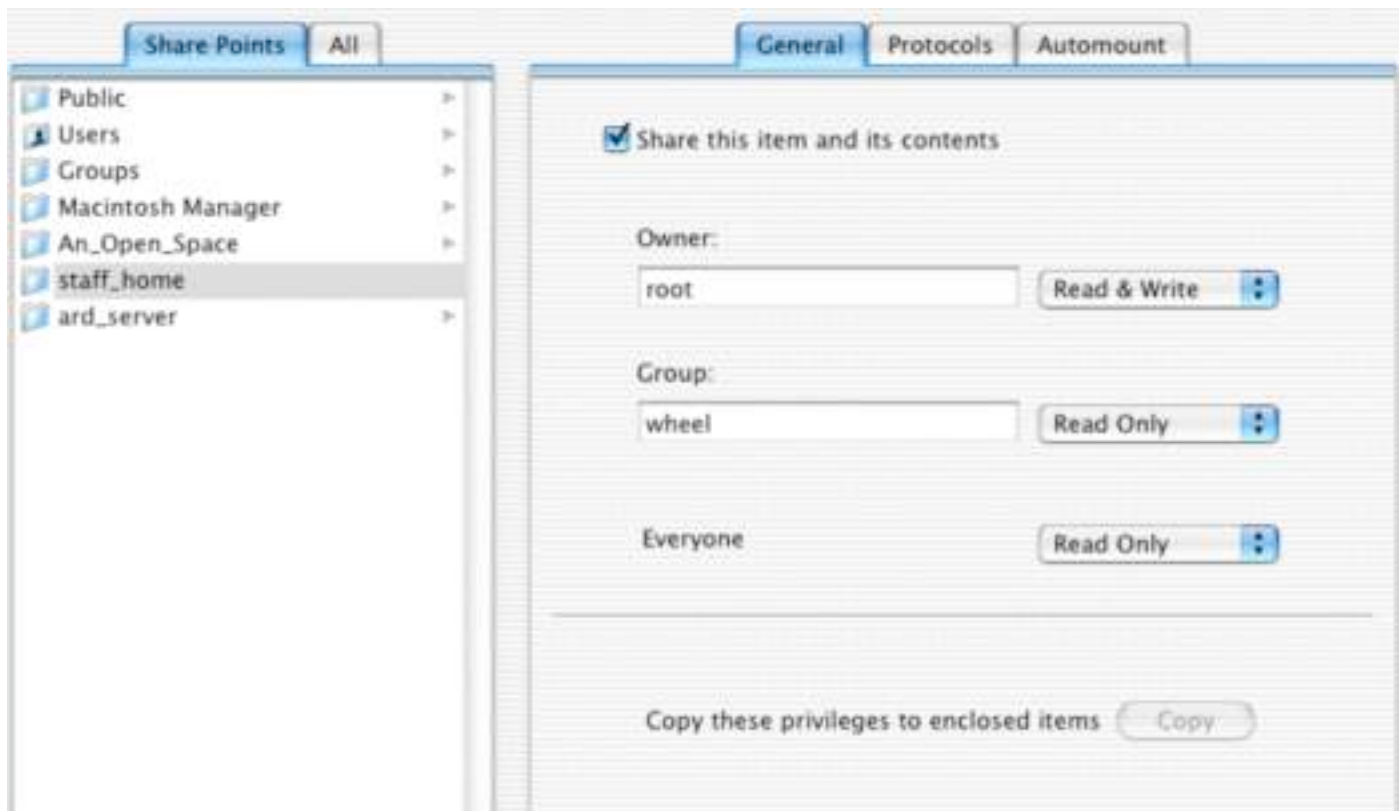
User home directories. These should be placed onto fast, clean partitions. The default location is the 'Users' folder on the boot drive. You can place them anywhere you want as long as you follow a few key tips.

- For MacOS X servers, the sharepoint should be a 'Network' item, automounted, and located at root level of any volume it sits on. If you plan on separating the user home folders into several sub-folders within this share space, you'll need to do a couple more steps; but even that is easily managed.

- For non-OSX servers, you are on your own. First of all, the versions of AFP (Apple File Protocol or Appleshare) on non-OSX servers are older and less reliable. Second, while home directories are automatically created on OSX servers, they must be manually created on non-OSX servers. Third, as you may have already figured out - best performance for Mac users happens with Mac servers.

1.b.3.a. Basic 'automount' home directories

For the basic setup, we'll create a sharepoint for our staff home directories on a server called 'main' (full name - main.apple.edu). The sharepoint is called 'home-staff' and is created at root level of the third drive on the server (xserve's are cool). Inside Workgroup Manager, you log onto the server as an administrator and click on the 'Sharing' icon in the toolbar, select the 'All' tab to find and select the folder, then click on the checkbox to share that item. The picture below shows the result of that process:

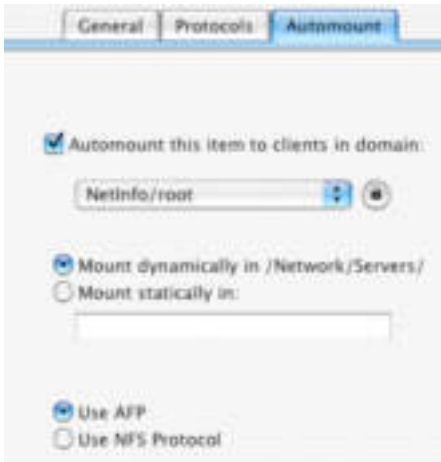


Once the sharepoint is 'shared' it will show up in the Share Points tab.

You'll notice that I changed the owner and group for this sharepoint. It was 'admin' and 'staff' by default; but I changed it to match the settings used for the default 'Users' folder. Is this necessary? Not really, I just do it for consistency, and for the fact that it always works.

Next, you would move to the 'Automount' tab and set the directory up as a network mount point: This

process allows you to have the home directory 'pre-mount' for the user when the computer logs in. The actual sharepoint is not mounted when the computer comes on the network; but a link (or alias in the old vernacular) is established and the sharepoint is located for mounting. This speeds up the process and helps in speeding up the user login experience.



You need to authenticate as 'root' or the primary 'admin' get to unlock the padlock.

Once the sharepoint is an automount item, it will show up for any new user in the 'Home' tab of the user account.

1.b.3.b. Advanced home directories

Another option for establishing home directories is to use the 'Advanced' settings in WGM to set up the location of the user's home directory. With the Advanced settings, you can specify home directories to be located in sub-folders within a sharepoint, as well as locating them on non-MacOS X servers. Key to setting this up correctly is making sure you follow the path names and conventions for the required URL's.

The first step is to actually create the folder structure for your user's home. In this case, we will use the faculty as our guinea pigs. :-) At the designated home directory server, you will create a primary home directory folder, in this case it is called 'staff_home' and will have a sub-folder for each school (elem, middle, high). In WGM, select the 'staff_home' folder and share it. Also, following the guidelines above, set it to be an automount point. You set the sharepoint to be automounted, not the sub-folders.

The second step will take place when we create the users and add the home directory attribute to their account record. We'll tackle that in the section 2.

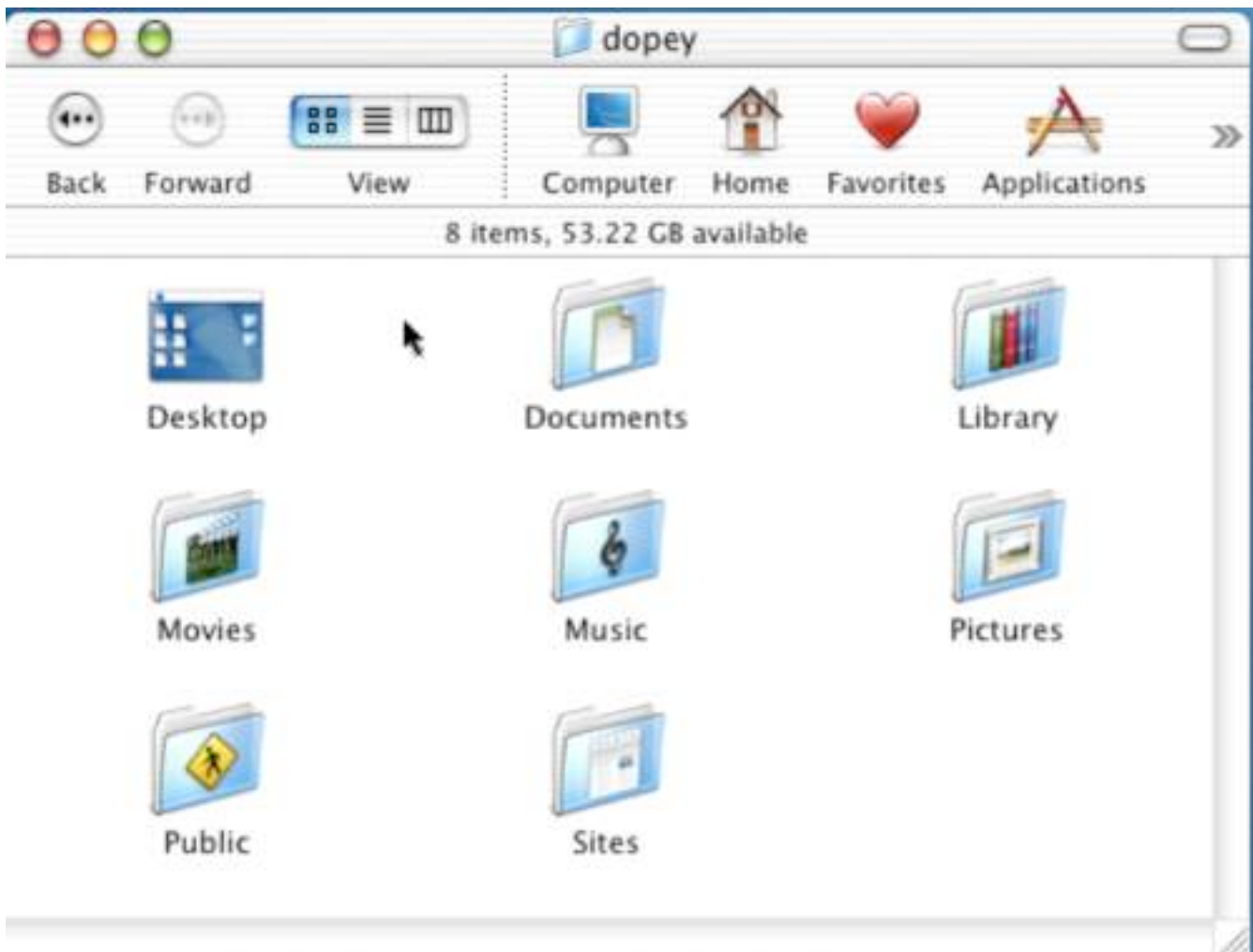
Note! Although the user has been assigned a home directory, the actual folder for that user won't get created yet. I'll cover that in the section on user accounts. If you are using a non-OSX server for home directories, you will need to create the home folder and its sub-folders yourself. Only MacOS X server supports auto-creation of the home directories.

1.b.3.c. Customizing the Home Directory template

The basic home directory template contains all of the sub folders and contents the MacOS X team thinks are needed by the average user. Recognizing that the logic behind this is to support the consumer with a focus on the iLife apps will help. A network/server admin has the ability to redesign the home directory layout, as well as pre-populate the folders with settings and documents that may enhance the client user's experience.

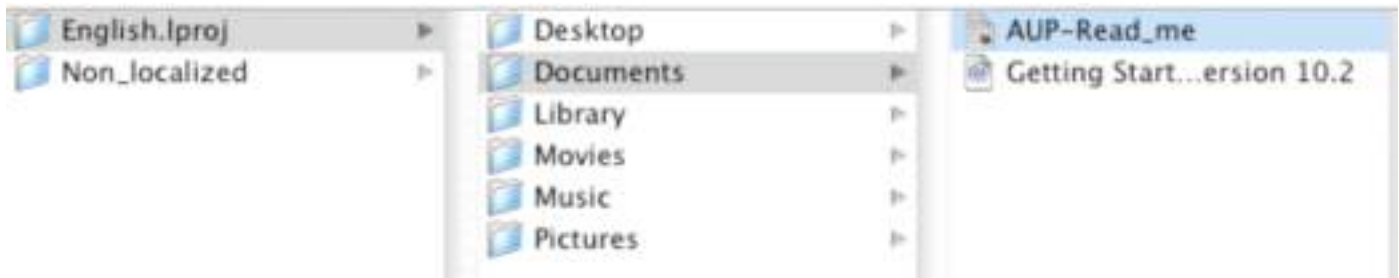
The default, or master, home directory template exists inside **/System/Library/User Template/English.lproj** (for English systems). This template is accessible only as root, otherwise, it will be locked. Permissions to the folder are set so that the user account owns the folder, the group 'wheel' by default has read-only access, and all other users -everyone- has read-only access. If you want to change the access levels to the home directories, you will need to either use Terminal or Macinmind's Passenger. The process for altering the permissions will be in an appendix to the T&T.

Here's what a default home directory looks like:



Dopey lives here.

To set up a custom home directory template, log into the server holding the home directory sharepoint(s) as root. Navigate to the **/System/Library/User Template/English.lproj** folder and open it. You may then remove or add folders as you see fit. You may also add documents or other items as desired to the various folders. An example would be adding a default set of templates for all users, such as book report and homework examples, a copy of the AUP, and special fonts that may be needed.



Modified /System/User Templates/English.lproj - home directory template

Changes made to this template will affect user home directories created -after- the fact. It does not alter existing home directories. **Key!** You must alter the home directory template on each server that provides home directories. The changes made on one home directory server do not alter other templates.

1.c. Network tips - unkinking the cables

Just a few quick items here to keep everything on track. Over 90% of the problems in the past several years that started with 'Macintosh Manager is too slow' were due to misconfigured networks. There are some basic items that really need to be set correctly in order to avoid network chokepoints. DNS is essential to the proper operation of the client/server operations. Although there are workarounds to a lack of DNS, they are no substitute for a proper DNS entry for each server on a DNS box inside your network. Many of the problems associated with connection failures comes from improper DNS configurations.

- Do **-not-** force Duplex or speed on a Mac when you are trying to autonegotiate. The very term 'autonegotiate' means -both- ends of the network come to an agreement. Macs default to half-duplex when nothing else seems to work.

- If Spanning Tree is on, make sure Portfast (fast start) is on also or else you will get Appletalk address errors on the network.

- Set up Airport basestations as bridges only. Do not turn on NAT/DHCP or any of the special settings. All of those slow down the Airport response.

- If at all possible - have a DNS inside your network! MacOS X server is highly dependent on DNS for many of its services. While you can use machine records for many lookup features, DNS is much cleaner. Given that currently, MacOS X server does not have a GUI for setting up DNS, it can be a hassle to do this, there are a couple of workarounds.

Men&Mice up in Iceland have QuickDNS Pro - a great solution for managing an internal DNS, and

even for running a huge external DNS. It uses wizards for helping you work through the setups and even provides a great auto-reverse DNS table creation. <http://www.menandmice.com>

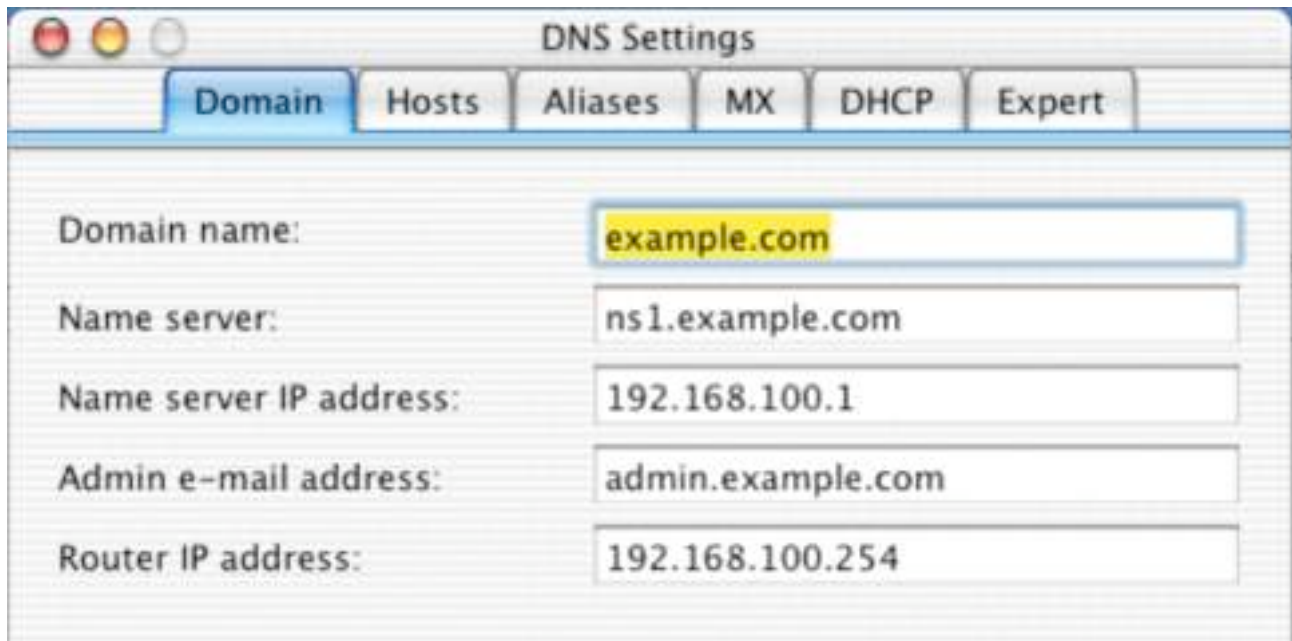
A wonderful piece of freeware popped up in VersionTracker called 'DNS Helper' - it is a MacOS X GUI for DNS setup. Not too sophisticated; but it does exactly what it is supposed to do - provide a front end to setting up the DNS entries on an OSX server. Look for DNS Helper by Josh Wisenbaker on Version Tracker - as of this doc the current version was 1.5.

DNS also needs to see inside and outside your network. If you are NAT'd (using fake IP addresses), your DNS must be able to resolve for you when you do a query from a workstation to the server - and back - inside the network. For your users to get to the Internet, your DNS needs to have **forwarders** enabled that are pointers to an external DNS, such as your district DNS or ISP. If you need external access to your server from outside the firewall, you need to open the appropriate ports in your firewall for the service you are passing. See the Server Admin Guide p. 578 (Chap 15) for more details on ports and port numbers.



Name	TTL	Type	Data	Comment
apple.edu.		NS	dns.lab.apple.edu.	lab zone
dp500.apple.edu.		A	10.0.0.250	
asip.apple.edu.		A	10.0.0.251	
localhost.apple.edu.		A	127.0.0.1	
dns.apple.edu.		CNAME	dp500.apple.edu.	
johnd.apple.edu.		A	10.0.0.101	
xserve2.apple.edu.		A	10.0.0.202	
main.apple.edu.		A	10.0.0.201	
mx1.apple.edu.		CNAME	xserve1.apple.edu.	
xserve1.apple.edu.		CNAME	main.apple.edu.	
ldap.apple.edu.		A	10.0.0.252	

QuickDNS Pro from Men & Mice



DNS Helper by Josh Wisenbaker

- And did I mention that you need to have DNS set up?

1.d. Additional information. For additional information on the material covered in this section, see the MacOS X Server Administrator's Guide (For version 10.2.3 or later), chapters 1, 4, 5, 11, and 14.

Next - Section 2 Users, Groups, and Open Directory