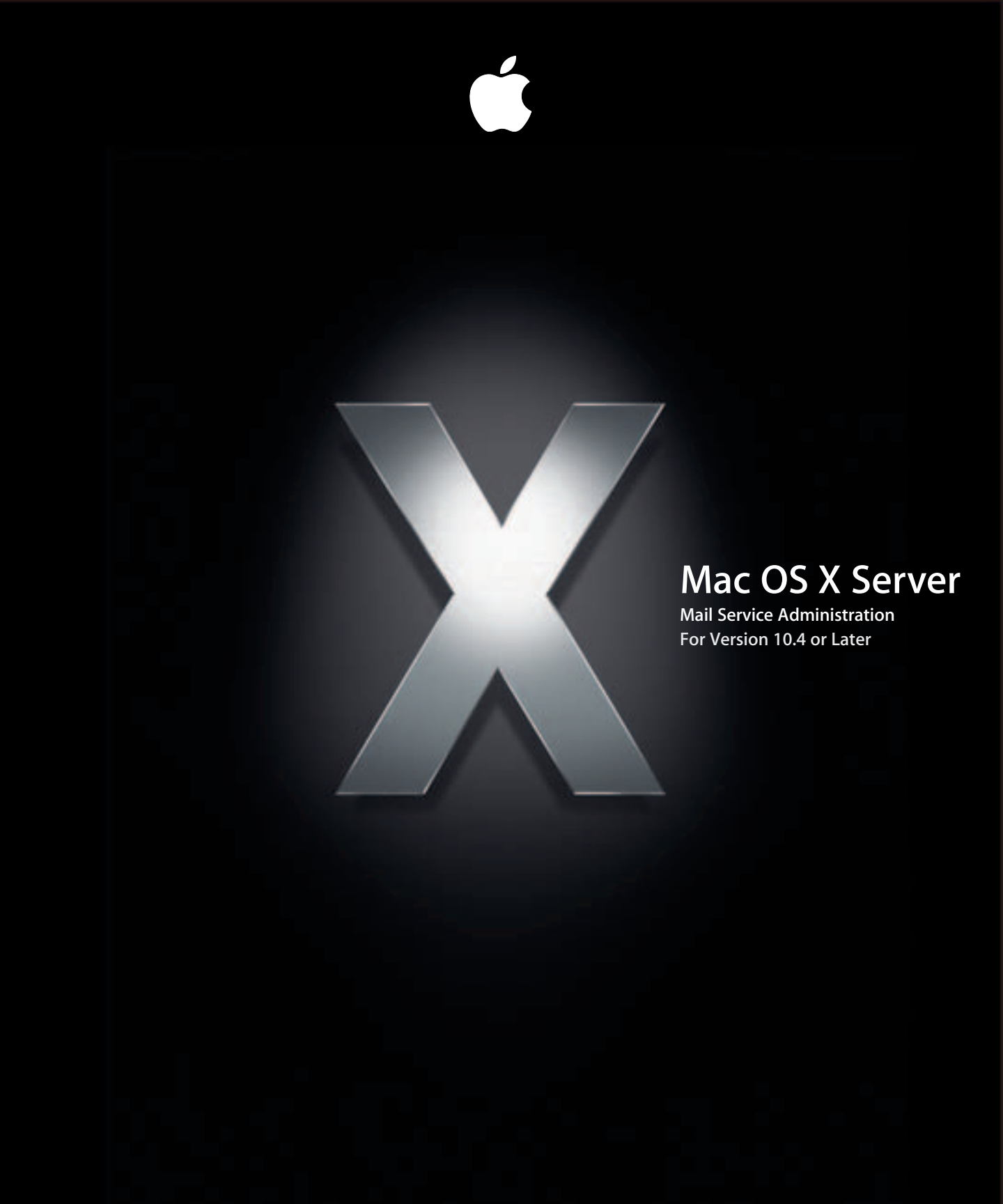


Mac OS X Server

Mail Service Administration

For Version 10.4 or Later

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

019-0163/03-24-05

Contents

About This Guide

This guide explains how to configure and administer Mac OS X Server Mail Services.

What's New in Version 10.4

Mac OS X Server's Mail Service includes many new valuable features. These include:

- New junk mail prevention rules
- Junk mail screening (based on SpamAssassin)
- Virtual Hosting
- Improved mail quota handling
- Integrated migration and maintenance tools

What's in This Guide

This guide is organized into three chapters and an appendix:

- Chapter 1, "Mail Service Setup," on page 15, includes everything you need to set up and configure mail service, as well as to support and configure mail users.
- Chapter 2, "Mail Service Maintenance," on page 57, includes information for ongoing mail server maintenance and administration.
- Chapter 3, "Mailing Lists," on page 73, explains the mailing list service in Mac OS X Server. Mailing lists are a powerful collaboration tool for disseminating and archiving email discussions.
- Appendix, "Certificates and Security" on page 93, describesServer Admin's Certificate Manager, an easy way to create, organize, and use security certificates for SSL-enabled services.

Using This Guide

The first chapter provides an overview of how the mail service works, what it can do for you, strategies for using it, how to set it up for the first time, and how to administer it over time.

Also take a look at any chapter that describes a service with which you're unfamiliar. You may find that some of the services you haven't used before can help you run your network more efficiently and improve performance for your users.

Most chapters end with a section called "Where to Find More Information." This section points you to websites and other reference material containing more information about the service.

Setting Up Mac OS X Server for the First Time

If you haven't installed and set up Mac OS X Server, do so now.

- Refer to *Mac OS X Server Getting Started for Version 10.4 or Later,* the document that came with your software, for instructions on server installation and setup. For many environments, this document provides all the information you will need to get your server up and running, and available for initial use.
- Read specific sections to learn how to continue setting up individual features of mail service. Pay particular attention to the information in these sections: "Setup Overview," and "Before You Begin."

Getting Help for Everyday Management Tasks

If you want to change settings, monitor services, view service logs, or do any other day-to-day administration task, you can find step-by-step procedures by using the onscreen help available within Mac OS X Server. All of the administration tasks are documented in the second chapter of this guide, but it may be more convenient to retrieve information from onscreen help while using your server.

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 by opening Workgroup Manager or Server Admin. From the Help menu, choose an option:

- *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, 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:
Mac OS X Server Getting Started for Version 10.4 or Later	Install Mac OS X Server and set it up for the first time.
Mac OS X Server Upgrading and Migrating to Version 10.4 or Later	Use data and service settings that are currently being used on earlier versions of the server.
Mac OS X Server User Management for Version 10.4 or Later	Create and manage users, groups, and computer lists. Set up managed preferences for Mac OS X clients.
Mac OS X Server File Services Administration for Version 10.4 or Later	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB.
Mac OS X Server Print Service Administration for Version 10.4 or Later	Host shared printers and manage their associated queues and print jobs.
Mac OS X Server System Image and Software Update Administration for Version 10.4 or Later	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.
Mac OS X Server Mail Service Administration for Version 10.4 or Later	Set up, configure, and administer mail services on the server.
Mac OS X Server Web Technologies Administration for Version 10.4 or Later	Set up and manage a web server, including WebDAV, WebMail, and web modules.
Mac OS X Server Network Services Administration for Version 10.4 or Later	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.

This guide...	tells you how to:
Mac OS X Server Open Directory Administration for Version 10.4 or Later	Manage directory and authentication services.
Mac OS X Server QuickTime Streaming Server Administration for Version 10.4 or Later	Set up and manage QuickTime streaming services.
Mac OS X Server Windows Services Administration for Version 10.4 or Later	Set up and manage services including PDC, BDC, file, and print for Windows computer users.
Mac OS X Server Migrating from Windows NT for Version 10.4 or Later	Move accounts, shared folders, and services from Windows NT servers to Mac OS X Server.
Mac OS X Server Java Application Server Administration For Version 10.4 or Later	Configure and administer a JBoss application server on Mac OS X Server.
Mac OS X Server Command-Line Administration for Version 10.4 or Later	Use commands and configuration files to perform server administration tasks in a UNIX command shell.
Mac OS X Server Collaboration Services Administration for Version 10.4 or Later	Set up and manage weblog, chat, and other services that facilitate interactions among users.
Mac OS X Server High Availability Administration for Version 10.4 or Later	Manage failover and failback for file, web, mail, IP, and other services.
Mac OS X Server Xgrid Administration for Version 10.4 or Later	Manage computational Xserve clusters using the Xgrid application.
Mac OS X Server Glossary: Includes Terminology for Mac OS X Server, Xserve, Xserve RAID, and Xsan	Interpret 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 web page: 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—gateway to extensive product and technology information.
www.apple.com/macosx/server/

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

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

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

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

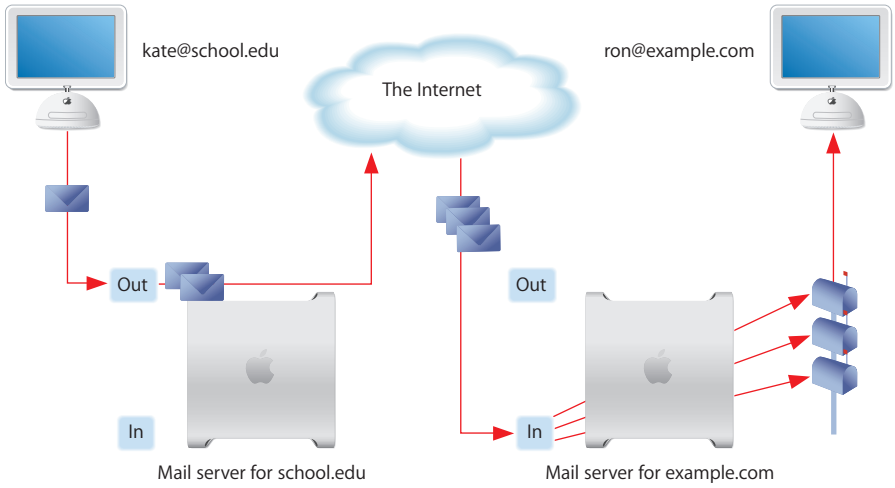
Mail Service Setup

1

Mail service in Mac OS X Server allows network users to send and receive email over your network or across the Internet. Mail service sends and receives email using the standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP). Mail service also uses a Domain Name System (DNS) service to determine the destination IP address of outgoing mail.

This chapter begins with a look at the standard protocols used for sending and receiving email. Then it explains how mail service works, summarizes the aspects of mail service setup, and tells you how to:

- Set up mail service for incoming and outgoing mail
- Support mail users
- Limit junk mail



Mail Service Protocols

A standard mail client setup uses SMTP to send outgoing email, and POP and IMAP to receive incoming email. Mac OS X Server includes an SMTP service and a combined POP and IMAP service. You may find it helpful to take a closer look at the three email protocols.

Outgoing Mail

Outgoing mail service is the means by which your users can send mail out to the Internet. Subject to restrictions that you control, the SMTP service also transfers mail to and from mail service on other servers. If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service.

Simple Mail Transfer Protocol (SMTP)

SMTP is a protocol used to send and transfer mail. SMTP queues outgoing mail messages from the user. These messages are transferred along the Internet to their destinations, to be picked up by the incoming mail protocols.

Mac OS X Server uses Postfix as its *mail transfer agent (MTA)*. Postfix fully supports the Internet standard SMTP protocol. Your email users will set their email applications' outgoing mail server to your Mac OS X Server running Postfix, and access their own incoming mail from a Mac OS X Server running incoming mail service. More information on Postfix can be found at:
www.postfix.org

If you choose to use another MTA (such as Sendmail), you won't be able to configure your mail service with Mac OS X Server administration tools.

If you want to use the Sendmail program instead of Postfix, you must disable the current SMTP service through Postfix, then install and configure Sendmail. For more information about Sendmail, see the website www.sendmail.org.

Incoming Mail

Mail is transferred from incoming mail storage to the email recipient's inbox by a *local delivery agent (LDA)*. The LDA is responsible for handling local delivery, making mail accessible by the user's email application. There are two different protocols available from Mac OS X Server's mail access agent: POP and IMAP.

Mac OS X Server uses Cyrus to provide POP and IMAP service. More information about Cyrus can be found at:
asg.web.cmu.edu/cyrus

Post Office Protocol (POP)

POP is used only for receiving mail, not for sending mail. The mail service of Mac OS X Server stores incoming POP mail until users have their computers connect to the mail service and download their waiting mail. After a user's computer downloads POP mail, the mail is stored only on the user's computer. The user's computer disconnects from the mail service, and the user can read, organize, and reply to the received POP mail. The POP service is like a post office, storing mail and delivering it to a specific address.

An advantage of using POP is that your server doesn't need to store mail that users have downloaded. Therefore, your server doesn't need as much storage space as it would using the IMAP protocol. However, because the mail is removed from the server, if any client computers sustain hard disk damage and lose their mail files, there's no way to recover these files without using data backups.

Another advantage of POP is that POP connections are transitory. Once the mail is transferred, the connection is dropped and the load on both the network and the mail server is removed.

POP isn't the best choice for users who access mail from more than one computer, such as a home computer, an office computer, and a laptop while on the road. When a user fetches mail via POP, the mail is downloaded to the user's computer and is usually completely removed from the server. If the user logs in later from a different computer, the user won't be able to see previously downloaded mail.

Internet Message Access Protocol (IMAP)

IMAP is the solution for people who need to use more than one computer to receive mail. IMAP is a client-server mail protocol that allows users to access their mail from anywhere on the Internet. Users can send and read mail with a number of IMAP-compliant email clients.

With IMAP, a user's mail is delivered to the server and stored in a remote mailbox on the server; to users, mail appears as if it were on the local computer. A key difference between IMAP and POP is that with IMAP the mail isn't removed from the server until the user deletes it.

The IMAP user's computer can ask the server for message headers, ask for the bodies of specified messages, or search for messages that meet certain criteria. These messages are downloaded as the user opens them. IMAP connections are persistent and remain open, maintaining load on the server and possibly the network as well.

User Interaction With Mail Service

Mail is delivered to its final recipient using a *mail user agent (MUA)*. MUAs are usually referred to as "email clients" or "email applications." These email clients often run on each user's local computer. Each user's email application must be configured to send messages to the correct outgoing server and receive messages from the incoming server. These configurations can affect your server's processing load and available storage space.

Where Mail Is Stored

Mail is stored in either an outgoing queue awaiting transfer to a remote server or in a local mail store accessible by local mail users.

Outgoing Mail Location

Outgoing mail messages are stored, by default, in the following spool directory on the startup disk:
/var/spool/postfix

This location is temporary, and the mail is stored until it's successfully transferred out to the Internet. These locations can be moved to any accessible volume (either local or NFS mounted) and symlinked to by the mail administrator.

Incoming Mail Location

The mail service keeps track of incoming email messages with a small database (BerkeleyDB 4.2.52), but the database doesn't contain the messages themselves. The mail service stores each message as a separate file in a mail folder for each user. Incoming mail is stored on the startup disk in the following directory:
/var/spool/imap/user/[user name]

Cyrus puts a database index file in the folder of user messages. You can change the location of any or all of the mail folders and database indexes to another folder, disk, or disk partition. You can even specify a shared volume on another server as the location of the mail folder and database, although using a shared volume incurs performance penalties. For remotely mounted filesystems, NFS isn't recommended. The incoming mail remains on the server until deleted by an MUA.

Cyrus mail storage can also be split across multiple partitions. This can be done to scale mail services, or facilitate data backup. See "Creating Additional Mail Store Locations" on page 62 for more information.

Maximum Number of Mail Messages Per Volume

Because the mail service stores each email message in a separate file, the number of messages that can be stored on a volume is determined by the total number of files that can be stored on the volume.

The total number of files that can be stored on a volume that uses Mac OS Extended format (sometimes referred to as *HFS Plus format*) depends on the following factors:

- The size of the volume
- The sizes of the files
- The minimum size of a file, which by default is one 4KB block

For example, a 4GB HFS Plus volume with the default block size of 4KB has one million available blocks. This volume could hold up to a million 4KB files, which means a million email messages that were 4KB or less apiece. If some email messages were larger than 4KB, this volume could hold fewer of them. A larger volume with the same default block size could hold proportionately more files.

Using Web Service with Mail

WebMail is a web-based *mail user agent* (MUA). It allows a web browser, such as Apple's Safari to compose, read, and forward email like any other email client. Mac OS X Server's WebMail functionality is provided by a software package called SquirrelMail at: www.squirrelmail.org.

WebMail relies on your mail server to provide the actual mail service. WebMail cannot provide mail service independent of the mail server. WebMail uses the mail service of your Mac OS X Server.

WebMail uses standard email protocols and requires your mail server to support them. These protocols are:

- Internet Message Access Protocol (IMAP) for retrieving incoming mail
- Simple Mail Transfer Protocol (SMTP) for exchanging mail with other mail servers (sending outgoing mail and receiving incoming mail)

WebMail doesn't support retrieving incoming mail via Post Office Protocol (POP). Even if your mail server has POP enabled, WebMail doesn't use it.

To use WebMail:

1. First, you need to enable and configure your mail server. This book has complete setup instructions to get your mail server running.
2. Then, after the mail server is configured, you need to enable the WebMail software.

   For instructions on setting up WebMail, see the "*Mac OS X Server Web Technologies Administration for Version 10.4 or Later*" guide, available at: www.apple.com/server/documentation/.

Using Network Services With Mail Service

Mail service makes use of network services to ensure delivery of email. Before sending an email, your mail service will probably have a Domain Name System (DNS) service determine the Internet Protocol (IP) address of the destination. The DNS service is necessary because people typically address their outgoing mail by using a domain name, such as example.com, rather than an IP address, such as 198.162.12.12. To send an outgoing message, your mail service must know the IP address of the destination. The mail service relies on a DNS service to look up domain names and determine the corresponding IP addresses. The DNS service may be provided by your Internet Service Provider (ISP) or by Mac OS X Server, as explained in the network services administration guide.

Additionally, a *mail exchange (MX)* record can provide redundancy by listing an alternate mail host for a domain. If the primary mail host isn't available, the mail can be sent to the alternate mail host. In fact, an MX record can list several mail hosts, each with a priority number. If the lowest priority host is busy, mail can be sent to the host with the next lowest priority, and so on.

Mail services use DNS like this:

1. The sending server looks at the email recipient's domain name (it's what comes after after the @ in the To address).
2. The sending server looks up the MX record for that domain name to find the receiving server.
3. If found, the message is sent to the receiving server.
4. If the lookup fails to find an MX record for the domain name, the sending server often assumes that the receiving server has the same name as the domain name. In this case, the sending server does an Address (A) lookup on that domain name, and attempts to send the file there.

Without a properly configured MX record in the DNS, mail may not reach your intended server.

Configuring DNS for Mail Service

Configuring DNS for mail service is enabling MX records with your own DNS server. If you have an ISP that provides you with DNS service, you'll need to contact the ISP so that they can enable your MX records. Follow these steps only if you provide your own DNS Service using Mac OS X Server.

To enable MX records:

1. In Server Admin, choose DNS in the Computer & Services list.
2. Click Settings.
3. Select the Zones tab.
4. Select the zone to which the MX record will be added.

   If there are no zones, you will need to create one. See the network services administration guide for more information.
5. Click the Edit (/) button beneath the zone list.
6. Select the Machines tab.
7. Click the Add (+) button beneath the machines list.
8. Enter the mail server's IP address.
9. Enter the mail server's hostname.

   Beneath the hostname, you'll see what will be the computer's Fully Qualified Domain Name.
10. Click the Add (+) button by the Alias box to add other names for this computer.

    Add as many aliases as you want.
11. Check the box labeled "This machine is a mail server of the zone."

    This field is the basis for the computer's MX record.
12. Set a mail server precedence number.

    Mail servers try to deliver mail at lower numbered mail servers first.
13. Enter any information about the computer's hardware and software in the appropriate boxes.
14. Enter any comments about the computer in the Comments box.

    You can store almost any text string in the comments box. For example, you might include the physical location of the computer (such as Upstairs server closet B) or the computer's owner (such as John's Computer) or any other information you may want to keep about the computer.
15. Click OK, and click Save.

    If you need to set up multiple servers for redundancy, you'll need to add additional MX records with different precedence numbers.

How Mail Service Uses SSL

Secure Sockets Layer (SSL) connections ensure that the data sent between your mail server and your users' mail clients is encrypted. This allows secure and confidential transport of mail messages across a local network. SSL transport doesn't provide secure authentication, just secure transfer from your mail server to your clients. See the Open Directory administration guide for secure authentication information.

For incoming mail, the mail service supports secure mail connections with mail client software that requests them. If a mail client requests an SSL connection, the mail service can automatically comply, if that option has been enabled. The mail service still provides non-SSL (unencrypted) connections to clients that don't request SSL. The configuration of each mail client determines whether it connects with SSL or not.

For outgoing mail, the mail service supports secure mail connections between SMTP servers. If an SMTP server requests an SSL connection, the mail service can automatically comply, if that option has been enabled. The mail service still can allow non-SSL (unencrypted) connections to mail servers that don't request SSL.

Enabling Secure Mail Transport With SSL

The mail service requires some configuration to provide SSL connections automatically. The basic steps are as follows:

Step 1: Obtain a security Certificate

This can be done in three ways:

1. Get a certificate from a Certificate Authority.
   a. Generate a Certificate Signing Request (CSR) and create a keychain.
   b. Use the CSR to obtain a Certificate from an issuing Certificate Authority.
2. Create a self-signed certificate in Server Admin's Certificate Manager.
3. Locate an existing certificate from a previous Mac OS X Server version 10.3 installation.

   If you already have generated a security certificate in a previous version of Mac OS X Server, you can import it for use.

See Appendix, "Certificates and Security" on page 93 for more information.

Step 2: Import the Certificate into Server Admin's Certificate Manager

You can either use the Certificate Manager to drag and drop Certificate information, or point the manager to an existing installed certificate.

See Appendix, "Certificates and Security" on page 93 for more information.

Step 3: Configure the desired service to use the Certificate

For detailed instructions for allowing or requiring SSL transport, see the following sections:

- "Configuring SSL Transport for POP Connections" on page 29
- "Configuring SSL Transport for IMAP Connections" on page 31
- "Configuring SSL Transport for SMTP Connections" on page 34

Before You Begin

Before setting up mail service for the first time:

- Decide whether to use POP, IMAP, or both for accessing mail.
- If your server will provide mail service over the Internet, you need a registered domain name. You also need to determine whether your ISP will create your MX records or you'll create them in your own DNS service.
- Identify the people who will use your mail service but don't already have user accounts in a directory domain accessible to your mail service. You must create user accounts for these mail users.
- Determine mail storage requirements, and ensure you have enough disk space for your anticipated mail volume.
- Determine your authentication and transport security needs.

How User Account Settings Affect Mail Service

In addition to setting up mail service as described in this chapter, you can also configure some mail settings individually for everyone who has a user account on your server. Each user account has settings that do the following:

- Enable or disable mail service for the user account, or forward incoming mail for the account to another email address.
- Specify the server that provides mail service for the user account.
- Set a quota on the amount of disk space for storing the user account's mail on the server.
- Specify the protocol for the user account's incoming mail: POP, IMAP, or both.

Moving Mail Messages From Apple Mail Server to Mac OS X Server Version 10.4

If you have upgraded your server from a version previous to Mac OS X Server v10.3, and you have an existing Apple Mail Server database, you must migrate your mail database to Mac OS X Server v10.4 mail service.

For more detailed instructions and tool descriptions, see "Converting the Mail Store and Database From an Earlier Version" on page 61.

Overview of Mail Service Tools

The following applications help you set up and manage mail service:

- *Server Admin:* Use to start, stop, configure, maintain, and monitor mail service when you install Mac OS X Server.
- *Workgroup Manager:* Use to create user accounts for email users and configure each user's mail options.
- *Terminal:* Use for tasks that involve UNIX command-line tools, such as backing up and restoring the mail database.

Setup Overview

You can have mail service set up and started automatically as part of the Mac OS X Server installation process. An option for setting up mail service appears in the Setup Assistant application, which runs automatically at the conclusion of the installation process. If you select this option, mail service is set up as follows:

- SMTP, POP, and IMAP are all active and using standard ports.
- Standard authentication methods are used (not Kerberos), with POP and IMAP set for clear-text passwords (APOP and CRAM MD-5 turned off) and SMTP authentication turned off.
- Mail is delivered only locally (no mail sent to the Internet).
- Mail relay is restricted.

If you want to change this basic configuration, or if you haven't set up your mail service, these are the major tasks you perform to set up mail service:

Step 1: Before you begin, make a plan

See "Before You Begin" on page 23 for a list of items to think about before you start full-scale mail service.

Step 2: Set up MX records

If you want users to be able to send and receive mail over the Internet, you should make sure DNS service is set up with the appropriate MX records for your mail service.

- If you have an ISP that provides DNS service to your network, contact the ISP and have the ISP set up MX records for you. Your ISP will need to know your mail server's DNS name (such as mail.example.com) and your server's IP address.
- If you use Mac OS X Server to provide DNS service, create your own MX records as described in "Configuring DNS for Mail Service" on page 21.
- If you do not set up an MX record for your mail server, your server may still be able to exchange mail with some other mail servers. Some mail servers will find your mail server by looking in DNS for your server's A record. (You probably have an A record if you have a web server set up.)

Note: Your mail users can send mail to each other even if you do not set up MX records. Local mail service doesn't require MX records.

Step 3: Configure incoming mail service
Your mail service has many settings that determine how it handles incoming mail. For instructions, see "Configuring Incoming Mail Service" on page 26.

Step 4: Configure outgoing mail service
Your mail service also has many settings that determine how it handles outgoing mail. For instructions, see "Configuring Outgoing Mail Service" on page 32.

Step 5: Secure your server
If your server exchanges mail with the rest of the Internet, make sure you're not operating an open relay. An open relay is a security risk and enables junk mail senders to use your computer resources for sending unsolicited commercial email. For instructions see "Limiting Junk Mail and Viruses" on page 46, and "Restricting SMTP Relay" on page 47.

Step 6: Configure additional settings for mail service
Additional settings that you can change affect how mail service stores mail, interacts with DNS service, limits junk mail, and handles undeliverable mail. See the following sections for detailed instructions:

- "Working With the Mail Store and Database" on page 60.
- "Limiting Junk Mail and Viruses" on page 46.
- "Working With Undeliverable Mail" on page 69.

Step 7: Set up accounts for mail users
Each person who wants mail service must have a user account in a directory domain accessible by your mail service. The short name of the user account is the mail account name and is used to form the user's mail address. In addition, each user account has settings that determine how your mail service handles mail for the user account. You can configure a user's mail settings when you create the user's account, and you can change an existing user's mail settings at any time. For instructions, see "Supporting Mail Users" on page 37, and "Configuring Email Client Software" on page 37.

Step 8: Create a postmaster alias (optional, but advised)
You need to make an administrative alias named "postmaster." The mail service or the mail administrators may send reports to the postmaster account. An alias allows mail sent to "postmaster@yourdomain.com" to be forwarded to an account of your choice.

You should set up forwarding of the postmaster's mail to a mail account that you check regularly. Other common postmaster accounts are named "abuse" (used to report abuses of your mail service) and "spam" (used to report unsolicited commercial email abuses by your users).

See "Creating Additional Email Addresses for a User" on page 38 to learn about creating an alias to an existing mail user.

Step 9: Start mail service
Before starting mail service, make sure the server computer shows the correct day, time, time zone, and daylight-saving settings in the Date & Time pane of System Preferences. Mail service uses this information to timestamp each message. An incorrect timestamp may cause other mail servers to handle a message incorrectly.

Also, make sure you've enabled one or more of the mail service protocols (SMTP, POP, or IMAP) in the Settings pane.

Once you've verified this information, you can start mail service. If you selected the Server Assistant option to have mail service started automatically, stop mail service now, then start it again for your changes to take effect. For detailed instructions, see "Starting and Stopping Mail Service" on page 57.

Step 10: Set up each user's mail client software
After you set up mail service on your server, mail users must configure their mail client software for your mail service. For details about the facts that users need when configuring their mail client software, see "Supporting Mail Users" on page 37.

Configuring Incoming Mail Service
Configuring incoming mail service is configuring mail to be retrieved by users and email client applications. It involves three basic steps:
- Choose and enable the type of access (POP, IMAP, or both).
- Choose a method for authentication of the email client.
- Choose a policy for secure transport of email data over SSL.

The following section contains information on how to accomplish these three steps.

Enabling POP Access
POP is used for receiving mail. The POP mail service stores incoming POP mail until users have their computers connect to the mail service and download their waiting mail. After a user's computer downloads POP mail, the mail is stored only on the user's computer. An advantage of using POP is that your server doesn't need to store mail that users have downloaded.

POP isn't the best choice for users who access mail from more than one computer, such as a home computer, an office computer, and a laptop while on the road because once messages are accessed by one computer, they are deleted from the server.

To enable POP access:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Enable POP.
5. Click Save.
6. Continue and configure security for POP authentication and transport.

See the following to continue configuration:

- "Enabling Secure POP Authentication" on page 28.
- "Enabling Less Secure Authentication for POP" on page 29.
- "Configuring SSL Transport for POP Connections" on page 29.

Enabling IMAP Access

IMAP is a client-server mail protocol that allows users to access their mail from anywhere on the Internet. With IMAP, a user's mail is delivered to the server and stored in a remote mailbox on the server; to users, mail appears as if it were on the local computer. A key difference between IMAP and POP is that with IMAP the mail isn't removed from the server until the user deletes it. IMAP connections are persistent and remain open, maintaining load on the server and possibly the network as well.

To enable IMAP access:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Enable IMAP.
5. Enter the number of concurrent connections you want to allow, then click Save.

   The default setting is 32, and the maximum is 300.
6. Click Save.
7. Continue and configure security for IMAP authentication and transport.

See the following to continue configuration:

- "Enabling Secure IMAP Authentication" on page 30.
- "Enabling Less Secure IMAP Authentication" on page 31.
- "Configuring SSL Transport for IMAP Connections" on page 31.

Choosing No Incoming Mail Retrieval

You can choose to enable SMTP mail service, but not supply POP or IMAP service for incoming mail retrieval. If neither POP nor IMAP are enabled, incoming mail from other mail servers will still be delivered to user, but users won't be able to access their mail with their email client applications.

Mail that has been accepted for local delivery will be queued until either POP and/or IMAP services are enabled, delivery to /var/mail is enabled, or the message expires and a Non Delivery Receipt (NDR) is sent to the sender (after 72 hours by default). If deliver to /var/mail has been enabled, users can still access mail using UNIX mail tools such as PINE or ELM. Messages delivered to /var/mail/ will not be available for delivery to users with Cyrus, once POP and/or IMAP is enabled again.

If both POP and IMAP are disabled, you can change where incoming mail is stored from its default location at /var/spool/imap/user/[user name] to /var/mail/[user name].

To change the local delivery directory:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Check "Deliver to /var/mail/..."
5. Click Save.

Enabling Secure POP Authentication

Your POP mail service can protect users' passwords by allowing Authenticated POP (APOP), or Kerberos. When a user connects with APOP or Kerberos, the user's mail client software encrypts the user's password before sending it to your POP service. Before configuring your mail service to require secure authentication, make sure that your users' email applications and user accounts support the method of authentication you choose.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide for more information.

If you want to *require* either of these authentication methods, enable only one method.

To set the POP authentication method:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Check APOP, or Kerberos (as desired) in the POP3 list.
6. Click Save.

Enabling Less Secure Authentication for POP

You can choose to allow basic password (clear text) authentication. This is considered less secure than APOP or Kerberos because the password itself is transmitted as unencrypted, clear text.

If you want to *require* clear text authentication, enable Clear as the only authentication method.

To enable clear text POP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Check Clear.
6. Click Save.

Configuring SSL Transport for POP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for POP (and IMAP) connections. Before using SSL connections, you must have a security certificate for mail use.

See "Certificate Manager in Server Admin" on page 95 to for more information about Certificates.

Setting SSL transport for POP also sets it for IMAP.

To set SSL transport for POP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Select Require or Use to enable (Don't Use to disable) in the IMAP and POP SSL section.
6. Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
7. Click Save.

Enabling Secure IMAP Authentication

Your IMAP mail service can protect users' passwords by requiring that connections use a secure method of authentication. You can choose CRAM MD-5, or Kerberos v5 authentication. When a user connects with secure authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Make sure that your users' email applications and user accounts support the method of authentication you choose.

If you configure your mail service to require CRAM MD-5, mail users' accounts must be set to use a Mac OS X Server Password Server that has CRAM MD-5 enabled. For information, see the Open Directory administration guide.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide for more information.

If you want to *require* any of these authentication methods, enable only one method.

To set secure IMAP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Select CRAM MD-5 or Kerberos (as desired) in the IMAP section.
6. Click Save.

Enabling Less Secure IMAP Authentication

Your IMAP mail service can supply users' passwords by less secure means. These authentication methods are less secure because they don't securely encrypt your users' passwords as they cross the network.

If you want to *require* any of these authentication methods, enable only one method.

To allow login, plain, or clear IMAP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Check LOGIN, PLAIN, or Clear in the IMAP list.
6. Click Save.

Configuring SSL Transport for IMAP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

See "Certificate Manager in Server Admin" on page 95 to for more information about Certificates.

Setting SSL transport for IMAP also sets it for POP.

To configure SSL transport for IMAP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click Require or Use to enable (Don't Use to disable) in the IMAP and POP SSL section.
6. Select the Certificate you want to use from the corres ponding pop-up menu, if you are using or requiring SSL.
7. Click Save.

Configuring Outgoing Mail Service

The mail service includes an SMTP service for sending mail. Subject to restrictions that you control, the SMTP service also transfers mail to and from mail service on other servers. If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service. Other mail services deliver messages for your mail users to your SMTP service, which then transfers the messages to your POP service and IMAP service.

Enabling SMTP Access

SMTP is used for transferring mail between mail service and sending mail from user's email clients. The SMTP mail service stores outgoing mail in a queue until it has found the mail exchange server at the email's destination. Then it transfers the mail to the destination server for handling and eventual delivery.

SMTP service is required for outgoing mail service, and accepting delivery of mail from mail servers outside your organization.

To enable SMTP access:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Enable SMTP.
5. Select "Allow incoming mail," if desired.

   If you allow incoming mail, enter the domain name to accept mail for, and the mail server's host name.
6. Click Save.

Understanding SMTP Authentication

If you don't choose any method of SMTP authentication or authorized specific SMTP servers to relay for, the SMTP server will allow anonymous SMTP mail relay, and is considered an "open relay." Open relays are bad because junk mail senders can exploit the relay to hide their identities and send illegal junk mail without penalty.

A distinction must be made between *relaying mail* and *accepting delivery of mail*. Relaying mail means passing mail from one (possibly external) mail server or a local user's email client to another (third) mail server. Accepting delivery means receiving mail from a (possibly external) mail server to be delivered to the server's own email users. Mail addressed to local recipients is still accepted and delivered. Enabling authentication for SMTP *requires* authentication from any of the selected authentication methods prior to *relaying mail*.

SMTP Authentication is used in conjunction with restricted SMTP mail transfer to limit junk mail propagation. For more information on these settings, see "Limiting Junk Mail and Viruses" on page 46.

Enabling Secure SMTP Authentication

Your server can guard against being an open relay by allowing SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) You can configure the mail service to require secure authentication using either the CRAM MD-5 or Kerberos method. You can also allow the less secure plain and login authentication methods, which don't encrypt passwords, if some users have email client software that doesn't support the secure methods.

If you configure your mail service to require CRAM MD-5, mail users' accounts must be set to use a password server that has CRAM MD-5 enabled. For information, see the Open Directory administration guide.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide.

Enabling SMTP Authentication will:

- Make your users authenticate with their email client before accepting any mail to send.
- Frustrate mail server abusers trying to send mail without your consent through your system.

If you want to *require* any of these authentication methods, enable only one method.

To allow secure SMTP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Check CRAM MD-5, or Kerberos (as desired) in the SMTP section.
6. Click Save.

Enabling Less Secure SMTP Authentication

Your server can guard against being an open relay by requiring SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) Requiring authentication ensures that only known users—people with user accounts on your server—can send mail from your mail service. You can choose to require, allow, or disallow less secure authentication methods (plain text, or login) for SMTP mail service.

Plain authentication sends mail passwords as plain text over the network. Login authentication sends a minimally secure crypt hash of the password over the network.

If you want to *require* any of these authentication methods, enable only one method.

To allow less secure authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Check either Plain or Login in the SMTP section.
6. Click Save.

Configuring SSL Transport for SMTP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

See "Certificate Manager in Server Admin" on page 95 to for more information about Certificates.

To configure SSL transport for SMTP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click Require or Use to enable (Don't Use to disable) in the SMTP SSL section.
6. Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
7. Click Save.

Relaying SMTP Mail Through Another Server

Rather than delivering outgoing mail directly to its various destinations, your SMTP mail service can relay outgoing mail to another server.

Normally, when an SMTP server receives a message addressed to a remote recipient, it will attempt to send that message directly to that server or the server specified in the MX record, if it exists. Depending on your network setup, this method of mail transport may not be desired or even possible. You may then need to relay all outbound messages through a specific server.

- You may need to use this method to deliver outgoing mail through the firewall set up by your organization. In this case, your organization will designate a particular server for relaying mail through the firewall.
- You may find this method useful if your server has slow or intermittent connections to the Internet.

Do not attempt to relay mail through a mail server outside your organization's control or without the relay server's administrator's permission. Trying to do so, without the express authorization of the relay server administrator, will label you as a mail service abuser.

To relay SMTP mail through another server:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Click the General tab.
4. Click "Relay all SMTP mail through this host" and enter the DNS name or IP address of the server that provides SMTP relay.
5. Click Save.

Limiting Incoming Message Size

You can set a maximum size for incoming messages. The default is 10 megabytes. You may not want to allow large attachments which add to the message size.

To set a maximum incoming message size:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Click the Quotas tab.
4. Check "Refuse Incoming Messages..." and type the number of megabytes you want to set as the limit.
5. Click Save.

Using ACLs For Mail Service Access

Access Control Lists (ACLs) are a method of designating service access to certain users or groups on an individual basis. For example, you may use an ACL to allow only one user access to a file server or shell login, without allowing any user on the server to access it.

Mail services are different from many other services which traditionally use ACLs for determining service access. Mail service is already specified on a per-user basis. Either you have an email account on a particular server or you don't. Merely being a user on a server doesn't automatically confer access to email storage and retrieval.

Some administrator's may find it easier to designate email access using ACLs, if they are doing all their other configuration using ACLs. They also may have mixed network environments that necessitate using ACLs to assign email access.

Mac OS X Server allows you to enable mail access for users using the access tab in a server's Server Admin listing. If you have enabled user access via Server Admin and traditional mail access using Workgroup Manager, the settings interact in the following manner:

Access via ACL	Access via Workgroup Manager	Result
On	On	User has mail access granted according to the IMAP and/or POP settings in the General Settings Mail panel in Server Admin.
On	Off	User has mail access granted according to the IMAP and/or POP settings in the General Settings Mail panel in Server Admin.
Off	On	User has mail access granted according to his user record settings in Workgroup Manager. This is the default behavior.
Off	Off	User has no mail access.

To enable a user's mail access using ACLs:

1. In Server Admin, select the server which has mail service running and the user who will receive an email account.
2. Click Access.
3. Deselect "Use same access for all services."
4. Select "Allow only users and group below."
5. Click the Add (+) button to reveal a Users and Groups drawer.
6. Drag the desired user to the access list.
7. Click Save.

Supporting Mail Users

This section discusses mail settings in your server's user accounts, user mail storage quotas, and mail service settings in email client software.

Configuring Mail Settings for User Accounts

To make mail service available to users, you must configure mail settings in your user accounts. For each user, you need to:

- Enable mail usage.
- Enter the DNS name or IP address of your mail server.
- Select the protocols for retrieving incoming mail (POP, IMAP, or both).
- Set a quota on disk space available for storing a user's mail.
- Configure any desired alternate mail storage location.

You configure these settings with the Workgroup Manager application. For detailed instructions, see the *Mac OS X Server User Management for Version 10.4 or Later*.

Configuring Email Client Software

Users must configure their email client software to connect to your mail service. The following table details the information most email clients need and the source of the information in Mac OS X Server.

Email client software	Mac OS X Server	Example
User name	Full name of the user	Steve Macintosh
Account name Account ID	Short name of user account	steve
Password	Password of user account	
Host name Mail server Mail host	Mail server's full DNS name or IP address, as used when you log in to the server in Server Admin	mail.example.com 192.168.50.1
Email address	User's short name, followed by the @ symbol, followed by one of the following: • Server's Internet domain (if the mail server has an MX record in DNS) • Mail server's full DNS name • Server's IP address	steve@example.com steve@mail.example.com steve@192.168.50.1
SMTP host SMTP server	Same as host name	mail.example.com 192.168.50.1
POP host POP server	Same as host name	mail.example.com 192.168.50.1
IMAP host IMAP server	Same as host name	mail.example.com 192.168.50.1

Email client software	Mac OS X Server	Example
SMTP user	Short name of user account	steve
SMTP password	Password of user account	

Creating an Administration Account

You may need to create a mail administrator account to maintain and watch mail folders, remove defunct user accounts, and archive mail. This administrator account doesn't need to be a server administrator. Also, this administrator account shouldn't receive mail. It isn't a normal mail account.

To create a mail administrator account:

1. Create a user to be mail administrator.
2. If you haven't created a user record for the mail administrator's account, see the user management guide.
3. Open `/etc/imapd.conf` in a text editor.

   If you aren't comfortable using a terminal text editor like emacs or vi, you can use TextEdit.
4. Find the line that reads "admins:"
5. Edit the line to add the account name of the administrator account after the colon.
6. Save your changes.

For more information see the man page for imapd.conf.

Creating Additional Email Addresses for a User

Mail service allows each individual user to have more than one email address, called an "alias." Every user has one email address that's formed from the short name of the user account. In addition, you can define more names for any user account by creating an alias file. Each additional name is an alternate email address for the user at the same domain. These additional email addresses aren't additional accounts that require separate quotas or passwords. Most often alias files are used to map "postmaster" users to a real account and give a "firstname.lastname@example.com" email address to a user with a short login account name.

There are two methods for creating email aliases: Mac OS X Server-style, and Postfix-style. Each one has its advantages and disadvantages. Mac OS X Server-style aliases are easy to make, and are listed with a user's login name. You can easily see what alias refers to which user. The downside of this kind of alias is that mail service's Sieve functionality doesn't understand Mac OS X Server-style aliases and will not filter mail based on the Mac OS X Server-style alias.

Postfix-style aliases require command-line administration, are less obvious to audit. However, the major benefit to using Postfix-style aliases is their use with Sieve scripting. Only aliases generated Postfix-style can be acted upon by Sieve scripts.

To create a Mac OS X Server-style alias:

1. In Workgroup Manager, open the user account you want to work with, if it isn't already open.

   To open the account, click the Accounts button, then click the globe icon below the tool bar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
2. Click the Basic tab.
3. Double-click under the last entry in the Short Names list.
4. Enter the alias.

   For example, if your domain is "example.com" and you want to give username "bob" an alias of "robert.fakeuser" you should enter:

   ```
   robert.fakeuser
   ```
5. Click Save.

Now mail to "robert.fakeuser@example.com" will be sent to user "bob," giving Bob two effective email addresses, bob@example.com and robert.fakeuser@example.com.

To create a Postfix-style alias:

1. Create a file to be used as an alias list in /etc/postfix/aliases, if none exists.
2. For each alias, make a line in the file with the following format:

   alias:localaddress1,localaddress2,...

   For example, for your domain example.com, if you want to give username "bob" an alias of "robert.fakeuser" you should enter:

   ```
   robert.fakeuser: bob
   ```

   This will take mail sent to your mail server for robert.fakeuser@example.com and actually send it to the real mail account bob@example.com.
3. Save your file changes.
4. In Terminal.app, enter the following command:

   ```
   postalias /etc/aliases
   ```

   The text file is processed into a database for faster access.
5. At the prompt, enter the following command:

   ```
   newaliases
   ```

   The alias database will reload.

Now mail to "robert.fakeuser@example.com" will be sent to user "bob," giving Bob two effective email addresses, bob@example.com and robert.fakeuser@example.com.

For further information about creating and maintaining email aliases, look at /etc/postfix/alias.

Setting Up Forwarding Email Addresses for a User

You may use this to provide an email redirection service for your users. Any mail sent to the user's email account will be forwarded to the indicated account.

There is an additional method of email forwarding using Sieve scripting. To learn more about that method, see "Sieve Scripting Support" on page 54.

To forward a users mail:

1. In Workgroup Manager, open the user account you want to work with, if it isn't already open.

   To open the account, click the Accounts button, then click the globe icon below the toolbar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
2. Click the Mail tab.
3. Select Forward.
4. Enter the forwarding email address in the Forward To field.

   Multiple addresses can be entered but must be separated by a comma.

Adding or Removing Virtual Domains

Virtual domains are other domains which can be used in email addresses for your mail users. A virtual domain also contains a list of all the domain names for which it's responsible. You should add any names that are likely to appear after @ in the addresses of mail directed to your server. You should also put any fully qualified domain name that would resolve to your mail server's IP address.

For example, the list might contain variations of the spelling of your domain name or company name. If you host mail for example.com and example.org, a virtual domain would allow bob@example.com to receive mail addressed to bob@example.com and example.org using the same mailbox. Additionally, mail.example.com might resolve to the same IP address as example.com, so make sure mail.example.com is in the virtual domain group.

In short: Virtual domains allow for one user name ("bob" in the example above) to receive mail in a single inbox, regardless of which of the virtual domains come after @ in the email address. The address "bob@example.com" delivers to that same address as "bob@example.org."

Your mail settings apply to all domain names in this list. You should never list the same domain in the virtual domain.

To use a virtual domain, you must have the domain registered and you should have an MX record pointing to your mail server for the domains you wish to enable.

To add or remove virtual domain names for the mail server:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Click the Add (+) button and type the domain name of a virtual mail host for which you want your server to be responsible.
5. To change a virtual domain, select it, and click the Edit (/) button.
6. To remove an item from the list, select it and click the Remove (-) button.

Note: You should set up MX records for each virtual domain. If a domain name in this list doesn't have an MX record, only your mail service recognizes it. External mail sent to this domain name will be returned.

Running a Virtual Host

Virtual hosting is a method that you can use to host more than one domain name on the same computer and IP address, with overlapping mail user names.
For instance, a mail server could be receiving mail transfer requests for two domains, mail.example1.com and mail.example.com, both of which resolve to the same IP address. For mail.example1.com, the server would deliver mail to "bob@example1.com" to a user mailbox for "bob," while it would also deliver mail to "bob@example2.com" to a *different* user mailbox. Virtual hosts are essentially the converse of virtual domains.

Enabling Virtual Hosting

Before you can enable virtual hosting, you must add a list of locally hosted virtual domains to your mail server. See "Adding or Removing Virtual Hosts" on page 42 for more information.

To enable virtual hosting:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Hosting.
5. Add at least one virtual host.

   See "Adding or Removing Virtual Hosts" for more information.

6 Select Enable Virtual Hosting.

You can now add or remove virtual hosts using the Add (+) or Remove (-) buttons.

7 Click Save.

Adding or Removing Virtual Hosts

Before you can enable virtual hosting, you must add a list of locally hosted virtual domains to your mail server. Virtual hosting must be enabled to add or remove virtual hosts. If virtual hosting is not enabled, see "Enabling Virtual Hosting" on page 41 for more information.

To add or remove virtual hosts:

1 In Server Admin, select Mail in the Computers & Services pane.

2 Click Settings.

3 Select the Advanced tab.

4 Select Hosting.

5 Click the Add (+) button next to the Locally Hosted Virtual Domain box and type the domain name of a virtual host for which you want your server to be responsible.

To change a virtual domain, select it, and click the Edit (/) button.

To remove an item from the list, select it and click the Remove (-) button.

6 Click Save.

Note: You should set up MX records for each virtual domain. If a domain name in this list doesn't have an MX record, only your mail service recognizes it. External mail sent to this domain name will be returned.

Associating Users to the Virtual Host

Associating uses to a virtual host requires creating an alias in their user records which contain the entire email address (such as bob@example.com, where example.com isn't the domain name of the mail server, but a virtual host).

There are two methods for creating aliases for virtual host users: Mac OS X Server-style, and Postfix-style. Each one has its advantages and disadvantages. Mac OS X Server-style aliases are easy to make, and are listed with a user's login name. You can easily see what alias refers to which user. The downside of this kind of alias is that mail service's Sieve functionality doesn't understand Mac OS X Server-style aliases and will not filter mail based on the Mac OS X Server-style alias.

Postfix-style aliases require command-line administration, are less obvious to audit. However, the major benefit to using Postfix-style aliases is their use with Sieve scripting. Only aliases generated Postfix-style can be acted upon by Sieve scripts.

To associate a user to a virtual host using Mac OS X Server-style aliases:

1. Add a Virtual Host Name using the directions in section "Adding or Removing Virtual Hosts" on page 42.
2. In Workgroup Manager, open the user account you want to work with, if it isn't already open.

   To open the account, click the Accounts button, then click the globe icon below the tool bar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
3. Click the Basic tab.
4. Double-click under the last entry in the Short Names list.
5. Enter the virtual host address alias.

   For example, if your domain is example.com and the virtual host domain is server.com, and you want mail addressed to "postmaster@server.com" to be delivered to user "bob," open "bob's" user record in Workgroup Manager, and enter:

   ```
   postmaster@server.com
   ```
6. Click Save.

   This will take mail sent to your mail server for "postmaster@server.com" and actually send it to the real mail account for user "bob." Meanwhile mail to postmaster@example.com will go to another designated mail account.

To associate a user to a virtual host using Postfix-style aliases:

1. Add a Virtual Host Name using the directions in section "Adding or Removing Virtual Hosts" on page 42.
2. Create a file to be used as an alias list in /etc/aliases, if none exists.
3. For each alias, make a line in the file with the following format:

   alias@virtualhost:localaddress1,localaddress2,...

   For example, if your domain is "example.com" and you are running a virtual host for "server.com," and if you want to have the user "bob" get mail sent to "postmaster@server.com," you should enter:

   ```
   postmaster@server.com: bob
   ```

   This will take mail sent to your mail server for postmaster@server.com and send it to user "bob." Mail sent to postmaster@example.com will be sent to some other designated recipient.
4. Save your file changes.
5. In Terminal.app, enter the following command:

   ```
   postalias /etc/aliases
   ```

   The text file is processed into a database for faster access.

6 At the prompt, enter the following command:

```
newaliases
```

The alias database will reload.

7 At the prompt, reload the mail server by entering the following command:

```
postfix reload
```

This will take mail sent to your mail server for "postmaster@server.com" and actually send it to the real mail account for user "bob." Meanwhile mail to postmaster@example.com will go to another designated mail account.

Managing Mail Quotas

Mail quotas define how much disk space a user's email can fill on the mail server. Quotas are set on a per-user basis in the user's record in Workgroup Manager. Although you don't set an email user's quota in Server Admin, you do manage quota enforcement and your server's response to quota violation. Mail quotas are especially important if the mail server hosts many IMAP accounts. IMAP doesn't require mail to be removed from the server when read, so IMAP users who get large attachments can fill their quotas very quickly.

Enabling Mail Quotas For Users

You can enable limits to mail storage on server. This is especially important if you use the IMAP protocol for incoming messages because email messages aren't necessarily deleted when downloaded to the user.

You use Workgroup Manager to enable a user's mail quota.

To enable a user's mail quota:

1 In Workgroup Manager, open the user account you want to work with, if it isn't already open.

To open the account, click the Accounts button, then click the globe icon below the tool bar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

2 Click the Mail tab.

If the user doesn't have mail enabled, enable it now.

3 Enter the number of MB for the user's mail storage in the Mail Quota box.

4 Click Save.

Configuring Quota Warnings

When a user's mailbox approaches its storage quota, you can choose to warn the users of an impending quota violation. You choose whether to warn the mail user, how often to warn him or her, and at what point to send the warning.

To configure quota warnings:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Quotas tab.
4. Click Enable Quota Warnings.
5. Enter the maximum percentage of storage usage before a warning is sent.
6. Enter the frequency of the warning notice, in number of days.
7. If you want to customize the quota warning notification, click Edit next to the quota warning message.
8. Click Save.

Configure Quota Violation Responses

When a mail user has more mail in storage than allowed for his or her quota, the mail server recognizes a quota violation. There are typically two responses to quota violation: a violation notice, and suspension of mail service.

To configure quota violation responses:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Other tab.
4. Click Enable Quota Warnings.
5. If you want to customize the quota violation notification, click Edit next to the over quota error message.
6. If you want to suspend mail service for users who exceed their quotas, select "Disable a user's mailbox...."
7. Click Save.

Limiting Junk Mail and Viruses

You can configure your mail service to decrease the volume of unsolicited commercial mail, also known as junk mail (or *spam*), and email containing viruses. You can take steps to block junk mail or viruses that are sent to your mail users. Additionally, you can secure your server against use by mail service abusers, who try to use your resources to send junk mail to others.

You can also take steps to prevent senders of junk mail from using your server as a relay point. A *relay point* or *open relay* is a server that unselectively receives and forwards all mail addressed to other servers. An open relay sends mail from any domain to any domain. Junk mail senders exploit open relay servers to avoid having their own SMTP servers blacklisted as sources of junk mail. You don't want your server blacklisted as an open relay, because other servers may reject mail from your users.

There are two main methods of prevent viruses and junk mail passing through or into your mail system. Using both of the methods in concert will help ensure your mail system integrity. The two points of control are:

- "Connection Control" (next).
- "Email Screening" on page 49.

Connection Control

This method of prevention controls which servers can connect to your mail system, and what those servers have to do to send mail through your mail system. Your mail service can do any of the following to exercise connection control:

- Require SMTP authentication
- Restrict SMTP relay, allowing relay only by approved servers
- Reject all SMTP connections from disapproved servers
- Reject mail from blacklisted servers
- Filter SMTP connections

Requiring SMTP Authentication

If your mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server.

Although SMTP authentication applies primarily to mail relay, your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they will be unable to send mail to remote servers. Mail sent from external mail servers and addressed to local recipients will still be accepted and delivered.

To require SMTP authentication, please see "Enabling Secure SMTP Authentication" on page 33, and "Enabling Less Secure SMTP Authentication" on page 34.

Restricting SMTP Relay

Your mail service can restrict SMTP relay by allowing only approved hosts to relay mail. You create the list of approved servers. Approved hosts can relay through your mail service without authenticating. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All hosts, approved or not, can deliver mail to your local mail users without authenticating.

Your mail service can log connection attempts made by hosts not on your approved list.

To restrict SMTP relay:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Relay tab.
4. Check "Accept SMTP relays only from these".
5. Edit the list of hosts.
   - Click the Add (+) button to add a host to the list.
   - Click the Remove (-) button to delete the currently selected host from the list.
   - Click the Edit (/) button to change the currently selected host from the list.

   When adding to the list, you can use a variety of notations.
   - Enter a single IP address, or the network/netmask pattern such as 192.168.40.0/21.
   - Enter a host name, such as mail.example.com.
   - Enter an Internet domain name, such as example.com.

SMTP Authentication and Restricted SMTP Relay Combinations

The following table describes the results of using SMTP authentication and restricted SMTP relay in various combinations.

SMTP requires authentication	Restricted SMTP relay	Result
On	Off	All mail servers must authenticate before your mail service will accept any mail for relay. Your local mail users must also authenticate to send mail out.
On	On	Approved mail servers can relay without authentication. Servers that you haven't approved can relay after authenticating with your mail service.
Off	On	Your mail service can't be used for open relay. Approved mail servers can relay (without authenticating). Servers that you haven't approved can't relay unless they authenticate, but they can deliver to your local mail users. Your local mail users don't have to authenticate to send mail. This is the most common configuration.

Rejecting SMTP Connections From Specific Servers

Your mail service can reject unauthorized SMTP connections from hosts on a disapproved-hosts list that you create. All mail traffic from servers in this list is denied and the SMTP connections are closed after posting a 554 SMTP connection refused error.

To reject unauthorized SMTP connections from specific servers:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Relay tab.
4. Check "Refuse all messages from these...".
5. Edit the list of servers.

   Click the Add (+) button to add a host to the list.

   Click the Remove (-) button to delete the currently selected host from the list.

   Click the Edit (/) button to change the currently selected host from the list.

   When adding to the list, you can use a variety of notations.

   - Enter a single IP address, or the network/netmask pattern such as 192.168.40.0/21.
   - Enter a host name, such as mail.example.com.
   - Enter an Internet domain name, such as example.com.

Rejecting Mail From Blacklisted Senders

Your mail service can reject mail from SMTP servers that are blacklisted as open relays by a *Real-time Blacklist Server (RBL)*. Your mail service uses an RBL server that you specify. RBLs are sometimes called *black-hole servers*.

Important: Blocking unsolicited mail from blacklisted senders may not be completely accurate. Sometimes it can prevent valid mail from being received.

To reject mail from blacklisted senders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Relay tab.
4. Check "Use these junk mail rejection servers."
5. Edit the list of servers by adding the DNS name of an RBL server.

   Click the Add (+) button to add a server to the list.

   Click the Remove (-) button to delete the currently selected server from the list.

   Click the Edit (/) button to change the currently selected server from the list.

   Enter the domain name of the desired RBL server, such as rbl.example.com.

Filtering SMTP Connections

You can use the firewall service of Mac OS X Server to allow or deny access to your SMTP mail service from specific IP addresses. Filtering disallows all communication between an originating host and your mail server. Mail service will never receive the incoming connection and no SMTP error will be generated and sent back to the client.

To filter SMTP connections:

1. In Server Admin, select Firewall in the Computers & Services pane.
2. Create a firewall IP filter using the instructions in the network services administration guide using the following settings:
   - Access: Denied
   - Port number: 25 (or your incoming SMTP port, if you use a nonstandard port)
   - Protocol: TCP
   - Source: the IP address or address range you want to block
   - Destination: your mail server's IP address
3. If desired, log the packets to monitor the SMTP abuse.
4. Add more new filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information on the firewall service, see the network services administration guide.

Email Screening

Once a mail delivery connection is made, and the message accepted for local delivery (relayed mail is not screened), the mail server can screen it before delivery. Mac OS X Server uses SpamAssassin (spamassassin.apache.org) to analyze the text of a message, and gives it a probability rating for being junk mail. No junk mail filter is 100% accurate in identifying unwanted email. It's for this reason that the junk mail filter in Mac OS X Server doesn't delete or remove junk mail from being delivered. Instead it marks the mail as potential junk mail. The user can then decide if it's really unsolicited commercial email and deal with it accordingly. Many email clients even use the ratings that SpamAssassin adds as a guide in automatically classifying the mail for the user.

Mac OS X Server uses ClamAV (www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can choose to deal with it several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called "freshclam."

Enabling Junk Mail Screening (Baysian Filters)

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure certain screening parameters. Bayesian mail filtering is the classification of mail messages based on statistics. Each message is analyzed and the word frequency statistics are saved. Mail messages that have more of the same words as junk mail receive a higher marking of probability that they are also junk mail. When the message is screened, the server adds a new header ("X-Spam-Level") with the junk mail probability score.

For example, let's say you have 400 mail messages. 200 of them are junk mail, and 200 of them are good mail. When a new message arrives, its text is compared to the 200 junk mail, and the 200 good mail. The the filter assigns it a probability of being junk or good, depending on what group it most resembles.

Bayesian filtering has shown itself to be a very effective method of finding junk mail, if the filter has enough data to go on. One of the strengths of this method is the more mail you get and classify (a process called "training"), the more accurate the next round of classification is. Even if junk mail senders alter their mailings, the filter takes that into account the next time around.

To enable junk mail screening:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Junk Mail.
5. Set the level of permissiveness (Least, Moderate, Most).

   The permissiveness meter sets how many junk mail flags can be applied to a single message before it processed as junk mail. If you set it as "Least permissive," any mildly suspicious email will be tagged and processed as junk mail. If you set it for "Most permissive" it will take a high score (in other words, a lot of junk mail characteristics) to mark it as junk.
6. Decide how to deal with junk mail messages.

   Bounced: Will send the message back to the sender. You can optionally send an email notification of the bounce to some email account, probably the postmaster.

   Deleted: Will delete the message without delivery. You can optionally send an email notification of the bounce to some email account, probably the postmaster.

   Delivered: Will deliver the message in spite of probably being junk mail. You can optionally add text to the subject line, indicating that the message is probably junk mail, or encapsulate the junk mail as a MIME attachment.

   Redirected: Will deliver the message to someone other than the intended recipient.

7 Choose how often to update the junk mail database updated, if desired.

8 Click Save.

For an explanation of other options, see "Filtering Mail by Language and Locale" on page 52.

Manually Training the Junk Mail Filter

It's important to teach the filter what is, and what isn't junk mail. Initially, the filter won't be very accurate at marking junk mail, but you can train it to do better. Accurate training requires a large sample, so a minimum of 200 messages of each type is advised.

To train the filter:

1 Choose a mailbox of 200 messages made of *only junk mail*.

2 Use Terminal and the filter's command-line training tool to analyze it and remember it as junk mail using the following command:

```
sa-learn --showdots --spam <junk mail directory>/*
```

3 Choose a mailbox of 200 messages made of *only good mail*.

4 Use Terminal and the filter's command-line training tool to analyze it and remember it as good mail using the following command:

```
sa-learn --showdots --ham <junk mail directory>/*
```

If the junk mail filter fails to identify a junk mail message, train it again so it can do better next time. Use `sa-learn` again with the `--spam` argument on the mislabeled message. Likewise, if you get a false positive (a good message marked as junk mail), use `sa-learn` again with the `--ham` argument to further train the filter.

Automatically Training the Junk Mail Filter

The junk mail filter needs to be told what is and isn't junk mail. Mac OS X Server provides a method of training the filter automatically with the help of the mail users. The server runs an automated command at 1 am (a cron job) which scans two specially named mail users' inboxes. It runs SpamAssassin's sa-learn tool on the contents of the inboxes and uses the results for its adaptive junk mail filter.

To automatically train the junk mail filter:

1. Enable junk mail filtering.

   See "Enabling Junk Mail Screening (Baysian Filters)" on page 50 for more information.
2. Create two local accounts: junkmail, and notjunkmail
3. Use Workgroup Manager to enable them to receive mail.

   If you need help with this, see "Configuring Mail Settings for User Accounts" on page 37.
4. Instruct your mail users to "Redirect" junk mail messages which have not previously been tagged as junk mail to "junkmail@<yourdomain>".
5. Instruct your mail users to "Redirect" real mail messages which were wrongly tagged as junk mail to "notjunkmail@<yourdomain>".
6. Each day at 1 am, the junk mail filter will learn what is junk and what was mistaken for junk, but is not.
7. Delete the messages in junkmail and notjunkmail's accounts daily.

Filtering Mail by Language and Locale

You may decide to filter incoming mail based on certain locales or languages. Mail composed in foreign text encodings are often erroneously marked as junk mail. You can configure your mail server to not mark designated originating countries or languages as junk mail.

To allow mail by language and locale:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Junk Mail.
5. Click the Edit (/) button next to Accepted Languages to change the list.
   a. Select the language encodings to allow as non-junk mail, and click OK.
6. Click the Edit (/) button next to Accepted Locales to change the list.
   a. Select the country codes to allow as non-junk mail, and click OK.
7. Click Save.

Enabling Virus Screening

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure certain screening parameters.

Mac OS X Server uses ClamAV (www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can choose to deal with it several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

To enable virus screening:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Viruses.
5. Decide how to deal with junk mail messages.

   Bounced: Will send the message back to the sender. You can optionally send an email notification of the bounce to an email account (probably the domain's postmaster) and notify the intended recipient.

   Deleted: Will delete the message without delivery. You can optionally send an email notification to some email account, probably the postmaster, as well as the intended recipient.

   Quarantined: Will deliver the message to a directory for further analysis. You can optionally send an email notification of the quarantine to some email account, probably the postmaster.
6. Optionally, choose to notify the intended recipient if the message was filtered in some way.
7. Choose how often to update the virus database, if desired.

   A minimum of twice a day is suggested. Some administrators choose eight times a day.
8. Click Save.

Advanced Configuration Tools and Options

Mac OS X Server ships with some power tools to help administer you mail service. These advanced configuration tools use the command line and require a basic familiarity with working within a shell, and basic scripting concepts.

cyradm

The tool cyradm is included with Mac OS X Server. It is an administration shell for Cyrus, the IMAP mail service package. It communicates with the Cyrus::IMAP::Admin Perl module. Cyradm can be used to create, delete or rename mailboxes, as well as set ACLs for mailboxes (for email clients that support them).

Things to note:

- Cyradm is a limited shell: It supports shell-style redirection, but does not understand pipes.
- Cyradm can be used interactively or be scripted, but Perl scripting with Cyrus::IMAP::Admin will be more flexible.
- All spaces in file or directory names must be escaped with a "\" just as you would in a shell.

For a complete list of commands for cyradm, consult its man page via the Terminal by entering:

```
man cyradm
```

Sieve Scripting Support

Mac OS X Server supports Sieve scripting for mail processing. Sieve is an Internet standard mail filtering language for server side filtering. Sieve scripts interact with incoming mail before final delivery.

Sieve acts much like the "rules" in various email programs to sort or process mail based on user-defined criteria. In fact, some email clients use Sieve for client-side email processing. Sieve can provide such functions as vacation notifications, message sorting, mail forwarding, among other things.

Sieve scripts are kept for each user on the mail server at:

```
/usr/sieve/<first letter of username>/<user>
```

The directory is owned by the mail service, so users normally don't have access to it, and can't put their scripts there for mail processing. For security purposes, users and administrators upload their scripts to a Sieve process (timsieved) which transports the scripts to the mail process for use. There are various ways of getting the scripts to timsieved: Perl shell scripts ("sieveshell"), web mail plugins ("avelsieve"), and even some email clients.

Enabling Sieve Support

In order for Sieve to function, you must enable its communications port. Sieve has the vacation extension added by default. All scripts must be placed in the central script repository at /usr/sieve/, and Sieve scripts cannot be used to process mail for email aliases set up in Workgroup Manager; you must use Postfix-style aliases.

To enable Sieve support:

1. Add the following entry in /etc/services/

   ```
   sieve 2000/tcp #Sieve mail filtering
   ```

2. Reload the mail service.

Learning Sieve Scripting

Sieve's complete syntax, commands, and arguments are found in IETF RFC 3028: www.ietf.org/rfc/rfc3028.txt?number=3028

Other information about Sieve and a sample script archive can be found at: www.cyrusoft.com/sieve

Sample Sieve Scripts

The following scripts are examples of some common scripts that a user might want to use.

Vacation Notification Script

```
#--------
# This is a sample script for vacation rules.
# Read the comments following the pound/hash to find out
# what the script is doing.
#---------
#
# Make sure the vacation extension is used.
require "vacation";
# Define the script as a vacation script
  vacation
# Send the vacation response to any given sender only once every seven days
     no matter how many messages are sent from him.
  :days 7
#For every message sent to these addresses
  :addresses ["bob@example.com", "robert.fakeuser@server.com"]
# Make a message with the following subject
  :subject "Out of Office Reply"
# And make the body of the message the following
"I'm out of the office and will return on December 31. I won't be able to
     replay until 6 months after that. Love, Bob.";
# End of Script
```

Self-Defined Forwarding

```
#--------
# This is a sample script to illustrate how Sieve could be used
# to let users handle their own mail forwarding needs.
# Read the comments following the pound/hash to find out what the
# script is doing.
#---------
#
# No need to add any extension. 'redirect' is built-in.
# Redirect all my incoming mail to the listed address
redirect "my-other-address@example.com";
# But keep a copy of it on the IMAP server
    keep;
# End of script
```

Basic Sort and Anti-Junk Mail Filter

```
#--------
# This is a sample script to show discarding and filing.
# Read the comments following the pound/hash to find out
# what the script is doing
#---------
#
# Make sure filing and rejection are enabled
require "fileinto";
#
# If it's from my mom...
if header ["From"] :contains ["Mom"]{
# send it to my home email account
     redirect "home-address@example.com";
  }
#
# If the subject line has a certain keyword...
else if header "Subject" :contains "daffodil" {
# forward it to the postmaster
     forward "postmaster@server.edu";
  }
#
# If the junk mail filter has marked this as junk...
else if header :contains ["X-Spam-Flag"] ["YES"]{
# throw it out
     discard;
  }
#
# If the junk mail filter thinks this is probably junk
else if header :contains ["X-Spam-Level"] ["***"]{
# put it in my junkmail box for me to check
     fileinto "INBOX.JunkMail";
  }
#
# for all other cases...
else {
# put it in my inbox
     fileinto "INBOX";
  }
# End of script
```

Mail Service Maintenance

2

After setting up your mail service, there are some ongoing tasks to keep your mail service running efficiently and smoothly. The Server Admin application has a number of features that help you with these day-to-day tasks.

This chapter describes the maintenance of basic mail service, database, and mail store, including archiving. It also contains information about mail monitoring, logging, and undeliverable mail.

Starting and Stopping Mail Service

Mail service is ordinarily started automatically after you complete the Server Assistant. You can also use the Server Admin application to start and stop mail service at your discretion.

You may not want to stop mail service entirely, but instead hold outbound mail or block incoming mail connections. If you want to only partially disable mail service, see the following sections:

- "Holding Outbound Mail Service" on page 58
- "Blocking Inbound Mail Connections" on page 58

You don't have to stop and start mail service to load new settings into the mail software. If you want only new settings to take effect, see the following section:

- "Reloading Mail Service" on page 59

To start or stop mail service:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Make sure at least one of the mail protocols (SMTP, POP, or IMAP) is enabled.
5. Click Start Service or Stop Service in the menu bar.

   When the service is turned on, the Stop Service button is available.

   If you plan to turn off mail service for an extended period of time, notify users before you stop the mail service.

Holding Outbound Mail Service

You can prevent the mail service from sending new outgoing mail. You could do this to isolate a problem, or to prevent conflicts with another mail service running on your network. Furthermore, you could use this to stop virus propagation or spam relay originating with your server.

Holding the mail service isn't the same as disabling the SMTP service. Disabling would prevent all user connections for outgoing mail, while holding outbound mail service queues the mail for later sending. All mail is held in the outbound mail queue for inspection or deletion until you stop the hold.

To hold outbound mail:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Hold Outbound Mail.
5. Click Save.

Blocking Inbound Mail Connections

You can prevent the mail service from receiving new inbound mail from external servers. You could do this to isolate a problem, or to prevent conflicts with another mail service running on your network. Furthermore, you could use this to stop virus propagation or spam relay originating from external servers.

Blocking the inbound mail service isn't the same thing as disabling the SMTP service. Disabling would prevent all queued mail from being sent out, while blocking inbound mail merely stops accepting any connections to add new mail to the queue. All attempted mail deliveries are bounced and returned to sender.

To block inbound connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Block Inbound Connections.
5. Click Save.

Reloading Mail Service

Sometimes it's necessary to reload the mail server for mail service setting changes to take effect, for example, after restoring from backup, or altering the alias file. Reloading the mail service can be done without interrupting current mail service.

To reload outgoing mail service:

1. Start Terminal.
2. As root, enter the following command:

```
postfix reload
```

Changing Protocol Settings for Incoming Mail Service

You can change the settings for your incoming mail service. By choosing POP3, IMAP, or both.

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Click the General tab.
4. Enable or disable the IMAP or POP checkbooks as needed.

Improving Performance

Mail service needs to act very fast for a short period of time. It sits idle until a user reads or sends a message, then it transfers the message immediately. Therefore, it puts intense but brief demands on the server. As long as other services do not place heavy continuous demands on a server (as a QuickTime streaming server would, for example), the server can typically handle several hundred connected users.

As the number of connected mail users increases, the demand of mail service on the server increases. If your mail service performance needs improvement, try the following:

- Adjust the load mail users can put on your server by limiting the number of mail connections. For instructions, see "Enabling IMAP Access" on page 27.
- Move the mail storage location to its own hard disk or hard disk partition. For instructions, see "Specifying the Location for the Mail Database and Mail Store" on page 62.
- Run other services on a different server, especially services that place frequent heavy demands on the server. (Each server requires a separate Mac OS X Server license.)

Working With the Mail Store and Database

The mail database keeps track of messages for all mail service users. Mail service stores messages in separate files. You can do the following with the mail database and files:

- View and Repair the Mail Store Database.
- Repair User Mail Stores.
- Convert the mail database from an earlier version of Mac OS X Server.
- Specify the location where the mail database and files are stored.
- Backup and restore the mail store.

All these tasks are described in this section.

Viewing the Location for the Mail Database and Mail Store

You can view the location of the mailstore and database, as well as the total size of the mailstore. You may need to keep track of the current size of the mail store to better plan mail server resources.

You do not change the location of the mail database or mailstore here. See "Specifying the Location for the Mail Database and Mail Store" on page 62 if you want to change their locations.

To view the location of the mail store and mail database:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Select the Database tab.

Repairing the Mail Database

The mail service reads from its mailbox list database each time it tries to deliver a message to a user's inbox. Sometimes the mail server's mailbox list database can become corrupted. When mail isn't making it the correct user, or messages aren't being sent properly, the mail database may be corrupted and need to be reconstructed.

Reconstructing a database can be done while the mail server is running. However, it would be best to block incoming connections before recontructing, to make sure that incoming mail is processed according to the fresh database. For instructions on blocking incoming connections, see "Blocking Inbound Mail Connections" on page 58.

To repair a corrupted mail server database:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Select the Database tab.
4. Click Repair.

Repairing the Mail User's Account Database

The mail service updates the user's database of stored messages each time a message is added, deleted, or moved. Sometimes during these updates, the mailstore's database can become corrupted. When users report that mail messages have "disappeared" or become unreadable, the mail store database may be corrupted and need to be reconstructed. You repair an individual user's database when corruption is evident, and reconstruction only repairs the affected mailbox.

Reconstructing a database can be done while the mail server is running.

To reconstruct a corrupted user mail database:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Select the Accounts tab.
4. Select the affected user's account.
5. Click Reconstruct.

Converting the Mail Store and Database From an Earlier Version

If you have used any previous version of Apple Mail Service, you'll need to convert your users' mail messages and mail database to the current format. For example, if you're upgrading Mac OS X Server from versions 10.1 or 10.2 to 10.4, you need to migrate your mail store and database.

If you're upgrading from Mac OS X Server version 10.3 you do not need to migrate your mail installation.

To convert the mail store database:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Select the Migration tab.
4. Click Select and choose the location of the old Apple Mail Service database.

   By default the location for versions 10.1 and 10.2 was /Library/AppleMailServer.
5. Select the user account to migrate, and click Migrate User.
6. If you want to migrate all the users, simply click Migrate All.

Mail is exported to the default destination directory, creating target mailboxes as needed.

Note: To complete the mail database conversion successfully, the server must have enough available disk space. The amount of available disk space should equal the size of the database file being converted. If there's not enough disk space available, Server Admin won't convert the mail database and messages.

Specifying the Location for the Mail Database and Mail Store

If you're starting mail service for the first time and you have no existing mail database, you can specify where the mail database and message files will be stored. By default, the mail database location is /var/imap/ and the mail store location is /var/spool/imap/.

Note: Changing the mail store location of an existing mail system doesn't move the mail from the old location to the new one.

To specify where mail is stored on the server:

1. If mail service is already running, stop the mail service. See "Starting and Stopping Mail Service" on page 57 for details.

   When mail service starts for the first time, it creates an empty mail store at the default location. You can ignore this or delete it after you have specified an alternate mail storage location and restarted mail service.
2. In Server Admin, select Mail in the Computers & Services pane.
3. Click Settings.
4. Click the Advanced tab.
5. Click Database.

   You'll see the current location of the mail database and the mail store.
6. Click Change next to the Database Location field.
7. In the Database Location field, enter the path of the location where you want the mail database to be stored.

   You can browse for a location by clicking Change next to the location field.
8. In the Mail Store Location field, enter the path of the location where you want the mail files to be stored.

   You can browse for a location by clicking Browse next to the location field.

Creating Additional Mail Store Locations

Mail service can scale well as your storage needs change. You can spread the mailstore across several disks or filesystems. New partitions can be added to the mailstore at any time without requiring downtime, or even the users' knowledge.

To use the new mailstore locations, you'll have to designate in the user record which partition has his or her mail store. To do so, enter the mail store path in the user's mail settings using Workgroup Manager. See *Mac OS X Server User Management for Version 10.4 or Later* for more instructions.

The mailstore partitions you add can be additional hard disk partitions or remotely mounted file systems. For remotely mounted filesystems, NFS isn't recommended.

Note: Creating new locations doesn't automatically put mail in those locations. Edit the User records in Workgroup Manager to start delivering mail to the new partitions. Deleting a location doesn't delete the mail at that location, but makes any mail folders there inaccessible.

To split the mail store:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Click the Advanced tab.
4. Click Database.

   Listed, you'll see the current location of the mail database, and the mail store.
5. To add a location, click the Add (+) button next to the Additional Mail Store Locations box.
   a. Enter a descriptive name for the new mail store location (for example, "Marketing" or "Executive").
   b. Enter the path to the new location (such as /Volumes/mailstore2).
   c. Click OK.
6. To change a location, click the Edit (/) button next to the Additional Mail Store Locations box.
   a. Edit the path to the new location.
   b. Click OK.
7. To remove a location, select the location to be deleted and click the Remove (-) button next to the Additional Mail Store Locations box.
8. Click Save.

Backing Up and Restoring Mail Messages

You can back up the mail service data by making a copy of the mail service folder. If you need to restore the mail service data, you can replace the mail service folder with a backup copy. You can back up individual mail storage folders, or the entire mail store, as needed. One command line tool that can be used to back up your mail messages is ditto. See ditto's man page for information.

Important: Stop mail service before backing up or restoring the mail service folder. If you back up the mail service folder while mail service is active, the backup mail database file may go out of sync with the backup folder. If you restore while mail service is active, the active mail database file might go out of sync with the active folder.

An incremental backup of the mail service folder can be fast and efficient. If you back up your mail data incrementally, the only files copied are the small database file and the message files that are new or changed since the last backup.

After restoring the mail service folder, notify users that messages stored on the server have been restored from a backup copy.

An excellent source for information on backing up the mail messages can be found at: acs-wiki.andrew.cmu.edu/twiki/bin/view/Cyrus/Backup

Monitoring Mail Messages and Folders

This section describes how to perform common administrator tasks for monitoring mail messages. It shows how to:

- Designate an account as a mail administrator account.
- Save mail messages for monitoring and archival purposes.

Allowing Administrator Access to the Mail Folders

You can configure IMAP to allow the server administrator to view the mail service hierarchy. Administrators cannot view mail itself, only users' folder locations. When you connect as the IMAP administrator, you see all the user mail folders stored on the server. Each user's mailbox appears as a separate folder in your mail client. You can remove inactive mailbox folders that belonged to deleted user accounts.

To configure administrator access to the mail folders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab and select Enable IMAP, if it isn't already checked.
4. Select an existing user or create a new user using Workgroup Manger to be an IMAP administrator.
5. If you haven't created a user record for the mail administrator's account, see the user management guide.
6. Open /etc/imapd.conf in a text editor.

   If you aren't comfortable using a terminal text editor like emacs or vi, you can use TextEdit.
7. Find the line that reads "admins:"
8. Edit the line to add the UID number of the administrator account after the colon.
9. Save your changes.
10. In your email client application, create an account that uses IMAP to connect to your mail service using the mail administrator name.

    For more information, see the man page for imapd.conf.

Saving Mail Messages for Monitoring and Archival Purposes

You can configure mail service to send blind carbon copies (Bcc) of each incoming or outgoing message to a user or group that you specify. You might want to do this if you need to monitor or archive messages. Senders and receivers of mail don't know that copies of their mail are being archived.

You can set up the specified user or group to receive the blind carbon copies using POP, then set up a client email application to log in periodically and clean out the account by retrieving all new messages. Otherwise, you may want to periodically copy and archive the messages directly from the destination directory with automated shell commands. You can set up filters in the email client to highlight certain types of messages. Additionally, you can archive all messages for legal reasons.

To save all messages:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Check "Copy incoming and outgoing messages to" and type a user name or group name.
5. Click Save.

Monitoring Mail Service

This section describes how to use the Server Admin application to monitor the following:

- Overall mail service activity, including the number incoming or outgoing connected mail connections.
- Current connected mail users.
- Mail accounts.
- Mail service logs.

This section also describes how Mac OS X Server reclaims disk space used by logs and how you can reclaim space manually.

Viewing Overall Mail Service Activity

You can use Server Admin to see an overview of mail service activity. The overview reports whether the service is running, when mail service started, and incoming and outgoing connections by protocol.

To see an overview of mail service activity:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Overview button.

Viewing the Mail Connections List

The Server Admin application can list the users who are currently connected to the mail service. For each user, you see the user name, IP address of the client computer, type of mail account (IMAP or POP), number of connections, and the connection length.

To view a list of mail users who are currently connected:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Connections button.

Checking the Outgoing Mail Queue

You may need to check mail which is waiting to be sent. If you have a message backlog, or you have interrupted outbound mail, you may have a number of items in the queue. Additionally, you may want to monitor mail delivery to ensure that mail is getting delivered to both local and remote hosts.

When checking the queue, you see the message ID number, sender, recipients, date, and message size. You can select a message in the queue and further inspect the message headers.

To check the outgoing mail queue:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Click the Mail Queue tab.
4. To further inspect an individual message, select it.

Clearing Messages From the Outgoing Mail Queue

Your outgoing mail queue may have a backlog of messages. These are messages that can't be sent for any number of reasons: the message might be improperly addressed, the destination server might be unresponsive, or the destination account may be over quota. In such circumstances, you may want to clear any number of messages in the queue backlog.

To clear a message from the outgoing queue:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Click the Mail Queue tab.
4. Select the message to be deleted.
5. Click Delete.

Viewing Mail Accounts

You can use the Server Admin application to see a list of users who have used their mail accounts at least once. For each account, you see the user name, disk space quota, disk space used, and the percentage of space that's available to the user. Mail accounts that have never been used aren't listed.

To view a list of mail accounts:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Accounts button.

Viewing Mail Service Logs

The mail service maintains four logs, and you can use Server Admin to view them.

- *Mail Access:* General mail service information goes into the Server log.
- *IMAP log:* IMAP-specific activity goes into this log.
- *POP log:* POP specific activity goes into this log.
- *SMTP log:* SMTP specific activity goes into this log.
- *Mailing List logs:* Mailman's activity, including service, error, delivery failures, postings, and subscriptions.

All the logs can be further refined by using the text filter box in the window.

To view a mail service log:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Logs button.
3. Choose a log type from the Show pop-up menu.
4. Click Save.

Setting Mail Service Log Detail Level

Mail service logs can show several levels of reported detail. The three levels of detail are:

- Low (errors only)
- Medium (errors and messages)
- High (all events)

You can choose log detail for each service category (outgoing, incoming, or junk mail filter).

To set the mail service log detail:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Other tab.
4. Select the Service whose log detail you want to set.
   a. SMTP is outgoing mail and connections from external mail servers.
   b. POP/IMAP is incoming mail retrieval for users.
   c. Junk Mail/Virus log is for the junk mail service.
5. Choose a detail level from the Log Detail Level pop-up menu.
6. Click Save.

Archiving Mail Service Logs by Schedule

Mac OS X Server automatically archives mail service logs after a certain amount of time. Each archive log is compressed and uses less disk space than the original log file. You can customize the schedule to archive the logs after a set period of time, measured in days.

To archive logs by schedule:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Other tab.
4. Click "Archive Logs Every _____ Days."
5. Enter the desired number of days.
6. Click Save.

Reclaiming Disk Space Used by Mail Service Log Archives

Mac OS X Server automatically reclaims disk space used by mail service logs when they reach a certain size or age. If you're comfortable using the Terminal application and UNIX command-line tools, you can use the command-line tool "diskspacemonitor" to monitor disk space whenever you want, and delete or move the log archives. For additional information, see "diskspacemonitor" in the command-line administration guide.

Dealing With a Full Disk

Mail services become erratic and suffer from data corruption if the disk storing your mail reaches maximum capacity. When your disk reaches full capacity, you'll experience the following behaviors:

Postfix behavior

If the operating system can still spawn the smtpd process, Postfix will try to function and attempt to accept the message. The message will then be rejected with a "disk full" error. Otherwise, its behavior is unpredictable.

Cyrus behavior

If the operating system can still spawn an imapd or pop3d process, the server will attempt to open the user's mail account. Upon success, the user can access mail as normal. Any changes that require database additions and causing the database to grow can cause the process to hang and corrupt the database.

Working With Undeliverable Mail

Mail messages might be undeliverable for several reasons. You can configure your mail service to forward undeliverable incoming mail, limit attempts to deliver problematic outgoing mail, report failed delivery attempts, and change mail service timeouts to increase chances of connection success.

Incoming mail might be undeliverable because it has a misspelled address or is addressed to a deleted user account. Outgoing mail might be undeliverable because it's misaddressed or the destination mail server isn't working.

Forwarding Undeliverable Incoming Mail

You can have mail service forward messages that arrive for unknown local users to another real local person or a group in your organization. Whoever receives forwarded mail that's incorrectly addressed (with a typo in the address, for example) can forward it to the correct recipient. If forwarding of these undeliverable messages isn't explicitly enabled, the messages are returned to sender.

To set up forwarding of undeliverable incoming mail:

1. Open /etc/postfix/main.cf in a text editor.

   If you aren't comfortable using a terminal text editor like emacs or vi, you can use TextEdit.

2. Find the line that reads "luser_relay."
3. Remove the hash character ("#") at the beginning of the line, if present.
4. Edit the line to add the user name, alias, or group of the destination account after the equal sign ("=").
5. Save your changes.
6. Reload the mail server.

   For more information on reloading Postfix, see "Reloading Mail Service" on page 59.

Copy Undeliverable Incoming Mail

You can have mail service copy messages that arrive for unknown local users to another person or a group in your organization, usually the postmaster. You can use this setting to keep track of mail delivery failures such as SMTP connection rejections, misaddressed mail or determining the source of junk mail

To keep a copy of undeliverable incoming mail:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the General tab.
4. Select "Copy undeliverable messages to" and type a user name, group name, or alias.
5. Click Save.

Retrying Undelivered Outgoing Messages

Sometimes the outgoing mail queue has undelivered messages. These messages are properly addressed, but for some reason (destination server is down, the firewall was blocking the outgoing port for SMTP, etc.) the messages aren't sent. You can attempt to send them again. Normally, the mail server will attempt to retry sending all by itself, but you may want to trigger it manually instead of waiting.

To try to send an outgoing message again:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Click the Mail Queue tab.
4. Select the message to retry sending.

   Hold down the shift key or the command key to select more than one message.
5. Click Retry.

Where to Find More Information

You can find more information about mail service in books and on the Internet.

Books

For general information about mail protocols and other technologies, see these books:

- A good all-around introduction to mail service can be found in *Internet Messaging,* by David Strom and Marshall T. Rose (Prentice Hall, 1998).
- For more information on MX records, see "DNS and Electronic Mail" in *DNS and BIND,* 3rd edition, by Paul Albitz, Cricket Liu, and Mike Loukides (O'Reilly and Associates, 1998).
- Also of interest may be *Removing the Spam: Email Processing and Filtering,* by Geoff Mulligan (Addison-Wesley Networking Basics Series, 1999).
- To learn about email standards, see *Essential email Standards: RFCs and Protocols Made Practical,* by Pete Loshin (John Wiley & Sons, 1999).
- To learn more about Postfix, see *Postfix*, by Richard Blum (Sams; 1st edition, 2001)
- To learn more about Cyrus, see *Managing IMAP,* by Dianna Mullet, Kevin Mullet (O'Reilly & Associates, 2000)

Internet

There is an abundance of information about the different mail protocols, DNS, and other related topics on the Internet.

A high level overview of email systems can be found at this website:
www.wikipedia.org

Request for Comments (RFC) documents provide an overview of a protocol or service and details about how the protocol should behave. If you're a novice server administrator, you may find some of the RFC background information helpful. If you're an experienced server administrator, you'll find all the technical details about a protocol in its RFC document. You can search for RFC documents by number at this website:
www.faqs.org/rfcs

For technical details about how mail protocols work, see these RFC documents:

- *POP:* RFC 1725
- *IMAP:* RFC 2060
- *SMTP:* RFC 821 and RFC 822
- *Sieve:* RFC 3028

For more information about Postfix, go to:
www.postfix.org

For more information about Cyrus, go to:
asg.web.cmu.edu/cyrus

For more information about Sendmail, go to:
www.sendmail.org

For more information about SquirrelMail, go to:
www.squirrelmail.org

For more information about Sieve, go to:
www.cyrusoft.com/sieve

You can find out more about servers that filter junk mail at this website:
www.ordb.org

Mailing Lists

3

Mailing lists distribute a single email message to multiple recipients. Mailing lists differ from workgroups in a few fundamental ways. First, mailing lists aren't linked to file or directory permissions. Mailing lists can be administered by someone other than the workgroup or server administrator. More importantly, mailing list subscribers do not have to have any kind of account (mail or file access) on the list's server; any email address can be added to the list. Finally, list subscribers can often remove themselves from lists, and add themselves to lists.

Mac OS X Server uses Mailman version 2.1.2 for its mailing list service.

Some of Mailman's main features include (from www.list.org/features.html):

- Web-based list administration for nearly all tasks, including list configuration, moderation (post approvals), management of user accounts.
- Web-based subscribing and unsubscribing, and user configuration management. Users can temporarily disable their accounts, select digest modes, hide their email addresses from other members, and so on.
- A customizable home page for each mailing list.
- Per-list privacy features, such as closed-subscriptions, private archives, private membership rosters, and sender-based posting rules.
- Configurable (per-list and per-user) delivery mode.
- Integrated bounce detection within an extensible framework
- Automatic disposition of bouncing addresses (disable, unsubscribe).
- Integrated spam filters.
- Built-in web-based archiving, with hooks for external archivers.
- Integrated Usenet gatewaying.
- Integrated autoreplies.
- Majordomo-style email-based commands.
- Multiple list owners and moderators are possible.
- Support for virtual domains.
- Compatible with most web servers and browsers, and most SMTP servers. Requires Python 2.1.3 or newer.
- An extensible mail delivery pipeline.
- High-performance mail delivery, with a scalable architecture.

You can find more information about Mailman at the website:
www.list.org

Setting Up a Mailing List

This section describes the process of setting up a mailing list. To do this, you enable the service, define a list name, and add subscribers to the list.

When you first create a mailing list, you need to specify a master password that gives you control over all the lists. Do not use an administrator's or user's login password. Additionally, you need to specify the email addresses of other administrators who get the master password.

Enabling Mailing Lists

Before you can define mailing lists and subscribers, you need to enable the list service and create the administrator's default mailing list. When you enable mailing lists, you also create a password that allows administration of all lists on the server and automatically create a special list for mailing list administrators. Mailing list administrators get a copy of the master list password and error notifications.

Note: This list (called "Mailman") must exist in order for mailing lists to function correctly. Do not remove the master list.

To enable the mailing lists:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click Enable Mailing Lists.
5. Enter the master list password.
6. Enter the email addresses of the list administrators.

   You must enter at least one administrator who will receive notifications about the mailing list service. You can add as many as you like.
7. Click Save.

   The Mailman list is created, and sends the master password to the indicated administrators.

Creating a New Mailing List

Mailing lists distribute a single email message to multiple recipients. Once you create a mailing list, any email sent to the list's address is sent to all the subscribers on the list. Mailing lists have list administrators who can change list membership and list features. Lists can be made self-subscribing, so list administrator's don't have to add and remove subscribers; the subscribers can do so themselves.

To create a new list:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Click the Add (+) button under the Lists pane.
5. Enter the list's name.

   The list name is the email account name to which mailing list users will send their mail. The name isn't case-sensitive, and cannot contain spaces.
6. Enter the list administrator's email address.

   If you only enter a name, it must be a username on the server. If you enter a username@domain, the administrator doesn't have to be a local user.
7. Click Users May Self Subscribe, if desired.
8. Choose the default language for the list.

   You can choose English, German, Japanese, Korean, Russian, or Spanish. This setting encodes the text generated by the list appropriately for the default language.
9. Choose any additional languages supported by the list.

   This setting also encodes the text generated by the list appropriately for the default language.
10. Click OK.
11. Click Save.

Now, you can add subscribers to the list. To add subscribers, see "Adding Subscribers" on page 80.

If you have allowed users to self-subscribe, they can subscribe themselves through email or the web administration page.

Setting Maximum Message Length

You can set the maximum size message that the list accepts. You may want to disallow large attachments by setting a small maximum size, or allow file collaboration by setting an unlimited message size.

You use Server Admin to set the maximum message length.

To set a list's maximum message length:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the list whose message length you want to set.
5. Click the Edit (/) button under the Lists pane.
6. Enter the maximum message length (in KB).

   If you enter 0, the maximum length is unlimited.
7. Click OK.

Creating a Mailing List Description

Sometimes, its difficult to know what the scope and subject matter of a mailing list is from just the short list name. The list information page contains a description of the list, what subject matter it covers, and maybe even who is permitted to subscribe. These are especially good for self-subscription lists; a potential subscriber can decide whether to subscribe from the list's description.

You use the web-based interface to set the mailing list description. Web services must be enabled to access the web-based interface.

To create a list description:

1. In a web browser, enter the URL of the list administration page. This is usually: <server.domain.tld>/mailman/admin/<listname>
2. Enter the master list password, and click "Let me in."

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.
3. Make sure that General Options is selected from the Configuration Categories link section.
4. Enter a short phrase in the description text box.
5. Enter a few paragraphs about the list, its rules, and its content expectations in the info text box.
6. Click Submit Your Changes.

Customizing the Mailing List Welcome Message

When new subscribers join a mailing list, either by assignment or self-subscription, they receive an automated welcome message. The message explains where to find the list archives, and how to unsubscribe. You can customize it by adding additional text, describing the list culture and rules, or any other information you want the subscribers to have.

You use the web-based interface to set the mailing list welcome message. Web services must be enabled to access the web-based interface.

To customize a subscriber welcome message:

1. In a web browser, enter the URL of the list administration page. This is usually: <server.domain.tld>/mailman/admin/<listname>
2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.
3. Make sure that General Options is selected from the Configuration Categories link section.
4. Enable "Send welcome message to newly subscribed members."
5. Enter the text you want to include in the "List-specific text prepended..." text box.
6. Click Submit Your Changes.

Customizing the Mailing List Unsubscribe Message

When a user unsubscribes from a mailing list, either by the list administrator or unsubscribing himself, he or she receives an automated unsubscribe message. The message confirms the unsubscribing. You can customize it by adding any information you want the users to have after leaving the list.

You use the web-based interface to set the mailing list welcome message. Web services must be enabled to access the web-based interface.

To create a subscriber welcome message:

1. In a web browser, enter the URL of the list administration page.

   This is usually <server.domain.tld>/mailman/admin/<listname>
2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.
3. Make sure that General Options is selected from the Configuration Categories link section.

4 Enable "Send goodbye message to members..."

5 Enter the text you want to include in the "Text sent to people leaving the list..." text box.

6 Click Submit Your Changes.

Enabling a Mailing List Moderator

You may want to create a moderated list, where the posts must be approved by a list administrator before the post is sent to the list. You designate "list moderators," who have very limited administrative privileges. They can't change list options, but they can approve or reject subscription requests and postings.

When moderators enter their password in the list administration page, they get a page with their own moderating tasks available.

You use the web-based interface to set mailing list moderation. Web services must be enabled to access the web-based interface.

To enable list moderation:

1 In a web browser, enter the URL of the list administration page.

This is usually <server.domain.tld>/mailman/admin/<listname>

2 Enter the master list password.

This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.

3 Make sure that General Options is selected from the Configuration Categories link section.

4 Enter the list moderator addresses you want to include in the "The list moderator email addresses" text box.

5 Click Submit Your Changes.

6 Select the Password Options in the Configuration Categories link section.

7 Enter a password in the moderator password field, and confirm it.

8 Click Submit Your Changes.

Setting Mailing List Message Bounce Options

When a list message bounces and returns to the list server, you can choose how the list server handles the resulting bounce message.

You use the web-based interface to set the mailing list bounce options. Web services must be enabled to access the web-based interface.

To set bounce options:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   <server.domain.tld>/mailman/admin/<listname>

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.

3. Select Bounce Processing in the Configuration Categories link section.

4. Select the bounce processing options you want.

   In each option section there is a link to a help page which explains the option setting.

5. Click Submit Your Changes.

Designating a Mailing List as Private

You may not want to show certain lists on the web-based list access page. You can designate a list as "private" so it isn't shown at:
<server.domain.tld>/mailman/listinfo

You use the web-based interface to set a list's privacy options. Web services must be enabled to access the web-based interface.

To set privacy options:

1. In a web browser, enter the URL of the list administration page.

   This is usually <server.domain.tld>/mailman/admin/<listname>

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.

3. Select Privacy Options then Subscription Rules in the Configuration Categories link section.

4. Deselect "Advertise this list..." in the privacy list.

5. Click Submit Your Changes.

Adding Subscribers

Use Server Admin to add mailing list subscribers to a list. Mailing list subscribers need not have any kind of account (mail or file access) on the list's server; any email address can be added to the list. You must have an existing list to add a subscriber.

If the subscriber is a user on the mail server, you can use the Users and Groups button to add a local subscriber to the list.

To add subscribers:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the list to which you want to add a subscriber.
5. Click the Add (+) button under the Members pane.
6. Enter the recipient's email address.

   If you're entering multiple subscribers, enter all the recipients' email addresses or drop a text list into the User Identifiers box. If the subscribers are users on the mail server, you can use the Users and Groups button to add a local groups to the list.
7. Assign the subscriber privileges.

   Users subscribed to list: This means the user will receive mail sent to the list address.

   Users may post to list: This means the list will accept mail from the user.

   Users can administer list: This means the user has administrative privileges for the list.
8. Click OK.

Administering Mailing Lists

Mailing lists can be administered by a designated list member, called "list administrators," or "list managers." List administrators can add or remove subscribers, and can designate other list administrators. List administrators can also designate "list moderators," who have very limited administrative privileges. They can't change list options, but they can approve or reject subscription requests and postings.

Mailman uses a web-based interface as well as email-based administration. Web services must be enabled to access the web-based interface. There are dozens of configuration options available for Mailman mailing lists that are not accessible using Server Admin. Web-based administration interface is found at:
<server.domain.tld>/mailman/listinfo

Information and access to a specific list is found at:
<server.domain.tld>/mailman/listinfo/<listname>

For documentation of these functions for users, list administrators, and server administrators, see:
www.list.org/docs.html

Viewing a Server's Mailing Lists

You can view public (non-private) lists which are being run on a server. This is viewed through the server's web-based information portal. Web services must be enabled to access the web-based interface.

To see the lists:

- Open a web browser, and enter the list's URL.
<server.domain.tld>/mailman/listinfo

Viewing a Mailing List's Information Page

Each list has an information page on the server which shows some basic information about the list, how to post to it, how to subscribe to it, and how to access your own subscription preferences. You access the list information page with a web browser.

Web services must be enabled to access the web-based interface.

To see the list's information page:

- Open a web browser, and enter the list's URL.
<server.domain.tld>/mailman/listinfo/<listname>

Designating a List Administrator

When you set up a list, you designate at least one user to administer the mailing list. This administrator has access to the other list settings pages for all the lists on the server. You can designate more than one list administrator, and change any subscriber to or from being a list administrator. You can add remove or change the list administrator using these instructions.

List administrators do not have to be users (neither administrator nor regular) on the server. They are listed as email addresses. Giving list administrator privileges to a subscriber does not give them any other privileges on the mailing list server besides making and removing lists, and editing list preferences.

To designate a list administrator:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list which has the subscriber to be given list administrator privileges.

   If the user isn't already subscribed to the list, you'll have to add him first. See "Adding Subscribers" on page 80 for more information.
5. Select the desired subscriber.
6. Check or uncheck "Admin" in the subscriber list, as desired.
7. Click OK.

Accessing Web-based Administrator Options

List administrators need to set preferences for mailing list behavior, and view pending moderation requests for mailing lists are being run on a server. These tasks and many more are accomplished through the server's web-administration portal. Web services must be enabled to access the web-based interface.

Server Admin does not give access to the incredible range of preferences available for a mailing list. List administrators are encouraged to use the web-based interface for all but the most basic setup tasks. Information about what options are available via the web interface can be found at:
www.list.org/docs.html

To access a list's web-based options:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   <server.domain.tld>/mailman/admin/<listname>
2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.
3. Change list settings as desired.

Designating a List Moderator

When you set up a list, you can designate another user to moderate the list.

To designate a list moderator:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the list which has the desired subscriber.
5. Click the Edit (/) button under the Lists pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Uncheck or check "User can administer the list" as necessary.
7. Click OK.

Archiving a List's Mail

All the messages sent to a mailing list can be archived and browsed at a later time. The messages are group into archival volumes by time and date. You can choose whether a list's archive is accessible by nonsubscribers, and how often the archives are updated. By default, the archives are found at:
<server.domain.tld>/pipermail/<listname>

You use the web-based interface to set the mailing list archive preferences. Web services must be enabled to access the web-based interface.

To archive a list's mail:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   <server.domain.tld>/mailman/admin/<listname>
2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.
3. Select "Archiving Options" from the Configuration Categories section.
4. Select Yes next to "Archive messages?"
5. Select whether the archive will be public or private.
6. Select how often to start a new archive volume.
7. Click Submit Your Changes.

Viewing Mailing List Archives

If the list administrator has enabled message archiving, you can access and search the archived messages.

To view a list's archives:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/archives/<listname>

2. Select the year and month of the archive you'd like to browse.

Working With Mailing List Subscribers

After a list is created, you can add or remove people from an existing list. You may want to give list administration privileges to a user, or change a user's ability to receive or post to the list.

Adding a Subscriber to an Existing List

This is the same procedure as adding a user to a newly created list.

To add a subscriber to an existing list:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the List to which you want to add a subscriber.
5. Click the Add (+) button under the Members pane.
6. Enter the recipient's email address.

   The email address must match the return address of the recipient to post messages without administrator approval.

   If a user was added via the "Users and Groups" button, the email address in the list will be in the form of "user@server.domain.com". If necessary, change the email address in the mailing lists panel of Server Admin to match the return address used by the client.
7. Assign the subscriber privileges.
8. Click OK.

Removing a List Subscriber

You can remove a subscriber from a mailing list, either forcibly or by request.

To remove a list subscriber:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the list from which you want to remove a subscriber.
5. Select the subscriber from the User pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Click the Remove (-) button under the Members pane.
7. Confirm the delete.

Changing Subscribers' Posting Privileges

Sometimes you may want an "announce only" list, where recipients can't post to the address.

To add or remove a subscriber's posting privileges:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the List which has the desired subscriber.
5. Click the Edit (/) button under the Lists pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Uncheck or check "User can post to list" as necessary.
7. Click OK.

Suspending a Subscriber

You can keep a user on a mail list and still allow him or her to post to a list without receiving the list messages. In this case, you can temporarily suspend a user's subscription to a list.

To suspend a user's subscription to a list:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Lists tab.
4. Select the List which has the desired subscriber.
5. Click the Edit (/) button under the Lists pane.

   Hold down the Shift or Command key to select multiple subscribers.

6 Uncheck or check "User subscribes to list" as necessary.

7 Click OK.

List Subscriber's Options

A subscriber can customize certain aspects of their mailing list subscriptions. Without being designated a "list administrator," or having any user privileges on the server, the user has control of a number of aspects of his or her subscriptions.

The following section gives instructions on a few common settings that your users may want to customize. A full list of possible configurable options, and instructions for use can be found on Mailman's documentation page:
www.list.org/docs.html

Subscribing to a Mailing List Via Email

You can subscribe to lists using email. You send a message to the list subscription address. Depending on the list's settings, you may have to confirm your subscription or wait for moderator approval. In any case, you do not have to subscribe via email and via the web. Just one will suffice.

You can subscribe only yourself, if the list allows self-subscription.

To subscribe via email:

1 Open your email mail program which sends from the address you want to subscribe.

2 Send an email message to the list subscription address, which will usually be:

LISTNAME-join@DOMAIN

The subject and body of the message will be ignored.

1 Open your email mail program which sends from the address you want to subscribe.

2 Send an email message to the list subscription address, which will usually be:

LISTNAME-join@DOMAIN

The subject and body of the message will be ignored.

Subscribing to a Mailing List Via Web

You can subscribe to lists using the web interface. You go to the information page for the list and provide your email address and a password for your list preferences. Depending on the list's settings, you may have to confirm your subscription or wait for moderator approval. In any case, you do not have to subscribe via the web and via email. Just one will suffice.

You can subscribe only yourself, if the list allows self-subscription.

To subscribe via web:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address and name (the name is optional)

3. Choose a password for use with the list, and enter it twice to confirm it.

   This should not be a login password, or used for any other purpose than for list option administration. It will occasionally be mailed to you in plain text.

4. Select your digest message mode preference.

   If you choose to receive a daily digest, instead of getting each list posting separately, you will get one daily post.

   If you want to change your digest mode after you've subscribed, see "Toggling Digest Mode" on page 89.

5. Click Subscribe.

Unsubscribing From a Mailing List Via Email

Unsubscribing from a mailing list is a similar process to Subscribing to a Mailing List Via Email. Depending on the list's settings, you may have to confirm your subscription removal or wait for moderator response.

To unsubscribe via email:

1. Open your email mail program which sends from the address which receives the mailing list posts.

2. Send an email message to the list subscription address, which will usually be:

   LISTNAME-leave@DOMAIN

   The subject and body of the message will be ignored.

3. Follow the directions in the confirmation email.

Unsubscribing From a Mailing List Via Web

Unsubscribing from a mailing list via the web is a similar process to Subscribing to a Mailing List Via Web. Depending on the list's settings, you may have to confirm your subscription removal or wait for moderator response.

To unsubscribe via web:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Click Unsubscribe.

Setting and Changing a Your Mailing List Password

Your mailing list password is used to alter your preferences for any given list. The password should not be a valuable one. It is sent in plain text as a reminder periodically from the lists you are subscribed to.

To setting or change your password:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Enter your password, and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via email or were subscribed via Server Admin, your password is blank.

4. Find the password section of the subscription page.

5. Enter a new password in the indicated field, and enter it again to confirm it.

   If you want to change your password for all the lists that you belong to on this server, select Change Globally.

6. Click Change My Password.

Disabling List Mail Delivery

You may wish to temporarily disable delivery of mailing list messages; for example, you may want to avoid excess mail while on vacation.

To disable list delivery:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Enter your password, and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via email or were subscribed via Server Admin, your password is blank.

4. In the Mail Delivery section, select Disabled.

   If you want to disable delivery for all the lists that you belong to on this server, select Change Globally.

5. Click Submit My Changes.

Toggling Digest Mode

Digest mode sends only one message per day regardless of list mail volume. You can switch between getting each message, or a single digest message.

If your list delivery has digest mode *On* you will receive a single digest message per day.

To toggle digest mode:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Enter your password, and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via email or were subscribed via Server Admin, your password is blank.

4. In the Set Digest Mode section, select whether or not you want a daily digest by clicking On or Off.

5. Click Submit My Changes.

Toggle MIME or Plain Text Digests

If you subscribe to a mailing list and receive digests (a single email with all of the days postings in it), you can choose whether to receive them as a MIME digest (a collection of individual posts) or a plain text digest (one message with the text of all the posts).

To toggle message types:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Enter your password, and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via email or were subscribed via Server Admin, your password is blank.

4. In the Get MIME Or Plain Text Digests section, select the desired digest type.

   If you want to set the digest type for all the lists that you belong to on this server, select Change Globally.

5. Click Submit My Changes.

Setting Additional Subscriber Options

Subscribers can change other list membership options including their:

- Email address
- Name on the list
- Posting acknowledgments
- Message copy handling

These options are available on your subscription options page.

To access these other options:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   <server.domain.tld>/mailman/listinfo/<listname>

2. In the Subscriber section of the web page, enter your email address, and click Unsubscribe Or Edit Options.

3. Find the option you want to change and follow the instructions on screen.

Where to Find More Information

Mailman's features and its capabilities, can be found at:
www.list.org

You will also find the following information at www.list.org/docs.html:

- Web-based administration and subscriber commands
- Email based administration and subscriber commands
- Frequently Asked Questions lists.

Certificates and Security

Mac OS X Server supports many services which use SSL to ensure encrypted data transfer. It uses a Public Key Infrastructure system to generate and maintain certificates of identity for use with SSL-enabled services.

Understanding Public Key Infrastructure

Public Key Infrastructure (PKI) systems allow the two parties in a data transaction to be authenticated to each other, and to use encryption keys and other information in identity certificates to encrypt and decrypt messages traveling between them.

PKI enables multiple communicating parties to establish confidentiality, message integrity and message source authentication without having to exchange any secret information in advance.

SSL (Secure Socket Layer) technology relies on a PKI system for secure data transmission, and user authentication. It creates an initial secure communication channel to negotiate a faster, secret key transmission. Mac OS X Server uses SSL to provide data encrypted data transmission for mail, web, and directory services.

The following sections contain more background information about key aspects of PKI:

- "Public and Private Keys"
- "Certificates"
- "Certificate Authorities (CA)"
- "Identities"

Public and Private Keys

Within a PKI, two digital keys are created: the public key, and the private key. The private key isn't meant to be distributed to anyone, and is often encrypted itself by a passphrase. The public key, on the other hand, is distributed to other communicating parties. Basic key capabilities can be summed up as:

Key Type	Capabilities
Public Keys	• Can encrypt messages that can only by decrypted by the holder of the corresponding Private key. • Can verify the signature on a message originating as coming from a Private key.
Private Keys	• Can digitally sign a message or certificate, claiming authenticity. • Can decrypt messages which were encrypted with the Public key. • Can encrypt messages which can only be decrypted by the Private key, itself.

Web, Mail, and Directory Services use the public key with SSL to negotiate a shared key for the duration of the connection. For example, a Mail server will send its public key to a connecting client and initiate negotiation for a secure connection. The connecting client uses the public key to encrypt a response to the negotiation. The mail server, since it has the private key, can decrypt the response. The negotiation continues until both the mail server and the client have a shared secret to encrypt traffic between the two computers.

Certificates

Public keys are often contained in certificates. A user can digitally sign messages using his private key, and another user can verify the signature using the public key contained in signer's certificate which was issued by a Certificate Authority (CA) within the PKI.

A public key certificate (sometimes called an "identity certificate") is a file in a specified format (Mac OS X Server uses the x.509 format) which contains:

- The public key half of a public-private key pair.
- The key user's identity information, such as a person's name and contact information.
- A validity period (how long the certificate can be trusted to be accurate).
- The URL of someone with the power to revoke the certificate (its "revocation center").
- The digital signature of either a CA, or the key user himself.

Certificate Authorities (CA)

A Certificate Authority (CA) is an entity which signs and issues digital identity certificates claiming trust of the identified party. In this sense, it's a trusted third party between two transactions.

In x.509 systems, CAs are hierarchical in nature, with CAs being certified by CAs, until you reach a "root authority." The hierarchy of certificates is always a top-down, with a root authority's certificate at the top. A root authority is a CA that's trusted by enough or all of the interested parties, so that it doesn't need to be authenticated by yet another trusted third party.

A CA can be a company that, for a fee, signs and issues a public key certificate which states that the CA attests that the public key contained in the certificate belongs to its owner, as recorded in the certificate. In a sense, CA is a "digital notary public." One applies to the CA for a certificate by providing identity and contact information, as well as the public key. A CA must check an applicant's identity, so that users can trust certificates issued by that CA to belong to the identified applicant.

Identities

Identities, in the context of the Mac OS X Server Certificate Manager, are the combination of a signed certificate for both keys of a PKI keypair. The identities are used by the system keychain, and are available for use by various services that support SSL.

Self-Signed Certificates

Self-signed certificates are certificates that are digitally signed by the private key of the keypair included in the certificate. This is done in place of a CA signing the certificate. By self-signing a certificate, you're attesting that you are who you say you are. No trusted third party is involved.

Certificate Manager in Server Admin

Mac OS X Server's Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services.

Certificate Manager provides integrated management of SSL certificates in Mac OS X Server for all services that allow the use of SSL certificates.

The Certificate Manager allows creation of self-signed certificates, and certificate-signing requests (CSRs), to obtain a certificate signed by a CA. The certificates, either self-signed, or signed by a CA, are accessible by the services that support SSL.

Identities that were previously created and stored in OpenSSL files can also be imported into the Certificate Manager, and are then accessible to all the services that support SSL.

The Certificate Manager in Server Admin doesn't allow you to sign and issue certificates as a CA, nor does it allow you to sign and issue certificates as a root authority. If you need any of these functions, you can use Apple's CA Assistant in /Applications/Utilities/. It allows these functions, and others. Self-signed and CA-issued certificates created in Apple's CA Assistant can be used in the Certificate Manager, by importing the certificate.

The Certificate Manager displays the following for each certificate:

- The domain name for which the certificate was issued.
- Its dates of validity.
- Its signing authority (such as the CA entity or if the certificate is self-signed, it reads "Self-Signed"

Readying Certificates

Before you can use SSL in Mac OS X Server's services, the certificates must be created or imported. You can create your own self-signed certificate, generate a Certificate Signing Request (CSR) to send to a CA, or import a certificate previously created with OpenSSL.

Requesting a Certificate From a CA

The manager helps you create a certificate signing request (CSR) to send to your designated CA.

To request a signed certificate:

1. In Server Admin, select the server which has services that support SSL.
2. Click Settings.
3. Select the Certificates tab.
4. Click the Add (+) button.
5. Fill out identity information.

   The common name is the fully qualified domain name of the server which will use SSL-enabled services.
6. Enter starting and ending validity dates.
7. Select a private key size (1024 bits is the default).
8. Enter a passphrase for the private key.
9. This passphrase should be more secure than a normal password.

   It is recommended you use at least 20 characters, include mixed case, numbers and/or punctuation, have no characters repeat, and having no dictionary terms.
10. Click "Request Signed Certificate...."
11. Follow the onscreen directions for requesting a signed certificate from your chose CA.

    For example, you may need to do it online or enter the email address.

12 Click Send Request.

13 Click Save.

14 When the CA replies to the email, it will include it in the text of an email.

15 Make sure the Identity is open from the Certificates tab, again.

16 Click Add Signed Certificate.

17 Copy the characters from "==Begin CSR==" to "==End CSR==" into the text box.

18 Click OK.

19 Click Save.

Creating a Self-Signed Certificate

Whenever you create an identity in the Certificate Manager, you're creating a self-signed certificate. Certificate Manager creates a private–public key pair in the system keychain with the key size specified (512 - 2048 bits). It then creates the corresponding self-signed certificate in the system keychain.

A Certificate Signing Request (CSR) is also generated at the same time that the self-signed certificate is created. This isn't stored in the keychain, but is written to disk at /etc/certificates/cert.common.name.tld.csr, where "common.name.tld" is the Common Name of the certificate that was issued.

To create a self-signed certificate:

1 In Server Admin, select the server which has services that support SSL.

2 Click Settings.

3 Select the Certificates tab.

4 Click the Add (+) button.

5 Fill out identity information.

The common name is the fully qualified domain name of the server which will use SSL-enabled services.

6 Enter starting and ending validity dates.

7 Select a private key size (1024 bits is the default).

8 Enter a passphrase for the private key.

9 This passphrase should be more secure than a normal password.

It is recommended you use at least 20 characters, include mixed case, numbers and/or punctuation, have no characters repeat, and having no dictionary terms.

10 Click Save.

Importing a Certificate

You can import a previously generated OpenSSL certificate and private key into Certificate Manager. The items are stored as available in the list of identities, and available to SSL-enabled services.

To import an existing OpenSSL style certificate:

1. In Server Admin, select the server which has services that support SSL.
2. Click Settings.
3. Select the Certificates tab.
4. Click the Import button.
5. Enter the existing certificate's file name and path.

   Alternately, browse for it's location.
6. Enter the existing private key file's name and path.

   Alternately, browse for it's location.
7. Enter the private key passphrase.
8. Click Import.

Managing Certificates

Once created and signed, you shouldn't have to do much more with the certificates. They are only editable in Server Admin, and cannot be changed once a CA signs the certificate. Self-signed certificates can be changed. Certificates should be deleted if the information they possess (contact information, etc.) is no longer accurate, or you believe the keypair has been comprimised in some way.

Editing a Certificate

Once the certificate signature of a CA is added, it can't be edited.

A self-signed certificate can be edited. All the fields of the certificate (including domain name and private key passphrase, private key size, etc.) can be modified. If the identity was exported to disk from the system keychain, it will have to be re-exported.

To edit a certificate:

1. In Server Admin, select the server which has services that support SSL.
2. Click Settings.
3. Select the Certificates tab.
4. Select the Certificate Identity to edit.

   It must be a self-signed certificate.
5. Click the Edit (/) button.
6. Click Save.

Deleting a Certificate

When a certificate has expired, or been compromised, you'll need to delete it.

To delete a certificate:

1. In Server Admin, select the server which has services that support SSL.
2. Click Settings.
3. Select the Certificates tab.
4. Select the Certificate Identity to delete.
5. Click the Remove (-) button.
6. Click Save.

Using The Certificates

In Server Admin, the various services like Web, Mail, and so on will display a pop-up list of certificates that the administrator can choose from. The services themselves vary in appearance and therefore pop-up list location. Consult with the administrator's guide for the service you're trying to use with a certificate.

Glossary

This glossary defines terms and spells out abbreviations you may encounter while working with online help or other Mac OS X Server Documentation. References to terms defined elsewhere in the glossary appear in *italics*.

access control A method of controlling which computers can access a network or network services.

access control list See **ACL**.

access privileges See **permissions**.

ACL A list maintained by a system that defines the rights of users and groups to access resources on the system.

address A number or other identifier that uniquely identifies a computer on a network, a block of data stored on a disk, or a location in a computer memory. See also **IP address**, **MAC address**.

alias Another email address at your domain that redirects incoming email to an existing user.

alphanumeric Containing characters that include letters, numbers, and punctuation characters (such as _ and ?).

APOP authentication An extension to the POP3 mail protocol. It ensures that the username and password are encrypted before being used to authenticate to a mail server.

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.

back up (verb) The act of creating a backup.

backup (noun) A collection of data that's stored for purposes of recovery in case the original copy of data is lost or becomes inaccessible.

bit A single piece of information, with a value of either 0 or 1.

byte A basic unit of measure for data, equal to eight bits (or binary digits).

canonical name The "real" name of a server when you've given it a "nickname" or alias. For example, mail.apple.com might have a canonical name of MailSrv473.apple.com.

certificate Sometimes called an "identity certificate" or "public key certificate." A file in a specific format (Mac OS X Server uses the x.509 format) that contains the public key half of a public-private keypair, the user's identity information such as name and contact information, and the digital signature or either a *Certificate Authority* (CA) or the key user.

Certificate Authority An authority that issues and manages digital certificates in order to ensure secure transmission of data on a public network. See also **public key infrastructure** and **certificate**.

certification authority See **Certificate Authority**.

character A synonym for byte.

cleartext Data that hasn't been encrypted.

client A computer (or a user of the computer) that requests data or services from another computer, or server.

command line The text you type at a shell prompt when using a command-line interface.

command-line interface A way of interfacing with the computer (for example, to run programs or modify file system permissions) by entering text commands at a shell prompt.

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 hostname*.

cracker A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to hacker.

decryption The process of retrieving encrypted data using some sort of special knowledge. See also **encryption**.

digital signature An electronic signature that can be used to verify the identity of the sender of a message.

directory Also known as a folder. A hierarchically organized list of files and/or other directories.

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

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."

domain name See **DNS name**.

Domain Name System See **DNS**.

encryption The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications. See also **decryption**.

Ethernet A common local area networking technology in which data is transmitted in units called packets using protocols such as TCP/IP.

Ethernet ID See **MAC address**.

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.

full name See **long name**.

GB Gigabyte. 1,073,741,824 (2^{30}) bytes.

gigabyte See **GB**.

hacker An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

host Another name for a server.

host name A unique name for a server, historically referred to as the UNIX hostname. The Mac OS X Server host name is used primarily for client access to NFS home directories. A server determines its host name by using the first name available from the following sources: the name specified in the /etc/hostconfig file (HOSTNAME=some-host-name); 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 multicast DNS *local hostname*; the name "localhost."

identity certificate See **certificate**.

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.

Internet Message Access Protocol See **IMAP**.

Internet Protocol See **IP**.

Internet service provicer See **ISP**.

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.

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.

IPv4 See **IP**.

IPv6 Internet Protocol version 6. The next-generation communication protocol to replace IP (also known as IPv4). IPv6 allows a greater number of network addresses and can reduce routing loads across the Internet.

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

KB Kilobyte. 1,024 (2^{10}) bytes.

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.

kilobyte See **KB**.

LDA Local delivery agent. A mail service agent that transfers mail messages from incoming mail storage to the email recipient's inbox. The LDA is responsible for handling local delivery of messages and for making mail accessible to the user's email application.

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

Lightweight Directory Access Protocol See **LDAP**.

list administrator A mailing list administrator. List administrators can add or remove subscribers from a mailing list and designate other list administrators. List administrators aren't necessarily local machine or domain administrators.

local area network See **LAN**.

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

local hostname A name that designates a computer on a local subnet. It can be used without a global DNS system to resolve names to IP addresses. It consists of lowercase letters, numbers, or hyphens (except as the last characters), and ends with ".local" (e.g, bills-computer.local). Although the name is derived by default from the computer name, a user can specify this name in the Network pane of System Preferences. It can be changed easily, and can be used anywhere a DNS name or fully qualified domain name is used. It can only resolve on the same subnet as the computer using it.

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

MAA Mail access agent. A mail service that communicates with a user's email program to download mail message headers to the user's local computer.

MAC address Media access control address. A hardware address that uniquely identifies each node on a network. For AirPort devices, the MAC address is called the AirPort ID.

Mac OS X The latest version of the Apple operating system. Mac OS X combines the reliability of UNIX with the ease of use of Macintosh.

Mac OS X Server An industrial-strength server platform that supports Mac, Windows, UNIX, and Linux clients out of the box and provides a suite of scalable workgroup and network services plus advanced remote management tools.

mail access agent See **MAA**.

mail exchange record See **MX record**.

mail host The computer that provides your mail service.

mail transfer agent See **MTA**.

mail user agent See **MUA**.

mailing list A mail service used to distribute a single email message to multiple recipients. Mailing list subscribers do not have to be mail users on your mail server. Mailing lists can be administered by someone other than a workgroup or server administrator. Mailing list subscribers can often add or remove themselves from lists.

MB Megabyte. 1,048,576 (2^{20}) bytes.

megabyte See **MB**.

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.

MUA Mail user agent. A mail process on a user's local computer that works with the MAA to download mail messages and headers to the user's local computer. This is most commonly referred to as an email application, or email program.

MX record Mail exchange record. An entry in a DNS table that specifies which computer manages mail for an Internet domain. When a mail server has mail to deliver to an Internet domain, the mail server requests the MX record for the domain. The server sends the mail to the computer specified in the MX record.

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**.

node A processing location. A node can be a computer or some other device, such as a printer. Each node has a unique network address. In Xsan, a node is any computer connected to a storage area network.

open relay A server that receives and automatically forwards mail to another server. Junk mail senders exploit open relay servers to avoid having their own mail servers blacklisted as sources of junk mail.

Open Relay Behavior-modification System See **ORBS**.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

ORBS Open Relay Behavior-modification System. An Internet service that blacklists mail servers known to be or suspected of being open relays for senders of junk mail. ORBS servers are also known as "black-hole" servers.

permissions Settings that define the kind of access users have to shared items in a file system. You can assign four types of permissions to a share point, folder, or file: read/write, read-only, write-only, and none (no access). See also **privileges**.

plaintext Text that hasn't been encrypted.

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.

port A sort of virtual mail slot. A server uses port numbers to determine which application should receive data packets. Firewalls use port numbers to determine whether or not data packets are allowed to traverse a local network. "Port" usually refers to either a TCP or UDP port.

Post Office Protocol See **POP**.

private key One of two asymmetric keys used in a PKI security system. The private key is not distributed and usually encrypted with a passphrase by the owner. It can digitally sign a message or certificate, claiming authenticity. It can decrypt messages encrypted with the corresponding public key. Finally, it can encrypt messages that can only be decrypted by the private key.

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

public key One of two asymmetric keys used in a PKI security system. The public key is distributed to other communicating parties. It can encrypt messages that can be decrypted only by the holder of the corresponding private key, and it can verify the signature on a message originating from a corresponding private key.

public key certificate See **certificate**.

public key cryptography A method of encrypting data that uses a pair of keys, one public and the other private, that are obtained from a certification authority. One key is used to encrypt messages, and the other key to decrypt them.

public key infrastructure A secure method of exchanging data over an unsecure public network, such as the Internet, by using public key cryptography.

queue An orderly waiting area where items wait for some type of attention from the system. See also **print queue**.

RBL Real-time black-hole list. An Internet service that blacklists mail servers known to be or suspected of being open relays for senders of junk mail.

real-time black-hole list See **RBL**.

record type A specific category of records, such as users, computers, and mounts. For each record type, a directory domain may contain any number of records.

relay In QuickTime Streaming Server, a relay receives an incoming stream and then forwards that stream to one or more streaming servers. Relays can reduce Internet bandwidth consumption and are useful for broadcasts with numerous viewers in different locations. In Internet mail terms, a relay is a mail SMTP server that sends incoming mail to another SMTP server, but not to its final destination.

relay point See **open relay**.

round robin An Xsan storage pool allocation strategy. In a volume consisting of more than one storage pool, Xsan allocates space for successive writes to each available pool in turn.

Secure Sockets Layer See **SSL**.

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

Simple Mail Transfer Protocol See **SMTP**.

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.

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.

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

TB Terabyte. 1,099,511,627,776 (2^{40}) bytes.

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.

terabyte See **TB**.

UCE Unsolicited commercial email. See **spam**.

UDP User Datagram Protocol. A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

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

virtual domain Another domain that can be used in email addresses for your mail users. Also, a list of all the domain names for which your mail server is responsible.

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

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.

wide area network See **WAN**.

wildcard A range of possible values for any segment of an IP address.

Index

S

T

U

V