Mac OS X Evaluation

Final Report

Introduction

In 1999 Apple announced the specifications for its next generation operating system, an upgrade to OS 9. This next operating system would be OS X; a complete overhaul of OS 9. The announcement settled speculation and rumors revolving around Apple's plans since the return of Steve Jobs. Jobs returned to the helm of Apple after a several year hiatus where he headed several startups. The most significant and successful of these were NeXT Computers and Pixar Animation. NeXT Computers was involved in bringing the best of the Macintosh to the UNIX world. NeXT offered a line of computers running the NeXTStep operating system. NeXTStep was based on the Mach kernel developed originally at Carnegie Mellon University. Despite some innovative technologies and user refinements NeXT was never a commercial success and eventually went out of business. Jobs retained the intellectual rights to most of the innovations that came from NeXT. When he returned to Apple in 1997, he brought those innovations along with the core team of developers and systems engineers responsible for NeXTStep. These innovations and refinements became the core of OS X.

At its heart OS X is based on Mach 3.0 from Carnegie-Mellon University and FreeBSD 3.2--derived from the University of California at Berkeley's BSD 4.4-Lite. It is a fully functional, POSIX compliant, UNIX operating system with a proprietary graphical user interface (GUI) called Aqua. Aqua is the old Mac GUI with touches of UNIX X11 and Motif. It is visually appealing and presents a fluid appearance. Hence, the name Aqua.

Apple has done a good job of concealing the underlying UNIX complexity from the end user. While the UNIX can be accessed directly from the command line, Apple has provided tools that turn UNIX into a non-factor for the average user. All configuration items have graphical tools that present a straightforward, easy to understand appearance. This does not mean that there are no issues involving the UNIX core. It is possible to configure a system that does not meet the minimum level of security necessary to safely connect to Stanford's open network. This is due, in part, to the fact that Stanford's environment is non-standard in comparison to the average corporate network where one or more layers of firewalls must be traversed in order to gain access. Security, by its very nature, is often in direct conflict with ease of use.

Evaluation Procedure

The evaluation involved a team selected for a particular expertise. Each evaluator concentrated on a subset of the operating system. The subsets evaluated were infrastructure requirements, security, networking, interoperability, and user support. Two versions of OS X were evaluated; Developer Preview 4 (DP4) released at the Apple Worldwide Developer's Conference in San Jose in June and the Public Beta released in September. This document will describe the results of the evaluation effort as well as provide recommendations and simple instructions for installing, upgrading, configuring, and using the OS X operating system.

OS X Installation

Installation of OS X is smooth and fast, depending on the options selected. The only requirement is that if you want to use legacy (OS 9) applications the system must have a functional OS 9 system installed prior to installing OS X. Simply boot the system to OS 9, insert the CDROM and run the OS X installation program. The system will reboot and a wizard will step you through the installation process (See Appendix A).

OS X can be installed directly into an OS 9 partition or installed to a separate partition. If a separate partition is selected, that partition can be formatted as Mac Extended (HFS+) or UNIX File System (UFS). There are benefits and drawbacks to each configuration. If a single partition is selected, it is imperative that all perishable user data files be backed up prior to installation. Apple claims that OS X can be uninstalled if desired, but this was not tested. If the system has one partition and the separate partitions option is chosen, the entire disk will need to be reformatted and OS 9 reinstalled prior to installing OS X. This can be quite a task if the current OS 9 has been extensively customized. As noted in the OS X recommendation, technical support or expertise is required.

Supportability & Use

The primary issues involved in supportability and use are differences in the file system structure and changes to the GUI. Users and support personnel will need to become familiar with the new file structure. It may be initially frustrating to long-time Mac users, but learning the Aqua interface is not difficult and most users will become comfortable in a short time. Of more concern are the changes to the file system.

The old paradigm of the system folder that contains everything about the configuration and preferences for the operating system has shifted. The OS X file system resembles a typical UNIX file system. Files are categorized by ownership. System files go in one section and user files in another. Apple tried to retain as much of the old structure as possible but was faced with fitting a square peg in a round hole. Many items look out of place. The UNIX portion of the file system is somewhat transparent to normal users. For additional information about the changes to the directory structure go to:

http://www.macworld.com/2001/10/howto/osxsecrets.html

Another paradigm shift is the concept of multiple users on one system. OS X is a fully functional, multi-user operating system. It supports multiple accounts with individual ownership of files based on permissions of the user. It is possible for multiple users to have accounts on a single system with storage space on the local system that they control. In other words, each user can have a home directory in the OS X partition for storing files. These home directories are accessible to others based on the permissions set by the owner. This also means that the system must be able to identify the user logged in. This is accomplished by having all users login at the start of a session. This login/authentication at startup identifies the current user and is the basis for system access. Users enter their username and password and are then authenticated to the system. This feature can be turned off when OS X is installed if only one user is going to use the system.

Another new concept in OS X is that of the super user or root account. The root account reserves the ability to modify the system. Under OS 9 any user could add or remove applications, change the look of the interface, or modify the system folder. Under OS X only the root account has those permissions. Consequently, users must be aware of the power of the super user account and the need to guard it accordingly.

The fundamental concepts of system troubleshooting have not changed, but the approach takes a different path. Mac system administrators and technical support engineers now have a command line interface with a number of UNIX tools that can reveal information about many aspects of the system. These are commands that have long been employed in the UNIX community and are the foundation of UNIX system administration. This does not imply that Mac support personnel will need to become fully qualified UNIX administrators, but that the differences between the two are narrowing. Chief among these command line benefits is the ability to individually terminate applications or services that have become unresponsive without needing to restart the system. This is one of the benefits of the fully functional, multi tasking operating system in OS X.

Security

Security Summary

OS X provides a robust and secure UNIX-like environment. However, OS 9 and OS X need to be installed together to run legacy applications. When OS 9 is installed with OS X, the security reverts to that of OS 9; a single user system with virtually no protection between user processes and files.

In a dual installation mode, any user who boots to OS 9 has complete root access to all OS X system files residing on the OS 9 partition. Installing to a separate UFS partition is an option during initial OS X install, albeit not the default.

The security model is determined by the strength of the weakest link. The Stanford Security Office advises that when an OS X system is installed alone it can be properly secured for multi-user access and services. If OS 9 functionality is required, OS X should be treated the same as OS 9; as a single-user workstation offering no multi-user security services.

System Overview

OS X is composed of three parts: a MACH kernel, FreeBSD 4.4, and the Aqua user interface. OS X was designed to be a full-featured, UNIX-like, multi-user operating system. When installed alone, OS X provides the same degree of protection as FreeBSD 4.4 running minimal services.

System and user services assume a standalone Mac OS X system *without* Classic support i.e., OS 9 is not installed on the same partition.

System Services

By default OS X installs and runs at boot:

- portmapper: portmapper maps RPC services to system ports. portmapper binds to TCP/UDP port 111.
- syslog: syslog is the generic UNIX system logging utility. syslog binds to UDP port 514.
- netinfobind: netinfobind is used for the traditional Macintosh netinfo service. netinfobind binds to TCP port 735 and UDP port 732.
- ssh: ssh provides secure, remote access.

None of these services are likely to be a security risk in the near future.

OS X also provides several services that must be explicitly enabled by the user including:

- Apache: Apache is the standard UNIX web server. Apache's track record indicates it is a secure and robust web server. The Apache web server should not be confused with the OS 9 web publishing utilities.
- sendmail: sendmail is the traditional UNIX mail transmission agent. sendmail is notoriously difficult to configure. In addition, it requires frequent updates. Running sendmail is not recommended except by qualified UNIX system administrators.
- NFS: NFS provides network file sharing. NFS can be enabled on initial install through a single wizard. NFS has a long history of security vulnerabilities. Using NFS is not recommended.
- NIS: NIS is used for synchronizing user authorization data across multiple machines. NIS transfers sensitive user data in the clear across the network. In addition, a history of security problems strongly suggests that NIS should not be enabled.
- DHCP: The DHCP service is used to dynamically assign IP addresses. DHCP is an infrastructure service already provided by ITSS and need not be enabled.

Each service is complex and should only be enabled when the functionality is needed. The Security Office recommends that only competent UNIX system administrators enable these services.

User Services

A user service is defined as a service that gives access to infrastructure services. OS X ships with:

- Kerberos V: Currently only Kerberos IV is supported on campus, but Kerberos V support is expected in the near future. However, OS X only provides authentication. Utilities such as kerberized telnet must be developed before OS X can fully integrate into the Leland environment.
- E-Mail client: The native OS X email client supports both POP3 and IMAP. The client does not support kerberized authentication, i.e., all connections transmit the password in clear text. Its recommended that this client not be used for email until kerberos authentication becomes an option. Legacy email clients such as Eudora function perfectly in the OS X classic layer.
- Web Browsing: OS X installs a native version of Microsoft Internet Explorer. All browsers are historically buggy and will require ongoing testing.
- Read the Software License Agreement and accept it.
- Select the destination drive/partition and the partition format (HFS+/UFS).
- --Installation will commence and take about 25 minutes for HFS+ and about 55 minutes for UFS.
- Restart

Post-Installation

- Setup Assistance Introduction.
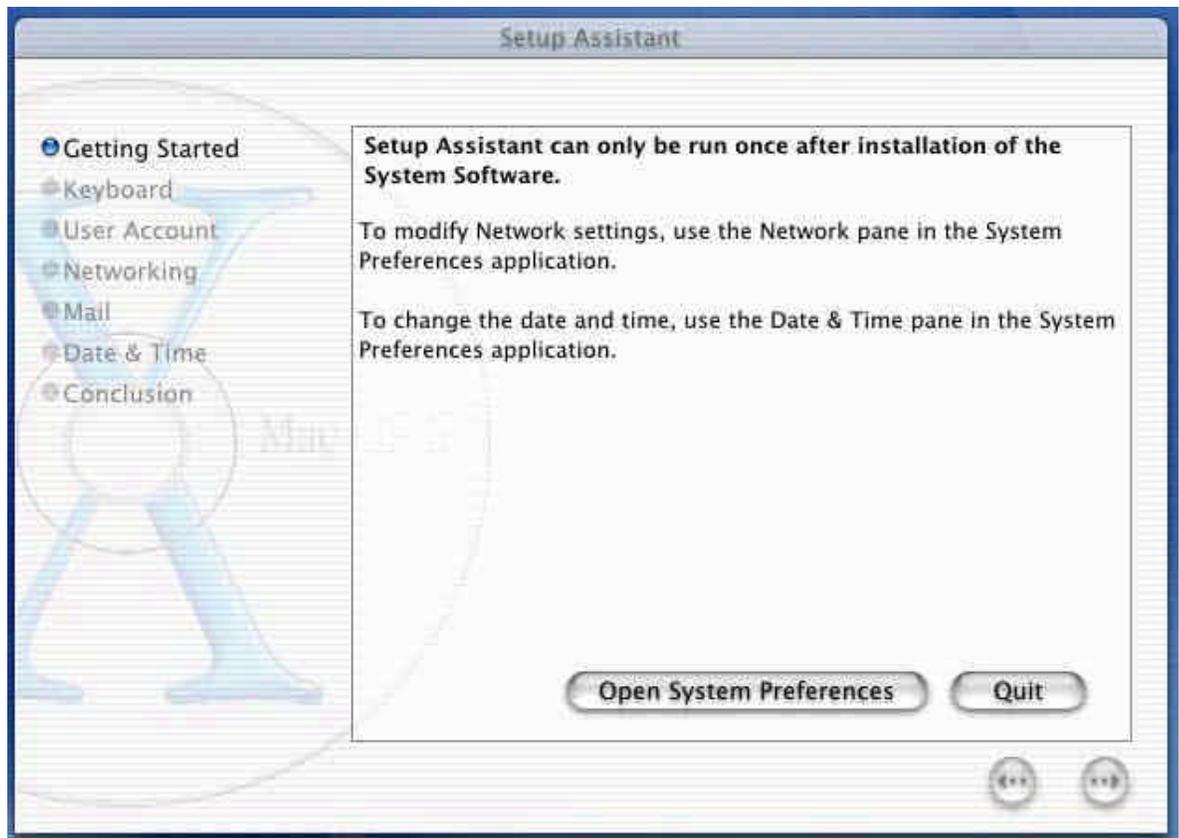
- Select keyboard layout.
- Create user account.
- This account is the primary user of the system. If the system is a shared computer with no primary user then consider creating an Administrator account. The account you create during this step will have administrator rights on the system.

Configure network connection.

- IP address, netmask, default router, DNS name servers, default DNS domain.

Mail setup.

- This step creates an email account in the default OS X email client. This email client DOES NOT support kerberos authentication and should not be used. Until a kerberos-compliant email client is available for OS X, users should continue to use Eudora.

Geographic Location

- Sets the Time and Date along with Time zone.
- Finish and Restart.

Appendix B: OS X Configuration

Networking

If you need to reconfigure networking after completion of the installation follow these steps:

- Open System Preferences from the Dock or from the Desktop pull down menu.
- Select the Network icon.
- If you are not logged in as the 'root' user then you will need to authenticate by clicking on the padlock icon in the lower left corner of the System Preferences window.
- After you successfully authenticate by entering the Administrator password you can change all or any of the settings. At a minimum this needs to be done once after OS X installation in order to activate AppleTalk. AppleTalk is not activated by default at installation.
- When all changes have been made, click the Apply button in the lower right corner. You will need to reboot after any changes to the network parameters.
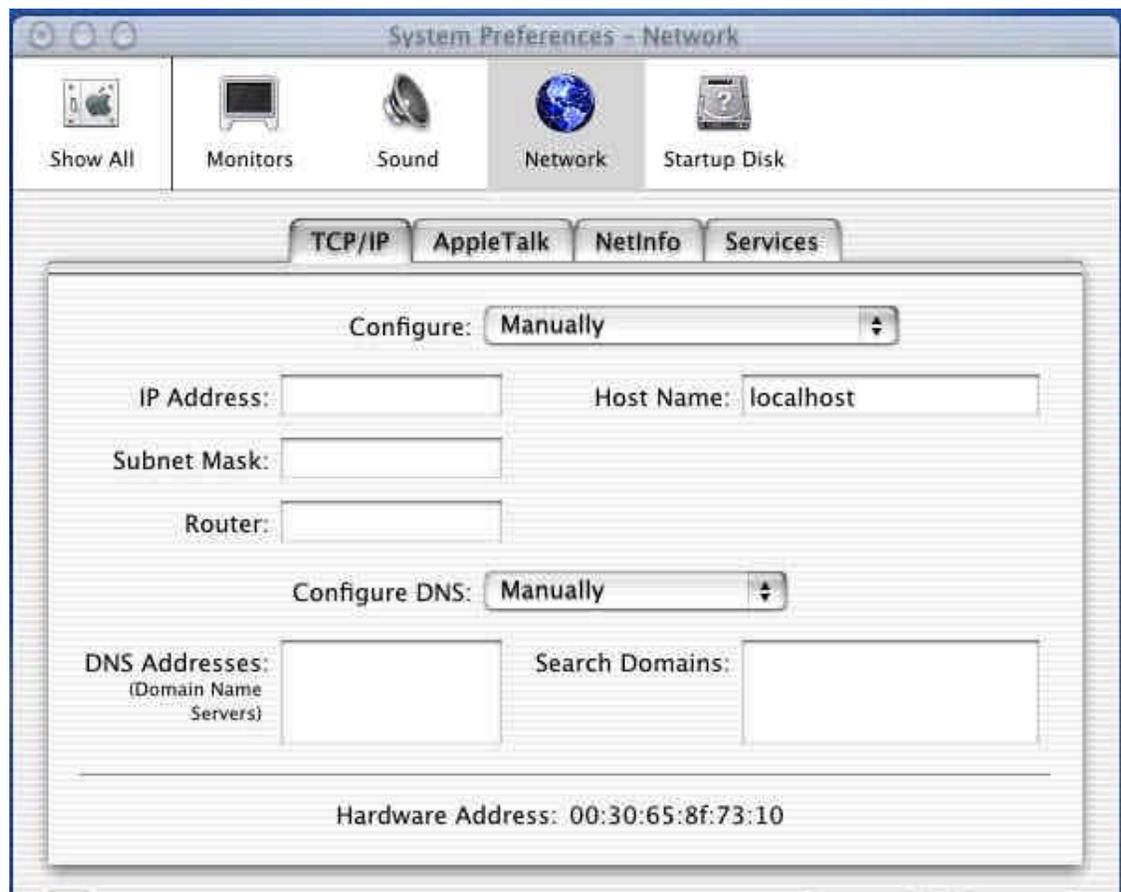
Printing

To install a printer do the following:

- Click on the Desktop icon in the Dock. This will open the finder window.
- Click on the Applications icon in the top center of the window.
- Find the Print Center icon and double click it.
- If you have not previously installed a printer a dialogue window will open instructing you to install a printer. Printers can be IP, TCP, AppleTalk or Directory.
- Follow the instructions for the type printer of your choice.

Dialup Networking
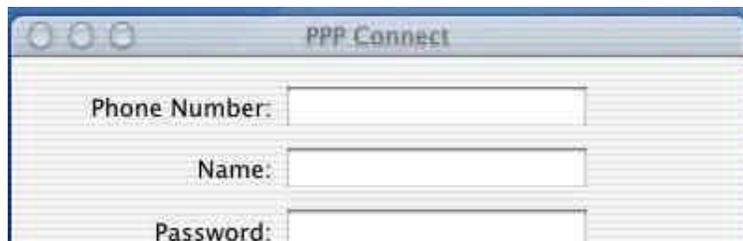
User Account Setup

To add additional users on the system do the following:

- Click on the Desktop icon in the Dock. This will open the finder window.
- Click on the Applications icon in the top center of the window.
- Find the Multiple Users icon and double click it.
- Follow the instructions on the screen for adding user accounts.
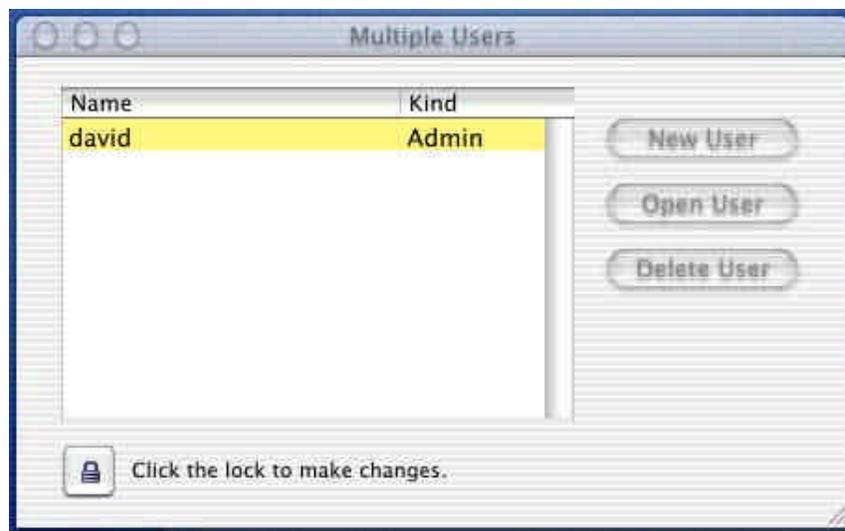
Appendix C: Applications Compatibility

Although we could not test every application available for Macs, the way the Classic layer works leads us to believe that only applications that require direct access and control of hardware will not be compatible with OS X. Apple has specifically addressed the issue of applications that require hardware access so it is not surprising that they will not work in OS X. If you are contemplating an early upgrade and have that type of application dependency, dual booting the system is the only option until the application is rewritten specifically for OS X.

MacStanford

1. MacLeland

   MacLeland is completely compatible with OS X. It runs in the Classic layer and is available whenever a Classic application that requires MacLeland is started. Mounting of AFS devices is currently not supported. This is because the AFS folder is mounted directly to the OS 9 desktop. The OS X desktop is not able to perform this mount so, although the folder is mounted, it cannot be displayed or accessed.

2. MacSamson

   Completely compatible with OS X. Runs in the Classic layer.

3. Eudora 4/5

   Completely compatible with OS X. Runs in the Classic layer.

4. Netscape Communicator 4.7x

   Completely compatible with OS X. Runs in the Classic layer.

5. Adobe Acrobat Reader

   Completely compatible with OS X. Runs in the Classic layer.

6. MacWhois

   Completely compatible with OS X. Runs in the Classic layer.

7. MacFetch

   Completely compatible with OS X. Runs in the Classic layer.

8. MacWebster

   Completely compatible with OS X. Runs in the Classic layer.