Netboot Services

Jason Healy, Director of Networks and Systems

Last Updated Nov 07, 2009

Contents

Chapter 1

Netboot Services

Last updated 2009/11/07

1.1 Introduction

All recent models of Macintosh computer have the ability to be **NetBooted**, where the computer boots its operating system off of a special server on the network. This approach has several advantages in a managed setting, including the ability to manage software and OS settings in lab environments and not needing to clean public machines manually (as changes are lost after reboots).

Here at Suffield, we do not have many public labs (each student has their own laptop). We primarily use NetBoot as a "rescue disk" for computers. By booting off of the network, the internal hard drive can be examined, repaired, erased, or reimaged with fresh software. Our NetBoot image contains various file repair utilities, as well as installers and system imaging software.

This document describes how to set up a NetBoot server that will service clients. Additionally, we describe how to build a "rescue disk" to serve to clients for repairs and system imaging.

Note: we mainly use our NetBoot image for booting damaged machines and repairing or reimaging them. Reimaging is done using a program called **NetRestore**. While we discuss the installation of NetRestore in this document, it only covers the use of the client. For more information about setting up NetRestore on the server, and for information on building images to install on client machines, see our HOWTO on creating NetRestore images.

1.2 Configuring Netboot Services

To provide NetBoot services to your network, you'll need a machine running Mac OS X Server. These instructions assume version 10.4, though they should work equally well for 10.3. (10.2 is significantly different, however, so these instructions will **not** work for that version.) You should use an **unlimited** client license version of OS X, or else you will only be able to boot a limited number of machines simultaneously.

Please refer to Apple's documentation regarding the specifications of the server hardware itself. Depending on the number of clients, image size, network speed, and other factors, you may need to scale up your hardware. As our server is lightly used (fewer than 15 clients booted simultaneously), we get by with a G4 500Mhz machine with mirrored IDE drives for storage and SCSI for client data.

1.2.1 Initial Setup

Begin by installing and configuring a machine running Mac OS X Server. Disable any services you will not be using. At a minimum, however, you must be running **AFP**, **DHCP**, and **NetBoot** to run a NetBoot server.

(**Note:** on Mac OS X Server 10.3, the **DHCP** service must also be enabled, even if it serves no actual addresses. This bizzare requirement has been dropped as of 10.4.)

1.2.2 AFP Settings

Apple automatically configures a few sharepoints via AFP when you enable NetBoot. You should not alter or remove these sharepoints at any time.

You do not need to make any special changes to AFP to use NetBoot by itself. However, if you plan to use NetRestore for system imaging, you will need to create a sharepoint for the saved disk image files. Create a folder (or volume) on the server, and share it via AFP. You may wish to create a new user account that has access to this share, and disable guests (this prevents people from getting access to the raw image files). You can use the **Workgroup Manager** tool for these tasks.

1.2.3 NFS Settings

In **Server Admin**, click on the **NFS** item. Confirm that the NFS service is running. If you plan to have a heavily loaded server, you may wish to increase the number of server daemon processes.

1.2.4 NetBoot Settings

In **Server Admin**, click on the **NetBoot** item. You should see an overview status of the other services that NetBoot depends on. Ensure that these services are shown as running (except DHCP, if your network already has a DHCP server).

Click on the **Settings** tab at the bottom of the window. Under the **General** tab, you'll have a few choices on how to store client data and images. Note that "images" here refers to images that the clients will boot off of, not system restore images.

Check the box(es) for the drives you wish to use for the different types of data. If possible, split up the data between drives (this helps with speed).

At this point, you don't have any images to serve via NetBoot, so there are no other settings to change. See the next section for information on creating a NetBoot image that clients can start up from.

1.2.5 Network Settings

If you're booting your clients on the same subnet as the server, you should be set to go. However, if you're going to be booting accross subnets, you'll need to do a little more work.

Because NetBoot discovery requests are sent from the client using DHCP, packets from the client must be forwarded on to the server. If you have Cisco equipment, you must use the `ip helper-address` statement in your router configuration to forward the packets.

For example, if your server is on VLAN 10 with IP address 172.16.10.100 and your client is on VLAN 20, your configuration should look something like this:

```
interface Vlan10
  description Server VLAN
  ip address 172.16.10.1

interface Vlan20
  description Client VLAN
  ip address 172.16.20.1
  ip helper-address 172.16.10.100
```

This tells the router to forward broadcast packets accross VLANs to the address you specify. By default, DHCP packets are forwarded, along with other common broadcast traffic. See your network equipment manuals for more information on the default forwarded ports.

Additionally, you must ensure that you are not blocking any traffic between the clients and the server. NetBoot images are served via TFTP, AFP, HTTP, or NFS, so these ports (and any "return" ports for protocols such as NFS) must be open. If your setup doesn't seem to be working, try opening all ports to confirm that the problem isn't networking-related.

1.3 Building a Rescue Image

Using NetBoot, we can create a "rescue disk" that can boot client computers that are damaged or that need system software installation. This is a simple way to keep all your system utilities in a single place, and makes repairing and restoring systems very easy.

1.3.1 Selecting a Machine

To build your rescue image, you'll need a machine to install the software on. We'll call this machine the **master** machine.

Your master machine should be the best computer available to you. Macintosh computers will often run systems from computers that are more recent, but the reverse is not always true.

You may wish to use an external drive to build the system image. This prevents you from having to erase a production machine, and makes loading the image onto the NetBoot server very easy. Alternately, you may prepare the image on a machine's internal hard drive, and then boot it into Target Mode to transfer the image.

You will be installing a system from scratch onto this machine. Make sure you've backed everything up, in case something goes wrong.

1.3.2 Base Installation

OS X Installation

Begin by booting the master machine with the latest installation media you have.

You should choose a full **Erase and Install** option from the installer to ensure that you do not have any leftover cruft from the previous system.

Additionally, you should choose to perform a **Custom Install**. On the customization screen, deselect any options that are not necessary. This includes

Additional Fonts, **Language Translations**, and **Additional Applications**. These things all take up space, and are not needed for our repair image.

When the installation completes, you will be brought to a confirmation screen. Do **not** continue yet.

Enabling The Root Account

While still booted from the installation DVD, choose **Reset Password** from the **Utilities** menu.

In the Reset Password Utility, select the hard drive you just installed OS X onto. Then choose the **System Administrator (root)** account from the drop-down menu.

Set the password for the root account to our standard password.

Quit **Reset Password**.

Disabling Registration

While still booted from the installation DVD, choose **Terminal** from the **Utilities** menu.

For the next step, you must know the name of the drive you installed OS X onto. Typically, the drive will be called "Macintosh HD". In the steps below, replace "Macintosh HD" with the actual name of the drive.

Type the following command (all on one line, capitalized exactly as shown):

```
touch /Volumes/Macintosh HD/private/var/db/.AppleSetupDone
```

Type `exit` on the command line, and quit Terminal.

Initial Boot

Now continue the installation DVD steps, which should cause the computer to restart.

Log in as "root", with the password you specified earlier.

If you are prompted to register the machine, simply quit the registration application.

1.3.3 System Configuration

OS Updates

Run **Software Update** and install any pending updates. Reboot as necessary, and continue running until no further updates are pending.

Resources Folder

Create an alias to the "Resources" folder on Veronica on the Desktop.

Finder Preferences

Show **Connected Servers**.

New Finder windows should open **Applications**.

Sidebar should only show **Hard Disks**, **External Disks**, **CDs, DVDs, and iPods**, **Connected Servers**, **Home**, and **Applications**.

Show all file extensions.

Disable Spotlight

Spotlight is a resource hog, and not useful in a repair image. You can disable it by running the following commands:

For Leopard (10.5):

```
launchctl unload -w /System/Library/LaunchAgents/com.apple.Spotlight.plist
launchctl unload -w /System/Library/LaunchDaemons/com.apple.metadata.mds.plist
```

For Snow Leopard (10.6):

```
launchctl unload -w /System/Library/LaunchAgents/com.apple.metadata.mdwrite.plist
launchctl unload -w /System/Library/LaunchDaemons/com.apple.metadata.mds.plist
chmod 600 /System/Library/CoreServices/Search.bundle/Contents/MacOS/Search
```

Disable Bonjour

Additionally, we don't want to allow bonjour requests to or from netbooted machines. Add the following firewall rules to deny Bonjour traffic in /etc/rc.local:

```
/sbin/ipfw add 1000 deny udp from any to any dst-port 5353 out
/sbin/ip6fw add 1001 deny udp from any to any 5353 out
```

Disable Safe Sleep

Safe Sleep keeps a large file (the size of physical RAM) on the boot volume to allow for hibernation. This is a huge performance hit, so we disable it for our repair image.

Add the following to /etc/rc.local

```
pmset -a hibernatemode 0
```

"Reserved" Space

Under 10.6, System Image Utility shrinks the avilable netboot image size to be only slightly (1GB) larger than the amount of space required by the files on the image. This can cause "out of disk space" warnings.

To combat this, we create a large file on the hard drive (10GB):

```
dd if=/dev/zero of=/private/var/vm/suffield-reserved-space bs=1g count=10
```

Then, we add the following to /etc/rc.local:

```
rm -f /private/var/vm/suffield-reserved-space
```

This has the effect of building the image with 10GB of space that will be freed up immediately on boot.

System Font Replacement

For some reason, our Netboot systems think the system fonts are "damaged" after System Image Utility has worked from a master machine. To prevent this issue from happening, open **Font Book** and go to its preference screen. There, **uncheck** the "Alert me when system fonts change" checkbox.

Then, rename the following directory to "ProtectedFonts.backup" (the lines below should be typed all on one line as a single path):

```
/System/Library/System/Library/Frameworks/ \
ApplicationServices.framework/Versions/A/Frameworks/ \
ATS.framework/Versions/A/Resources/ProtectedFonts/
```

Background Image

To easily identify a computer that has been NetBooted, it is helpful to have a special background image. Suffield has such an image, stored in the **Tech Repair** folder on the server.

To install an image on the master machine, copy it onto the computer and name it `DefaultDesktop.jpg`. Move the file into the folder `/System/Library/CoreServices/`, replacing any existing version.

Disabling Network Authentication

By default, our DHCP server advertises an LDAP server to all booted clients. This LDAP server helps with network authentication, servers, printers, and other centralized services.

Because the rescue image is not really multi-user, we don't need many of these authentication-related services. Additionally, they just slow down the operation of the system when not needed. Therefore, we disable these services for the rescue image.

To disable LDAP authentication, open the **Directory Access** program in `/Applications/Utilities`. Click the **LDAPv3** service and click the **configure** button to access the settings. In the window that appears, *deselect* the **Add DHCP-supplied LDAP servers to automatic search policies** checkbox. Click **OK** to save your changes.

Network Speed Tweaks

By default, Mac OS X comes with conservative networking settings that do not maximize performance over fast (100Mb/s and up) links. Since most of our NetBooted machines will be on a link that is at least this fast, we apply some tweaks to increase the performance of the networking stack.

To do this, edit (or create, if it does not exist) the file `/etc/sysctl.conf`. Add the following lines:

```
net.inet.tcp.mssdflt=1460
net.inet.tcp.sendspace=1048576
net.inet.tcp.recvspace=1048576
net.inet.udp.recvspace=65535
net.inet.udp.maxdgram=57344
kern.ipc.maxsockbuf=10485760
net.inet.tcp.newreno=1
net.inet.tcp.always_keepalive=1
net.inet.tcp.keepidle=3600
```

```
net.inet.tcp.keepintvl=150
net.inet.tcp.slowstart_flightsize=4
```

As always, you may wish to comment the lines to make future edits easier.

1.3.4 System Preferences

Open the **System Preferences** and make the following changes:

Appearance

Set appearance and colors to **Graphite**.

Desktop & Screen Saver

Set the desktop to the replaced DefaultDesktop you installed earlier.

Set the screen saver to **Computer Name**, and enable **Show with clock**. Have the screen saver start after 30 minutes.

Dock

Have the doc appear on the left-hand side of the screen, with size small enough to fit all the icons.

Expose & Spaces

Set the hot corners as follows:

- Top-left: none
- Top-right: Start Screen Saver
- Bottom-right: Disable Screen Saver
- Bottom-left: Desktop

Security

Uncheck all items under the **General** tab.

Displays

Check **Show displays in menu bar**.

Energy Saver

Set the **Computer Sleep** time to **Never**. Set the **Display sleep** time to **1 hour**.

Change the battery status menu to show estimated time.

Print & Fax

Add the **Multimedia Lab** printer.

Network

Disable the **AirPort** card (netbooted machines have a hardwired connection, so there's no need for Airport).

Sharing

Name the computer "Repair-and-Restore". Enable **Remote Login** and **Remote Management**.

Accounts

Set the computer to autologin to the root account, using the password you specified earlier.

Date & Time

Set the clock automatically to `ntp.suffieldacademy.org`.

Confirm that the time zone is set correctly.

Turn on showing the time with seconds.

Software Update

Disable checking for updates.

Time Machine

Turn off, and disable showing status in the menu bar.

1.3.5 Software Installation

Below we describe how to install the standard suite of repair software used by Suffield Academy.

DeployStudio

Download the latest stable version of DeployStudio:

http://www.deploystudio.com/

Launch the installer, and choose **Customize**.

Select only **DeployStudio Runtime** (plus any mandatory greyed-out options).

Install the software.

Add **DeployStudio Runtime** from the **Utilities** folder into the dock.

Run **DeployStudio Admin** and set the server and login credentials. Set the password to be saved for future use. The server address is:

```
http://veronica.suffieldacademy.org:60080/
```

Start **DeployStudio Runtime** and confirm that the credentials have been saved correctly. Log in and confirm that everything is working as planned.

DiskWarrior

Copy DiskWarrior from the original media into the **Applications** folder on the master machine. Add it to the dock.

Launch the program once to ensure that it is correctly installed.

DataRescue

Copy DataRescue II from the original media into the **Applications** folder on the master machine. Add it to the dock.

Launch the program. On the first time through, it will prompt you to activate the registration for the software. Enter in the correct information and quit the program when it has been registered.

TechTool Pro

Run the TechTool Pro installer from the original media and install it onto the master machine. Start the program and register it properly. If any updates are available, install them as well.

Reboot the machine, and **disable** the active protection in the Tech Tools system preference.

memtest

Mount the memtest distribution folder and copy it to `/usr/bin`.

rsync 3 (patched)

Compile and install a patched version of rsync 3 with ACL/metadata support and put it in /usr/local/bin.

Firmware Password Utility

This program may be found on any Mac OS X installer disk. It is used to lock or unlock the firmware on the computer.

System Image Utility

This program is included on Mac OS X server machines, and is used to create Netboot sets. We put it on our image to make it easier to create Netboot sets from any machine.

Safari

Show the status bar.

Show the tab bar.

In the preferences, set the default home page to:

```
http://web.suffieldacademy.org/ils/crc/
```

Save downloaded files to the Desktop.

For Bookmarks, only include Bonjour, and disable all collections.

Set RSS never to update.

Disable all forms AutoFill.

Clear the history, empty the cache, and quit.

Terminal

Set the Terminal to "Pro".

Set dimensions to 80x40.

Set the window to close when the shell exits cleanly.

1.3.6 Performance Tweaks

Deleting Unused Files

To save space on the image, you should delete any applications and files you know you will not need. Good candidates include the **iLife** suite, any games, obscure utilities (**ColorSync**, **ODBC**, etc), screen savers, background pictures, sample media, and developer tool samples.

Delete /private/var/vm/sleepimage

Download and run Monolingual (monolingual.sourceforge.net) to remove all but English localizations from the machine.

1.3.7 Building the Image

At this point, you should have a disk with a fully-functional NetBoot image on it. You must now connect this disk to a machine with Apple's **System Image Utility** installed on it (it is included with Mac OS X Server).

The simplest way to do this is to connect the master image directly to the NetBoot server via firewire. If your image is on a firewire drive, simply connect it. If your image is built directly on a master machine, boot the machine into firewire target disk mode and connect it. Then:

1. Perform any last-minute housekeeping (deleting the files in `/var/vm/`, cache files, etc).
2. Start **System Image Utility** on the server.
3. Choose **New Boot** from the toolbar.
4. Give your new image a name, ID, and description.
5. Under the **Contents** tab, select your master image disk.
6. Click the **Create** button. Save the image to your NetBoot images folder on the server (or elsewhere, if you wish to move it later).

1.3.8 Installing the Image

If you used **System Image Utility** to create an image directly into your NetBoot server folder, then the image is installed and ready to be used.

If you saved the image elsewhere, you must copy it into the **SPxxx** folder on your NetBoot server. The folder name varies depending on how many volumes you have enabled to host NetBoot images. In most cases, the folder is called `SP0` and is located in `/Library/NetBoot/` on the main drive.

If you want this image to be the default NetBoot image, use **Server Admin** to set this image to be the default.

1.3.9 Testing the Image

The moment of truth! NetBoot one of your client machines to your new image and test out the software.

If your client machines won't NetBoot correctly, confirm that there are no firewall or ACL problems between the client and server machines. Recall that a proper NetBoot requires DHCP, TFTP, NFS, and AFP to work properly. Here are the symptoms of one of these protocols not working:

- **DHCP** Machine will not boot at all. Other machines on subnet won't get IP addresses assigned to them.
- **TFTP** Machine will not get to "spinning globe" stage of NetBoot (only flashing globe icon). TFTP is needed to send the initial booter file to clients, so if your boot fails early, check the TFTP service on the server.
- **NFS** NFS is needed to mount the NetBoot image and complete the boot process. If you get to the "spinning globe", but freeze up afterwords, check to make sure you're passing NFS traffic over UDP correctly.
- **AFP** Diskless NetBoot requires AFP be enabled on the NetBoot server, so clients can connect and use space for temporary files. Non-diskless boots do not require AFP. If AFP is not working properly, diskless boot will either fail, or will not allow you to unmount the local hard drive.

If your clients boot, test the software and confirm that they are all properly running and registered. Once that's done, you're all set!