



Mac OS X Server

Getting Started

For Version 10.4 or Later

Supplement to Second Edition

🍏 Apple Computer, Inc.
© 2006 Apple Computer, Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X Server software may reproduce this publication for the purpose of learning to use such software. No part of this publication may be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid-for support services.

Every effort has been made to ensure that the information in this manual is accurate. Apple Computer, Inc., is not responsible for printing or clerical errors.

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the “keyboard” Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AirPort, AppleShare, AppleTalk, FireWire, iBook, iMac, iPod, Keychain, LaserWriter, Mac, Mac OS, Macintosh, Power Mac, Power Macintosh, Quartz, QuickTime, WebObjects, and Xserve are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Apple Remote Desktop, eMac, Finder, Xcode, and Xgrid are trademarks of Apple Computer, Inc.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products.

019-0741/7-21-06

Contents

Preface	7 About This Supplement
	7 What's New in Version 10.4
	7 High-Performance Computing
	8 User Access Management
	9 Server Administration
	10 Collaboration Services
	10 What's in This Supplement
	11 Using Onscreen Help
	11 The Mac OS X Server Suite
	13 Getting Documentation Updates
	13 Getting Additional Information
Chapter 1	15 Mac OS X Server in Action
	16 Departments and Workgroups
	19 Small and Medium Businesses
	21 Higher-Education Facilities
	22 K–12 Labs and Classrooms
	24 Computational Clustering
	26 Data Centers
Chapter 2	29 Inside Mac OS X Server
	29 Core System Services
	30 Open Directory
	30 Using Mac OS X Server Directories
	30 Using Non-Apple Directories
	31 Directory Management
	31 Search Policies
	32 Authentication
	32 Single Sign-On
	33 Discovery of Network Services
	33 User Management
	33 User Accounts
	33 Group Accounts

34	Computer Lists
34	Home Directories
34	Macintosh User Management
36	Windows User Management
36	System Imaging Services
37	NetBoot
37	Network Install
37	Software Update Service
38	File Services
38	Sharing
39	Apple File Service
39	Windows Services
40	Network File System (NFS) Service
40	File Transfer Protocol (FTP)
41	Web-based Distributed Authoring and Versioning (WebDAV)
41	Print Service
42	Web Service
43	Mail Service
44	Network Services
44	DHCP
44	DNS
45	Firewall
45	NAT
46	VPN
46	Gateway Setup Assistant
47	IP Failover
47	Media Streaming and Broadcasting
48	Application Server Support
48	Apache Tomcat
48	JBoss
49	WebObjects
49	Collaboration Services
50	Integrating Into Existing Environments
51	High Availability
51	High-Performance Computing
52	Server Administration
52	Migrating and Upgrading
Appendix A	53 Mac OS X Server Worksheet
Appendix B	65 Setup Example
	65 Mac OS X Server in a Small Business
	66 How to Set Up the Server

Glossary 73

Index 83

About This Supplement

This supplement provides an orientation to the features of Mac OS X Server version 10.4, a worksheet for installation and setup, and a setup example.

This supplement to the getting started guide will help you understand how your server can serve your network users and your business needs.

What's New in Version 10.4

Mac OS X Server version 10.4 offers major enhancements in the following key areas:

- High-performance computing
- User access management
- Server administration
- Collaboration services

Version 10.4.7 adds support for Macintosh desktop computers and servers that have Intel processors.

High-Performance Computing

Mac OS X Server offers a high-performance, cost-effective approach to computationally intensive activities:

- **Xgrid service.** Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared Mac OS X computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster.
- **64-bit computing.** Support for 64-bit processing includes 64-bit addressable memory and the ability to run 64- and 32-bit applications simultaneously.
- **Accelerated networking.** Link aggregation lets you configure several physical network links as a single logical link to improve the capacity of network connections. You can also take advantage of jumbo frames and IP over FireWire to optimize network transmissions.

User Access Management

Numerous new features in version 10.4 enhance your ability to both facilitate and manage user access to services:

- **Access Control Lists (ACLs).** ACLs give you a way to craft share point, folder, and file access permissions with a high degree of precision. A wide range of permissions can be assigned to individual users and to groups, which can be nested. In addition, you can use inheritance to propagate permissions through a file system hierarchy.
- **Nested groups.** A nested group is a group that's a member of another group. Nesting groups lets you manage groups of users at both a global level (when you want to influence all members of a group) and at a smaller, more focused level (when you want to influence only certain members of a group).
- **Unified locking.** Mac OS X Server unifies file locking across AFP and SMB/CIFS protocols. This feature lets users working on multiple platforms simultaneously share files without worrying about file corruption.
- **Service access.** You can specify which users and groups can use services hosted by a server.
- **Pervasive Kerberos support.** The following services on Mac OS X Server now support Kerberos authentication: AFP, mail, File Transfer Protocol (FTP), Secure Shell (SSH), login window, LDAPv3, Virtual Private Network (VPN), screen saver, and Apache (via the SPNEGO protocol).
- **Network browsing.** You can set up managed network views, which are custom views that users see when they select the Network icon in the sidebar of a Finder window. A managed network view is one or more network neighborhoods, which appear in the Finder as folders. Each folder contains a list of resources that an administrator has associated with the view. Managed network views offer a meaningful way to present network resources. You can create multiple views for different client computers. And because the views are stored using Open Directory, a computer's network view is automatically available when a user logs in.
- **Site-to-site VPN.** Site-to-site VPN connects two networks. It offers a secure connection that's easy to establish when it's necessary to set up a network at another site, as when a business expands. Site-to-site VPN makes both networks appear as one to users working at either site.
- **Mobility.** Users with portable computers can use trusted binding to make sure that servers accessed as they move around are trustworthy. Trusted binding offers a way for a client computer to authenticate to an LDAP server and for the LDAP server to authenticate to the client.
- **Trusted directory binding.** Trusted directory binding, also called authenticated directory binding, provides an authenticated connection between a client computer and an LDAP directory on Mac OS X Server. Because the client computer authenticates the LDAP server before connecting to it, a malicious user can't control the client computer by interposing a counterfeit, unauthenticated LDAP server.

- **Importing accounts.** The performance of importing accounts into an LDAPv3 directory has been greatly improved. In addition, you can now import password policy settings, control whether presets are applied during import, and specify the amount of information logged.

Server Administration

Mac OS X Server management continues to become easier and more effective:

- **Open Directory schema replication.** You can now store LDAP schema in the directory, letting you add new schema without manually copying configuration files. Changes are automatically propagated from the Open Directory master to all its replicas.
- **Preference editor.** If you want fine-grain control of preference settings, you can work with preference manifests using Workgroup Manager's new preference editor. Preference manifests are files that describe the structure and values of an application's or utility's preferences. The preference editor lets you work with preference manifests for the predefined preferences or add new preference manifests for applications and utilities of interest.
- **Junk mail and virus filtering.** Mail service protects users from junk mail and other annoying or unauthorized messages. You can define filters that help minimize junk mail and viruses, filter out unsolicited commercial email, and detect messages that contain particular content. Junk mail filtering, based on the powerful SpamAssassin, includes an autolearning option.
- **Network gateway setup.** A new application, Gateway Setup Assistant, automates the configuration of a simple gateway between the local network and the Internet. A gateway lets you share the server's Internet connection among computers on the local area network (LAN). Gateway Setup Assistant configures Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), firewall, DNS, and VPN services automatically.
- **Secure Sockets Layer (SSL) certificate management.** Server Admin makes it easy to manage SSL certificates that can be used by mail, web, Open Directory, and other services that support them. You can create a self-signed certificate, and generate a Certificate Signing Request (CSR) to obtain an SSL certificate from an issuing authority and install the certificate.

Collaboration Services

Collaboration services promote interactions among users, facilitating teamwork and productivity. Mac OS X Server continues to provide such collaborative support as mailing list management, group account and folder management, and cross-platform file sharing. Two new collaborative services have been added for version 10.4:

- **Weblog service.** Mac OS X Server provides a multiuser weblog server that complies with the RSS and Atom XML standards. Weblog service supports Open Directory authentication. For additional safety, users can access Weblog service using a website that's SSL enabled.
- **iChat service.** Mac OS X Server provides instant messaging for Macintosh, Windows, and Linux users. User authentication is integrated into Open Directory, and setup and administration of iChat service is done using the graphical Server Admin application.

What's in This Supplement

This getting started supplement includes two chapters, two appendixes, and a glossary.

- Chapter 1, "Mac OS X Server in Action," provides a brief graphical tour that highlights services and configurations in some popular deployment scenarios.
- Chapter 2, "Inside Mac OS X Server," introduces the services that Mac OS X Server offers and tells you where to find more information about them.
- Appendix A, "Mac OS X Server Worksheet," is a form for recording information you'll need when you install and set up Mac OS X Server.
- Appendix B, "Setup Example," illustrates how you might install Mac OS X Server and perform initial server setup in a small business.
- The glossary briefly defines the terms used in the getting started guide and this document.

This document supplements the second edition of *Mac OS X Server Getting Started for Version 10.4 or Later*, which concentrates on instructions for installing and setting up the server software. The first edition of the getting started guide combined those instructions with the content of this document.

The getting started guide is included with Mac OS X Server as a printed book and as a PDF file in the Documentation folder of the server installation disc and the *Mac OS X Server Admin Tools* CD. The getting started guide is also available for downloading from the server documentation website:

www.apple.com/server/documentation/

Note: Because Apple frequently releases new versions and updates to its software, images shown in this book may be different from what you see on your screen.

Using Onscreen Help

You can view instructions and other useful information from this and other documents in the server suite by using onscreen help.

On a computer running Mac OS X Server, you can access onscreen help after opening Workgroup Manager or Server Admin. From the Help menu, select one of the options:

- *Workgroup Manager Help* or *Server Admin Help* displays information about the application.
- *Mac OS X Server Help* displays the main server help page, from which you can search or browse for server information.
- *Documentation* takes you to www.apple.com/server/documentation/, from which you can download server documentation.

You can also access onscreen help from the Finder or other applications on a server or on an administrator computer. (An administrator computer is a Mac OS X computer with server administration software installed on it.) Use the Help menu to open Help Viewer, and then choose Library > Mac OS X Server Help.

To see the latest server help topics, make sure the server or administrator computer is connected to the Internet while you're using Help Viewer. Help Viewer automatically retrieves and caches the latest server help topics from the Internet. When not connected to the Internet, Help Viewer displays cached help topics.

The Mac OS X Server Suite

The Mac OS X Server documentation includes a suite of guides that explain the services and provide instructions for configuring, managing, and troubleshooting the services. All of the guides are available in PDF format from:

www.apple.com/server/documentation/

This guide ...	tells you how to:
<i>Getting Started, Getting Started Supplement, and Mac OS X Server Worksheet</i>	Install Mac OS X Server and set it up for the first time.
<i>Collaboration Services Administration</i>	Set up and manage weblog, chat, and other services that facilitate interactions among users.
<i>Command-line Administration</i>	Use commands and configuration files to perform server administration tasks in a UNIX command shell.
<i>Deploying Mac OS X Computers for K-12 Education</i>	Configure and deploy Mac OS X Server and a set of Mac OS X computers for use by K-12 staff, teachers, and students.
<i>Deploying Mac OS X Server for High Performance Computing</i>	Set up and manage Mac OS X Server and Apple cluster computers to speed up processing of complex computations.

This guide ...	tells you how to:
<i>File Services Administration</i>	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB/CIFS.
<i>High Availability Administration</i>	Manage IP failover, link aggregation, load balancing, and other hardware and software configurations to ensure high availability of Mac OS X Server services.
<i>Java Application Server Guide</i>	Configure and administer a JBoss application server on Mac OS X Server.
<i>Mac OS X Security Configuration</i>	Secure Mac OS X client computers.
<i>Mac OS X Server Security Configuration</i>	Secure Mac OS X Server computers.
<i>Mail Service Administration</i>	Set up, configure, and administer mail services on the server.
<i>Migrating to Mac OS X Server From Windows NT</i>	Move accounts, shared folders, and services from Windows NT servers to Mac OS X Server.
<i>Network Services Administration</i>	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.
<i>Open Directory Administration</i>	Manage directory and authentication services.
<i>Print Service Administration</i>	Host shared printers and manage their associated queues and print jobs.
<i>QuickTime Streaming Server 5.5 Administration</i>	Set up and manage QuickTime streaming services.
<i>System Imaging and Software Update Administration</i>	Use NetBoot and Network Install to create disk images from which Macintosh computers can start up over the network. Set up a software update server for updating client computers over the network.
<i>Upgrading And Migrating</i>	Use data and service settings that are currently being used on earlier versions of the server software.
<i>User Management</i>	Create and manage user accounts, groups, and computer lists. Set up managed preferences for Mac OS X clients.
<i>Web Technologies Administration</i>	Set up and manage a web server, including WebDAV, WebMail, and web modules.
<i>Windows Services Administration</i>	Set up and manage services including PDC, BDC, file, and print, for Windows computer users.
<i>Xgrid Administration</i>	Manage computational Xserve clusters using the Xgrid application.
<i>Mac OS X Server Glossary</i>	Learn about terms used for server and storage products.

Getting Documentation Updates

Periodically, Apple posts new onscreen help topics, revised guides, and solution papers. The new help topics include updates to the latest guides.

- To view new onscreen help topics, make sure your server or administrator computer is connected to the Internet and click the Late-Breaking News link on the main Mac OS X Server help page.
- To download the latest guides and solution papers in PDF format, go to the Mac OS X Server documentation webpage: www.apple.com/server/documentation/.

Getting Additional Information

For more information, consult these resources:

Read Me documents—important updates and special information. Look for them on the server discs.

Mac OS X Server website (www.apple.com/macosx/server/)—gateway to extensive product and technology information.

Apple Service & Support website (www.apple.com/support/)—access to hundreds of articles from Apple's support organization.

Apple customer training (train.apple.com/)—instructor-led and self-paced courses for honing your server administration skills.

Apple discussion groups (discussions.info.apple.com/)—a way to share questions, knowledge, and advice with other administrators.

Apple mailing list directory (www.lists.apple.com/)—subscribe to mailing lists so you can communicate with other administrators using email.

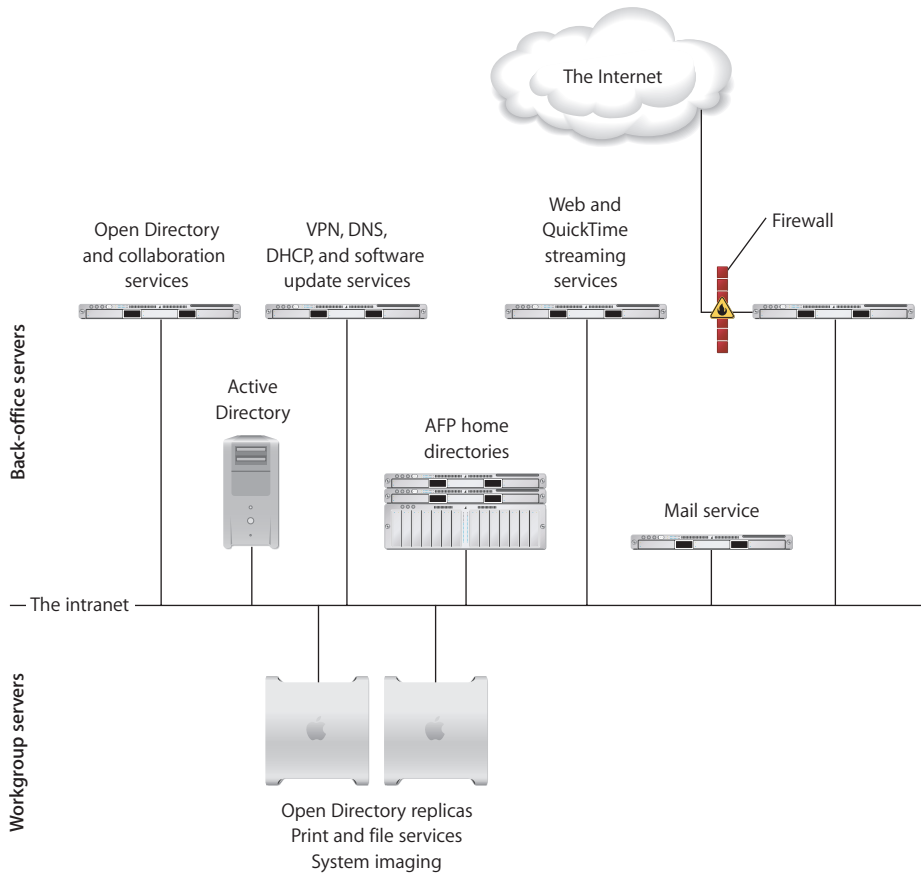
Mac OS X Server addresses the needs of many environments.

This chapter is a brief graphical tour that highlights services and configurations of special interest in some popular scenarios:

- Departments and workgroups
- Small and medium businesses
- Higher-education facilities
- K–12 labs and classrooms
- Computational clustering
- Data centers

Departments and Workgroups

In large organizations, Mac OS X Server helps you support the special needs of departments and workgroups, yet centralize corporate-level services.



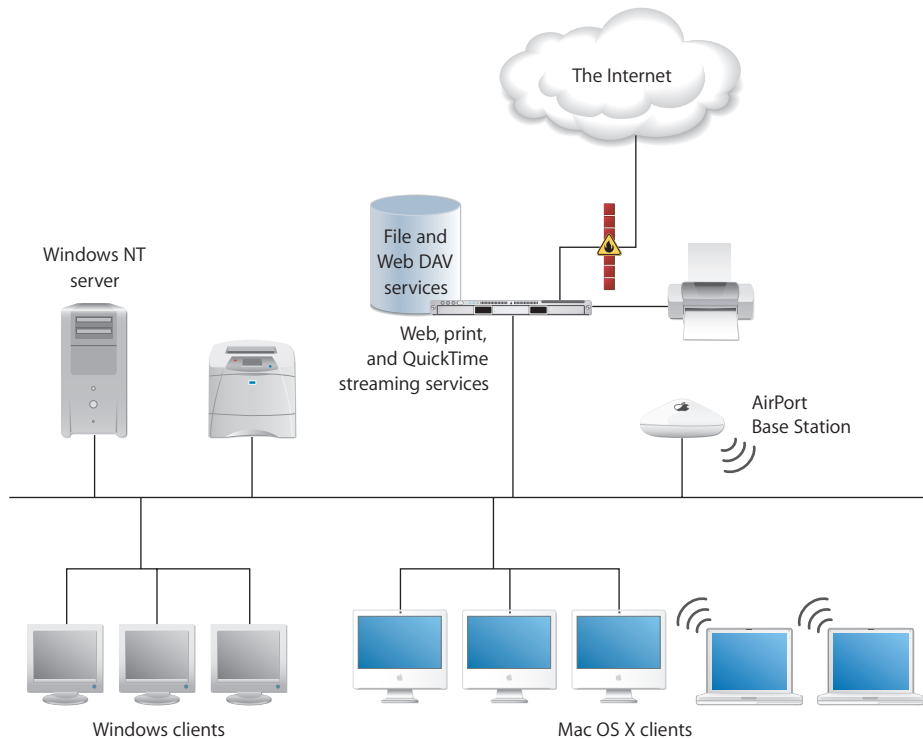
Back-office servers and services address business-wide needs:

- Open Directory lets you manage directory data centrally, but distribute it geographically using replication.
- Collaboration services help employees interact with each other while protecting the content they exchange. For example, the iChat server provides employees with instant messaging that's secure and encrypted.
- Software update service lets you control which updated Apple software to make available to particular employees.
- Other enterprise-level services might include DNS, Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), mail, web, and streaming.
- The popular open-source Apache HTTP web server is built into Mac OS X Server.
- Mac OS X Server integrates well with existing corporate services, from directory systems such as Active Directory to Simple Network Management Protocol (SNMP) implementations.

Workgroup servers support the unique requirements of individual departments.

- Departmental servers frequently host replicated Open Directory information, file and print services that reflect the workgroup's needs, and system imaging services. System imaging lets you automate the setup of Mac OS X computers by using installation and boot images that reside on the server.
- For departments that use Windows computers, you can provide VPN support and file and printer sharing, Active Directory authentication integration, and Open Directory support for managing computer and group preferences. You can also use a Windows NT Server and Windows NT File Server for Windows home directories.

Here's an example of a departmental server that provides some of these services for creative professionals who design and produce video and audio projects.

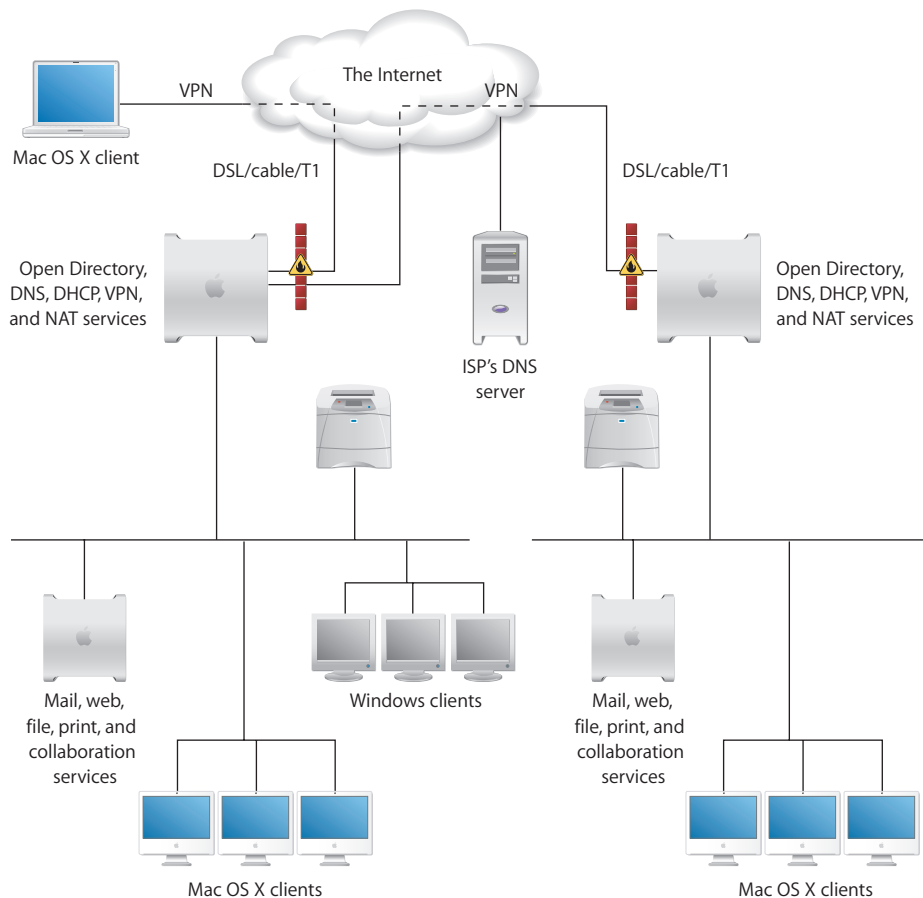


- Using Xserve as the departmental computer provides the bandwidth needed for large-file transfers. Xserve supports jumbo frame Ethernet packets and can utilize both built-in Ethernet interfaces.
- Web-based Distributed Authoring and Versioning (WebDAV) technology, integrated into Mac OS X Server's web service, lets you use a web server as an Internet file server. Users can author and access documents over the web from Mac OS X computers. You can use WebDAV for collaborative editing and file management even while a website is running.
- QuickTime streaming service lets you broadcast streaming video to client computers in real time using industry-standard streaming protocols.
- Mac OS X Server lets you set up mobile accounts for departmental employees who carry portable computers back and forth to client sites. Mobile accounts let users experience a similar work environment on and off the network.

Small and Medium Businesses

Small businesses (fewer than 100 employees) and medium businesses (about 100 to 500 employees) benefit from cross-platform file and printer sharing and numerous other services, including network, mail, web, and collaboration.

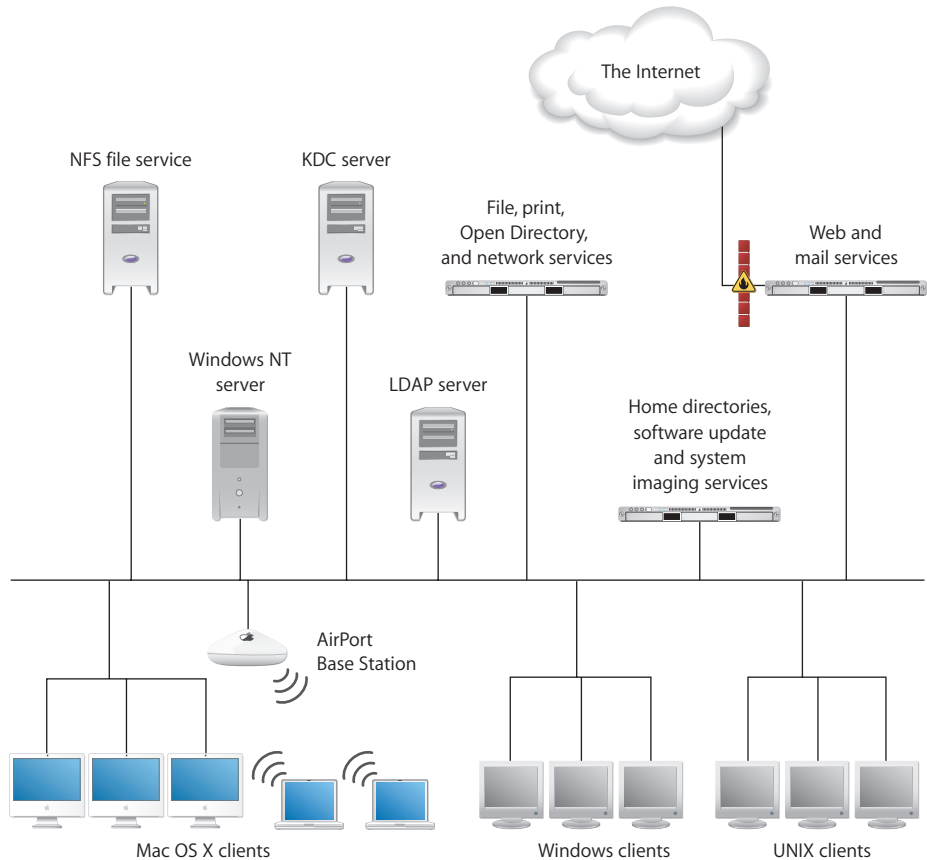
The following picture depicts a business with two small networks, joined by a VPN connection. Referred to as “site-to-site VPN,” this kind of secure connection is easy to establish when needed, as when a business needs to open another office. It offers the additional advantage of making both networks appear as one to employees working at either site. Using VPN service also lets employees access the company intranet to use mail, file and other services when away from the office.



- The directory and network services in each network reside on one Mac OS X Server, and a second server hosts mail, web, and other employee productivity services. In small businesses, all services might reside on a single server.
- Setting up basic network services, such as the Network Address translation (NAT), firewall (IP filter), DHCP, and DNS services in this scenario, are easy thanks to Gateway Setup Assistant. This tool configures a server as a gateway, linking a local area network (LAN) to the external Internet and letting you share a server's Internet connection among computers on the LAN.
- The firewall between Mac OS X Server and the Internet protects the company intranet from access by unauthorized users.
- An authoritative DNS server hosted by another company provides domain name (example.com) resolution. DNS services on Mac OS X Server provide names for the intranet devices (such as printers and client computers) that have static IP addresses and cache DNS lookups for faster name resolution.
- DHCP services provide dynamic IP addresses to some of the Macintosh and Windows clients.
- Like all the other services shown, VPN supports both Macintosh and Windows clients. If the organization uses a lot of Windows computers, you can set up Mac OS X Server as a Primary Domain Controller (PDC) so you can host Windows home directories.
- NAT service lets employees share a single Internet connection. NAT converts all client IP addresses to one IP address for Internet communications.
- Web service's proxy caching speeds up response times and reduces network traffic by storing recently accessed files in a cache on the web server so they can be retrieved quickly when requested again.
- You can customize what users see in the Finder when they select the Network icon in the sidebar of a Finder window by defining managed network views. Managed network views simplify finding files and folders that reside on network servers when they're used to list network resources in a fashion meaningful to users.

Higher-Education Facilities

Colleges and universities have heterogeneous computer environments, since the students and the computer systems they use are highly diverse. Mac OS X Server fits well into such an environment because of its capacity to integrate with a wide variety of existing services, protocols, and directory infrastructures.



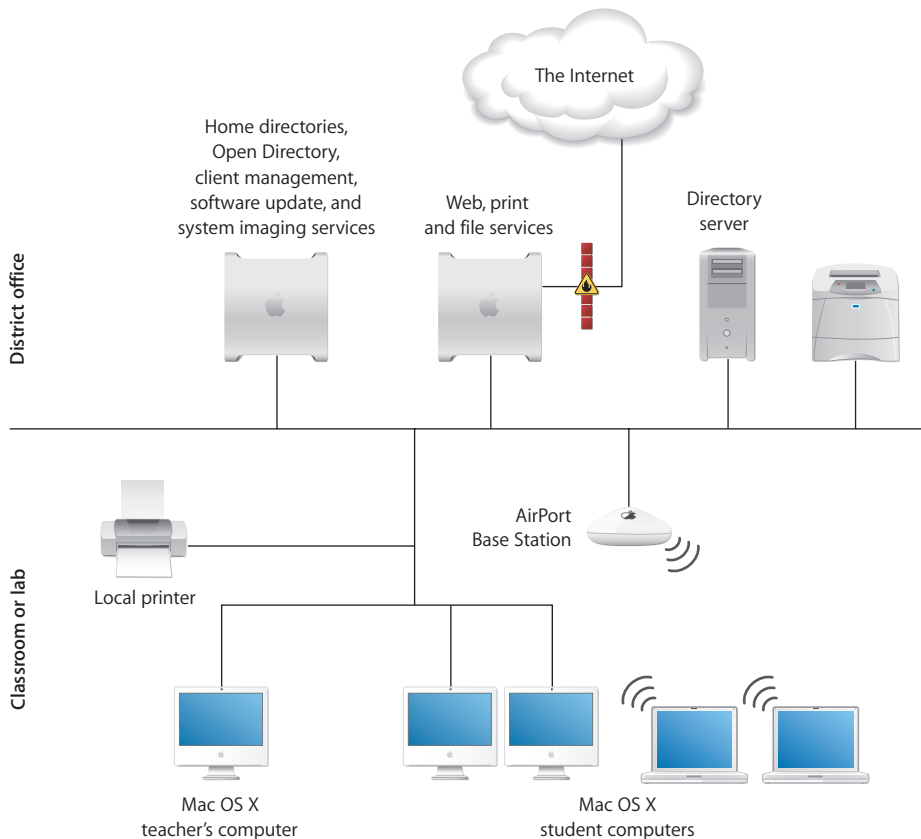
- The wide range of client computers (Macintosh, Windows, UNIX, Linux) demands flexible file access support. The highly scalable IP-based file services in Mac OS X Server support file access from anywhere on the network via AFP, NFS, FTP, and SMB/CIFS.
- Mac OS X Server can host home directories for users of all these client computers.
- User and network resource information can be retrieved by Mac OS X Server from existing directory systems, such as Lightweight Directory Access Protocol (LDAP), Active Directory, and Network Information Service (NIS) servers.
- Mac OS X Server can also use an existing directory system, such as LDAP or Kerberos Key Distribution Center (KDC), to authenticate users.

- Network Install makes it easy to change software configurations, over the network, on hundreds of Macintosh client computers, as often as necessary. It automates the setup of lab and faculty computers, facilitates software upgrades, and quickly refreshes computers to an original, preconfigured state.
- Mac OS X Server offers PostScript-compatible print spooling and job accounting for print jobs submitted using the Line Printer Remote (LPR) protocol, the industry-standard Transmission Control Protocol (TCP) protocol, the Windows SMB/CIFS protocol, and AppleTalk. The server supports both PostScript and non-PostScript print spooling using the Internet Printing Protocol (IPP).
- Because higher education networks are complex, network services are critically important. DNS and DHCP can be set up on Mac OS X Server to help client computers and services find resources on a network. IP filtering can be used to provide a security firewall around sensitive data.

K–12 Labs and Classrooms

In K–12 educational scenarios, students need access to their own files and must be able to turn in assignments electronically or in print. Students also need access to applications (such as iLife) that facilitate learning, but must also be prevented from using non-instructional applications (such as iChat).

Teachers need file services support so they can make lesson plans and teaching materials available to students online. Teachers also need a way to retrieve and update student records and other administrative information that's centralized on a remote server.



- Mac OS X Server's client management service provides a way to control student Macintosh computer work environments.

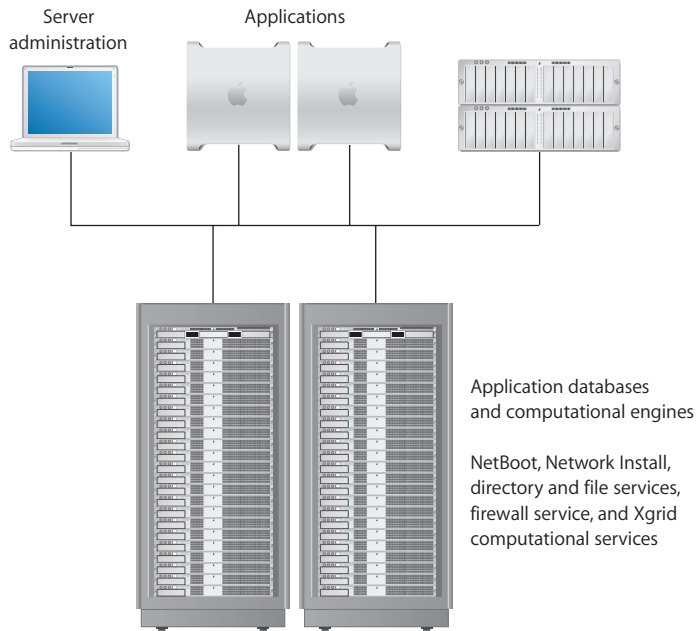
Many preferences, such as Dock and Finder preferences, are used to customize the appearance of student desktops. For example, you can set up Dock preferences and Finder preferences so that the work environment of lower-grade students is dramatically simplified.

Other preferences are used to manage what a student can access and control. For example, you can set up Media Access preferences to prevent students from burning CDs and DVDs or making changes to a computer's internal disk. Also, you can control which students can access the Internet.

- Many school districts have an LDAP or Active Directory server set up as a master directory server for all schools in the district. Mac OS X Server can use these existing centralized repositories for accessing student and teacher information, but host other services, such as file and printer sharing, on the server in a lab or classroom.
- Mobile accounts support students who use portable Macintosh computers such as the iBook. They let students work on assignments at home in an environment that mimics the classroom environment.
- Mac OS X Server's print service lets teachers manage student usage of classroom printers, including non-PostScript (inkjet) printers.
- NetBoot and Network Install images provide fast initial setup of student computers and rapid refresh of lab computers. To keep student operating systems and applications up to date you can use Network Install images or the server's software update service.
- The Gateway Setup Assistant quickly and easily configures basic network settings and lets you share a server's Internet connection among computers on a LAN.

Computational Clustering

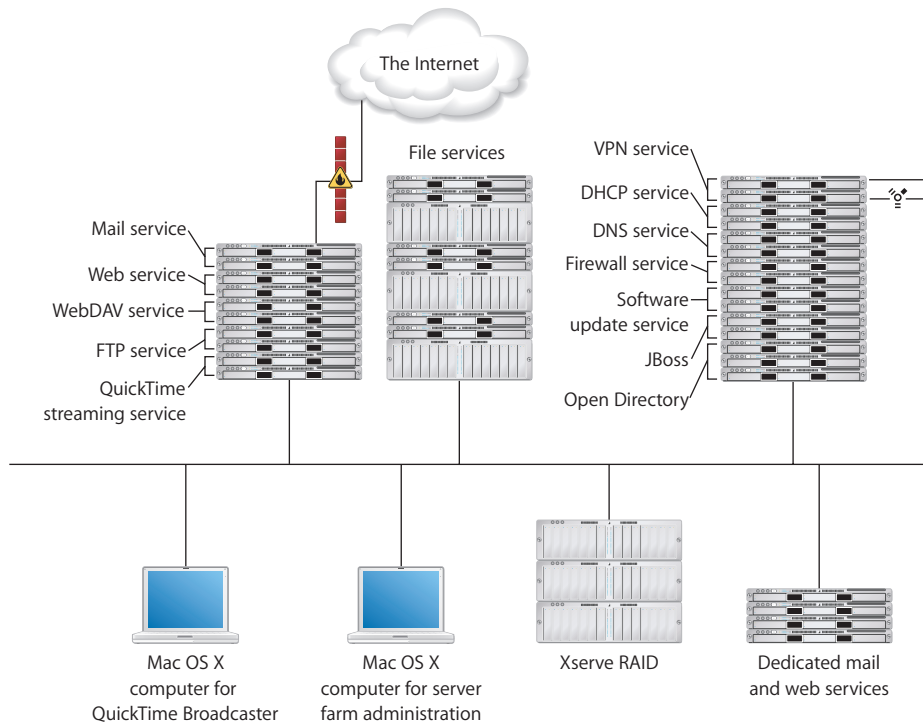
Clusters of Xserve computers offer a high-performance, cost-effective approach to the computationally intensive processing needed for genetic research, video production, or other high-bandwidth computing.



- One Xserve in a rack is usually set up as a master computer, called the *head node*. The head node runs NetBoot and Network Install and hosts directory services and other shared facilities for other computers in the rack, which are used for data processing and numerical computations.
- The head node is also likely to be set up as an AFP and NFS file server and implement an IP firewall that protects access to the cluster by unauthorized users.
- The head node can also be set up as an Xgrid cluster controller. Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster.
- Scientists, videographers, and other application users work at Mac OS X computers to remotely configure and monitor applications and databases residing on the Xserve computers.
- Mac OS X Server offers scientists and researchers familiar UNIX utilities, shells, scripting languages, and compilers for building specialized software. A full suite of developer tools comes with Mac OS X Server, including the gcc command-line compiler and a development environment called Xcode Tools.
You can write, compile, and debug using C, C++, Objective-C, or Java. Xcode Tools can be used to port command-line applications to Mac OS X and Mac OS X Server or to enhance them with a Mac OS X user interface.
- An administrator computer, such as an iBook running Mac OS X Server administrative applications, can be used to manage the entire network.

Data Centers

Mac OS X Server provides the full range of services you need if you host ecommerce websites or provide other Internet services that require high availability and scalability.



- High-availability support includes automatic restart after a service or power failure, software RAID, disk space monitoring, file system journaling, and Open Directory replication. In addition, IP failover can be configured using IP over FireWire, which lets you interconnect redundant servers without using up gigabit Ethernet ports.
- On some computers, you can improve physical connection availability by using link aggregation. Link aggregation configures several physical network links as a single logical link to improve the capacity and availability of network connections.
- You can host many websites on a single server. You can host each site with its own IP address (multihoming) or you can configure multiple sites with a single IP address (virtual hosting).
- Mac OS X Server's web service lets you set up Secure Sockets Layer (SSL) protection for secure Internet connections.
- Mac OS X Server has built-in support for Perl, Java Servlets, JavaServer Pages, and PHP Hypertext Preprocessor (PHP).

- You can deploy enterprise Java applications using the JBoss application server. JBoss, which runs on Java 1.4.2, implements the Enterprise Edition (J2EE) technologies. The Mac OS X Server implementation includes easy-to-use administration tools to help you configure and monitor the application servers. Because of its clustering capabilities, JBoss might be run on several Xserve computers.
- QuickTime Streaming Server lets you broadcast multimedia in real time, including live QuickTime Broadcaster streams.
- Xserve RAID provides extended storage.

Mac OS X Server blends a mature, stable UNIX foundation with open standards support and Macintosh ease of use.

This chapter introduces the services that Mac OS X Server offers and tells you where to find more information about them.

Core System Services

Mac OS X Server is built on top of Darwin, the core Mac OS X operating system. Darwin integrates Mach 3.0 operating-system services based on FreeBSD (Berkeley Software Distribution) 4.8 and the latest advances from FreeBSD 5.0. It includes high-performance networking facilities. It provides support for multiple integrated file systems, BSD symmetric multiprocessing with fine-grain locking, and 64-bit applications. Advanced networking capabilities include support for IPv6, IPSec, and link aggregation.

A key factor in the stability of the system is Darwin's advanced memory protection and management system. Darwin ensures reliability by providing applications and processes with their own unique address space. The Mach 3 microkernel supports multitasking and multiprocessing, memory management, real-time scheduling, unified buffer cache, hot-plug drivers, and power management.

Ease of use and simplicity are hallmarks of Mac OS X. It's visually powerful, using graphics technologies based on OpenGL, Quartz, and QuickTime. Mac OS X Server takes advantage of these capabilities by providing administrators with server management applications that are easy to use, but powerful and secure. Administrators who prefer to work in a command-line environment can do so. A complete shell environment, including popular UNIX utilities, offers a full palette of command-line administration techniques.

Read on to learn about the services that Mac OS X Server provides to extend its Mac OS X core in order to support Macintosh, Windows, UNIX, and Linux clients over a network. To learn more about server administration tools, see the getting started guide. The Preface tells you where you can find it.

Open Directory

Open Directory is the Mac OS X directory services framework. It encompasses directory services, authentication, and service discovery for Mac OS X and Mac OS X Server.

Directory services are the means by which a server and its clients (users and services) locate and retrieve information needed for authentication, network resource discovery, and other crucial system activities. User and group information is needed to authenticate users when they log in and to authorize their access to services and files. Information about network resources is used to make printers, computers, and other devices visible for browsing.

Directory services retrieve this information from directories, repositories of information about users and computing resources. Open Directory lets your server retrieve information from:

- Directories on Mac OS X Server computers
- Directories on non-Apple servers
- Configuration files on Mac OS X Server or other servers

Open Directory also supports several protocols for discovering network resources:

- Multicast DNS
- Server Message Block/Common Internet File System (SMB/CIFS)
- AppleTalk
- Service Location Protocol (SLP)

The Open Directory administration guide provides complete details about how to set up and use Open Directory. Some highlights of the many features that Open Directory offers follow.

Using Mac OS X Server Directories

Mac OS X Server can host Lightweight Directory Access Protocol (LDAP) directories. These are LDAPv3 directories that store shared directory data you want to be used by other computers.

LDAP directories are easy to manage, can be replicated for performance and backup, support a very high volume of information, and give you read-write control over directory data.

Using Non-Apple Directories

Open Directory lets you take advantage of information you've already set up in non-Apple directories and in flat files:

- On other LDAPv3 servers
- On Active Directory servers
- In BSD configuration files

- In Sun Microsystems Network Information System (NIS) files

Mac OS X Server provides full read/write and Secure Sockets Layer (SSL) communications support for LDAPv3 directories.

Directory Management

Several Open Directory features help you effectively and efficiently manage your directory data:

- **Automatic LDAP schema replication.** You can store LDAP schema in the directory, letting you add new schema without manually copying configuration files. Changes are automatically propagated from the Open Directory master to all its replicas. This feature lets you efficiently propagate administrative policy changes without manually updating servers on which directory replicas reside.
- **Directory access controls.** You can store data specifying user access to directory information in a directory.
- **Backing up directory services data.** You can back up Open Directory authentication and LDAP directory data with the click of a button in the Server Admin application.

Search Policies

Before a user can log in to or connect with a Mac OS X client or server, the user must enter a name and password associated with a user account that the computer can find. A Mac OS X computer can find user accounts that reside in a directory listed in the computer's search policy. A search policy is simply a list of directories the computer searches when it needs configuration data.

You can configure the search policy of Mac OS X computers on the computers themselves, using the Directory Access application:

- You can automate Mac OS X client directory setup by using Mac OS X Server's built-in Dynamic Host Configuration Protocol (DHCP) Option 95 support. With this approach, a DHCP server identifies the server from which a Mac OS X computer should obtain directory data at the same time the DHCP server provides an IP address to the client computer. This approach is intended for use by computers connected directly to a wired network.
- For mobile computers, frequently used in a wireless environment, trusted directory access binding is available. Trusted binding offers a way for a client computer to authenticate to an LDAP server and for the LDAP server to authenticate to the client. This mutual authentication offers the safest way to set up directory server connections in a wireless environment.

Authentication

You have several options for authenticating users:

- **Open Directory authentication.** Based on the standard Simple Authentication and Security Layer (SASL) protocol, Open Directory authentication supports many authentication methods, including CRAM-MD5, APOP, WebDAV, SHA-1, LAN Manager, NTLMv1, and NTLMv2. It's the preferred way to authenticate Windows users.

Authentication methods can be selectively disabled to make password storage on the server more secure. For example, if no clients will use Windows services, you can disable the NTLMv1 and LAN Manager authentication methods to prevent storing passwords on the server using these methods. Then someone who somehow gains access to your password database can't exploit weaknesses in these authentication methods to crack passwords.

Open Directory authentication lets you set up password policies for individual users or for all users whose records are stored in a particular directory, with exceptions if required. Open Directory authentication also lets you specify password policies for individual directory replicas.

For example, you can specify a minimum password length or require a user to change the password the next time he or she logs in. You can also disable login for inactive accounts or after a specified number of failed login attempts.

- **Kerberos v5 authentication.** Using Kerberos authentication allows integration into existing Kerberos environments. The Key Distribution Center (KDC) on Mac OS X Server offers full support for password policies you set up on the server. Using Kerberos also provides a feature known as *single sign-on*, described in the next section.

The following services on Mac OS X Server support Kerberos authentication: Apple Filing Protocol (AFP), mail, File Transfer Protocol (FTP), Secure Shell (SSH), login window, LDAPv3, Virtual Private Network (VPN), screen saver, and Apache (via the SPNEGO Simple and Protected GSS-API Negotiation Mechanism, protocol).

- **Storing passwords in user accounts.** This approach may be useful when migrating user accounts from earlier server versions. However, this approach may not support clients that require certain network-secure authentication protocols, such as APOP.
- **Non-Apple LDAPv3 authentication.** This approach is available for environments that already have an LDAPv3 server set up to authenticate users.

Single Sign-On

When a Mac OS X user is authenticated using Kerberos, the user doesn't have to enter a user name and password every time a Kerberized service is used.

The user enters the Kerberos name and password at login, but doesn't need to reenter it when using services that support Kerberos authentication.

Discovery of Network Services

Information about file servers and other services tends to change much more frequently than user information, so it isn't typically stored in directories. Instead, information about these services is discovered as the need arises.

Open Directory can discover network services that make their existence and whereabouts known. Services make themselves known by means of standard protocols. Open Directory supports the following service discovery protocols:

- Multicast DNS, for discovering file and print services on the local network
- SMB/CIFS, the protocol used by Microsoft Windows
- AppleTalk, the legacy Mac OS protocol for file services, also used for print services via Printer Access Protocol (PAP)
- SLP, an open standard for discovering file and print services

To make network browsing easy for users, you can use managed network views. See “Managed Network Views” on page 35 for more information.

User Management

Mac OS X Server helps you manage access to network resources, files, and services by Macintosh, Windows, UNIX, and Linux computer users.

The user management guide contains a full description of the server's user management capabilities. Some highlights follow.

User Accounts

User accounts contain the information needed to prove a user's identity: user name, password, and user ID. Other information in a user's account is needed by various services, to determine what the user is authorized to do and perhaps to personalize the user's environment.

Group Accounts

Group accounts offer a simple way to manage a collection of users with similar needs. A group account stores the identities of users who belong to the group as well as information that lets you customize the working environment for members of a group.

You can also use nested groups and group folders:

- A nested group is a group that's a member of another group. Nesting groups lets you set folder access privileges for groups of users at both a global level (when you want to influence all members of a group) and at a smaller, more focused level (when you want to influence only certain members of a group).

- A group folder is a place for group members to exchange ideas and receive information that's relevant to the group. By default, group folders contain three folders: Documents, Library, and Public, and there's a Drop Box folder in the Public folder. If needed, you can customize these folders and automatically mount them on the desktop of group members at login.

Computer Lists

Computer lists let you manage collections of computers.

For example, you can use a computer list to reserve high-capacity computers for film students. You'd set up a computer list consisting of the high-capacity computers, assign film students to a group, and give access to the computer list to only that group. A student who isn't a film student can't log in to one of those computers.

Home Directories

A home directory is a folder where a user's files and preferences are stored. Other users can see a user's home directory and read files in its Public folder, but they can't (by default) access anything else in that directory.

Mac OS X Server can host home directories for Macintosh, UNIX, and Windows users. With a home directory, these users can access their applications, documents, and individual settings regardless of the computer to which they log in.

You can impose disk quotas on home directories to regulate server disk usage for users with home directories.

Macintosh User Management

Mac OS X Server offers work environment personalization for Mac OS X computer users to:

- Manage preferences and set up mobile accounts and managed network views, features summarized next.
- Automate operating system images used by Macintosh client computers, as "System Imaging Services" on page 36 describes.

Preference Management

You can use Mac OS X Server to manage the work environments of Mac OS X users by defining preferences. Preferences are settings that customize and control a user's computer experience.

- Preferences can be used to change the appearance of a user's desktop. For example, you dramatically simplify the appearance of the Dock and the Finder for lower-grade students.

- Preferences can be used to manage what a user can access and control. For example, you can set up Media Access preferences to prevent students from burning CDs or DVDs or making changes to a computer's internal disk. You can also control which system preferences a user can change.
- Preferences can be used to configure a computer's network behavior. For example, you can enable or disable Internet sharing, or configure network proxy settings for a user's computer by defining a computer list and setting preferences for the list.
- Preferences can be used to automatically mount network home directories and group folders or to open applications at login. They can also be used to control the options visible in a computer's login window.

The Workgroup Manager application lets you define preferences that affect users, groups, and computers. A graphical interface offers a quick and easy way to work with preferences that are predefined.

If you want additional control of preference settings, you can work with preference manifests using Workgroup Manager's preference editor. Preference manifests are files that describe the structure and values of an application's or utility's preferences. The preference editor lets you work with preference manifests for the predefined preferences or add new preference manifests for applications and utilities of interest.

You can use DHCP Option 95 to identify a server from which a client computer retrieves directory information at login so that preference settings are automatically downloaded from the network without the need to configure the client computer directly.

Mobile Accounts

You can set up mobile accounts to support Mac OS X users who use their computers both on and off the network.

Mobile accounts let a user log in locally or use the network with the same network name and password. And they let the user experience similar work environments on and off the network.

While mobile accounts are especially useful for mobile computer users, they're advantageous for any user who needs to access network resources only occasionally. When most of the computer work can be done locally, using a mobile account reduces network traffic.

Managed Network Views

You can set up managed network views, which are custom views that users see when they select the Network icon in the sidebar of a Finder window.

A managed network view is one or more network neighborhoods, which appear in the Finder as folders. Each folder contains a list of resources an administrator has associated with the folder.

Managed network views offer a meaningful way to present network resources. You can create multiple views for different client computers. And because the views are stored using Open Directory, a computer's network neighborhood is automatically available when a user logs in.

Windows User Management

You can maximize the support you provide for Windows users by setting up a Windows primary domain controller (PDC) on Mac OS X Server and defining Windows settings for a user. When you do so, the server:

- Provides domain Open Directory authentication for Windows NT 4.x, Windows 2000, and Windows XP clients.
- Hosts home directories for Windows users in the domain.
- Supports roaming user profiles for home directories.

If you have more than one Mac OS X Server system, you can make one server a PDC and other servers BDCs (backup domain controllers). BDCs provide automatic failover and backup for the PDC. The PDC and BDCs have synchronized copies of directory and authentication data, and they share client requests for this data. If the PDC becomes unavailable, the BDCs automatically take over its load.

A user account can contain both Macintosh and Windows attributes, so users can log in from either type of computer. Windows users can use Mac OS X Server's VPN, file, and print services, as described later in this chapter.

The Windows services administration guide describes how to set up the many Windows-specific options that Mac OS X Server supports.

System Imaging Services

You can create disk images and then set up Mac OS X Server to host the images, letting Mac OS X computers start up from the images or install the images over the network. NetBoot images are used for remote startup, and Network Install images are used for remote installations.

The source of an image can be a CD, DVD, or DMG (disk image). You can also create an image that mimics an existing system already set up the way you want client computers to be set up. In this case, the source of the image is a volume or partition.

The system image administration guide provides complete information about NetBoot and Network Install.

NetBoot

NetBoot lets Macintosh clients, including Mac OS X clients without a local hard drive, start up from a system disk image located on Mac OS X Server instead of on the client computer's disk drive:

- NetBoot simplifies the administration of large-scale deployments of network-based Macintosh systems or racks of Xserve computers. It's ideal for an organization with computers that need to be identically configured; for example, NetBoot can offer a web service provider a way to configure multiple web servers.
- NetBoot also lets you set up multiple NetBoot disk images, so you can boot clients into Mac OS X or even customize the Macintosh environment for different groups of computers.
- NetBoot allows administrators to configure and update client computers instantly by updating a boot image stored on the server. Any changes made on the server are automatically reflected on the clients when they reboot. Systems that are compromised or otherwise altered can be instantly restored by rebooting.

Network Install

Network Install is a centrally managed installation service that lets administrators selectively install, restore, or upgrade Macintosh computers. You don't have to insert multiple discs to set up a system; all the installation data resides on the server.

Here are some of the advantages that Network Install offers:

- Network Install is one solution for operating system migrations and installing software updates.
- You can install site-licensed or custom applications, restore computer classrooms and labs, and reimage desktop and portable computers.
- You can define custom installation images for various departments in an organization, such as marketing, engineering, and sales.
- You can define post-installation scripts that invoke actions after the installation of a software package or system image.
- You can set up an automated install image. This type of image includes answers to all of the usual installer questions so that, when the client boots from the image, installation occurs without user intervention.

Software Update Service

You can distribute Apple software updates to users by setting up a software update server on Mac OS X Server.

Using a software update server lets you conserve your Internet bandwidth. Instead of having all your users download new software from Apple, they can download it from a server on your own network.

Users select from the updates you choose to make available. You can prevent user downloads of particular updates until you've evaluated them or until your organization is ready for them.

See the system image and software update administration guide for details about software update service.

File Services

Mac OS X Server makes it easy to share files using the native protocols of different kinds of client computers. Mac OS X Server includes these file services:

- Apple file service, which uses the Apple Filing Protocol (AFP), lets you share resources among Macintosh clients.
- Windows services use the SMB/CIFS protocol to let you share resources with clients who use Windows, and to provide name resolution service for Windows clients. These services support users of Microsoft Windows 95, 98, ME, XP, NT 4.0, and 2000.
- File Transfer Protocol (FTP) service lets you share files with anyone using FTP.
- Network File System (NFS) service lets you share files and folders with users who have NFS client software (UNIX users).
- Web-based Distributed Authoring and Versioning (WebDAV) lets you use a web server as if it were a file server.

The file services administration guide describes how to set up and manage AFP, SMB/CIFS/ FTP, and NFS file services. The Windows services administration guide provides additional information on sharing files with Windows users. The web technologies administration guide covers WebDAV.

Sharing

You share files among users by designating *share points*. A share point is a folder, hard disk (or hard disk partition), or CD that you make accessible over the network. It's the point of access at the top level of a group of shared items.

You can use a share point over multiple protocols: AFP, SMB/CIFS, NFS, and FTP.

On Mac OS X client computers, share points can be found in the /Network directory and by using the Finder's Connect To Server command. On Windows computers, users use Network Neighborhood.

Sharing offers several features that make your shared-file environment more secure and efficient:

- **Access Control Lists (ACLs).** ACLs give you a way to craft share point, folder, and file access permissions with a high degree of precision. A wide range of permissions, including the right to modify access permissions, the right to create and delete or change files, the right to read permissions, and others, can be assigned to individual users and to groups, which can be nested. In addition, you can use inheritance to propagate permissions through a file system hierarchy.
- **Unified file locking.** Mac OS X Server unifies file locking across AFP and SMB/CIFS protocols. This feature lets users working on multiple platforms simultaneously share files without worrying about file corruption.
- **Authentication options.** Mac OS X Server's Kerberos supports AFP and FTP authentication. For Windows users, the server supports Active Directory's Kerberos authentication.

Apple File Service

Apple Filing Protocol (AFP) allows Macintosh client users to connect to the server and access folders and files as if they were located on the user's own computer.

AFP offers:

- File sharing support for Macintosh clients over TCP/IP
- Autoreconnect support when a file server connection is interrupted
- Encrypted file sharing (AFP through SSH)
- Automatic creation of user home directories
- Kerberos v5 authentication for Mac OS X version 10.2 and later clients
- Fine-grain access controls for managing client connections and guest access
- Automatic disconnect of idle clients
- IPv6 support for AFP clients and server
- ACLs

AFP also lets you reshare NFS mounts using AFP. This feature provides a way for clients who aren't on the local network to access NFS volumes via a secure, authenticated AFP connection.

Windows Services

Windows file service in Mac OS X Server allows Windows clients to connect to Mac OS X Server using SMB/CIFS over TCP/IP.

When you enable Windows file service, you can also enable several additional native Windows services:

- Windows Internet Naming Service (WINS), which allows clients across multiple subnets to perform name/address resolution

- Browsing, which allows clients to browse for available servers across subnets

You can set up (and replicate) Primary Domain Controller (PDC) services, which:

- Provide Windows domain authentication from the Windows login window.
- Support Windows roaming profiles on Mac OS X Server.

Mac OS X Server provides unified file locking across AFP and SMB/CIFS protocols, letting Windows users share files with users on other computers without conflict or corruption. SMB/CIFS also supports ACLs.

Network File System (NFS) Service

NFS is the protocol used for file services on UNIX computers.

The NFS term for sharing is *export*. You can export a shared item to a set of client computers or to “World.” Exporting an NFS volume to World means that anyone who can access your server can also access that volume.

NFS doesn’t support name/password authentication. It relies on client IP addresses to authenticate users and on client enforcement of permissions, not a secure approach in most networks. Therefore, use NFS only if you’re on a local area network (LAN) with trusted client computers, or if you’re in an environment that can’t use Apple file sharing or Windows file sharing. If you have Internet access and plan to export to World, your server should be behind a firewall.

You can reshare NFS mounts using AFP, Windows, and FTP so that users can access NFS volumes in a more restricted fashion.

File Transfer Protocol (FTP)

FTP allows computers to transfer files over the Internet. Clients using any operating system that supports FTP can connect to your FTP file server and download files, depending on the permissions you set. Most Internet browsers and a number of freeware applications can be used to access your FTP server.

FTP service in Mac OS X Server supports Kerberos v5 authentication and, for most FTP clients, resumption of interrupted FTP file transfers. Mac OS X Server also supports dynamic file conversion, allowing users to request compressed or decompressed versions of information on the server.

Mac OS X Server supports anonymous FTP and by default prevents anonymous FTP users from deleting files, renaming files, overwriting files, and changing file permissions. Explicit action must be taken by an administrator to allow uploads from anonymous FTP users, and then only into a specific share point.

Web-based Distributed Authoring and Versioning (WebDAV)

Mac OS X Server supports WebDAV Internet file sharing as part of the built-in Apache web server and Mac OS X Server's web services.

Originally designed for collaborative web publishing, this enhancement to the HTTP protocol turns a website into a document database, enabling collaborative creation, editing, and searching from remote locations. With WebDAV enabled, any authorized WebDAV client, on any platform, can open files, make changes or additions, and save those revisions back to the web server. And because it uses HTTP (port 80), WebDAV can support file sharing through firewalls that don't allow FTP sharing.

Print Service

Print service in Mac OS X Server lets you share network and direct-connect printers among clients on your network. Print service also includes support for managing print queues, monitoring print jobs, extensive logging, and using print quotas.

Print service lets you:

- Share network PostScript printers with Mac OS 9 (PAP, LaserWriter 8), Mac OS X (IPP, IP/LPR), Windows (SMB/CIFS), and UNIX (IP/LPR) clients.
- Share PostScript and non-PostScript printers that are directly connected to Mac OS X Server with Mac OS X version 10.2 and later clients.
- Share directly connected non-PostScript printers as generic PostScript printers over LPR, SMB/CIFS, and AppleTalk.
- Connect to network printers using AppleTalk, LPR, and IPP, and connect to direct-connect printers using USB.
- Make printers easy for users to discover using Open Directory.
- Impose per-user print quotas to limit printer usage; in addition, you can impose a quota on individual printers.
- Set up printer pools for load balancing. A printer pool is a group of printers you designate to handle print jobs submitted to two or more print queues. A job is printed by the first available printer in the pool.
- Define cover pages for print jobs in a particular print queue.

The print service administration guide provides information about how to set up and administer print service.

Web Service

Web service in Mac OS X Server is based on Apache, an open-source HTTP web server. The server comes with both Apache 1.3 and Apache 2.0, but Apache 2.0 is included for evaluation only. Server Admin supports Apache 1.3.

Open-source software allows anyone to view and modify the source code to make changes and improvements. Those features have led to Apache's widespread use, making it the most popular web server on the Internet today.

Web service includes a high-performance, front-end cache that improves performance for websites that use static HTML pages. With this cache, data files don't need to be accessed by the server each time it's requested.

Web service also includes support for Web-based Distributed Authoring and Versioning (WebDAV). With WebDAV capability, your client users can check out web pages, make changes, then check the pages back in while the site is running. In addition, Mac OS X users can use a WebDAV-enabled web server as if it were a file server.

Web service's SSL support enables secure encryption and authentication for ecommerce websites and confidential materials. An easy-to-use digital certificate provides unforgeable proof of your website identity. Web service also supports Kerberos v5 authentication (via the SPNEGO protocol).

Mac OS X Server offers extensive support for dynamic websites:

- Web service supports Java Servlets, JavaServer Pages, MySQL, PHP, Perl, and CGI scripts or programs.
- Mac OS X Server includes a JBoss server and high-level administration tools for configuring and managing it. See "Application Server Support" on page 48 for more information about JBoss.

The web technologies administration guide provides information about configuring and managing web service.

Mail Service

Mac OS X Server provides an enterprise-capable mail server, which supports the SMTP, POP, and IMAP protocols, allowing you to select a local or server-based mail storage solution for server users.

Outgoing mail (SMTP) has these features:

- The SMTP mail transfer agent is based on Postfix. For complete information about this open-source agent, see www.postfix.org/.
- Authentication using the following methods is available: PLAIN, LOGIN, CRAM-MD5, and Kerberos v5.

Incoming mail (POP and IMAP) highlights include these:

- The mail access agent is a Cyrus POP and IMAP server. See asg.web.cmu.edu/cyrus/ for information about this agent.
- Authentication supported for IMAP is clear text, PLAIN, LOGIN, CRAM-MD5, and Kerberos v5. POP authentication options are clear text, APOP, and Kerberos v5.
- The mail database is extremely fast.
- Vacation rules and quotas for individual users are available.
- Mailman is used to create and maintain mailing lists.

Mail service protects your users from junk mail and other annoying or unauthorized messages. You can define filters that help you minimize junk mail and viruses, filter out unsolicited commercial email, and detect messages that contain particular content. Junk mail filtering, based on the powerful SpamAssassin, includes an autolearning option.

Flexible quotas let you set custom warning levels for user mail disk consumption and define customized warning messages. You can set up to three different warning levels based on percent of mail quota consumed. When a user has exceeded a certain quota level, the system sends an email warning with either a default message or a custom message. You can optionally enforce user quotas by denying new mail delivery for users who have exceeded their quota.

Virtual host support lets a single server host several different email domains. For example, your server can host email accounts for `postmaster@yourhost.com` and `postmaster@myhost.com`.

Mac OS X Server also includes SquirrelMail for web-based mail retrieval. For information about SquirrelMail, see www.squirrelmail.org.

The mail service administration guide tells you how to set up and manage mail service. The web technologies administration guide describes how to enable WebMail, the server's implementation of SquirrelMail.

Network Services

Mac OS X Server helps you manage network communications by providing:

- Dynamic Host Configuration Protocol (DHCP) service
- Domain Name System (DNS) service
- Firewall service
- Network Address Translation (NAT) service
- Virtual Private Network (VPN) service
- Network time service
- Gateway Setup Assistant
- IP failover

The network services administration guide provides information about network services.

DHCP

DHCP is especially useful when an organization has more clients than IP addresses. IP addresses are assigned on an as-needed basis, and when they're not needed they're available for use by other clients.

DHCP helps you administer and distribute IP addresses dynamically to client computers from your server. From a block of IP addresses that you define, your server locates an unused address and “leases” it to client computers as needed. The server's DHCP service also supports static IP address assignment to computers with a specific Ethernet (MAC) address.

As you learned in “Search Policies” on page 31, you can automate the directory services setup of Mac OS X clients using your DHCP server's Option 95 support. This option lets client computers learn about their directory settings from a DHCP server.

DNS

DNS service lets users connect to a network resource, such as a web or file server, by specifying a name (such as `server.example.com`) rather than an IP address (such as `192.168.11.12`). DNS is a distributed database that maps IP addresses to domain names.

A server that provides DNS service keeps a list of names and the IP addresses associated with the names. When a computer needs to find the IP address for a name, it sends a message to the DNS server (also known as a *name server*). The name server looks up the IP address and sends it back to the computer. If the name server doesn't have the IP address locally, it sends messages to other name servers on the Internet until the IP address is found.

If you don't have an Internet service provider (ISP) who handles DNS for your network, you can set up a DNS server on your Mac OS X Server. See individual service administration guides for information about DNS dependencies for each service.

Mac OS X Server provides administration tools for service configuration management, zone control, and monitoring, providing a graphical way to:

- Enable zone transfers and recursion
- Work with log files
- Manage zones and records for the machines in those zones

Firewall

Firewall service protects your server and its contents from intruders. It provides a software firewall, scanning incoming IP packets and accepting or rejecting them based on filters you define.

You can set up server-wide restrictions for packets from specific IP addresses. You can also restrict access to individual services, such as web, mail, and FTP, by defining filters for the ports used by the services. IP firewall can be used to block access to specific service ports or to allow access only to certain ports.

IP firewall also provides a sophisticated mechanism, stateful packet inspection, for determining whether an incoming packet is a legitimate response to an outgoing request or part of an ongoing session, allowing packets that would otherwise be denied.

NAT

NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications. For example, the AirPort Base Station uses NAT. By default, a base station assigns IP addresses using DHCP to computers on an Ethernet network, then uses NAT to convert those addresses when any of the computers needs to access the Internet.

NAT is becoming increasingly popular because it preserves IP addresses. It also increases the security of Internet access, because it supports only connections that originate on an internal network.

NAT is closely related to IP firewall. The firewall diverts network packets to the NAT process so they can be translated.

VPN

You can set up a VPN using Mac OS X Server.

VPN is a network transmission protocol that uses encryption and other technologies to provide secure communications over a public network. Typically the public network is the Internet, but VPNs are also used to support connections between multiple intranets within the same organization and to join networks between two organizations to form an extranet.

Site-to-site VPN connects two networks. It offers a secure connection that's easy to establish when the need arises to set up a network at another site, as when a business expands. Site-to-site VPN makes both networks appear as one to users working at either site.

VPNs transmit encrypted IP packets so that only legitimate targets can interpret them, protecting the contents of messages from network sniffing. Mac OS X Server lets you set up and manage VPN policies that support different authentication and authorization options and network connection attributes.

Mac OS X Server's VPN service serves Mac OS X, Windows, and UNIX clients, and supports strong authentication using MS-CHAP, IPSec, and Kerberos v5.

Gateway Setup Assistant

Gateway Setup Assistant automates the configuration of a simple gateway between the local network and the Internet. A gateway lets you share your server's Internet connection among computers on your local area network (LAN).

Gateway Setup Assistant automatically configures DHCP, NAT, firewall, DNS, and VPN as well as the server's network configuration. For example:

- Certain 192.168.x.x addresses are set aside for DHCP and VPN.
- A DHCP server is enabled and configured to provide addresses to computers on the LAN.
- NAT and firewall services are enabled so that all packets from the Internet except those required for connections with the server are blocked.
- A DNS server is configured as a caching server.
- A VPN server is optionally enabled for L2TP.

If you want to adjust the automatic settings after running Gateway Setup Assistant, you can do so using the Server Admin application.

"Setup Example" on page 65 describes how to use Gateway Setup Assistant in a small business.

IP Failover

You can configure IP failover to help maximize server availability.

IP failover is a way to set up a standby server that will take over if the primary server fails. The standby server takes over the IP address of the failed server, which takes the IP address back when it is online again. IP failover is useful for DNS servers, web servers hosting websites, media broadcast servers, and other servers that require minimal data replication.

Media Streaming and Broadcasting

QuickTime Streaming Server (QTSS) lets you stream multimedia in real time using the industry-standard RTSP/RTP protocols. QTSS supports MPEG-4, MP3, and QuickTime file formats.

You can deliver live and prerecorded media over the Internet to both Macintosh and Windows users, or relay streamed media to other streaming servers. You can provide unicast streaming, which sends one stream to each individual client, or multicast streaming, which sends the stream to a group of clients.

- For more information about QTSS, refer to the QuickTime website (www.apple.com/quicktime/products/qtss/).
- For information about managing streaming services on Mac OS X Server, see the QuickTime Streaming Server administration guide.

Two QuickTime applications that come with Mac OS X Server help you prepare content for streaming:

- QTSS Publisher lets you upload content to the streaming server and prepare it for delivery. It provides these key features: creation and management of playlists, generation of content directory websites, and editing of content annotations. The QuickTime Streaming Server administration guide describes how to use QTSS Publisher.
- QuickTime Broadcaster lets you produce a live event. QuickTime Broadcaster allows you to stream live audio and video over the Internet. QuickTime Broadcaster provides preset broadcast settings and the ability to create custom settings. Built on top of the QuickTime architecture, QuickTime Broadcaster enables you to produce a live event using most codecs that QuickTime supports.

For information about QuickTime Broadcaster, go to www.apple.com/quicktime/ and navigate to the QuickTime Broadcaster page.

Application Server Support

An application server is software that runs and manages other applications, usually web applications, which are accessed using a web browser. The managed applications reside on the same computer where the application server runs.

One of the duties of the application server is to make sure the applications it manages are always available. For example, if an application fails or becomes unresponsive, the application server restarts it. Some application servers provide load balancing, which spreads application load among two or more computers.

This section highlights three integrated application server technologies that Mac OS X Server offers: Apache Tomcat, JBoss, and WebObjects. All of them are preinstalled with the server and can be used in conjunction with Apache Axis, which is also preinstalled. Axis is an open source Java framework for implementing web services over XML-based SOAP (Simple Object Access Protocol). For more information about SOAP, go to:

www.w3.org/TR/SOAP/

The web technologies administration guide provides more information about open-source applications and modules included with Mac OS X Server.

Apache Tomcat

Tomcat is an open-source JavaServer Pages (JSP)/servlet container used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies.

- The specification for Java Servlet is at java.sun.com/products/servlets/.
- The specification for JavaServer Pages is at java.sun.com/products/jsp/.

JBoss

JBoss is a widely used full-featured Java application server. It provides a full Java 2 Platform, Enterprise Edition (J2EE) technology stack with features such as:

- An Enterprise Java Bean (EJB) container
- Java Management Extensions (JMX)
- Java Connector Architecture (JCA)

Mac OS X Server provides easy-to-use graphical tools for configuring and monitoring JBoss and simplifying the deployment of JBoss applications. The Java application server guide describes how to manage Mac OS X Server's JBoss server, and is available from www.apple.com/server/documentation/.

- For more information about J2EE, see java.sun.com/j2ee/.
- For more information about JBoss, see www.jboss.org/.

By default, JBoss uses Tomcat as its web application container, but you can use other web application containers, such as Jetty.

WebObjects

WebObjects is the Apple solution for rapid development and deployment of ecommerce and other Internet applications. WebObjects applications can connect to multiple databases and dynamically generate HTML content. WebObjects offers a comprehensive suite of tools and run-time libraries that facilitate developing standards-based web services and Java server applications.

Mac OS X Server includes the WebObjects run-time libraries and an unlimited deployment license, making it the ideal platform for your J2EE-compatible WebObjects applications. Also provided are easy-to-use graphical tools for configuring and monitoring WebObjects from within the Server Admin application. You can optionally purchase the WebObjects development tools from the Apple Store (store.apple.com), Apple's retail stores, and authorized Apple resellers.

For more information and documentation on WebObjects, go to:

www.apple.com/webobjects/ or developer.apple.com/referencelibrary/WebObjects/

Collaboration Services

Collaboration services promote interactions among users, facilitating teamwork and productivity.

These are the collaboration services on Mac OS X Server:

- **Weblog service.** Mac OS X Server provides a multiuser Weblog server (based on Blojsom) that complies with the RSS and Atom XML standards. Weblog service supports Open Directory authentication. For additional safety, users can access Weblog service using a website that's SSL enabled.
- **iChat service.** Instant messaging for Macintosh, Linux, and Windows users is provided by a Jabber/XMPP (Extensible Messaging and Presence Protocol) server. User authentication is integrated into Open Directory. Setup and administration of iChat service is done using the graphical Server Admin application.
- **Mail service.** In addition to the features summarized in "Mail Service" on page 43, Mac OS X Server provides a graphical interface for Mailman, one of the most widely deployed mailing list managers. You can easily create and manage lists and take advantage of content filtering, digest delivery, and other options. See www.list.org for information about Mailman.
- **Group accounts, preferences, and folders.** See "Group Accounts" on page 33 for highlights.
- **File sharing.** See "File Services" on page 38 for a summary of file sharing options.

Integrating Into Existing Environments

Mac OS X Server offers many ways to interoperate with existing environments.

Open Directory offers several options for using existing directory information:

- You can use an existing Kerberos KDC or Active Directory (including Active Directory's Kerberos) to authenticate users.
- You can integrate AFP and SMB/CIFS file services with an Active Directory Kerberos environment.
- You can share information stored in an LDAPv3 directory system that's accessible from your server.
- You can retrieve configuration information from Berkeley Software Distribution (BSD) configuration files or Sun Microsystems Network Information System (NIS) files.

For Windows users, your server can:

- Provide VPN service
- Provide printer sharing
- Provide Open Directory authentication
- Act as a domain controller to provide Windows domain login and single sign-on
- Host home directories (if the home directory server is a PDC, a member of another Mac OS X Server's Windows domain, or a member of an Active Directory domain)
- Provide WINS naming service

You'll find instructions for setting up a server to work with other vendors' products in several guides:

- The Open Directory administration guide provides guidelines and instructions for integrating into existing directory systems.
- The Windows services administration guide describes how to set up print service and file services for Windows computer users, how to configure Windows options for individual users, and how to set up PDC support for Windows users.
- The Windows NT migration guide describes how to move accounts, user data, and service settings from Windows NT servers to Mac OS X Server.

High Availability

Mac OS X Server features that promote high availability include:

- Open Directory LDAP replication, including the authentication services of Open Directory Password Server and Kerberos KDC (see the Open Directory administration guide)
- Automatic restart after application, system, or power failures
- Disk space monitoring (see the command-line administration guide for information about log-rolling scripts and the `diskspacemonitor` tool)
- Software RAID, or mirroring (see Disk Utility online help)
- Journaled HFS disks (see the command-line administration guide for how to use disk journaling)
- Remote server monitoring (see the getting started guide for information about server administration tools)
- Link aggregation (see the high availability administration guide). On some computers you can improve physical connection availability by using link aggregation. Link aggregation configures several physical network links as a single logical link to improve the capacity and availability of network connections.

High-Performance Computing

Mac OS X Server offers a high-performance, cost-effective approach to the computationally intensive processing needed for genetic research, video production, or other high-bandwidth computing.

For example, Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared Mac OS X computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster. The Xgrid administration guide describes how to set up and manage computational clustering.

“Computational Clustering” on page 24 provides other examples of Mac OS X Server’s support for high-performance computing.

Server Administration

Mac OS X Server provides an extensive range of tools and applications for managing your servers.

Administrators can use graphical applications or command-line tools for initial server setup, service configuration, day-to-day server management. Server administration can be conducted from a server or from a Mac OS X computer that has administration applications installed.

The getting started guide has more information about the Mac OS X Server tools and applications. The Preface tells you where you can find it.

Migrating and Upgrading

You can reuse data and settings you've been using on Macintosh servers earlier than version 10.4 or on Windows NT servers:

- If you're using Mac OS X Server version 10.3.9 or 10.2.8 and you don't need to move to different computer hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data.
- If you can't perform an upgrade installation, such as when you need to reformat the system disk or upgrade your server hardware, you can migrate data and settings to a computer onto which you've installed Mac OS X Server version 10.4. Migration from Mac OS X Server versions 10.3.9, 10.2.8, 10.1.4, 10.1.5, and 1.2; and from AppleShare IP version 6.3.3 are supported.
- If you want to replace a Windows NT computer with Mac OS X Server, you can migrate users, groups, files, and more.

The upgrading and migrating guide provides instructions for reusing Macintosh data and settings. The Windows NT migration guide provides instructions for migrating from a Windows NT server.

You can't update to a later 10.4 version by using a Mac OS X Server installation disc. The getting started guide explains how to keep current with the latest Mac OS X Server release. The Preface tells you where you can find the getting started guide.

Settings for the following server appear in the tables below:

Server:

Item	Description	Your information
Identity of remote server for installation and setup	For interactive installation and setup of a remote server on the local subnet, one of these values for the server: - IP address in IPv4 format (000.000.000.000) - host name (someserver.example.com) - MAC address (00:03:93:71:26:52). For command-line or remote-subnet installations and setups, the target server's IP address, in IPv4 format.	
Preset password (for remote installation and setup)	The first 8 digits of the target server's built-in hardware serial number, printed on a label on the computer. For older computers with no such number, use 12345678 for the password.	
Type of installation	Upgrade from version 10.3.9 or 10.2.8, complete installation without disk formatting, or clean installation. The target volume (partition) is erased when you do a clean installation.	
Target disk or partition	Name of the target disk or partition (volume).	
Disk format (when erasing the disk is OK)	A format for the target disk. In most cases, use Mac OS Extended (Journaled). You can also use Mac OS Extended. Don't use UNIX File System or any case-sensitive format.	
Disk partitioning (when erasing the disk is OK)	Indicate whether you want to partition the target disk. The minimum recommended size of a target disk partition is 10 GB.	

Item	Description	Your information
RAID mirroring (when erasing the disk is OK and you have a second physical drive on the target server)	Indicate whether you want to set up RAID mirroring. The second disk is used automatically if the primary disk isn't available. If the target disk has a single partition and the second physical drive has a single partition and no data, you can set up RAID mirroring after installation. However, to prevent data loss, set up RAID mirroring as soon as possible.	
Using saved setup data	If you want to use saved setup data to set up this server, identify the file or directory storing the data you want to use. If the data is encrypted, also identify the passphrase. If you want to save settings in a file or directory, use one of the next two rows.	
Saving setup data in a file	Name the file using one of these options: - <MAC-address-of-server>.plist (include any leading zeros but omit colons). For example, 0030654dbcef.plist. - <IP-address-of-server>.plist. For example, 10.0.0.4.plist. - <partial-DNS-name-of-server>.plist. For example, myserver.plist. - <built-in-hardware-serial-number-of-server>.plist (first 8 characters only). For example, ABCD1234.plist. - <fully-qualified-DNS-name-of-server>.plist. For example, myserver.example.com.plist. - <partial-IP-address-of-server>.plist. For example, 10.0.plist (matches 10.0.0.4 and 10.0.1.2). - generic.plist (a file that any server will recognize, used to set up servers that need the same setup values). If you choose to encrypt the file, you can save the passphrase in a file named using the above conventions, except use the extension .pass, not .plist. Place the file(s) in a location where the target server or servers can detect it. A server can detect files that reside on a volume mounted locally in /Volumes/*/Auto Server Setup/, where * is any device mounted under /Volumes.	

Item	Description	Your information
Saving setup data in a directory	Navigate to the directory where you want to save the setup, and name the setup record using one of these options: - <MAC-address-of-server> (include any leading zeros but omit colons). For example, 0030654dbcef. - <IP-address-of-server>. For example, 10.0.0.4. - <partial-DNS-name-of-server>. For example, myserver. - <built-in-hardware-serial-number-of-server> (first 8 characters only). For example, ABCD1234. - <fully-qualified-DNS-name-of-server>. For example, myserver.example.com. - <partial-IP-address-of-server>. For example, 10.0 (matches 10.0.0.4 and 10.0.1.2). - generic (a file that any server will recognize, used to set up servers that need the same setup values). If you choose to encrypt the file, you can save the passphrase in a file named using the above conventions, except add the extension .pass. Place the passphrase file in a location where the target server or servers can detect it. A server can detect the file if it resides on a volume mounted locally in /Volumes/*/Auto Server Setup/, where * is any device mounted under /Volumes.	
Language	The language to use for server administration (English, Japanese, French, or German). The language affects the server's time and date formats, displayed text, and the default encoding used by the AFP server.	
Keyboard layout	The keyboard for server administration.	

Item	Description	Your information
Serial number	The serial number for your copy of Mac OS X Server. The format of the server serial number is xsvr-104-999-x-zzz-zzz-zzz-zzz-zzz-zzz-z, where x is a letter, 9 is a digit, and z is a letter or digit. The first element (xsvr) and the fourth one (x) must be lowercase. Unless you have a site license, you need a unique serial number for each server. You'll find the server software serial number printed on the materials provided with the server software package. If you have a site license, a registered owner name and organization must be entered exactly as specified by your Apple representative. If you set up a server using a generic setup file or directory record and the serial number isn't site licensed, you must enter the server's serial number using Server Admin.	
Administrator's long name (sometimes called full name or real name)	A long name can contain no more than 255 bytes. The number of characters ranges from 255 Roman characters to as few as 85 3-byte characters. It can include spaces. It can't be the same as any predefined user name, such as System Administrator. This name is case sensitive in the login window, but not when accessing file servers.	
Administrator's short name	A short name can contain as many as 255 Roman characters, typically eight or fewer. Use only a through z, A through Z, 0 through 9, _ (underscore), or - (hyphen). Avoid short names that Apple assigns to predefined users, such as "root."	
Administrator's password	This value is case sensitive and must contain at least 4 characters. It is also the password for the root user. If you record this value, be sure to keep this worksheet in a safe place. After setup, use Workgroup Manager to change the password for this account.	

Item	Description	Your information
Host name	You can't specify this name during server setup. Server Assistant sets the host name to AUTOMATIC in /etc/hostconfig. This setting causes the server's host name to be the first name that's true in this list: - The name provided by the DHCP or BootP server for the primary IP address - The first name returned by a reverse DNS (address-to-name) query for the primary IP address - The local hostname - The name "localhost"	
Computer name	The AppleTalk name and the default name used for SLP/DA. Specify a name 63 characters or fewer but avoid using =, :, or @. The Network browser in the Finder uses SMB/CIFS to find computers that provide Windows file sharing. Spaces are removed from a computer name for use with SMB/CIFS, and the name can contain no more than 15 characters, no special characters, and no punctuation.	
Local hostname	The name that designates a computer on a local subnet. It can contain lower-case letters, numbers, and/or hyphens (but not at the ends). The name ends with ".local" and must be unique on a local subnet.	
Network interface data	Your server has a built-in Ethernet port and may have an additional Ethernet port built in or added on. Record information for each port you want to activate.	Use the table provided later in this worksheet to record data for each port.
Directory usage	Select one: - Standalone Server (use only the local directory). - Connected to a Directory System (get information from another server's shared directory). If you choose this option, use one of the next four rows in this table to indicate how the server will connect with the directory. - Open Directory Master (provide directory information to other computers). If you choose this option, use the row for "Using Open Directory Master." - No change (for upgrades only).	
Using "As Specified by DHCP Server"	The directory to use will be identified by a DHCP server set up to provide the address and search base of an LDAP server (DHCP option 95) or the address and tag of a legacy NetInfo server.	

Item	Description	Your information
Using “Open Directory Server”	The directory to use will be an LDAP directory identified by a DHCP server or identified by specifying an IP address or domain name for the LDAP server.	
Using “NetInfo Server”	The directory to use will be a NetInfo parent directory on an existing Apple server. Choose one or more ways to locate that directory: - Broadcast - DHCP - Static IP Address (specify IP address and NetInfo tag)	
Using “Other Directory Server”	The directory or directories to use will be configured using the Directory Access application after you’re finished setting up the server.	
Using “Open Directory Master”	Optionally indicate you want to enable a Windows Primary Domain Controller on the server. Provide a Windows computer name and domain for the server. The computer name and domain can contain a-z, A-Z, 0-9, -, but no . or space and can’t contain only numbers. Finish setting up the directory you want to host by using Server Admin after completing server setup.	
Automating service startup	Indicate whether you want any of the following to start automatically every time the server starts; these items need no additional configuration to be useful: - Apple file service - Apple Remote Desktop - FTP service - iChat service - Mail service - NetBoot service - Network time service - QuickTime Streaming service - Software update service - Web service - WebDAV service - Weblog service - Windows file service - Xgrid Agent service - Xgrid Controller service	
Time zone	Choose the time zone you want the server to use.	
Network time	Optionally indicate a Network Time Server for the server. Apple recommends that you keep your server’s clock accurate by synchronizing it with a network time server.	

Configuration settings for the following port appear in the table below:

Port Name: Built-in Ethernet

Item	Description	Your information
Device name	A UNIX name for the port in the format enx, where x starts with 0. See your hardware manual for the value of x for the port you're describing. The value en0 always designates a built-in Ethernet port.	en0
Ethernet address	The Media Access Control (MAC) address of the port (00:00:00:00:00:00). This value is usually on a sticker on the server hardware, but you can run Apple System Profiler or a command-line tool such as networksetup to discover the value.	
TCP/IP and AppleTalk	Indicate whether you want to enable the port for TCP/IP and/or AppleTalk. You can connect a port to the Internet by enabling TCP/IP and use the same or a different port for AppleTalk. Enable no more than one port for AppleTalk.	
Order of ports	If you enable more than one port, indicate the order in which the ports should be accessed when trying to connect to a network. All non-local network traffic uses the first active port.	
TCP/IP settings	Use one of the next four rows in this table.	
"Manually"	Specify these settings if you want to manually specify TCP/IP settings: - IP address (000.000.000.000). A unique static address. - Subnet mask (000.000.000.000). Used to locate the subnet on the local area network where the server resides. This mask is used to derive the network part of the server's address; what remains identifies the server computer on that network. - Router (000.000.000.000) that supports the subnet the server's on. The router is the machine on the local subnet to which messages are sent if the target IP address isn't on the local subnet. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	

Item	Description	Your information
"Using DHCP with Manual IP address"	Specify these settings if you want to use a DHCP server to assign a static IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup: - IP address (000.000.000.000). A unique static address. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	
"Using DHCP"	Specify these settings if you want to use a DHCP server to assign a dynamic IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup: - DHCP client ID (optional). A string that's useful for recognizing a port when its IP address changes. Don't specify a DHCP client ID when using Server Assistant to set up the server remotely. Instead, after setup, use the server's Network preferences to define a DHCP client ID. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	
"Using BootP"	Specify these settings if you want to use a Bootstrap Protocol server to assign an IP address for the identified port. With BootP, the same IP address is always assigned to a particular network interface. It's used primarily for computers that start up from a NetBoot image: - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified domain names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	

Item	Description	Your information
IPv6	To configure IPv6 addressing for the port, select Automatically or Manually. Choose Automatically if you want the server to automatically generate an IPv6 address for the port. Choose Manually to specify IPv6 settings: - IPv6 address. Generally written in the form 0000:0000:0000:0000:0000:0000:0000:0000. - Router. The IPv6 address of the router on the local subnet. - Prefix length. The number of significant bits in the subnet mask that are used to identify the network.	
Ethernet settings	To automatically configure Ethernet settings for the port, choose Automatically. You may want to choose Manually (Advanced) to specify settings if you have specific requirements for the network the server's connected to. Note that incorrect Ethernet settings can affect network performance or render a port unusable: - Speed. The maximum Ethernet speed, in number of bits per second, that can be transmitted using the port. Select one of these options: autoselect, 10baseT/UTP, 100baseTX, and 1000baseTX. - Duplex. Determine whether input and output packets are transmitted at the same time (full-duplex) or alternately (half-duplex). - Maximum Packet Size (MTU). The largest packet the port will send or receive. MTU stands for maximum transfer unit, expressed in bytes. Increasing the packet size improves throughput, but the devices that receive the packet (switches, routers, and so forth) must support the packet size. Select one of these options: Standard (1500), Jumbo (9000), or Custom (enter a value from 72 to 1500).	

Configuration settings for the following port appear in the table below:

Port Name:

Item	Description	Your information
Device name	A UNIX name for the port in the format enx, where x starts with 0. See your hardware manual for the value of x for the port you're describing. The value en0 always designates a built-in Ethernet port.	
Ethernet address	The Media Access Control (MAC) address of the port (00:00:00:00:00:00). This value is usually on a sticker on the server hardware, but you can run Apple System Profiler or a command-line tool such as networksetup to discover the value.	
TCP/IP and AppleTalk	Indicate whether you want to enable the port for TCP/IP and/or AppleTalk. You can connect a port to the Internet by enabling TCP/IP and use the same or a different port for AppleTalk. Enable no more than one port for AppleTalk.	
Order of ports	If you enable more than one port, indicate the order in which the ports should be accessed when trying to connect to a network. All non-local network traffic uses the first active port.	
TCP/IP settings	Use one of the next four rows in this table.	
"Manually"	Specify these settings if you want to manually specify TCP/IP settings: - IP address (000.000.000.000). A unique static address. - Subnet mask (000.000.000.000). Used to locate the subnet on the local area network where the server resides. This mask is used to derive the network part of the server's address; what remains identifies the server computer on that network. - Router (000.000.000.000) that supports the subnet the server's on. The router is the machine on the local subnet to which messages are sent if the target IP address isn't on the local subnet. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	

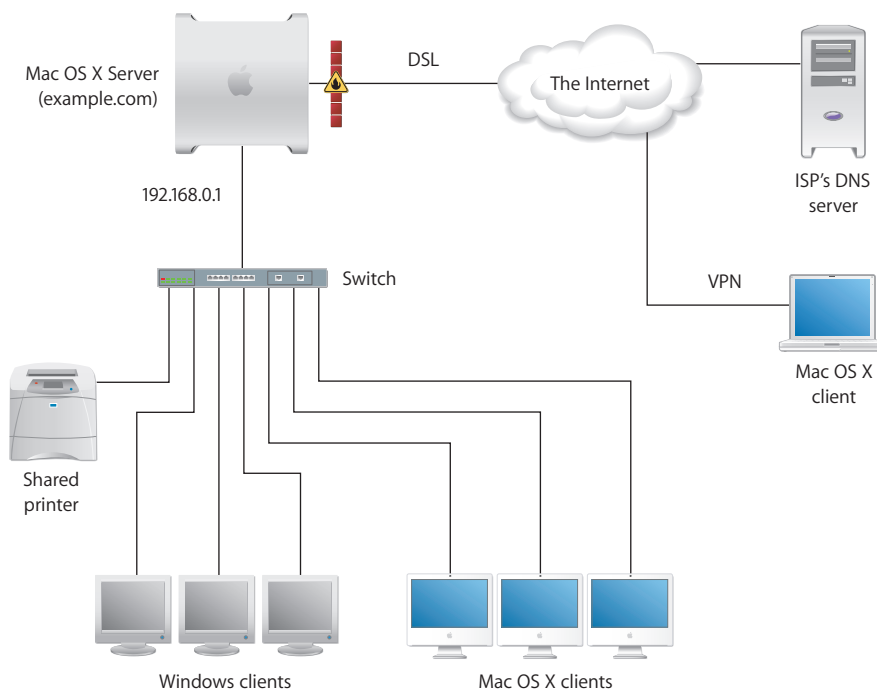
Item	Description	Your information
"Using DHCP with Manual IP address"	Specify these settings if you want to use a DHCP server to assign a static IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup: - IP address (000.000.000.000). A unique static address. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	
"Using DHCP"	Specify these settings if you want to use a DHCP server to assign a dynamic IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup: - DHCP client ID (optional). A string that's useful for recognizing a port when its IP address changes. Don't specify a DHCP client ID when using Server Assistant to set up the server remotely. Instead, after setup, use the server's Network preferences to define a DHCP client ID. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	
"Using BootP"	Specify these settings if you want to use a Bootstrap Protocol server to assign an IP address for the identified port. With BootP, the same IP address is always assigned to a particular network interface. It's used primarily for computers that start up from a NetBoot image: - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu.	

Item	Description	Your information
IPv6	To configure IPv6 addressing for the port, select Automatically or Manually. Choose Automatically if you want the server to automatically generate an IPv6 address for the port. Choose Manually to specify IPv6 settings: - IPv6 address. Generally written in the form 0000:0000:0000:0000:0000:0000:0000:0000. - Router. The IPv6 address of the router on the local subnet. - Prefix length. The number of significant bits in the subnet mask that are used to identify the network.	
Ethernet settings	To automatically configure Ethernet settings for the port, choose Automatically. You may want to choose Manually (Advanced) to specify settings if you have specific requirements for the network the server's connected to. Note that incorrect Ethernet settings can affect network performance or render a port unusable: - Speed. The maximum Ethernet speed, in number of bits per second, that can be transmitted using the port. Select one of these options: autoselect, 10baseT/UTP, 100baseTX, and 1000baseTX. - Duplex. Determine whether input and output packets are transmitted at the same time (full-duplex) or alternately (half-duplex). - Maximum Packet Size (MTU). The largest packet the port will send or receive. MTU stands for maximum transfer unit, expressed in bytes. Increasing the packet size improves throughput, but the devices that receive the packet (switches, routers, and so forth) must support the packet size. Select one of these options: Standard (1500), Jumbo (9000), or Custom (enter a value from 72 to 1500).	

The setup example in this appendix illustrates one way to set up the directory and network infrastructure of Mac OS X Server in a small business scenario.

Mac OS X Server in a Small Business

In this example, Mac OS X Server provides directory, network, and productivity services to employees in a small business.



The small business in this example had been using an office LAN to share files and a printer. Acquiring Mac OS X Server made it possible to implement an intranet that uses an ISP's DNS and digital subscriber line (DSL) services.

Here's a summary of the scenario's characteristics:

- An Open Directory master LDAP directory on the server centralizes user management, including authentication of Mac OS X and Windows users.
- The ISP's DNS service provides a DNS domain name for the company (example.com).
- A DNS server running on Mac OS X Server provides name services for the server, the printer, and any other intranet device that has a static IP address.
- A firewall between the server and the Internet protects the intranet from unauthorized access.
- NAT service lets intranet users share the ISP's IP address for Internet access, while VPN lets employees access the intranet securely over the Internet when they're working away from the office.
- DHCP service on Mac OS X Server provides dynamic IP addresses to intranet client computers. The server and printer have static addresses, but client computers have dynamic addresses.

How to Set Up the Server

The following steps summarize how to set up Mac OS X Server in this hypothetical small business. For complete information about setting up directory services, see the Open Directory administration guide. For details about network service setup (IP firewall, DHCP, and so forth), see the network services administration guide.

Step 1: Set up the network

- 1 Make sure the server has two Ethernet interfaces (ports), one for the intranet (LAN) connection and one for the DSL modem connection. Use the faster interface for the server connection. A 10-Mbit connection is more than sufficient for the DSL connection.
- 2 Connect the server to the LAN using the faster interface. In this example, the server is plugged in to a switch used to connect the existing client computers and shared printer. We'll refer to this interface as the "internal" interface.

Intranet devices should be connected to a hub or switch using good-quality CAT-5 Ethernet cables. A high-speed 10/100/1000 megabit switch would be able to support advanced server features such as NetBoot that work best over a fast connection.

- 3 Connect the server to the DSL modem using the other Ethernet interface. We'll refer to this interface as the "external" interface.

Step 2: Set up the server and the master directory

- 1 Start the server from the installation DVD. The procedure you use depends on the server hardware.

In this example, assume the computer has a display, keyboard, and DVD-ROM drive. Turn on the computer, insert the installation DVD into the optical drive, and restart the computer while holding down the C key on the keyboard.

The getting started guide has instructions for other installation methods, such as installing on a server without an optical drive and installing from a remote computer. The Preface tells you where to find the getting started guide.

- 2 When the Installer opens, proceed through its panes by following the onscreen instructions. If you need to format the target disk, see the getting started guide for instructions on preparing disks for installing Mac OS X Server.

When installation is complete, the server restarts and Server Assistant opens.

- 3 Fill out the worksheet on page 53. You'll need the information as you move through the Assistant's panes.
- 4 Use the Language and Keyboard panes to reflect the server's administration language.
- 5 In the Administrator Account pane, enter the server administrator's names and password. Click Continue.
- 6 In the Network Names pane, enter the computer name and local hostname for your server. Click Continue.
- 7 Make sure the Network Interfaces pane lists your external and internal Ethernet interfaces.

Also make sure that the external interface is the first one listed in the Network Interfaces pane. The first interface listed is the primary, or default, interface. Network traffic initiated by the server is routed through the primary interface. VPN uses it as the Public network, treating all others listed as Private.

Click Continue.

- 8 The TCP/IP Connection pane appears for each Ethernet interface.

For the external interface, choose Manually from the Configure IPv4 pop-up list, then enter the IP address, subnet mask, and DNS server IP address, or addresses, provided to you by the ISP. In addition, make sure you add the local DNS server IP address (192.168.0.1) to those supplied by the ISP. For best performance, make the local DNS server IP address appear first in the list. Click Continue.

If you'll be using Gateway Setup Assistant to configure network settings, you don't need to set up an internal interface. Otherwise, enter these values for the internal interface then click Continue:

Configure IPv4: Manually

IP Address: 192.168.0.1 (192.168 values are reserved for internal LANs)

Subnet Mask: 255.255.0.0

Router: 192.168.0.1

DNS Servers: 192.168.0.1

- 9 In the Directory Usage Pane, choose Open Directory Master to set up a shared LDAP directory on the server.

Select Enable Windows Primary Domain Controller and enter a Domain/Workgroup name. These settings will set up a Windows PDC so that employees who use Windows NT, Windows 2000, and Windows XP workstations can log in to the PDC, change passwords during login, and have roaming user profiles and network home directories on the server. With one user account, a user can log in from a Windows workstation or a Mac OS X computer and access the same network home directory.

Click Continue.

- 10 Proceed through the remaining Assistant panes, then click Apply to initiate server setup.

When setup is complete, the server restarts automatically.

- 11 Log in to the server as the administrator you defined when using Server Assistant.
- 12 Configure the server's network settings.

The simplest way to do this is to use the Gateway Setup Assistant, as Step 3 describes. Alternatively, you can individually configure each network service using Server Admin, as Steps 4 through 8 describe.

Step 3: Use Gateway Setup Assistant to automate the server's network configuration

- 1 Open Server Admin by clicking its icon in the Dock.
- 2 Open Gateway Setup Assistant by choosing View > Gateway Setup Assistant.
- 3 Proceed through the panes, specifying information when prompted.

On the WAN Port pane, select the port you configured during initial setup as the external interface.

On the VPN settings pane, enable VPN and specify a shared secret for client connections to use.

On the LAN Ports pane, select the port you want to use as the internal interface.

- 4 When Gateway Setup Assistant has completed network setup and you've quit the application, go to Step 9.

Step 4: Set up the firewall

- 1 Open Server Admin by clicking its icon in the Dock.
- 2 Authenticate as the server administrator.
- 3 In the Computers & Services list, click Firewall.
- 4 Click Start Service in the toolbar.
- 5 Click Settings, and in the Address Groups pane select the IP address group named 192.168-net. The group includes 65,535 IP addresses.

- 6 Click Services and select “Allow” for services you want employees working at the office to be able to access. At a minimum select Domain Name Service, DHCP, and NetBoot.
- 7 Click Address Groups, then select the IP address group named “any.”
- 8 Click Services and select “Allow” for services you want external clients to be able to access behind the firewall.
- 9 Click Save.

Step 5: Set up DNS service

- 1 In Server Admin, select DNS in the Computers & Services list.
- 2 Click Settings.
- 3 Make sure that “Zone transfers” isn’t enabled and that “Recursion” is enabled.
- 4 Click Zones, then click the Add button (+) under the Zones list to set up a zone for the intranet.

Enter the following values using the General pane, then click OK:

Zone Name: example.com

Server Name: myserver

Server IP Address: 192.168.0.1

Administrator email: admin@example.com

Using the Machines pane, add machines to the zone. For example, to add a printer, click the Add button and specify values for the printer, then click OK:

IP address: 192.168.100.2

Name: hp_laserjet_2000

- 5 Click Save, then click Start Service.

Step 6: Set up DHCP service

This step sets up a DHCP server that provides employee computers dynamic IP addresses as well as the identity of the DNS, LDAP, and WINS servers they should use. When a client computer’s search policy is set to Automatic (using the Directory Access application on the client computer), the identity of the DNS, LDAP, and WINS servers is supplied automatically at the same time an IP address is supplied.

- 1 In Server Admin, make sure that DNS is running.
- 2 Select DHCP in the Computers & Services list.
- 3 Click Settings.

- 4 Click the Add button to define the range of addresses to dynamically assign. The range should be large enough to accommodate current and future client computers. But make sure you exclude some addresses (at the start or end of the range) so they're reserved for devices that need static IP addresses or for VPN users.

Here are some sample values:

Starting IP Address: 192.168.0.2

Ending IP Address: 192.168.0.102

Subnet Mask: 255.255.0.0

Network Interface: En1

Router: 192.168.0.1

- 5 Make sure the DNS pane contains the following values:

Default Domain: example.com

Name Servers: 192.168.0.1

- 6 Click LDAP to configure DHCP to identify the server you're configuring as the source of directory information for clients who are served dynamic IP addresses.

The server you're setting up should be identified in the Server Name field, because you set up the server as an Open Directory master when you used Server Assistant. Other settings are optional for this example.

- 7 Click WINS to configure DHCP to serve Windows-specific settings to clients who are served dynamic IP addresses.

Supply these values:

WINS/NBNS Primary Server: 192.168.0.1

NBT Node Type: Broadcast (b-node)

- 8 Click Save, click the back arrow, enable the internal Ethernet interface, then click Start Service.

Step 7: Set up NAT service

- 1 In Server Admin, select NAT in the Computers & Services list.
- 2 Click Settings.
- 3 Select the external interface from the "External network interface" pop-up menu.
- 4 Click Save, then click Start Service.

Step 8: Set up VPN service

- 1 In Server Admin, select VPN in the Computers & Services list.
- 2 Click Settings.
- 3 Enable L2TP over IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) for Mac OS X version 10.4 computer users, Linux or UNIX workstation users, and Windows XP users. While PPTP, described in the next step, can also be used, L2TP provides the greatest security because it runs over IPSec.

Enter a starting and ending IP address to indicate which addresses the VPN server can assign to clients. Avoid addresses the DHCP server is set up to serve. Also avoid addresses you specify if you enable PPTP.

Specify the shared secret by typing a string in “Shared secret”. Enter a string that isn’t intuitive. For example, specify digits, symbols, and uppercase and lowercase characters in unusual combinations. The recommended string length is 8 to 12 characters.
- 4 Enable PPTP (Point to Point Tunneling Protocol) if employees will need to access the intranet from Windows workstations other than Windows XP computers or from Mac OS X version 10.2 computers when they’re away from the office. If you need to support older Windows clients that don’t have 128-bit PPTP support, select “Allow 40-bit encryption keys in addition to 128-bit”.

Enter a starting and ending IP address to indicate which addresses the VPN server can assign to clients. Avoid addresses the DHCP server is set up to serve. Also avoid addresses you specified when you enabled L2TP over IPSec.
- 5 Click Save, then click Start Service.

Step 9: Set up productivity services

The infrastructure you need to set up file, print, and other productivity services is now available. Follow the instructions in the relevant administration guides, listed on page 11, to configure the services of interest. Many services, such as Apple file service, require minimal setup. Simply start them using Server Admin.

Step 10: Create user accounts and home directories

- 1 Open Workgroup Manager. The Open Directory master LDAP directory is automatically available for editing. You’ll add an account for each employee to this master directory.
- 2 Click the New User button.
- 3 Specify user settings in the panes that appear.

The user management guide tells you how to set up all the user account attributes, including home directories. It also describes how to manage users by setting up group accounts and computer lists and how to set up preference settings that customize the work environments of Macintosh clients.

The Windows administration guide focuses on how to implement support specifically for Windows workstation users. Use this document to supplement the user management guide and the Open Directory administration guide if your server will support Windows users.

Step 11: Configure client computers

The information that follows applies to Mac OS X version 10.4 computers.

For information about how to support Windows client computers, see the Windows administration guide.

- 1 If necessary, configure Mac OS X clients to retrieve information from the DHCP server.

Mac OS X version 10.4 computers are preconfigured to use DHCP to obtain IP addresses and retrieve information about an LDAP directory from the DHCP server. After you configure DHCP service with information about an LDAP directory, that information is delivered automatically to Mac OS X clients when they receive IP addresses from the DHCP server.

These are the settings that are preconfigured:

Network preferences are set to use DHCP. To access the setting, select System Preferences, open Network preferences, select the internal Ethernet interface, and select "Using DHCP with manual address" or "Using DHCP" from the Configure IPv4 pop-up menu.

The computer's search policy is set to be defined automatically. To access this setting, open Directory Access (in /Applications/Utilities/) and click Authentication. If the lock icon is locked, click it and authenticate as an administrator. Choose Automatic from the Search pop-up menu, then click Apply.

The use of DHCP-supplied LDAP information is enabled. To access this setting, open Directory Access and click Services. If the lock icon is locked, click it and authenticate as an administrator. Select LDAPv3 in the list of services, then click Configure. Click "Use DHCP-supplied LDAP Server," then click OK.

- 2 Configure Mac OS X clients so they can use the VPN server.

Open the Internet Connect application (in /Applications/) and click VPN in the toolbar.

Select L2TP over IPSec or PPP and click Continue. Choose Edit Configurations from the Configurations pop-up menu. Enter the external IP address from the ISP, the user name and password for the computer user, and, for L2TP over IPSec, the shared secret. Click OK.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined “admin” group.

administrator computer A Mac OS X computer onto which you’ve installed the server administration applications from the Mac OS X Server Admin CD.

AFP Apple Filing Protocol. A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

Apache An open-source HTTP server integrated into Mac OS X Server. You can find detailed information about Apache at www.apache.org.

application server Software that runs and manages other applications, usually web applications, that are accessed using a web browser. The managed applications reside on the same computer where the application server runs.

authentication The process of proving a user’s identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user’s level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

authorization The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an authentication process proves the user’s identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

BIND Berkeley Internet Name Domain. The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

BootP An older method of allocating IP addresses to clients on a network. See also DHCP.

boot ROM Low-level instructions used by a computer in the first stages of starting up.

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

CGI Common Gateway Interface. A script or program that adds dynamic functions to a website. A CGI sends information back and forth between a website and an application that provides a service for the site.

computer list A list of computers that have the same preference settings and are available to the same users and groups.

computer name The default name used for SLP and SMB/CIFS service registrations. The Network Browser in the Finder uses SLP to find computers advertising Personal File Sharing and Windows File Sharing. It can be set to bridge subnets depending on the network router settings. When you turn on Personal File Sharing, users see the computer name in the Connect To Server dialog in the Finder. Initially it is “<first created user>’s Computer” (for example, “John’s Computer”) but can be changed to anything. The computer name is used for browsing for network file servers, print queues, Bluetooth discovery, Apple Remote Desktop clients, and any other network resource that identifies computers by computer name rather than network address. The computer name is also the basis for the default local host name.

CUPS Common UNIX Printing System. A cross-platform printing facility based on the Internet Printing Protocol (IPP). The Mac OS X Print Center, its underlying print system, and the Mac OS X Server print service are all based on CUPS. For more information, visit www.cups.org.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a lease period—the length of time the client computer may use the address.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a directory node or simply a directory.

directory node See **directory domain**.

directory services Services that provide system software and applications with uniform access to directory domains and other sources of information about users and resources.

disk image A file that, when opened, creates an icon on a Mac OS desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

DNS domain A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

DNS name A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

DSL Digital subscriber line. A broadband data transmission technology that operates over telephone lines.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a website visitor.

export In the Network File System (NFS), a way of sharing a directory with clients on a network. TBD for RAID context.

filter A "screening" method used to control access to a server. A filter is made up of an IP address and a subnet mask, and sometimes a port number and access type. The IP address and the subnet mask together determine the range of IP addresses to which the filter applies.

firewall Software that protects the network applications running on your server. IP firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

FireWire A hardware technology for exchanging data with peripheral devices, defined by IEEE Standard 1394.

FTP File Transfer Protocol. A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

gateway A network node that interfaces one network to another. Often, it refers to a computer that links a private LAN to a public WAN, with or without Network Address Translation. A router is a special kind of gateway that links related network segments.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group folder A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among themselves.

guest computer An unknown computer that isn't included in a computer list on your server.

guest user A user who can log in to your server without a user name or password.

home directory A folder for a user's personal use. Mac OS X also uses the home directory, for example, to store system preferences and managed user settings for Mac OS X users.

host Another name for a server.

HTML Hypertext Markup Language. The set of symbols or codes inserted in a file to be displayed on a World Wide Web browser page. The markup tells the web browser how to display a webpage's words and images for the user.

HTTP Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. The HTTP protocol provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

IANA Internet Assigned Numbers Authority. An organization responsible for allocating IP addresses, assigning protocol parameters, and managing domain names.

ICMP Internet Control Message Protocol. A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

IGMP Internet Group Management Protocol. An Internet protocol used by hosts and routers to send packets to lists of hosts that want to participate in a process known as multicasting. QuickTime Streaming Server (QTSS) uses multicast addressing, as does Service Location Protocol (SLP).

IMAP Internet Message Access Protocol. A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local computer. Mail remains on the server until the user deletes it.

Internet Generally speaking, a set of interconnected computer networks communicating through a common protocol (TCP/IP). The Internet (note the capitalization) is the most extensive publicly accessible system of interconnected computer networks in the world.

intranet A network of computers operated by and for the benefit of an organization's internal users. Access is commonly restricted to members of the organization. Many times, it refers to a web site for the organization which is accessible only from within the organization. Intranets use the same networking technologies as the Internet (TCP/IP), and sometimes bridge legacy information systems with modern networking technologies.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP address A unique numeric address that identifies a computer on the Internet.

IPP Internet Printing Protocol. A client-server protocol for printing over the Internet. The Mac OS X printing infrastructure and the Mac OS X Server print service that's built on it support IPP.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

ISP Internet service provider. A business that sells Internet access and often provides web hosting for ecommerce applications as well as mail services.

JBoss A full-featured Java application server that provides support for Java 2 Platform, Enterprise Edition (J2EE) applications.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

Kerberos realm The authentication domain comprising the users and services that are registered with the same Kerberos server. The registered services and users trust the Kerberos server to verify each other's identities.

LAN Local area network. A network maintained within a facility, as opposed to a WAN (wide area network) that links geographically separated facilities.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

lease period A limited period of time during which IP addresses are assigned. By using short leases, DHCP can reassign IP addresses on networks that have more computers than available IP addresses.

load balancing The process of distributing client computers' requests for network services across multiple servers to optimize performance.

local domain A directory domain that can be accessed only by the computer on which it resides.

local home directory A home directory that resides on disk on the computer a user is logged in to. It's accessible only by logging directly in to the computer where it resides unless you log in to the computer using SSH.

long name The long form of a user or group name. See also **user name**.

LPR Line Printer Remote. A standard protocol for printing over TCP/IP.

mail host The computer that provides your mail service.

managed client A user, group, or computer whose access privileges and/or preferences are under administrative control.

managed network The items managed clients are allowed to "see" when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a "network view."

managed preferences System or application preferences that are under administrative control. Workgroup Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients.

MTA Mail Transfer Agent. A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

multihoming The ability to support multiple network connections. When more than one connection is available, Mac OS X selects the best connection according to the order specified in Network preferences.

MySQL An open-source relational database management tool frequently used by web servers.

name server A server on a network that keeps a list of names and the IP addresses associated with each name. See also **DNS**, **WINS**.

NAT Network Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications.

nested group A group that is a member of another group. Nested groups enable administrators to manage groups of users at a global level (to influence all members of a group) and at a smaller level (to influence only certain members of a group).

NetBoot server A Mac OS X server on which you've installed NetBoot software and have configured to allow clients to start up from disk images on the server.

NetInfo One of the Apple protocols for accessing a directory domain.

network installation The process of installing systems and software on Mac OS X client computers over the network. Software installation can occur with an administrator attending the installations or completely unattended.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, NetInfo, or Active Directory protocols; BSD configuration files; and network services.

Option 95 A new option in the Bootstrap Protocol (BootP) and the Dynamic Host Configuration Protocol (DHCP) that lets clients find LDAP servers, their ports, base distinguished names (DNs), and other attributes. The configuration is returned to the DHCP client as a list of LDAP URLs according to a predefined syntax.

owner The owner of an item can change access permissions to the item. The owner may also change the group entry to any group in which the owner is a member. By default the owner has Read & Write permissions.

PAP Printer Access Protocol. The standard protocol based on AppleTalk that is used on Mac OS X, Mac OS X Server, and other platforms for transmitting print job data to a printer or print server.

PHP PHP Hypertext Preprocessor (originally Personal Home Page). A scripting language embedded in HTML that's used to create dynamic webpages.

POP Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

predefined accounts User accounts that are created automatically when you install Mac OS X. Some group accounts are also predefined.

preference manifest A file that describes the structure of and default values for an application's preferences (for example, what the various preference keys do). Workgroup Manager's preferences editor uses these files to make it easier for an administrator to edit an application's managed preferences.

preferences cache A storage place for computer preferences and preferences for groups associated with that computer. Cached preferences help you manage local user accounts on portable computers.

presets Initial default attributes you specify for new accounts you create using Workgroup Manager. You can use presets only during account creation.

primary group A user's default group. The file system uses the ID of the primary group when a user accesses a file he or she doesn't own.

primary group ID A unique number that identifies a primary group.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

QTSS QuickTime Streaming Server. A technology that lets you deliver media over the Internet in real time.

RAID array A group of physical disks organized and protected by a RAID scheme and presented by RAID hardware or software as a single logical disk. In Xsan, RAID arrays appear as LUNs, which are combined to form storage pools.

RAID level A storage allocation scheme used for storing data on a RAID array. Specified by a number, as in RAID 3 or RAID 0+1.

realm General term with multiple applications. See **WebDAV realm**, **Kerberos realm**.

search path See **search policy**.

search policy A list of directory domains searched by a Mac OS X computer when it needs configuration information; also the order in which domains are searched. Sometimes called a search path.

shadow image A file created by the NetBoot daemon process for each NetBooted client where applications running on the client can write temporary data.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

short name An abbreviated name for a user. The short name is used by Mac OS X for home directories, authentication, and email addresses.

Simplified Finder A user environment featuring panels and large icons that provide novice users with an easy-to-navigate interface. Mounted volumes or media to which users are allowed access appear on panels instead of on the standard desktop.

SMB/CIFS Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB/CIFS to provide access to servers, printers, and other network resources.

SMTP Simple Mail Transfer Protocol. A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SNMP Simple Network Management Protocol. A set of standard protocols used to manage and monitor multiplatform computer network devices.

spam Unsolicited email; junk mail.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

static IP address An IP address that's assigned to a computer or device once and is never changed.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration. See also **IP subnet**.

system-less client A computer that doesn't have an operating system installed on its local hard disk. System-less computers can start up from a disk image on a NetBoot server.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

Tomcat The official reference implementation for Java Servlet 2.2 and JavaServer Pages 1.1, two complementary technologies developed under the Java Community Process.

UID User ID. A number that uniquely identifies a user within a file system. Mac OS X computers use the UID to keep track of a user's directory and file ownership.

URL Uniform Resource Locator. The address of a computer, file, or resource that can be accessed on a local network or the Internet. The URL is made up of the name of the protocol needed to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

USB Universal Serial Bus. A standard for communicating between a computer and external peripherals using an inexpensive direct-connect cable.

user name The long name for a user, sometimes referred to as the user's "real" name. See also **short name**.

virtual user An alternate email address (short name) for a user. Similar to an alias, but it involves creating another user account.

VPN Virtual Private Network. A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

WAN Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

WebDAV realm A region of a website, usually a folder or directory, that's defined to provide access for WebDAV users and groups.

Windows domain The Windows computers on a network that share a common directory of user, group, and computer accounts for authentication and authorization. An Open Directory master can provide the directory services for a Windows domain.

WINS Windows Internet Naming Service. A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

Index

A

- access control lists (ACLs) 39
- Active Directory 30
- AirPort 45
- Apache 42
- Apple File Service (AFP) 39
- AppleTalk 33
- application servers 48
 - AXIS 48
 - JBoss 48
 - SOAP 48
 - Tomcat 48
 - WebObjects 49
- automatic restart 51

B

- basic password validation 32
- Berkeley Software Distribution (BSD) 29, 30

C

- CGI scripts 42
- collaboration services 49
- core system services 29

D

- Darwin 29
- directory services 30
- disk space monitoring 51
- diskspacemonitor tool 51
- Disk Utility 51
- documentation 11
- Domain Name System (DNS) 44
- Dynamic Host Configuration Protocol (DHCP) 44
- dynamic websites 42

E

- example setup 65
- exporting NFS volumes 40

F

- file services 38
 - Apple File Service (AFP) 39

- File Transfer Protocol (FTP) 40
- Network File System (NFS) 40
- sharing 38
 - Windows 39
- file sharing 38
- File Transfer Protocol (FTP) 40

G

- group accounts 33

H

- high availability 51
- home directories 34

I

- iChat service 49
- installation and setup worksheet 53
- integrating into existing networks 50
- IP failover 47

J

- J2EE 48
- Java 42
- JBoss 48
- journaled HFS disks 51

K

- Kerberos 32

L

- LDAP 30
- link aggregation 51
- log rolling 51

M

- Macintosh user management
 - mobile accounts 35
 - preference management 34
- mail service
 - authentication 43
 - Cyrus 43
 - filtering junk mail and viruses 43

- Mailman 43
- Postfix 43
- SpamAssassin 43
- SquirrelMail 43
- managed network views 35
- mobile accounts 35
- multicast DNS 33
- MySQL 42

N

- nested groups 33
- NetBoot 37
- NetInfo 30
- Network Address Translation (NAT) 45
- network browsing using managed Network views 35
- Network File System (NFS) 40
- Network Information System (NIS) 30
- Network Install 37
- network services 44
 - DHCP 44
 - DNS 44
 - Gateway Setup Assistant 46
 - IP failover 47
 - IP firewall 45
 - managed network views 35
 - NAT 45
 - VPN 46

O

- Open Directory
 - automatic LDAP schema replication 31
 - definition 30
 - directory access controls 31
 - discovery of network services 33
 - Kerberos authentication 32
 - LDAP replication 51
 - password validation 32
 - search policies 31
 - trusted binding 31
 - using Apple directories 30
 - using non-Apple directories 30
- OpenLDAP 30
- operating system image services 36
- opportunistic locking 39

P

- password validation 32
- Perl 42
- PHP 42
- preference editor 35
- preference manifests 35
- print service 41

Q

- QTSS Publisher 47
- QuickTime Broadcaster 47
- QuickTime Streaming Server (QTSS) 47

R

- resharing NFS mounts 40

S

- scenarios
 - computational clustering 24
 - data centers 26
 - departments and workgroups 16
 - higher-education facilities 21
 - K-12 labs and classrooms 22
 - small and medium businesses 19
- search policies 31
- server administration guides 11
- Server Message Block /Common Internet File System (SMB/CIFS) 33
- server setup
 - example 65
- service discovery 30
- Service Location Protocol (SLP) 33
- share points 38
- sharing files 38
- Simple Authentication and Security Layer (SASL)
 - password validation 32
- single sign-on 32
- software RAID 51
- software update service 37
- SquirrelMail 43
- strict locking 39

T

- Tomcat 48

U

- unified file locking 39
- user management
 - group accounts 33
 - home directories 34
 - Macintosh user management 34
 - user accounts 33
 - Windows user management 36

V

- Virtual Private Network (VPN) 46

W

- Web-Based Distributed Authoring and Versioning (WebDAV) 42
- web cache 42
- Weblog service 49
- web service 42

Windows
 browsing 39
 file service 39
 integration 50
 user management 36

Windows Internet Naming Service (WINS) 39
worksheet 53

X

Xgrid computational service 51