Administrator's Guide

Netscape Messaging Server

Version 3.0

Version 3.0

Printed in USA
98 97 96 10 9 8 7 6 5 4 3 2 1

Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, CA 94043

Contents

Introduction 11
What's new in Messaging Server 3.0 11
Lightweight Directory Access Protocol 12
Authenticated SMTP 12
IMAP encryption and authentication 12
Remote network management 13
Message quotas 13
Single copy message store 13
Delivery status notification 13
Netscape Messaging Server plug-in API 14
About this guide 14
About the other guides 15
Conventions used in this guide 15
Pathname conventions 17

Chapter 1 Working with users and groups 19
Using the Administration Server 20
Starting and stopping the Administration Server 20
Accessing the Administration Server 21
Using the Server Administration page 21
Using the Messaging Server manager 22
What are email accounts? 22
Working with user and group forms 23
Managing user accounts 24
About the Mail User Information form 24
Primary Email Address field 24
Alternate Email Addresses field 25
Messaging Server field 26

Delivery Options fields 26
Auto-Reply Mode field 27
Auto-Reply Text field 28
Personal Description field 28
Managing group accounts 28
About the Mail Group Information form 29
Primary Email Address field 29
Alternate Email Addresses field 30
Send Errors To field 30
Messaging Server field 31
List of CC Recipients field 31
LDAP Criteria for Generating CC List field 31
Maximum Message Size field 32
Allowed Sender Domains field 32
Allowed Senders field 33
Rejection Notice field 33
Required and recommended groups 33
Required group: Postmaster 33
Recommended groups 34
Starting and stopping the Messaging Server 35

Chapter 2 Working with system settings 37
The Messages form 38
Host Finger Information field 38
Default Vacation-Mode Reply Message field 38
Default Echo-Mode Reply Message field 39
Default Reply-Mode Reply Message field 39
'Quota Exceeded' Message field 39
The SMTP Channel Aliases form 40
Setting up an SMTP channel alias 41
The SMTP Channel Options form 42
Maximum Number of MTA Hops field 43
Defer Delivery to remote hosts field 43

Verify each recipient's address field 43
SMTP Mail Routing Table field 44
Example: 45
Unknown Local Account, Maximum MTA Hops Exceeded, and Disk Quota Exceeded fields 45
The System Configuration form 46
Address Completion Domain field 46
Local Mail Domains field 47
Queued Mail Processing Interval field 47
Maximum Mail Queue Time field 47
Lookup Client Machine Names field 48
Default Maximum Number of Concurrent Network Servers field 48
Default Maximum Number of Concurrent Local Processes field 48
Minimum Free Disk Space field 49
Default User Disk Quota field 49
Recommended Account Management URL for Mail Users field 49
The Single Copy On/Off form 49
The Message Stores form 50
The Unix Mail form 50

Chapter 3 Ensuring a secure messaging system 53
System security 53
Runtime permissions 54
Access domains 55
Access domain algorithm 56
Encryption forms 57
The IMAP Encryption and Authentication form 57
The Security Preferences form 58

Chapter 4 Server status and reports 61
SNMP configuration and control 62
The SNMP Configuration form 62

Master Host field 63
Organization field 63
Location field 63
Contact field 63
SNMP Statistics Collection options 63
The SNMP Subagent Control form 63
Server logs and reports 64
The List of Queued Mail form 64
The Logging Preferences form 65
Log Directory field 65
The View Logs report 67
Error messages 67
Notification messages 67
Error-Handler Action form 68

Appendix A Messaging Server architecture 71
The dispatcher 72
The module configuration database 73
The message transfer agent 73
Message channels 74
The components of a message channel 74
The SMTP channel 75
Switching messages between channels 76
The local delivery channel 77
POP3 or IMAP4 delivery 78
Unix delivery 79
Program delivery 79
The message transfer agent handlers 79
The account handler 80
The error handler 81

The AutoReply utility 81
Directory databases 82
The Messaging Server finger service 82

Appendix B Compatibility with sendmail 83
Functional compatibility 83
SMTP network interface 84
Incoming mail 84
Outgoing mail 84
Aliases and mail forwarding 84
Delivery to programs 85
Delivery to files 85
Mailing lists 86
Command-line compatibility 86
Sending mail with the sendmail replacement 86
Starting the Messaging Server with sendmail 87
Checking the mail queue 87
Other modes 88
Sendmail replacement program reference 88
Alternate names for sendmail 88
Options for sendmail 91

Appendix C Program delivery 93
About program delivery 93
Program delivery terminology 94
Trusted and untrusted operating modes 96
Configuring for program deliveries 98
Enabling the program delivery module 98
Removing the **NO-PROGRAM-DELIVERIES** file 99
The program delivery module 99
Setting up the trusted program directory 99
Setting up the list of valid shells 100

Disabling the program delivery module 100
Program deliveries through the
New User form 101
Program deliveries and the Unix form 101

Appendix D Command-line operations and utilities 103
Command-line operations 103
Starting the system 103
Shutting down the system 104
Checking the mail queue 104
Delivering mail in the queue 105
Command-line utilities 105
CheckPO 105
Synopsis 105
Description 105
Options 106
DelMbx 109
Synopsis 109
Description 110
MoveUser 110
Synopsis 110
Description 110
Requirement 111
Components of LDAP URL 111
bindDN 112
bindDN password 112
Examples 112
MTA-migrate 113
Migration to an LDAP Directory Server 115
Migration to a Local directory database 116
Preview mode in MTA-migrate 116
Customization of distinguished name 117
Migration from 2.x post office 117
Migration from 2.x mailbox 118

Migration in stages 118
MTA-migrate examples 119

Glossary 121

Index 127

Introduction

Welcome to Netscape Messaging Server. Netscape Messaging Server is an open, standards-based client-server messaging system that lets users easily exchange information within a company as well as across the Internet. Controlled by forms accessed through the World Wide Web (WWW), Netscape Messaging Server lets server administrators manage Messaging Server functions with the easy-to-use Netscape Navigator interface from any desktop in the network. It addresses the major security vulnerabilities associated with email systems and delivers superior performance. Because the messaging server is based on Internet open standards (such as SMTP, POP3, IMAP4, LDAP, and MIME), you avoid costly dependence on proprietary solutions and are assured of maximum compatibility with other systems.

What's new in Messaging Server 3.0

Netscape Messaging Server 3.0 offers a variety of new features designed to enhance your electronic mail (email) system:

- Lightweight Directory Access Protocol (LDAP) support
- authenticated Simple Mail Transfer Protocol (SMTP) support
- Internet Message Access Protocol (IMAP) encryption and authentication
- remote network management through Simple Network Management Protocol (SNMP) support
- message quotas
- single copy message store
- delivery status notification
- Netscape Messaging Server API

Lightweight Directory Access Protocol

Netscape Messaging Server 3.0 supports the *Lightweight Directory Access Protocol (LDAP)* standard, allowing the Messaging Server to integrate with local or centralized directory services flexibly. A centralized directory service gives server administrators a single point where they can add, change, and delete users. And that user information can be shared across all Netscape SuiteSpot Servers, including Netscape Messaging Server.

Netscape Messaging Server employs LDAP user address information for message routing and address resolution. It also takes advantage of LDAP search capabilities, allowing you to create criteria-based mail groups. That is, you can define a mail group by indicating the criteria you want to use to define a mail group—for example, a group composed of all users who belong to a particular organizational unit.

For users, LDAP means controlling their own account information, including passwords, automated replies, and automated message forwarding, thereby reducing administration costs.

Authenticated SMTP

Netscape Messaging Server 3.0 supports authenticated *Simple Mail Transfer Protocol (SMTP)* for greater security in sending messages over the SMTP channel. When supported by the user's mail client, authenticated SMTP requires users to enter their password before being allowed to send messages. Recipients can determine whether a message has been sent by an authenticated sender: the sender's name is followed by an indication that the message is internal.

IMAP encryption and authentication

Netscape Messaging Server 3.0 lets you specify the level of encryption and authentication for receiving messages with *Internet Message Access Protocol (IMAP)* clients. It provides a variety of options for encryption using *Single Socket Layers (SSL)* and authentication with passwords and client certificates.

Remote network management

Netscape Messaging Server 3.0 also includes *Simple Network Management Protocol (SNMP)* support for unified network management with any SNMP-compatible network management tool.

Message quotas

Netscape Messaging Server 3.0 supports message quotas. With the quota system enabled, server administrators can limit users to a fixed mailbox size by setting disk size limits. In this way, administrators have a manageable mechanism with which to control their potentially explosive messaging growth. The Messaging Server also provides warnings when users are nearing their message quotas. Messages received after a user's message quota has been reached are returned to the sender with a message indicating the reason for the message rejection.

Single copy message store

Netscape Messaging Server 3.0 includes a new single-copy message store capability that, if enabled, stores a single copy of any message sent to multiple recipients rather than one copy per recipient. This feature is designed to conserve disk space.

Delivery status notification

Netscape Messaging Server 3.0 can confirm message delivery, whether messages are sent within the enterprise or across the Internet. The Messaging Server's delivery status notification feature is based on the prevailing Internet standards (RFCs 1891 through 1894). Consequently, email users are apprised of message delivery not only by Netscape Messaging Server but also by other internal or Internet messaging systems that support these standards.

Netscape Messaging Server plug-in API

Netscape Messaging Server 3.0 provides an application program interface (API) that allows third parties to "plug in" site-specific functionality in the Messaging Server. It is intended for developers who wish to extend the functionality of the Messaging Server for site-specific reasons.

About this guide

This guide is intended for Netscape Messaging Server administrators, those responsible for setting up and administering the Messaging Server after it has been installed. For instructions on installing Netscape Messaging Server, see the *Installation and Deployment Planning Guide*.

Here's what you'll find in this guide:

- Chapter 1, "Working with users and groups" provides information on Netscape Administration Server's user and group forms that you will use to create mail accounts.
- Chapter 2, "Working with system settings" explains how to use the forms in the System Settings menu to configure your Messaging Server.
- Chapter 3, "Ensuring a secure messaging system" discusses the various ways Netscape Messaging Server keeps your mail secure. It also provides instructions on using the IMAP Encryption and Security Preferences forms.
- Chapter 4, "Server status and reports" explains how to enable the Messaging Server for remote monitoring through the server's SNMP subagent. It also provides information on how to select logging preferences.
- Appendix A, "Messaging Server architecture"provides a comprehensive discussion of the messaging server software architecture, including message channels and the Messaging Server managers.
- Appendix B, "Compatibility with sendmail" discusses compatibility issues between sendmail and Netscape Messaging Server. This appendix will help system administrators manage migration from sendmail to Netscape Messaging Server.

- Appendix C, "Program delivery" explains how to set up the Messaging Server to deliver incoming messages to external programs. Because program delivery is currently available only on the Unix platform, this appendix is of interest only to administrators running Netscape Messaging Server on a Unix system.
- Appendix D, "Command-line operations and utilities" provides information on how to operate certain Netscape Messaging Server 3.0 functions from the Unix command line. It also presents a variety of command-line utilities that you can use with Netscape Messaging Server 3.0.

This guide also includes a glossary of terms and an index.

About the other guides

This guide provides instructions on administering Netscape Messaging Server. Here's what you'll find in the other Netscape guides:

- The *Installation and Deployment Planning Guide* provides all the information a system administrator needs to install Netscape Messaging Server 3.0. It presents four common installation scenarios, discusses preinstallation issues, and provides a preinstallation checklist and step-by-step installation instructions.
- *Managing Your Netscape Servers* is a general introduction to administering Netscape servers. It also explains the role of Netscape Administration Server, a server installed along with Netscape Messaging Server that centralizes many common administrative tasks across a variety of individual Netscape servers and that you'll use to create and maintain user and group accounts.

Conventions used in this guide

This guide uses standard naming conventions. The following table describes those naming conventions and provides examples of their use. It also describes the typeface conventions and margin notes used in this book.

Convention	Examples	Description
Naming Conventions		
City names	sunnyvale, london, rome	Cities are used as example hostnames.
Organizational group names	sales, marketing, engineering	Organizational groups are used as example subdomain names (rather than hostnames).
host.domain	london.dispatch.com rome.sales.dispatch.com	A fully qualified domain name.
user@host.domain	ufirst.lastname@host.domain jane.doe@london.dispatch.com	An email address that uses a host-specific, fully qualified domain name.
domain	dispatch.com sales.dispatch.com	A non-host-specific domain name. (The hostname is excluded.)
user@domain	first.lastname@domain jane.doe@dispatch.com	An email address that uses a non-host-specific domain name. (The hostname is excluded.)

Convention	Examples	Description
Typeface Conventions		
Italic	*Mail clients* are programs that help users carry out email tasks. MX records for your domain *must* be available or mail addressed to your domain will not be deliverable. `/var/mail/login_name`	Italics are used to introduce new terms, for emphasis, and for "substitutables" (that is, for items that vary from case to case, as in the path name shown in the third example at the left).
`Monospace`	The package contents need to end up in the `/var/spool/pkg` directory.	Monospace font is used to represent text as it appears onscreen and to indicate anything you must type.
Margin Notes		
Unix	n/a	Identifies a section of the guide that applies only to Netscape Messaging Server running on a Unix system.
NT	n/a	Identifies a section of the guide that applies only to Netscape Messaging Server running on a Windows NT system.

Pathname conventions

This guide provides information about two versions of the Netscape Messaging Server: one for Unix, the other for Windows NT. In cases where pathnames for Unix and Windows NT differ only in their use of their respective slash conventions—the forward slash (/) for Unix, the backslash (\) for Windows NT—for brevity, this guide presents the pathname only in the Unix format.

Note Windows NT supports both forward slash and backslash characters.

In cases where the differences between Unix and Windows pathnames are significant and go beyond their differing slash convention, the pathnames are provided in both forms and identified with a margin note.

Chapter

1

Working with users and groups

This chapter provides information that you'll need in working with user and group directory entries to create email accounts.

Here's what you'll read about in this chapter:

- "Using the Administration Server" on page 20 explains the role of the Netscape Administration Server in creating user and group directory entries.
- "What are email accounts?" on page 22 explains the concept of email accounts, the types of information they contain, and how the Messaging Server uses this information.
- "Working with user and group forms" on page 23 provides information on the fields in the Administration Server's User and Group forms.
- "Required and recommended groups" on page 33 explains the need for a special required group account called *postmaster*, as well as other, recommended groups that you should create for use with the Messaging Server.
- "Starting and stopping the Messaging Server" on page 35 explains how to start up and stop Messaging Server 3.0.

Using the Administration Server

When you installed Netscape Messaging Server 3.0, another server—the Administration Server—was also installed with it. This Administration Server provides centralized user and group administration. That is, user and group entries are created and maintained with the Administration Server; the information is available to any Netscape SuiteSpot server that uses it.

The Administration Server means simplified account administration for the server administrator because user and group entries can be created once, in one place, rather than repeatedly for each server that needs the information. For users, this means signing on once, rather than having to maintain and enter a different password for each server used.

The Administration Server maintains user and group entries in a local directory database that can be shared by multiple SuiteSpot servers installed on the same machine. You can also use a *Lightweight Directory Access Protocol (LDAP)* Directory Server that can be shared by multiple SuiteSpot servers installed on across multiple hosts.

The forms used to create and manage user and group entries on the Administration Server provide a "General" portion, with fields that are non-server specific. Servers that require additional forms—such as the Messaging Server—automatically provide additional, server-specific forms that are accessed from within those user and group forms.

For more information about the Administration Server and how it works with other SuiteSpot servers, or for instructions on setting up and maintaining user and group accounts, see *Managing Netscape Servers*.

Starting and stopping the Administration Server

You can start and stop your Administration Server from the command line using the start-admin and stop-admin utilities that are available in your root installation directory. That is, if you installed your server in:

```
/usr/netscape/suitespot
```

then you can start your Administration Server by running:

```
/usr/netscape/suitespot/start-admin
```

Similarly, you can use the stop-admin utility to stop your Administration Server:

```
/usr/netscape/suitespot/stop-admin
```

In addition, you can stop your Administration Server by going to the **Server Preferences | Shut Down** form in the Administration Server interface.

For more information on stopping and starting your Administration Server, see *Managing Netscape Servers*.

Accessing the Administration Server

You use your web browser to connect to the Administration Server. Assuming that the Administration Server is running, you can connect to it by entering the server's hostname and port address to your web browser. For example, if your Administration Server is installed on the host `host.mydomain.com` at port number 1500, then you can access the Administration Server by entering the following to your web browser:

```
http://host.mydomain.com:1500
```

NT Note that if you are using a Windows NT machine, you can automatically start your Administration Server, launch your web browser, and connect to the Administration Server by clicking the Administration program item.

Using the Server Administration page

When you first connect to the Administration Server, you see a form that identifies the various Netscape servers that this Administration Server is managing. This is the *Server Administration page*. There are also several links on the Server Administration page that take you to general administration functions, such as setting up *Secure Socket Layer (SSL)*, managing users and groups, and so on. To manage your Messaging Server, click the button that represents your Messaging Server.

For a complete description of the Server Administration page, and of the various management functions available through the Administration Server, see *Managing Netscape Servers*.

Using the Messaging Server manager

This guide frequently mentions the *Messaging Server manager*. This term is used to refer to the collection of forms that you access when you click the Messaging Server button from the Server Administration page. These forms allow you to perform Messaging Server management tasks such as:

- Setting Messaging Server configuration preferences.
- Choosing IMAP encryption options and security preference settings.
- Configuring and turning on and off the Messaging Server's SNMP subagent.
- Reviewing queued mail and setting logging preferences and viewing Messaging Server logs.

All Netscape servers are managed through server managers that have the same look and feel as the Messaging Server manager. Consequently, if you have ever managed other Netscape servers before, there should be few surprises when you manage the Messaging Server.

What are email accounts?

Information about users and groups who receive email on your messaging system is organized by the Administration Server into directory entries. Because other types of servers can also provide additional attributes within these user and group entries, only a portion of the information contained in a directory entry may be used by the Messaging Server. It would be inaccurate to think of a directory entry as an email account. However, it *is* helpful to consider the relevant subset of attributes in a directory entry that are used by the Messaging Server as constituting an email "account," and it is in this sense that the term is used throughout this guide.

Email accounts comprise such information as the user's or group's name, email address or addresses, how and where email is delivered, and so on.

Of the many types of information potentially contained in a directory entry, here are some of the categories of information in each mail user's entry that are used by the Messaging Server to process incoming email messages:

- **General information** includes the name assigned to the entry and the password (stored in an encrypted format) associated with the entry.
- **Email addressing information** includes the Internet email address or addresses for that entry.
- **Local delivery information** specifies how messages for that entry are delivered to its recipient(s). For example, messages can be delivered through POP3/IMAP4, placed in a Unix maildrop file, or forwarded to another host.
- **Security parameters** determine the access domains for the entry.
- **Automatic reply information** is optional and covers configuration information for the AutoReply feature.
- **Message store path** allows you to assign an alternate spooling area—for instance, on other disk devices.
- **Messaging Server** specifies the name of the host on which the Messaging Server is running.

Although the server administrator controls most of the information in a directory entry, the entry's owner can change certain items that apply only to his or her entry—such as the password and auto-reply information, for instance.

Working with user and group forms

Managing Netscape Servers provides a general introduction to using HTML forms to manage Netscape servers. It also provides step-by-step instructions for creating, editing, renaming, and deleting user and group entries. The following sections provide information on the forms within the user and group entries that are used by the Messaging Server.

Managing user accounts

The Mail User Information form is the portion of a user's directory entry that you use to provide information about the user that the Messaging Server needs to process that user's messages. You access the Mail User Information form by clicking Mail in the user's directory entry form.

Figure 1.1 Jane Doe's directory entry form.

After you click Mail, the Mail User Information form appears.

About the Mail User Information form

The following sections describe each of the fields in the Mail User Information form.

Primary Email Address field

The primary email address is the *publicized address—that is, the address likely to be looked up by "white pages" applications*. The primary email address is used to select this account for email delivery. This is also the address that the Messaging Server will put on the "From:" line of all outgoing mail if the Messaging Server is set up to do so.

This field should include only one correctly formatted SMTP address. You can assign any valid address (that is, an address that conforms to RFC 821 specifications) to an account. However, you might want to choose a consistent convention for user addresses (such as `First.Lastname@mail_domain` or another common convention).

Note *Addresses are not case sensitive*. For example, the Messaging Server will not distinguish between `Dispatch.com` and `dispatch.com`.

Regardless of the convention you choose, you must set up the domain name system (DNS) so that mail addressed to the mail domain you use will be delivered to your network. The Messaging Server can accept messages for any number of domains; it's not limited to your "official" domains specified during installation.

Alternate Email Addresses field

Use this field to list any alternate email addresses. A message arriving for any of the listed addresses will be directed to this account and then delivered using the local delivery method selected for the account.

You can have as many alternate addresses per account as you like, but they *must all be unique*, just as all Internet addresses should be unique no matter where they are located.

A note on alternate addresses: Many sites prefer that the specific hostname not be included on the sender's outgoing email address. This technique is called *hostname hiding*. If you want to use hostname hiding, the account will need a primary address that does not include the hostname:

```
Jane.Doe@Dispatch.com
```

Unix Most Unix mail systems use the user's login ID as their mail address, so further alternate addresses might be required. For instance, if Jane Doe's Unix login is "jane," you might also have the following addresses in her account:

```
jane@sunnyvale.dispatch.com
jane@dispatch.com
```

Messaging Server field

This field specifies the hostname of the Messaging Server that handles this user's email. The name you enter here must be a fully-qualified domain name (FQDN). If the server has multiple hostnames (FQDNs), it must be the FQDN that is known by the Messaging Server on that machine.

Delivery Options fields

You have four delivery options to choose from: POP3/IMAP delivery, Unix delivery, program delivery, and forward delivery.

POP/IMAP Delivery

If this option is enabled, mail is held by the Messaging Server until the user checks for mail using a POP3/IMAP4 mail client. Users who employ this delivery must use the User ID specified in their directory entry as their POP/IMAP login name. You can also specify the specific message store path, mail quota, and access domains for this user:

Message Store Path field The message store path specifies an alternate location for the mail spool—for instance, to spread accounts over multiple disk drives. Leave this field blank to use the system default, which is configured when you install the Messaging Server. The directory you enter in this field must exist, and the Messaging Server account must be able to write to it.

Mail Quota field Use this field to specify a user's disk quota in bytes. You can leave the field blank to use the default. (You use the Messaging Server's System Configuration form to set the default.)

Access Domains field You can use this field to limit the access that users have to their accounts. Users can retrieve their mail through POP3/IMAP only from within their access domains. An access domain can be as restrictive as a single computer, a list of several computers, or an incomplete domain. For example, the access domain `dispatch.com` would include any computer whose DNS address includes the suffix `dispatch.com`. If you leave this field blank, the access domain will be unlimited. If you write "none," you prevent POP/IMAP logins. (Note that either domains entries or IP addresses can be used in this field.) See "Access domains" on page 55 for more information.

Unix Delivery

Unix If this option is enabled, messages are delivered to a maildrop file within a user's Unix account located on the same host as the Messaging Server. Unix delivery is available only on the Unix platform, and users' User IDs specified in their directory entries are taken to be their Unix login names. This option enables pickup with legacy Unix mail clients.

Forward Delivery

If this option is enabled, mail is forwarded to the addresses that you specify in the Addresses for Forward Delivery field. Follow the same rules as you would for an SMTP address (an Internet address). You can forward mail for an account to as many addresses as you like.

Program Delivery

Unix If this option is enabled, users can deliver messages to external programs such as procmail. Users' User IDs specified in their directory entries are taken to be their Unix login names. If the Program Delivery option is selected, the Messaging Server runs the programs listed in the Command lines for Program Delivery field when mail arrives for the account. Programs are run with the permissions of the user specified by the Unix login name and receive the incoming message as input. The format for entries is a complete command-line statement including options, such as

```
/usr/local/bin/procmail -f -
```

Note By default, program delivery is disabled when the Messaging Server is installed. Programs must be set up and program delivery enabled before the program delivery fields can be used. You should familiarize yourself with the special security considerations involved in using this feature before enabling it. See Appendix C, "Program delivery" for more information.

Auto-Reply Mode field

Select "None," Vacation," "Reply," or "Echo." See Chapter 2 for more information on these options.

Auto-Reply Text field

This field is used when you select the vacation, reply, or echo options for the Auto-Reply Mode option. You can leave it blank if a default reply message exists.

Personal Description field

This information is provided when the account receives a finger query for this user.

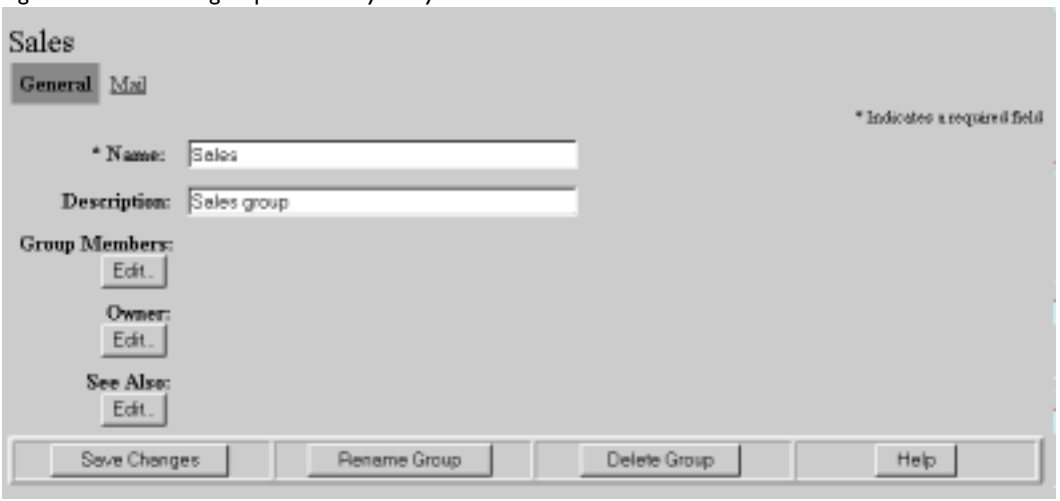
Managing group accounts

Mail group accounts are often useful when delivery is intended for several people in a single conceptual group, such as the sales staff. For example, there might be several people who need to receive any messages addressed to `sales@dispatch.com`.

There are other reasons you might want to create group accounts. For example, sites connected to the Internet might maintain a valid address for "webmaster," so that people can contact the person responsible for the corporate home page, and since more than one person may be assigned to that responsibility, each may need to receive mail at this address. Similarly, you might want to create a group called "support" to handle technical support questions or "info" to handle public relations questions. See "Required and recommended groups" on page 33 for more information.

Like user directory entry forms, group entry forms provide both a general and a mail-specific set of fields. The information provided in the General fields can be used by other SuiteSpot servers, for instance, to help organize access control. The Mail Group Information form is the portion of a group's directory entry that you use to provide information about the group that the Messaging Server needs to deliver that group's messages. You access the Mail Group Information form by clicking Mail in the group's directory entry form.

Figure 1.2 The Sales group's directory entry form.



After you click Mail, the Mail Group Information form appears.

About the Mail Group Information form

The following sections describe each of the fields in the Mail Group Information form.

Primary Email Address field

The primary email address is the *publicized address*. The primary email address is used to select this account for email delivery.

This field should include only one correctly formatted SMTP address. You can assign any valid address (that is, an address that conforms to RFC 821 specifications) to an account. However, you might want to choose a consistent convention for group addresses (such as `Groupname@mail_domain` or another common convention).

Note *Addresses are not case sensitive*. For example, the Messaging Server will not distinguish between `Dispatch.com` and `dispatch.com`.

Regardless of the convention you choose, you must set up the domain name system (DNS) so that mail addressed to the mail domain you use will be delivered to your network. The Messaging Server can accept messages for any number of domains; it's not limited to your "official" domains specified during installation.

The Primary Email Address *must be unique*, just as all Internet addresses should be unique no matter where they are located.

Alternate Email Addresses field

Use this field to list any alternate email addresses. A message arriving for any of the listed addresses will be directed to this account and then delivered using the local delivery method selected for the account.

You can have as many alternate addresses per account as you like, but they *must all be unique*, just as all Internet addresses should be unique no matter where they are located.

Send Errors To field

Use this field to specify the person to whom the Messaging Server should send error messages. You can leave this field empty to return error messages to the sender.

If this field is left empty, the group is treated as a mail *alias*. With an entry in this field, the group is considers a mailing *list*. The difference is in the degree to which they are managed. It is assumed that lists are more actively managed than aliases, and therefore error messages need to be sent to the person responsible for managing the list.

It is recommended that you usually create mailing lists by entering an address in this field so that the group manage can handle bounced messages, rather than bothering everyone in the mail group with error messages.

The entry should be in the form of a complete email address; for example, `jane@dispatch.com`.

Messaging Server field

Use this field to specify the hostname of the Messaging Server that handles this group's email. The name you enter here must be a fully-qualified domain name (FQDN). If the server has multiple hostnames (FQDNs), it must be the FQDN that is known by the Messaging Server on that machine. You can leave this field empty to allow any Messaging Server to handle mail for the group.

Note Leaving this field empty is usually more efficient, since it allows any Messaging Server to process this group's mail. You may want to list a specific hostname in cases where you want to force processing to specific machine. For example, if you are creating a very large group, you may want to force processing on a less busy machine.

The FQDN is indicated by the MessageHostName setting in the `/etc/netscape.mail.conf` file (Unix) or by the combined Host Name and Domain fields in the DNS configuration area of the Windows NT Network Control Panel.

List of CC Recipients field

Use this field to specify "email" group members—that is, recipients who are specified by their email address rather than by name. Enter one address per line (for example, `jdoe@example.com`).

For example, you may create a group that consists of top executives in your firm. You might list each executive's assistant in this field to provide copies of group email to the assistants without giving them access control.

You might also include in this field recipients who are external to your Messaging Server, or who do not have a directory entry in your directory database.

Note These members are "email-only" members, and email-only group members are not consideredgGroup members for any other purpose.

LDAP Criteria for Generating CC List field

This field is used for criteria-based mail group membership, and is useful when you want to create a group that includes everyone that meets certain criteria (for example, everyone in the organization or organizational unit, or everyone on a particular Messaging Server), instead of listing all the members explicitly.

Note These members are "email-only" members, and email-only group members are not considered Group Members for any other purpose.

This field requires that you know the syntax for specifying LDAP filters. Enter each LDAP search filter on its own line.

This field can be very useful for large groups and groups with very dynamic membership: you don't need to add and remove people individually since membership is conferred by meeting the LDAP criteria for the group.

For example:

```
ldap:///o=Ace
Corp,c=US???(&(mailHost=sunnyvale.ace.com)(objectClass=inetOrgPerson))
```

This filter would make everyone who has sunnyvale as a mail server a member of this group. You might use such a filter to notify everyone on the server when the server needs to be shut off for maintenance.

Another example:

```
ldap:///ou=Marketing, o=Ace Corp, c=US???(objectClass=inetOrgPerson)
```

This filter makes everyone in the marketing department a member of the group.

Note See RFC 1959 for information on constructing a LDAP filter. Note also that the "searchDN" and "filter" fields are currently used.

Important Generally, you will want at least a filter of `(objectClass=inetOrgPerson)` unless you want the group to include agents or other groups. Groups are not expanded within a search, even if they are not specifically excluded by the LDAP filter.

Maximum Message Size field

This field restricts the size in bytes of messages that can be received by this group. Messages that exceed this maximum size are rejected.

You can also leave this field blank to impose no limit on the message size.

Allowed Sender Domains field

This field restricts messages received by this group to messages sent from the domain you specify.

Important This feature can be "spoofed" and should therefore not be used as a security measure. The feature is useful, however, in restricting the volume of messages received by the group.

Allowed Senders field

This field restricts messages received by this group to messages sent by people or groups that you specify. For example, if you list the group you are creating in this field as the only allowed senders, only members of the group can send messages to the group.

Important This feature can be "spoofed" and should therefore not be used as a security measure. The feature is useful, however, in restricting the volume of messages received by the group.

Rejection Notice field

Use this field to provide a message that will be sent when messages addressed to this group are rejected. You have the option of including the original message along with the rejection notice.

Required and recommended groups

As Messaging Server administrator, you will need to maintain at least one required group, the *postmaster* group. You most likely will also want to maintain other groups that are often used by convention to assist routing messages to their appropriate recipients.

Required group: Postmaster

By convention, messaging systems need to provide an account for "postmaster" so that messages sent to `postmaster@`*`host.domain`* can be delivered successfully. Most often, the postmaster is the person responsible for setting up and maintaining the Messaging Server, but it can be others who share some responsibilities with the server administrator.

The postmaster group is created automatically from information you provide during Messaging Server installation. As server administrator, you should maintain a separate, personal email account and use the postmaster account merely to funnel messages addressed to `postmaster@host.domain` to you. You can add others to the postmaster group if you need or want to share administrative duties with others.

Important Assigning others to the postmaster group does not give them access to the full range of forms available to the Messaging Server administrator. Membership in the postmaster group merely channels messages addressed to *postmaster* to those assigned to that group. If you want or need to share server administrator responsibilities with others, you will need to provide access through shared passwords for logging on to the Messaging Server.

Recommended groups

Following are some generic group accounts that are used by convention to route messages to their appropriate recipients. The benefit of maintaining these accounts, of course, is that senders do not need to know a unique email address to send their messages successfully to the responsible recipient.

Note Members of these group accounts can be either people who have directory entries managed by the same local directory database or LDAP Directory Server (preferred), or people whose mail is forwarded elsewhere. Multiple aliases are supported (`customer_service@mydomain.com`, `support@mydomain.com`). Mail routing is independent of uppercase/lowercase—that `support@mydomain.com` is equivalent to `Support@mydomain.com.`

Table 1.1 Recommended group names and functions.

	Group ID	Common Name	Description
Business-related groups			
	INFO	Marketing	Packaged information about the organization, products, and or services, as appropriate
	MARKETING	Marketing	Product marketing and marketing communications

Table 1.1 Recommended group names and functions.

	Group ID	Common Name	Description
	SALES	Sales	Product purchase information
	SUPPORT	Customer Service	Problems with product or service
Network Operations			
	ABUSE	Customer Relations	Inappropriate public behavior
	NOC	Network Operations	Network infrastructure
	SECURITY	Network Security	Security bulletins or queries
Internet Services			
	HOSTMASTER	DNS	RFC 1033-RFC 1035
	USENET	NNTP	RFC 977
	NEWS	NNTP	Synonym for USENET
	WEBMASTER	HTTP	RFC 2068
	WWW	HTTP	Synonym for WEBMASTER
	UUCP	UUCP	RFC 976
	FTP	FTP	RFC 959

Starting and stopping the Messaging Server

You can start and stop the Messaging Server from the:

- Server Administration page—click the On/Off icon located to the left of the server's name in the Server Administration page. If the server is on, you will see a green light under the icon. Click the icon to turn the server off. To turn the server back on, click the icon again.
- Messaging Server manager—go to **System Setting** | **On/Off** and click the appropriate button.

When you successfully start your Messaging Server from the Server Administration page, the server issues the following message:

```
Success!

   The server has started up.
```

When you successfully stop your Messaging Server from the Server Administration page, the server will issue the following message:

```
Success!

   The server has been shutdown.
```

Chapter

2

Working with system settings

This chapter discusses Netscape Messaging Server configuration. Although the minimum set of mandatory configuration decisions are taken care of during installation, some refinements can enhance your email system by optimizing the Messaging Server for your specific needs.

This chapter provides information on the forms found in the Messaging Server's System Settings menu of forms. They include:

- "The Messages form" on page 38
- "The SMTP Channel Aliases form" on page 40
- "The SMTP Channel Options form" on page 42
- "The System Configuration form" on page 46
- "The Single Copy On/Off form" on page 49
- "The Message Stores form" on page 50
- "The Unix Mail form" on page 50

The Messages form

The Messages form allows you to compose and enable default messages for host finger information; vacation, reply and echo auto-reply; and error actions such as when message quotas are exceeded. Some of these default messages can be replaced when users provide their own messages—for instance, when using the User Management form to compose their own vacation message.

If the AutoReply handler is enabled and you do not have entries in this default form, users will be required to enter their own messages to activate the vacation feature. Also, server administrators will be required to specify messages for all accounts using the reply or echo feature.

The following sections describe the fields on the Messages form.

Host Finger Information field

This field contains the information provided to finger queries that don't include a username (and are therefore addressed more generally to your company or organization). This field is a good place to put miscellaneous information about your company and contact names and email addresses.

Default Vacation-Mode Reply Message field

This field contains the vacation message that will be used if users forget to write a personalized message. If this field is left blank, the account manager won't accept a User Management form if the vacation feature is selected and no vacation message is included.

Anyone who sends messages to a user's account while the vacation setting is activated will receive one notice about the user's absence. Any subsequent messages that person sends are ignored.

Warning In most cases, server administrators should not replace a user's current delivery with the vacation setting when they set up the AutoReply handler for that user's account. If they do this, the user will return from vacation only to find that all of his or her email has been thrown away. Rather, the vacation setting should be

used in addition to the normal delivery method, so the mail is held for the user to retrieve upon his or her return. (Users are prevented from making this mistake because the Messaging Server doesn't accept Information forms with a delivery of "Vacation" only.)

Default Echo-Mode Reply Message field

This field typically contains a generic message for users sending messages to this address. A common use of the echo feature is to return mail addressed to people who have moved on and left no forwarding address. If this field is left blank, the account manager will require that an echo message be included when the echo feature is selected on a Mail User Information form.

The echo feature generates a message to anyone who sends a message to the account. In addition, it returns the mail (as a MIME attachment) that was sent to the account, so that the sender gets back the original message as well as the message that you entered.

The echo feature, like the vacation feature, is intended to inform people about the status of the account they have contacted.

Default Reply-Mode Reply Message field

You can use this field to specify a message that can be used to advise the sender to contact the server administrator. If this field is left blank, the account manager will require a reply message when the reply feature is selected. It's usually best to leave this field blank.

The reply feature is useful for special accounts that are created to disseminate information of one kind or another. You can create a place where people can get files, analogous to a *File Transfer Protocol (FTP)* site on the Internet.

'Quota Exceeded' Message field

You can use this field to specify a message to advise senders that mail is undeliverable because the recipient's mailbox has reached its quota.

The SMTP Channel Aliases form

If all mail servers in your organization are Netscape Messaging Servers, and all use a common LDAP Directory Server, then the information in the Directory Server's user and group entries is sufficient for internal mail routing within the organization. In other cases, there are two recommended ways for the Messaging Server to route mail to dissimilar mail systems: SMTP channel aliases and Forward Delivery (an option in the Mail User Information form).

If you are using the LDAP Directory Server to administer multiple Messaging Servers in your mail system, the recommended procedure for forwarding messages from one host to another is to use the Addresses for Forward Delivery field in the Administration Server's Mail User Information form. There are two advantages to using this approach. First, forwarding information is centralized. You don't have to replicate the information in each Messaging Server configuration. Second, forwarding is automatic in the sense that you enter the forwarding address while setting up a user's mail account, and messages are forwarded without any further intervention.

The alternative to using the LDAP Forward Delivery option is to use an *SMTP channel alias*. *SMTP channel aliases* also handle incoming messages that are forwarded to another Messaging Server on a different host. However, SMTP channel aliases are not centralized: you must set up aliases on a per-server basis. Nor are SMTP channel aliases automatic: once you set up a user's mail account, you still need to create the aliases for that user "by hand."

SMTP channel aliases are required in mail systems that do not take advantage of a centralized LDAP Directory Server, or in a "mixed" mail system that includes non-LDAP-aware mail servers, such as sendmail.

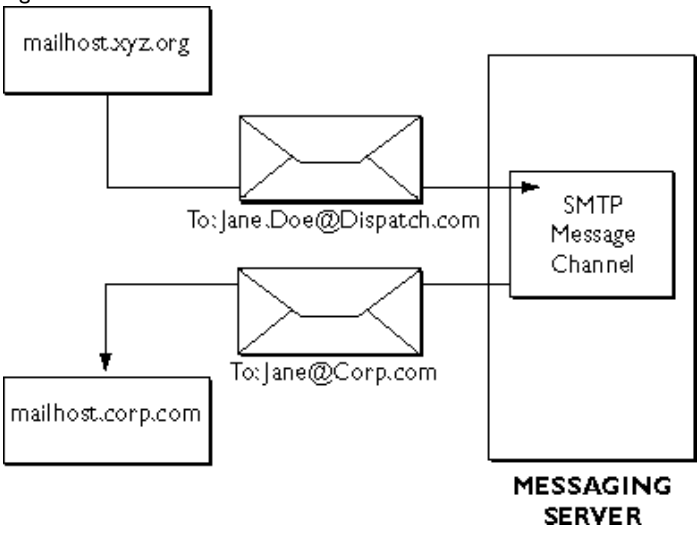
SMTP channel aliases are specific to the SMTP channel. Whenever a message enters the Messaging Server system destined for one of the listed SMTP channel aliases, the address is immediately rewritten and the message delivered to the new address at a remote host. The message is delivered to the remote machine without ever being seen by the Account handler. SMTP channel aliases are used extensively when a site sets up a mail hub through which all incoming messages are routed before being delivered to the intended user's host machine.

Figure 2.1 shows an SMTP channel alias in action. In the figure, someone of the XYZ organization occasionally sends mail to Jane Doe at `Dispatch.com`. Let's say, however, that Jane has recently left `Dispatch.com` to move to another building. To help Jane continue to receive her mail, an SMTP channel alias was set up for her using the SMTP Channel Aliases form:

```
<Jane.Doe@Dispatch.com> <Jane@Corp.com>
```

Whenever a message arrives addressed to `Jane.Doe@Dispatch.com`, the address is replaced with her new address. The message is then forwarded to its new destination, `Corp.com`.

Figure 2.1 An SMTP channel alias.



Setting up an SMTP channel alias

You can use the SMTP Channel Aliases form to set up aliases for the SMTP mail channel. To reach this form, choose **System Settings | Aliases**.

To set up an SMTP channel alias address, fill out the incoming and outgoing addresses and submit the form. Each line is a separate alias where you enter first the address for which the SMTP channel will accept messages followed by the address to which it will redirect these messages.

You must set up aliases one address at a time. For example, if Jane Doe leaves `Dispatch.com` to take a higher position in Washington, D.C., and her account at `Dispatch.com` has the following primary and alias addresses (all of which she uses), you will have to set up an alias for each of these addresses:

- `Jane.Doe@Dispatch.com`
- `jane.doe@sunnyvale.dispatch.com`
- `jd@sunnyvale.dispatch.com`
- `jd@dispatch.com`

The SMTP Aliases form also provides the option of specifying a simple text file with which to import Channel Alias data in the form of a list of entries, instead of entering the data directly on the form. The text file must contain entries in the same syntax as if you were entering the data directly in the SMTP Aliases form.

Note The filename you enter in the Import Channel Alias Table field should be an absolute path to a file on the system on which the Administration Server is running.

It does not matter if the field not selected has any content. For example, if the manual input option is selected and a filename is present in the Filename field, the input will not be taken from the file listed.

The SMTP Channel Options form

You can use the SMTP Channel Options form to configure the SMTP mail channel. This form is used to configure a variety of options specific to the SMTP channel but is not used to set channel aliases. This form includes configuration for the most common Messaging Server error, Unknown Local Account. It also includes the SMTP Mail Routing table.

The following sections describe the fields on the SMTP Channel Options form.

Maximum Number of MTA Hops field

Use this parameter to prevent infinite mail loops. Usually a mail loop is caused by having two email accounts on different machines that forward mail to one another. Fortunately, these loops can be detected and stopped because each MTA stamps all incoming messages as "Received." By counting the number of Received lines in the message header, the MTA can determine how many "hops" the message took to get there. If the number of hops exceeds the maximum specified in this field, the server administrator receives an error report. The recommended range for this parameter is 30 or more.

Note This error action can be customized with the Unknown Local Account field.

Defer Delivery to remote hosts field

This field is used to determine when mail is delivered. Normally, when a message needs to be delivered to another machine over the Internet, the Messaging Server attempts to deliver it immediately and queues it only if there is a problem. Setting this option to Yes causes the Messaging Server to instead queue all outgoing mail and attempt delivery only when it processes the queue. The Messaging Server processes the queue on intervals that you indicate in the Queued Mail Processing Interval field of the System Configuration form. This feature is useful if your system has only intermittent access to the Internet.

Verify each recipient's address field

This field is used to verify each recipient's address when accepting messages. When this option is set to Yes, the Messaging Server verifies each address listed as a recipient. Non-local addresses and addresses in mailing lists are *not* verified. The default setting for this option is No.

SMTP Mail Routing Table field

Mail can be routed to a machine other than the destination in the address using this optional field. This is done with a routing table. Normally rerouting is used only when a firewall prevents direct access to the destination mail server or when mail needs to be sent through a gateway to another network, such as a Unix to Unix Copy Protocol (UUCP) network.

The routing table is consulted only after the Messaging Server has determined—first through Channel Aliases, then an LDAP lookup, and finally NIS—that the address is not for a local mail account. The SMTP Mail Routing table is consulted before DNS/MX records.

The format for table entries is

```
*.domain:gateway.other_domain
```

An asterisk is used as a wildcard that will match any string of characters. In the example above all mail addressed to any machine or subdomain (because of the *) within the domain is routed to *`gateway.other_domain`* instead. The gateway then sends the mail to the machine indicated by the address. For example, to configure the Messaging Server to route mail to a UUCP gateway, you might use the following entry:

```
*.uucp:uucp.gateway.host
```

(You should, of course, substitute the actual address for your UUCP gateway in the place of `uucp.gateway.host`.)

Similarly, to route mail to a Fidonet gateway, you would use an entry similar to this:

```
*.fidonet:fidonet.gateway.host
```

You can set up a default route so that all mail goes to a single machine by using a single asterisk, as in this example:

```
*:mail.hub.machine
```

Note Use a default route only if it is absolutely necessary (as in a firewall situation) because it puts an additional burden on the mail hub machine and can slow it down.

Example:

```
*.example.com:*

example.com:hub.example.com

*:firewall.example.com
```

Unknown Local Account, Maximum MTA Hops Exceeded, and Disk Quota Exceeded fields

You can use these fields to specify what should be done with an undeliverable message. You select one or more options by clicking the button next to each item. Each of these error actions can assume appropriate combinations of the following values:

Return	Returns original message to sender.
Hold	Holds message for server administrator action (such as return to sender, resubmit with correction, or delete the message).
Notify	Sends notification of error to server administrator.
Log	Documents error in log file.

Inappropriate combinations, such as “log” by itself (which would log the error but delete the mail), should be avoided. You will probably always want to include a “return” entry or a “hold” and “notify” combination as part of your choices.

The Unknown Local Account error means that a message was addressed to a local domain but didn’t correspond to an email account or channel. The bad address could be a typographical error, or it could be a sign that you should set up an alias for a local user at the “bad” address (because people seem to think it is a reasonable address). Unless you get a prohibitive volume of unknown local account errors, you should set this on “notify” and “hold,” especially if you’re upgrading from a different mail system. This setting lets you know about each error and lets you intervene by resubmitting the message, creating a new

alias, returning the message to its sender, or throwing it away. Because many administrators prefer not to deal with bad addresses (because of the large volume they receive), the default is “return.”

The Max Hops Exceeded error usually occurs because of a mail loop. Mail loops are fairly serious problems and need to be resolved as soon as possible. Accordingly, the *strongly* recommended setting for this error is “notify” and “hold” so that you can reconfigure the responsible account and resubmit the message to verify that the problem has been corrected.

The Disk Quota Exceeded error occurs when a message arrives for a user whose disk quota has been exceeded. For this situation you probably want to choose the “return” and “notify” settings.

The System Configuration form

The System Configuration form lets you

- Make any changes to the domains served by the Messaging Server
- Increase the maximum number of processes allowed to run (this will increase the amount of processor time that the Messaging Server can theoretically use)
- Configure queue processing time and log activities

The following sections describe the fields on the System Configuration form.

Address Completion Domain field

When mail arrives for a recipient whose address doesn’t contain a domain, the domain specified in this field is added to the recipient’s address. If no domain is specified here, the hostname of the machine running the Messaging Server is assumed. For example, if this field is set to your domain name, mail addressed to `<user>` will be sent to `<user@your.domain>`.

In some cases there is an advantage to configuring the address completion domain to add your domain rather than your host address. When your system uses hostname hiding, a *`name@domain`* format will often fare better than a *`name@host.domain`* address completion.

Note Some mail clients won't send mail that doesn't have a complete address. In this case, mail sent to `<user>` will not be deliverable, and users must be instructed to type the whole address for each message sent, even when it's local.

Local Mail Domains field

This field is a list of all the mail domains that this machine handles exclusively. If a domain is listed here and mail comes in with an address within that domain, the message is delivered locally to an account, referred to the server administrator, or returned to the sender (if no account is found for the recipient). If a domain isn't listed here, this machine isn't the primary mail handler for that domain. (However, it can still receive mail for addresses in the unlisted domain if an account is set up with an appropriate alias.)

This field helps determine when a message gets bounced. Specifically, if a server has this set and cannot resolve an address, it bounces the message.

Queued Mail Processing Interval field

Messages that can't be delivered immediately are placed in a message queue. The system attempts to deliver queued messages at regular intervals as specified here in seconds. Typical intervals are from 30 minutes (1,800 seconds) to two hours (7,200 seconds).

Maximum Mail Queue Time field

Messages that can't be delivered in a timely manner are eventually returned to the sender with an error message. Use this parameter to set the maximum amount of time that a message remains in the queue before it's returned. Internet standards recommend at least four or five days for this. The minimum is normally two or three days (to accommodate a problem that occurs over a weekend, or to provide ample time to fix the problem).

Lookup Client Machine Names field

Enable this option (by choosing Yes) if you want to have the Messaging Server perform a name lookup (through the DNS) on all connecting client machines. If you enable this option, machines will be referred to by their domain names; otherwise they will be referred to by their Internet Protocol (IP) addresses. Places where these names show up include the process table, the log file, and "Received" lines in message headers. If you handle a large volume of messages, be aware that selecting this option will slow down the Messaging Server.

Default Maximum Number of Concurrent Network Servers field

This default covers the number of SMTP, POP3, and finger processes that can run at one time. Specific processes are counted, not the total of all three. Because this is a default, it's used only if the defaults for those modules aren't specified. The recommended default is 20, which is enough for most systems. However, if you're doing something like serving many users with POP3 or IMAP4, you should set the maximum run count for the POP3/IMAP4 module higher.

Default Maximum Number of Concurrent Local Processes field

This is the default for non-network processes such as the account handler. This default is applied only if a limit isn't specified in the configuration of a specific module. The recommended default is 5. If you need to assess the local processes and what they do, refer to Appendix A, "Messaging Server architecture".

Minimum Free Disk Space field

This field allows you to specify the minimum free disk space required to allow the Messaging Server to accept messages. A “0” means unlimited. The Messaging Server rejects all messages received if not enough disk space is available.

Default User Disk Quota field

This field allows you to specify a disk quota to apply to all users who do not have their own disk quota set. A “0” means unlimited. The Messaging Server rejects all messages received once the quota is reached and not enough disk space is available.

Recommended Account Management URL for Mail Users field

This field lists the recommended URL to gain access to the Messaging Server. The default entry is determined by information provided during installation.

This URL is provided to any mail client, such as Messenger 4.0 or greater, requesting it with a special POP/IMAP command. (With Messenger 4.0, the command is Edit|Manage Mail Account.) The URL is the location where end users can point their browsers in order to administer their mail accounts.

The Single Copy On/Off form

This form allows you to turn the single-copy message store feature on or off and to set the minimum message size.

If you turn on single-copy message store, the Messaging Server stores a single copy of any message sent to multiple recipients, rather than one copy per recipient. The advantage of turning on single-copy message store is that it

conserves disk space. If you turn single-copy message store off, messages will be delivered normally, with a copy stored in each recipient's mailbox. The advantage of turning single-copy message store off is better performance.

This field is set to "off" by default to favor performance.

The Minimum Message Size option is a performance-tuning parameter. Every operating system allocates a minimum number of bytes for a file (cluster size) regardless of the bytes in the file. (For example, it may allocate 2K bytes to store 2 bytes). If the minimum message size is small compared to the cluster size, space is wasted; if the minimum message size is large, then there is no single copy for all messages of smaller size, and again space is wasted. The optimal value can only be determined by a trade-off between the cluster size and the type of mail traffic at your server.

You will need to restart the Messaging Server for any changes to take effect.

The Message Stores form

This form is used to specify each directory on disk that contains a message store. The message store that a given user's mailbox is in is determined by the contents of the Messaging Server field in that user's Mail Information form. If a user's message store is different from the ones listed here, that user cannot have the Single Copy feature enabled. If a user's message store is left unspecified, the default message store is used.

Note If Single Copy is turned on, the default message store and all message stores listed on the form have single copy enabled.

The Unix Mail form

Unix This form is used to specify the interface to the Unix mail system and to select program delivery options.

The Local Mail Delivery Program field lets you specify the default Unix program used to deliver mail to any account that specifies Unix delivery in the Delivery Options field of the user's Mail User Information form. The default for this field is `/bin/mail`.

Program delivery options let you limit use of program delivery to the user and group specified in the Safe User ID and Safe Group ID fields for running root programs.

Chapter

3

Ensuring a secure messaging system

This chapter provides information about security features available in Netscape Messaging Server 3.0. The chapter is divided into two sections:

- "System security" on page 53
- "Encryption forms" on page 57

System security

The Messaging Server approach to system security is to carefully isolate the Messaging Server from the remainder of the system. During Messaging Server installation, a special account is created for the Messaging Server to operate under. The account's permissions are intentionally limited to those necessary to operate the Messaging Server. The majority of executable modules that constitute the Messaging Server are designed to operate in this intentionally limited environment.

Runtime permissions

With few exceptions (discussed later), the daemon, or service, portion of the Messaging Server is the only module allowed to use root permissions during runtime. Most Messaging Server executables are run under the MTA user account and group and cannot gain access to the host system beyond what is required for the messaging system.

The Messaging Server daemon, or service, known as the *dispatcher*, is the module that controls the overall operation of the messaging system, as well as permissions for the other Messaging Server modules. Because the dispatcher's main role is to manage mail delivery, it doesn't actually communicate with users or other machines.

Unix The dispatcher initially runs with root (or superuser) permissions when the Messaging Server is started so that it can initialize the network connections. Unix allows only a process with the root permissions to open and bind to a socket with a port number below 1024. The ports necessary for SMTP and POP3, for example, are 25 and 110, respectively, and thus root permission is required for those services.

Immediately following necessary initialization, and prior to accepting or processing any messages, the dispatcher irrevocably releases the root permission and hence takes only the permissions set up for the Messaging Server system during installation.

Thus, all special privileges are dropped, and only the MTA user's privileges are retained during normal operation. With few exceptions, the dispatcher runs all the Messaging Server modules with these limited permissions.

Note The exception to the rule of limited permissions is the utility module that works with Unix Deliver to create a maildrop file. Because of the ownership requirements of the Unix maildrop file—the owner is the person receiving the incoming mail, and the group is usually the mail group—there must be a special program that can create an empty file with the proper permissions to allow access for both the mail system (to deposit mail) and the user (to pick up mail from the file). This module is therefore owned by root and has root permissions.

In normal operation, the Messaging Server uses three directory trees: the executable, postoffice, and mailbox directories. The permissions for each of these directory trees allow proper operation of the Messaging Server modules while providing a secure envelope for the host system running the Messaging Server.

The owner and group on these directories are as follows:

Directory Tree	Owner	Group
executables	MTA	nsgroup (SuiteSpot group)
postoffice	MTA	nsgroup (SuiteSpot group)
mailbox	MTA	nsgroup (SuiteSpot group)

Access domains

An access domain restricts the places from which users can read their email. (The access domains are applied to the POP or IMAP mail client's hostname or IP address.)

Access can be limited to a single computer or a set of computers in an addressing hierarchy. You can specify a single computer by giving either its IP address or its fully qualified domain name (for example, `sunnyvale.dispatch.com`). Likewise, you can specify a set of computers by using an incomplete DNS or IP address. An incomplete DNS address is one that doesn't specify a particular host; an incomplete IP address is one that contains a 0, which acts as a wildcard, in any of the four numbers in the dotted quad address.

You can leave the access domain feature blank to allow access from anywhere (with the appropriate password), or you can enter the keyword "none" to prevent access to an account.

If a single computer is specified as the access domain—for instance, `sunnyvale.dispatch.com`—a user can't access mail from any other machine even when giving the correct password. If, instead, the access domain is specified as `dispatch.com`, the user can access his or her mail from any computer within the `dispatch.com` domain.

Use of domain names or IP addresses is a trade-off between flexibility and security. Using a hostname or domain name is easily understandable and immune to network topology changes, while an IP address or range might not be. Generally, IP addresses are safer than domain names as access domains. For maximum security, you can configure your access domain to be the IP address of a single computer.

Here's how an access domain might be set up:

```
sunnyvale.dispatch.com
128.123.45.0
math.csusj.edu
```

The domain entries would let you access the account from any of these computers:

```
sunnyvale.dispatch.com
complex.math.csusj.edu
fourier.math.csusj.edu
```

The IP entry would allow access from these hosts:

```
128.123.45.22
128.123.45.67
128.123.45.82
```

However, you would *not* be able to access the account from these:

```
newark.dispatch.com
laser.ece.csusj.edu
128.123.46.22
128.124.45.67
```

Access domain algorithm

This section describes the steps that the Messaging Server follows when it verifies and limits access domains during POP/IMAP logins.

When a client connects to your machine, the Messaging Server is given the IP address of the connecting computer. The algorithm used to determine if the client computer can access the server is as follows:

1. If the list is empty, access is allowed.
2. If the list contains the keyword "none," access is denied.

3. For each IP address or network in the list (for example, 123.4.5.67), the Messaging Server checks for a match with the client's IP address. Any zero is treated as a wildcard match, so 123.4.5.0 would allow any computer in the 123.4.5 class-C network to connect. If a match is found, access is allowed. (No addresses are looked up in the DNS when performing this step—the numbers are simply compared. Also note that a host file can be consulted instead of the DNS if your machine is configured to do so.)

4. For each domain name in the list, the Messaging Server checks if the hostname associated with the client's IP address is within the domain (the client's hostname is found by using the DNS or the host file). For example, if the client's hostname is determined to be `rome.dispatch.com`, the connection is allowed if `rome.dispatch.com`, `dispatch.com`, or `com` is in the list of access domains. If a match is found, access is allowed.

5. If no match is found, access is denied.

If the user's login name and password are valid, and the above check succeeds relative to the user's access domains, then the user's POP or IMAP login is successful.

Encryption forms

The Messaging Server provides two forms that you can use for added security—the IMAP Encryption form and the Security Preferences form.

The IMAP Encryption and Authentication form

This form lets you specify the level of encryption and authentication for receiving and managing messages with IMAP clients. Choose the encryption and authentication options that provide adequate security for your needs.

The IMAP Encryption form provides three options for encryption using *Secure Sockets Layer (SSL)*:

- Allow unencrypted access only

- Allow encrypted access only
- Allow both encrypted and unencrypted access

For authentications your options are:

- Use passwords only
- Use certificates only
- Use either passwords or certificates

The Encrypted port number field lets you specify a specific port for sending and receiving encrypted messages. The default is 220.

The Alias field provides a pull-down list of encryption aliases. Aliases are provided in the menu only if you have already created or imported them using the Administration Server's Generate Key or Import Alias forms. (For more information, see Chapter 4, "Understanding Encryption and SSL," in *Managing Netscape Servers*.)

The Security Preferences form

You can use the Security Preferences form to configure access domains for web form configuration.

1. Choose SSL version 3.

   Although the form presents SSL version 2 as an option, there are no IMAP clients that communicate over SSL with that version.

2. Choose the ciphers you want your server to use.

   The ciphers are listed for each version of SSL. A *cipher* is the algorithm used in encryption. Some ciphers are more secure, or stronger, than others. Generally speaking, the more bits a cipher uses during encryption, the harder it is to decrypt the data. Ciphers are described after this list.

3. Click OK.

Make sure you restart your server. When a browser initiates an SSL connection with the Messaging Server, it lets the server know what ciphers it prefers to use to encrypt information. In any two-way encryption process, both parties must use the same ciphers. Since a number of ciphers are available, you should consider enabling all ciphers.

You can choose ciphers from both the SSL 2 and SSL 3 protocols. Unless you have a compelling reason why you don't want to use a specific cipher, you should choose them all—except for the "No Encryption, only MD5 message authentication" option, as it does *not* protect data from eavesdropping. Unless there is a compelling reason to use it, this cipher should not be enabled.

Warning If no other ciphers are available in the browser, the server will use the "No Encryption, only MD5 message authentication" option, and no encryption will occur.

The SSL 2.0 ciphers are:

- **RC4 cipher with 40-bit encryption:** This cipher is an RC4 cipher, which means that it is the fastest available cipher. It has 40-bit encryption, which is the strongest encryption Netscape is permitted to export under U.S. law. Forty-bit encryption has approximately $1.1 * 10^{12}$ (a trillion) possible keys.
- **RC2 cipher with 40-bit encryption:** This cipher is an RC2 cipher, which means that it is slower than the RC4 cipher. It has 40-bit encryption, which is the strongest encryption permitted for export under U.S. law. Forty-bit encryption is not as strong as 128-bit encryption, and has approximately $1.1 * 10^{12}$ (a trillion) possible keys.

The SSL 3.0 ciphers are:

- **RC4 with 40-bit encryption and MD5 message authentication:** This cipher is the same as the SSL 2.0 version of RC4 with 40-bit encryption, but uses MD5 message authentication to detect attempts to modify data in transit.
- **RC2 with 40-bit encryption and MD5 message authentication:** This cipher is the same as the SSL 2.0 version of RC2 with 40-bit encryption, but uses MD5 message authentication to detect attempts to modify data in transit.

- **No encryption, only MD5 message authentication:** This cipher uses only MD5 message authentication to secure data. Any data sent using this cipher is sent in the clear. The data may be protected from modification, but it can be viewed by eavesdroppers.

Chapter

4

Server status and reports

Netscape Messaging Server 3.0 provides a variety of ways for you, as server administrator, to monitor the server's status and performance. Messaging Server 3.0 supports the *Simple Network Management Protocol (SNMP)* and provides controls for configuring its SNMP *subagent*. Messaging Server 3.0 also provides extensive logging and report capabilities that you can use to diagnose problems and fine-tune server performance. Finally, the server provides error messages that are automatically sent to "postmaster" and that provide valuable information and reply options for efficient server management.

This chapter is divided into three sections:

- "SNMP configuration and control" on page 62
- "Server logs and reports" on page 64
- "Error messages" on page 67

Note For more information about SNMP capabilities in Netscape server products, see *Managing Netscape Servers*.

SNMP configuration and control

Netscape Messaging Server 3.0 supports an SNMP-based subagent, which allows administrators to monitor a variety of server functions remotely through the use of an SNMP.V1-compatible network management station.

Depending on the platform you are run the Messaging Server on, the Messaging Server provides either one or two forms for configuring and controlling its SNMP subagent: the SNMP Configuration form (Unix and Windows NT) and the SNMP Subagent Control form (Unix only). To access these forms, click the Server Status button in the Netscape Messaging Server administration page.

Unix You must first configure and start the SNMP master agent via the Administration Server's Master Agent forms prior to configuring the Messaging Server subagent.

Important If the network management station has problems getting the Messaging Server's SNMP statistics, check the server's logs, as well as the SNMP process's log (located in `<server root>/mail-<nickname>/logs`).

Make sure the SNMP data collection process (`snmpcoll`) is started and running. If it is not, restart the Messaging Server.

Unix On Unix, also make sure the SNMP subagent (`ns-mailagt`) is also running. If it is not, start it from the SNMP Subagent Control form.

NT On Windows NT, make sure the SNMP Service is installed and started. Check the events in the Event Viewer to ensure that the SNMP Subagent is loaded by the SNMP Service without any error. To have SNMP traps sent to the management station, make sure that the SNMP trap is configured to contain the correct community and trap destination information. On Windows NT version 4.0, also make sure that the SNMP Trap service is started via the Control Panel.

The SNMP Configuration form

You use the SNMP Configuration form to configure the SNMP subagent. After you enter or modify the information in the fields in the SNMP Configuration form and click OK, a message appears reminding you to restart the subagent for the settings to take effect.

Unix Go to the SNMP Subagent Control form to restart the subagent.

NT Stop and restart the SNMP Service via the Control Panel.

Master Host field

Unix Use this field to specify the name of the host on which the SNMP master agent runs. What you specify here must be a machine name; IP address are not valid. (This field appears only in the Unix version of Netscape Messaging Server 3.0.)

Organization field

Use this field to specify the organization in which the Messaging Server is being used. Normally this will be a department or company name.

Location field

Use this field to specify the location of the Messaging Server, usually a street address.

Contact field

Use this field to specify the person to contact regarding issues related to the Messaging Server. This will usually be the name of the server administrator.

SNMP Statistics Collection options

Use these options to specify whether the subagent will be reporting statistics to the management station or not. If you choose "off," the subagent cannot be enabled.

The SNMP Subagent Control form

Unix Use this form after completing the SNMP Configuration form to control the SNMP subagent. The form provides three options: Start, Stop, and Restart. (This form appears only in the Unix version of Netscape Messaging Server 3.0.)

When you click Start, the Messaging Server attempts to start the subagent. The subagent cannot start successfully if the SNMP master agent has not been enabled via the Administration Server's SNMP Master Agent Control form. (See *Managing Netscape Servers* for more information.) You will see a message indicating whether the subagent has started successfully.

When you click Stop, the Messaging Server attempts to stop the subagent, if it is currently running. You will see a message indicating whether the subagent has stopped successfully.

After you modify the SNMP configuration in the SNMP Configuration form, the SNMP subagent process must be restarted for the configuration changes to take effect. When you click Restart, the Messaging Server attempts to stop and then restart the subagent. You will see a message indicating whether the subagent has restarted successfully.

Note If the SNMP Subagent fails to start or stop, check the SNMP Subagent log (located in `<server root>/mail-<nickname>/logs`).

Server logs and reports

Netscape Messaging Server 3.0 provides a variety of logging and report options that you can use to monitor and fine-tune server performance. Use the List of Queued Mail form to process queued mail. Use the Logging Preferences form to determine what components of the Messaging Server to log. You can access both of these forms by clicking the Reports button on the Messaging Server administration page.

The List of Queued Mail form

You can use the List of Queued Mail form to check the mail queue and, if you want, to tell it to attempt delivery. Messages are queued when they cannot be delivered. Once a message is queued, all subsequent messages to that address are held until the next scheduled queue processing interval (determined by the time interval you enter in the System Configuration form.)

The List of Queued Mail form provides three options:

- **Do nothing:** Netscape Messaging Server 3.0 will attempt delivery again in an hour or so, depending on how you've configured it in the System Configuration form.
- **Select the Process option:** Netscape Messaging Server 3.0 immediately attempts to deliver all queued messages to any hosts you indicated. (Note that the Queue form is organized by host.) Because of the time-out period for unreachable hosts, each host can take up to two minutes to attempt delivery.
- **Select the Expire option:** Netscape Messaging Server 3.0 gives messages queued for that host one last try. If it fails to deliver the messages, they are returned to the sender. Because of the time-out period for unreachable hosts, each host can take up to two minutes to attempt delivery.

Note These options appear only if messages are listed in the List of Queued Mail form.

The Logging Preferences form

You can use the Logging Preferences form to set the location of logs and select which logs you want to run. Following is information on the fields on the Logging Preferences form.

Log Directory field

Use this field to specify the location of the Messaging Server log. The default setting for the Log Directory field is the Messaging Server 3.0. The default setting stores the log file in the log subdirectory of the Messaging Server 3.0 postoffice (for example, `/var/spool/postoffice/log`). You don't need to specify the full pathname to use this default; instead, just type `default`.

If you want the log file stored in a different place, specify the full path to the directory here. Be sure that the permissions of that directory allow the Netscape Messaging Server access to the log file. Also, because the Messaging Server runs as a nonprivileged user for enhanced system security, it might not be able to create the log file if one doesn't already exist. In this case, simply move the existing log file to the new directory or create a new log file with proper permissions.

The Logging Preferences form provides an extensive list of the components of the Messaging Server's architecture, each entry preceded by On and Off buttons. Select the On button to log that component's activity.

Here are the components that you can log with this form:

- Netscape Messaging Server dispatcher
- Finger Server
- IMAP Server
- SIMAP4 Server
- POP3 Server
- SMTP Accept
- Account Handler
- Account Manager
- AutoReply Handler
- Configuration Manager
- Error Handler
- Mailbox Deliver
- Program Deliver
- SMTP Deliver
- SMTP Router
- Unix Deliver

Important You may want to set the logging option to "off" for the Messaging Server dispatcher and the POP3 and IMAP Servers; these modules tend to produce a high volume of log entries.

The View Logs report

The View Logs report contains a listing of all current logs in the default log file directory. The name of the log file is actually a link to the log file itself; click the name of the log (such as `NetscapeMail.log`) to view that log.

Error messages

Netscape Messaging Server 3.0 generates an error message addressed to "postmaster" whenever it cannot carry out a task. Most error messages have to do with addresses that the Messaging Server is unable to process, either because they aren't entered correctly or because they don't exist.

Users also receive error messages when they try to send a message to an address that the Messaging Server cannot recognize. (System administrators may also receive copies of these messages if they like.)

Netscape Messaging Server 3.0 provides two kinds of error messages: notification messages and the Error-Handler Action form.

Notification messages

Many messages don't require any action on your part and are sent simply to advise you that something has happened. Usually they warn you of an error condition, but occasionally are for your information only. For example, a notification message might tell you that somebody has tried to exploit a sendmail vulnerability to try to break into your system.

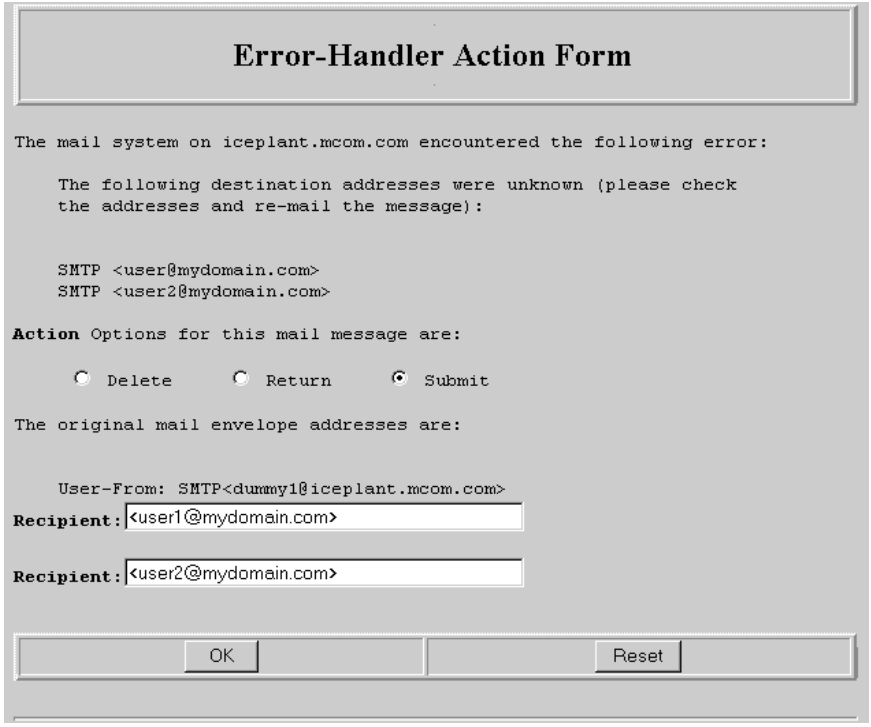
Netscape Messaging Server 3.0 will notify you if someone tries to send a message to an unknown address in your domain. Sometimes it's worth paying attention to such messages—for instance, if you get a deluge of messages for something like `help@`*`your.domain`*. In this case, it is likely that people trying to get messages through to this address are customers or potential customers, and this would be a hint for you to set up an account for the address `help`.

Error-Handler Action form

The Error-Handler Action form is sent as an attachment to an email message when an error occurs that requires you to decide how to deal with the error.

For example, you can set the Netscape Messaging Server 3.0 to consult with you every time you receive a piece of mail addressed to your domain but without a valid address. In this case, the Error-Handler Action form will indicated the faulty address and ask you whether you want to delete, return, or submit the message. Figure 4.1 shows an example of this type of message. In the example, the phrase "destination addresses were unknown" indicates that the Messaging Server was unable to recognize the message address and is waiting for you to indicate what to do with it.

Figure 4.1 A sample error message.



Don't ignore or throw away these messages, or the host machine disk will start to fill up with unresolved errors. Ignored messages are automatically returned to the sender, if possible, only when the maximum queue time (Days) has passed. The delete option shouldn't be used carelessly because only the system administrator receives an error notice.

To properly handle the error, click `Delete`, `Return,` or `Submit`. If you click Submit, you can edit the Recipient field if you want to redirect the message or fix an incorrect address. (If you choose `submit`, you must enter a valid address in the Recipient field.) When you have completed filling out the form, click OK. The error handler will process the form and either delete, return, or redirect the message, as you've indicated.

Appendix

A

Messaging Server architecture

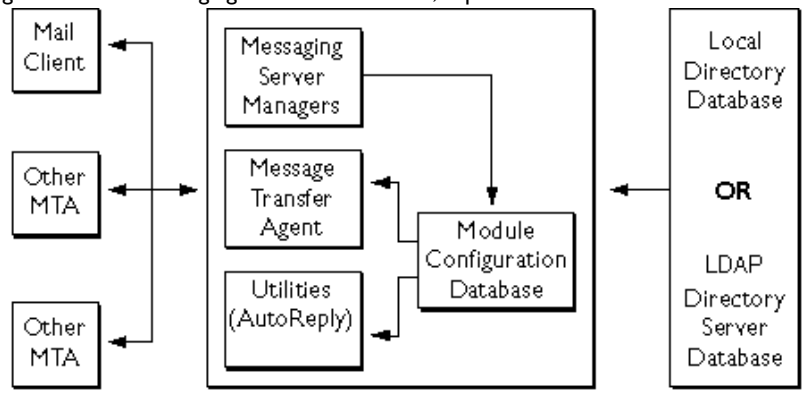
This appendix describes the design architecture of the Netscape Messaging Server software. This information is helpful if you need to assess the software architecture to alleviate security concerns or are curious about the inner workings of the Messaging Server.

The Messaging Server functions are distributed among a number of software modules that work together to carry out message handling and other activities. As Figure A.1 shows, the Messaging Server is divided into six major components. These components, which form the top-level architecture, all run under the supervision of the dispatcher:

- The dispatcher is the *daemon* (or *service*) component of the Messaging Server. It coordinates the activities of all other modules. In Figure A.1, the dispatcher can be thought of as an envelope that contains and initiates the processes of all items shown within the largest box.
- The module configuration database contains general configuration information for the other modules.
- The message transfer agent (MTA) handles all message accepting, routing, and delivery tasks.
- The Messaging Server managers facilitate remote configuration and operation of the system and ensure that the modules are doing their job and following the rules.

- The AutoReply utility lets the Messaging Server automatically reply to incoming messages with predefined responses of your choice.
- Directory databases—either local directory databases or Directory Servers—contain user and group account information for the other modules.

Figure A.1 The Messaging Server architecture, top level.



The following sections discuss each of these components.

The dispatcher

The dispatcher's job is straightforward: it monitors all network ports related to email and launches the appropriate modules to handle incoming connections. The dispatcher also controls the number of processes that can be operating simultaneously so that it can limit the amount of computer resources used to process email.

For example, when the dispatcher notices an incoming email message, it starts up the MTA, which takes the message in and processes it.

The module configuration database

The module configuration database contains the Messaging Server configuration information. Every Messaging Server module has a database that contains the configuration information for that module. For most modules, this database is fairly small because it contains only a few configuration options and a list of error messages.

The message transfer agent

The Messaging Server is first and foremost a message transfer agent, or *MTA*. The MTA is a powerful and complicated set of modules. Because the MTA represents the primary functionality of the Messaging Server system, it is described in detail in this section.

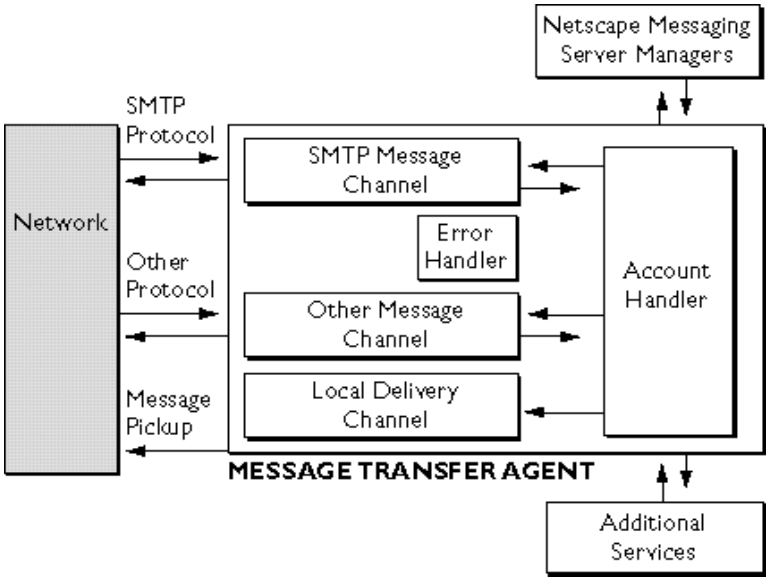
An MTA can be used to coordinate message transfer between a small number of computers on a local network or to orchestrate the transfer of thousands of messages beyond the local network to millions of Internet users.

The Messaging Server MTA is divided into three components: message channels, the local delivery channel, and handlers:

- Messages leaving the local host computer are sent to other MTAs through a message channel. Each message channel uses a specific protocol, such as the *Simple Mail Transfer Protocol (SMTP)*, to format messages. The Messaging Server's primary message channel is the SMTP channel, which formats messages according to the open standard employed on the Internet.
- Local mail and incoming messages for users with local accounts are delivered by the local delivery channel.
- Handlers help route messages. Usually, incoming messages are sent to the account handler, which determines to whom the message should be delivered. If there is some insurmountable problem (such as a bad address), the account handler can route the message to the error handler.

These three basic components of the Messaging Server MTA are shown in Figure A.2 and are discussed in greater detail in the following sections.

Figure A.2 Message channels, the local delivery channel, and handlers.



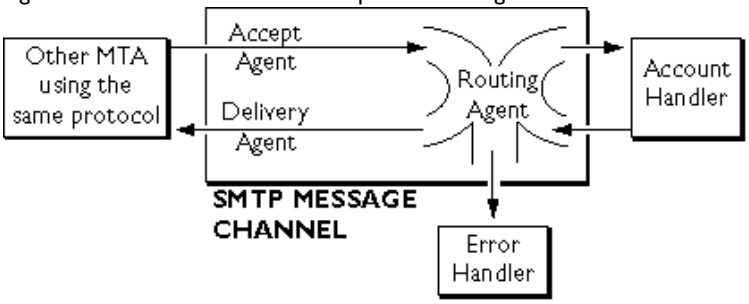
Message channels

The Messaging Server message channels exchange messages with other MTAs and accept new messages from mail clients. Message channels can relay messages to and from other the Messaging Server modules and, in some cases, accept and dispatch messages without consulting other modules. (If a channel alias is used, an incoming message can be immediately forwarded to another MTA without being handled by another module.) One of the principal message-channel tasks is to accept messages addressed to local recipients (users with Messaging Server accounts) and forward them to the local delivery channel.

The components of a message channel

A message channel is a group of Messaging Server modules that transfers messages using a single protocol such as SMTP or X.400. Each channel consists of an accept agent, a routing agent, and a deliver agent, as shown in Figure A.3.

Figure A.3 SMTP channel is an example of a message channel.



Accept agents are modules that accept incoming messages detected by the dispatcher. The accept agent can be configured to accept messages only for recipients that it recognizes (that is, for those who have Messaging Server accounts). The Messaging Server can also accept messages and forward them to other MTAs.

Once a message comes in, it is immediately transferred to the message-channel *routing agent*. The *routing agent* examines the message headers and makes sure that the instructions they contain are compatible with the way the message is being handled. It then forwards the message to the deliver agent (if the message is to be relayed to another MTA), the account handler (for delivery to a local user), or the error handler (if there is some confusion about what to do with the message). Messages can also enter the message channel at the routing agent if they originated in another module of the Messaging Server (such as the AutoReply handler) or from another message channel (that is, from a different protocol).

The *deliver agent* sends messages to other remote MTAs that use the same protocol (such as SMTP). The deliver agent takes a message from the routing agent, contacts the remote MTA for the recipient of that message, and delivers the message to that MTA. The deliver agent determines which remote MTA the message should be sent to.

The SMTP channel

The SMTP channel is a common example of a message channel and is a standard feature. (See Figure A.3.) Most MTAs on the Internet use SMTP to accept and relay messages.

In some cases, a message is transferred solely by the SMTP channel—this means that the message is accepted, routed, and delivered (to another MTA) through the SMTP channel. (For example, this is the process that is followed if the message is just being sorted and forwarded to another MTA on the Internet or your local network.)

In other cases, a message might be accepted by the SMTP accept agent, passed through the SMTP routing agent to the account handler, and then delivered by the local delivery channel to a user on this particular Messaging Server host (see the next section for more information on the local delivery channel).

In a third case, a message might be accepted by one message channel but be delivered by another channel. In this case it is accepted according to one protocol and delivered according to another, so that the Messaging Server acts as a switch (or gateway) between the different mail protocols.

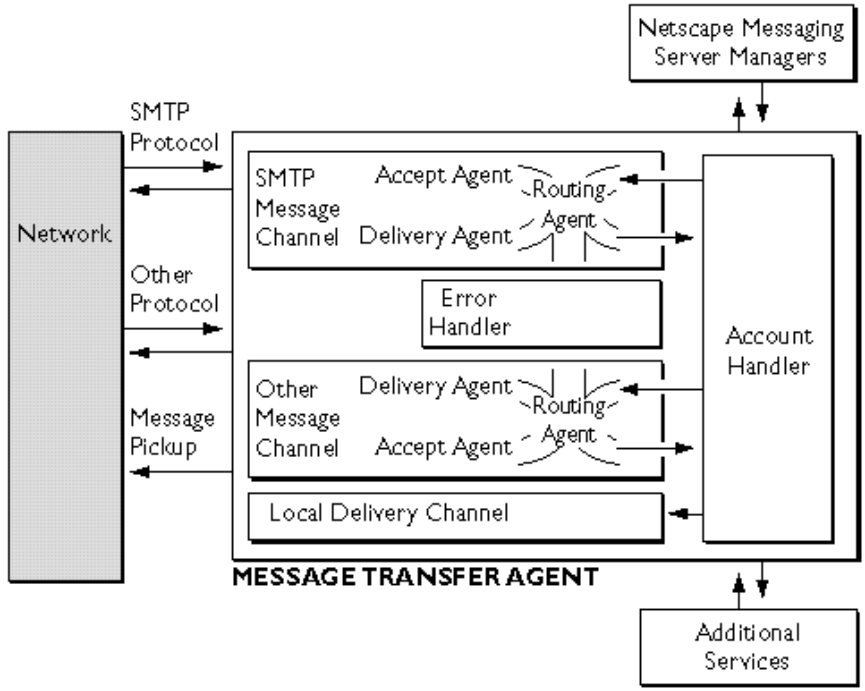
Switching messages between channels

When a message-channel routing agent examines a message envelope, it might determine that the message shouldn't be forwarded to the deliver agent. This happens when the address indicates either that the message should be delivered locally or that it should be delivered according to another protocol. If this occurs, the message is forwarded to the account handler, which determines what to do with the message.

When a message is transferred to another message channel, the account handler forwards it to the appropriate message channel routing agent. For example, a message might go from the SMTP routing agent to the account handler and finally to the routing agent of the X.400 channel.

When a message is transferred to the account handler because it is addressed to a local recipient, the account handler forwards the message to the local delivery channel. Figure A.4 shows the logical paths between message channels and the network.

Figure A.4 A detailed look at the role of the message channel.



The local delivery channel

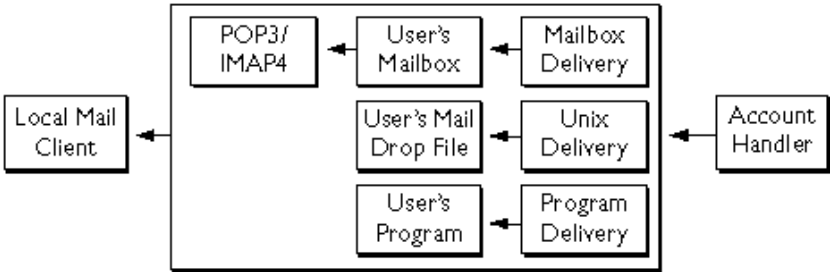
The local delivery channel consists of those Messaging Server modules that transfer messages to mail clients: POP3 or IMAP4 local delivery, Unix maildrop delivery, and program delivery. Only users with Messaging Server accounts can receive messages through the local delivery channel.

When the Messaging Server accepts a message (with one of the message channels) that it recognizes as being addressed to a local recipient (that is, to someone with an email account), the message is routed to the local delivery channel. The Messaging Server recognizes an address when it compares the address of an incoming message against the entries in the directory database.

The path (POP3, IMAP4, Unix, or program delivery) that a message takes to reach a recipient is determined by the choices you made when completing the New User form for a particular user. If users want to change how they receive their mail, they can use the Information form to do so.

Figure A.5 shows the delivery options in the local delivery channel, which are described in the following subsections.

Figure A.5 The local delivery channel—POP3/IMAP4, Unix, and program delivery.

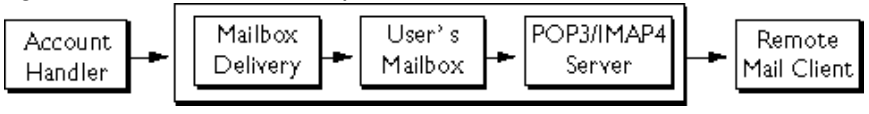


POP3 or IMAP4 delivery

The POP3 and IMAP4 delivery modules take incoming mail for users and file it in the user's mailbox directory, as shown in Figure A.6. The mail is retrieved later by a mail client running on a remote computer.

Note Users must choose either IMAP4 or POP3; they cannot access their mail from both.

Figure A.6 POP3 or IMAP4 delivery.

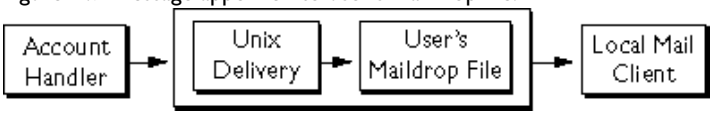


A user who would like an email account need only have a means of establishing temporary contact with the host machine (the computer on which the Messaging Server is running). Thus any computer that can connect to the host machine (generally through a network such as an Ethernet or the Internet) can be part of the email system that the Messaging Server coordinates.

Unix delivery

Unix Unix delivery is available on Unix machines. As Figure A.7 shows, Unix delivery adds new messages to the user's maildrop file. The mail client then looks to this file for any new messages. Unix delivery can be used only by users with a system account on the Messaging Server host (in addition to the Messaging Server account).

Figure A.7 Message appended to user's maildrop file.



Program delivery

As Figure A.8 shows, program delivery lets users have their messages delivered to a program.

Figure A.8 Message delivered to a program activated at the same time.

Users who receive a high volume of messages sometimes opt to have a program sort their messages as soon as they arrive. Mail-sorting programs can warn users of urgent messages or place different kinds of messages in different folders. For example, messages from mailing lists can go in one folder, professional-related mail in another, and personal mail in yet a third. As with Unix delivery, program delivery requires the user to also have a system account. Some mail clients sort through normal mailbox or Unix delivery and don't require program delivery. Program delivery must be set up by the server administrator or system administrator.

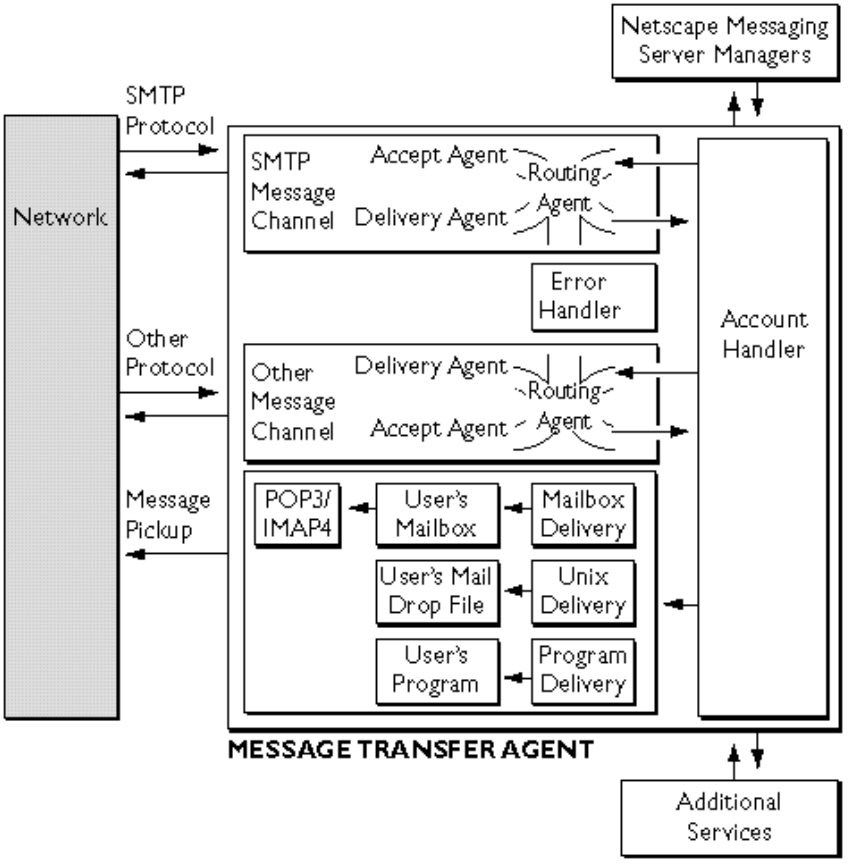
The message transfer agent handlers

Handlers determines what to do with messages and supervise the transfer of email between modules. Under normal circumstances, the account handler routes messages between the channels and modules. Unusual messages that the account handler cannot process are forwarded to the error handler.

The account handler

Figure A.9 hints at the central role the account handler plays in coordinating message transfer between message channels. The account handler makes its decisions based on information located in the databases maintained by the Messaging Server managers. It also shuttles messages to and from the AutoReply utility.

Figure A.9 The local delivery channel's role detailed in the MTA.



The error handler

Whenever the Messaging Server receives a message it can't process, it gives the message to the error handler. In some cases these messages are returned to the sender. Alternatively, the Messaging Server can be configured to hold these messages until the server administrator decides what to do with them.

If the error handler receives a message that the Messaging Server can't handle, it sends the server administrator an email explaining what happened. The server administrator has to decide how to handle the error. The error handler provides the server administrator with a form offering options for resolving the error; when this form is completed and submitted, the error is resolved. Alternatively, the server administrator is simply advised that the error occurred, and no action is required.

The AutoReply utility

The AutoReply utility lets you instruct the Messaging Server to automatically reply to messages an account receives.

When the account handler processes an incoming message for a local account, it has to determine whether the account invokes the AutoReply feature. If it does, the AutoReply module takes the AutoReply message (which is specific for that account), formats an automated outbound message in response to the message received, and passes this reply back to the MTA for delivery.

Incoming messages are routed from the message channel to the account handler. The account handler then consults the account database and can forward a message either to a message channel (to deliver to another address at another host) or to the local delivery channel (for delivery to a user).

Similarly, the account handler can forward a message to the AutoReply handler module. Because messages are forwarded to the account handler in much the same way as they are forwarded to the message and delivery channels, the account handler configuration fields are considered to be a specialized form of delivery.

Directory databases

The directory database contains the user's account information (see Figure A.1) and can be either a local database installed on the same system as the Messaging Server or a dedicated *Lightweight Directory Access Protocol (LDAP)* directory server, such as Netscape Directory Server, running either locally on the same system or on a remote system.

The directory database holds all the user account information and can therefore be quite large. All modules refer to the directory database when they need account information to process a message or otherwise carry out a task. Because all user information is in this database, a single configuration change updates all modules at once.

The Messaging Server finger service

The *finger service* is the most common directory service on the Internet and provides a means to obtain basic information about someone by using their email address.

The finger server receives inquiries directly from the network according to the finger protocol. Referring to the appropriate information in the directory database, it responds directly to the query over the network. Although the finger server and the Messaging Server MTA both refer to the directory database, they otherwise work independently. This independence, coupled with the fact that the finger service can be automated, facilitates easy management and consistency of information and greatly reduces the server administrator's workload. It also provides the added security of using one coordinated set of services (to which access can be limited as desired) rather than a haphazard array of individual servers.

For maximum security, access to the finger service can be limited to specific domains or hosts (or eliminated completely) at the discretion of the server administrator.

Appendix

B

Compatibility with sendmail

This appendix provides information for system administrators who are considering migrating, or who have already migrated, from sendmail to Netscape Messaging Server.

This appendix is divided into three sections:

- "Functional compatibility" on page 83 describes how tasks that you do with Unix sendmail can be accomplished with Netscape Messaging Server 3.0.
- "Command-line compatibility" on page 86 outlines the compatibility of Netscape Messaging Server 3.0 replacement sendmail program.
- "Sendmail replacement program reference" on page 88 lists all the available command-line arguments that Netscape Messaging Server 3.0 sendmail replacement program recognizes.

Functional compatibility

The following sections specify the differences between Unix sendmail and the Messaging Server sendmail replacement with regard to SMTP, aliases and mail forwarding, program delivery, file delivery, and mailing lists.

SMTP network interface

You can configure Unix sendmail to exchange mail with remote destinations using SMTP. Mail routing is achieved with rule sets containing address production rules written in a specialized programming language used to take addresses apart and put them back together in useful ways. Although this is a very powerful facility, it is error prone and requires extensive knowledge of Internet standards to set it up correctly.

In contrast, Netscape Messaging Server comes with a preconfigured SMTP channel for interacting with other machines on the Internet. If you have any special routing requirements, the Messaging Server provides channel aliases and a mail-routing table, which should cover those needs.

The following two sections describe mail flow through the SMTP channel of the Messaging Server.

Incoming mail

Incoming mail is received by the SMTP-Accept module of the Messaging Server. Its job is to read in one or more messages from a remote mail server and store them in the message queue. For each incoming message, SMTP-Accept invokes the SMTP-Router to determine how to route the message to its destination.

Outgoing mail

If the SMTP-Router determines that a message needs to be delivered to a remote site using SMTP, it gives the message to the SMTP-Deliver module. This module contacts the destination computer (actually one of its mail exchangers) and delivers the message. If for some reason delivery fails, the message remains queued for a later attempt or is returned (if the error is considered permanent).

Aliases and mail forwarding

Unix sendmail supports several types of aliases in the `/etc/aliases` file and in users' personal `.forward` files. The various types of aliases allow

- local users to receive mail at several addresses
- messages to be distributed to multiple recipients

- messages to be forwarded to users at other machines

With Netscape Messaging Server, each type of alias is created differently because of the structure of user accounts in the directory database.

Delivery to programs

Using Unix sendmail, you can create an alias or forward that delivers an incoming message to a program. The program then reads the message and performs some operation depending on the message contents. Usually these types of programs filter messages into different mailboxes or send out vacation notices. This functionality makes it easy to extend the mail system to do virtually anything you want but has been problematic with respect to security.

You can use the Administration Server's New User form to set up Netscape Messaging Server program delivery. Because there are security issues specific to program delivery, program delivery is disabled by default.

Delivery to files

Unix sendmail makes it possible to set up an alias or `.forward` file to append mail to a file. This can be used to keep a record of incoming mail or to delete incoming mail by sending it to `/dev/null`. However, the author of sendmail recommends using an alternate delivery agent for delivery-to-file needs invoked through the delivery-to-program facility.

The Messaging Server's sendmail replacement will append undeliverable messages to users' `dead.letter` files, for users with Unix Delivery enabled. No general delivery-to-file facility is planned for the Messaging Server; appending mail to a file should be done with the delivery-to-program facility.

Mailing lists

Mailing lists in Unix sendmail are implemented using aliases and program deliveries. List recipients are stored either in the aliases database or in an external file using an `:include:` alias. Several mailing-list administration programs are available that can automate the task of maintaining recipient distribution lists, while sendmail handles the delivery of the messages.

With Netscape Messaging Server 3.0, you create groups in the Administration Server's User and & Group forms to provide mail lists. (See Chapter 1, "Working with users and groups" for information on creating groups.)

Command-line compatibility

The Messaging Server mail system includes a program that replaces `/usr/lib/sendmail` on Unix machines. Most of Unix sendmail's functionality is performed by one or more modules in the Messaging Server, so the sendmail replacement actually has limited use. However, it is needed for compatibility with many mail programs that employ Unix sendmail rather than SMTP to deliver their mail. It can also be used to start up the Messaging Server mail system and to check and deliver the mail queue.

Sending mail with the sendmail replacement

The Netscape Messaging Server sendmail replacement program maintains compatibility with existing software that delivers mail using the sendmail command. This software runs the sendmail command and feeds it the message to be delivered. It is then up to the sendmail replacement program to deliver the message to all the recipients.

Some examples of commands that work for sending mail are

```
/usr/lib/sendmail -t < /tmp/message
```

```
cat file1 | /usr/lib/sendmail -oem recip1,recip2
```

For a complete list of command-line switches and options related to sending mail, see "Sendmail replacement program reference" on page 88.

Starting the Messaging Server with sendmail

Because Unix sendmail comes installed on most Unix-based machines, many scripts such as system boot scripts exist to start up sendmail. This is done with a command such as

```
/usr/lib/sendmail -bd -q30m
```

The Netscape Messaging Server sendmail replacement recognizes this command and starts up the Messaging Server if it isn't already running. The `-q30m` switch is ignored in this command because queue intervals are set up in the system configuration of the Messaging Server.

Checking the mail queue

Many system administrators are used to typing `mailq` to check for queued messages. The sendmail replacement provided with the Messaging Server will respond to this command with the contents of the mail queue. However, many server administrators prefer to use the Messaging Server mail queue form, which makes processing the queue a little easier.

To check the mail queue, type `mailq` at a command prompt. If there are no queued messages, that fact will be reported:

```
% mailq
Mail queue is empty.
%
```

If there are queued messages, each host that has queued messages waiting to be delivered will be listed, along with the number of pending deliveries. For example, output might look like this:

```
% mailq
       Queued Messages    Destination Host
       ---------------    ----------------
              2           math.csusj.edu
              3           expertelligence.com
%
```

In this example, five messages are waiting for delivery. Delivering all of them should require two connections to other machines because the Messaging Server attempts to deliver all queued mail for a host before disconnecting.

Other modes

The Unix sendmail program has several other operating modes that aren't necessary or aren't supported in Messaging Server 3.0. For a complete list of supported operating modes and command-line switches and options, see "Sendmail replacement program reference" next.

Sendmail replacement program reference

This reference section lists all the available command-line arguments that the Messaging Server 3.0 sendmail replacement program recognizes. It also describes the behavior to expect when they are used. Certain options are recognized (through the `-O` command-line switch); their effects are noted in a separate table.

Alternate names for sendmail

The Unix sendmail program can be run under several names as a shorthand way to specify the action to perform. The Messaging Server 3.0 sendmail replacement program recognizes several alternate names. The behavior that results from invoking the sendmail replacement with one of the alternate names is summarized in Table B.1.

Table B.1 Invoking sendmail with alternate names

Name	Default behavior
sendmail	Sends a single mail message.
newaliases	Prints an error message because the aliases file is not used.
mailq	Reports the contents of the mail queue.

Table B.1 Invoking sendmail with alternate names

Name	Default behavior
smtpd	Runs the Messaging Server daemon.
bsmtp	Prints an error message because batch SMTP is not supported.

Note The behavior listed in Table B.1 will result if no other behavior is specified using a command-line option such as `-b` or `-I`.

Command-line switches are processed using `getopt(3)` as in V8 sendmail. All of the switches supported by V8 sendmail, IDA sendmail, and other versions of sendmail are recognized; the extent of support for these switches is given in Table B.2.

Table B.2 Command-line switches

Switch	Impact on Behavior
-B	If set to 7 bit, the high bit is stripped from every byte of the input message.
-b	Changes the mode of operation. The following modes are supported: • -be Starts the Messaging Server mail system. • -bm Sends a single mail message. • -bp Shows the status of the mail queue. These modes are recognized but not supported: • -ba Uses Arpanet protocols. • -bb Does batch SMPT on standard input. • -bi Initializes the aliases database. • -bs Does SMTP on standard input. • -bt Goes into address-testing mode. • -bz Freezes the configuration.
-C	None. There is no configuration file, so this switch is ignored.
-c	None. This switch is obsolete.
-d	None. This switch is ignored because there is no debug mode.
-e	Sets the error reporting mode (see option e in the following table).

Table B.2 Command-line switches

Switch	Impact on Behavior
-F	Sets the full name of the sender. If the user running sendmail isn't root, daemon, UUCP, SMTP, mail, or sendmail, a header is added to the message indicating the actual sender.
-f	Sets the email address of the sender. The same precaution is taken as in the -F switch.
-h	None. The hop count is determined by counting the number of received headers in the message.
-I	Runs as if invoked a s "newaliases," which just prints an informational message.
-i	None. This is the default behavior. If sendmail is run interactively, a single "." (period) will end the message. If it is run noninteractively (for example, through a pipe to standard input), the end-of-file condition determines the end of the message.
-M	The entire queue is processed regardless of the specified Message ID.
-m	None. This is the default behavior. The sender is never removed from the list of recipients if it is listed as a recipient.
-n	None. This switch is not supported.
-o	Sets an option. See the next section for a list of supported options.
-p	None. This switch is not supported.
-q	The deferred message queue is processed. If a time interval is given (as in "sendmail -bd -q30m"), this switch is ignored. If specified as -qR, -qS, or -qI (as in V8 sendmail), then the behavior is the same as -R, -S, or -M, respectively.
-R	Attempts to process the queue for hosts matching the pattern provided (for example, sendmail -Rabc will start delivery of queued messages for all hosts containing the string "abc").
-r	Same as -f switch.
-S	The entire queue is processed regardless of the specified sender.
-s	None. This switch is obsolete.
-T	None. This switch is obsolete.
-t	Recipients are gathered from both the command line and the message header, and the message is delivered.

Table B.2 Command-line switches

Switch	Impact on Behavior
-v	Output is more verbose when sending mail.
-x	None. This is an illegal switch that is recognized only to prevent printing an error message.
-Z	None. There is no frozen configuration file (or even a regular configuration file).

Options for sendmail

The Netscape Messaging Server sendmail replacement doesn't need a configuration file (`sendmail.cf`), yet most of Unix sendmail's options can be set from the command line. Many of the options are meant for the sendmail daemon, but some of them are relevant to the normal operation of sending mail.

All the options supported by V8 sendmail are recognized, and the extent of the support for these options is shown in Table B.3. The options listed in Table B.3 refer only to the replacement sendmail program, not to Netscape Messaging Server as a whole. Many of the options not supported by the sendmail replacement are supported by the Messaging Server in one way or another. Refer to the relevant sections of this guide to determine how to set parameters within the Messaging Server.

Table B.3 Options supported by V8 sendmail.

Option	Impact on Behavior
7	If set, the high bit is stripped from every byte of the input message. Also see the -B command-line switch.
B	This is always set to "." (period) and cannot be changed.
d	None. Because messages are always just posted to the local SMTP server, the turn-around time is fairly quick, so the "i" or interactive mode, is always used. However, support for other delivery modes may be added in the future.

Table B.3 Options supported by V8 sendmail.

Option	Impact on Behavior
e	Changes the error-reporting mode. Valid modes are e, m, p, q, and w. The behavior for each mode is the same as sendmail. However, if the local SMTP server is unavailable for some reason and mode m is chosen, the error message will not be deliverable either. In this case, the message is saved in the sender's ~/dead.letter file.
f	None. When a "From:" line is received, it is changed to "X-Unix-From:" so that it will be RFC822 compliant.
i	None. See the -i command-line switch for details.
o	None. This is the default behavior and cannot be disabled.
v	Turns on verbose output. Also see the -v command-line switch.
Others	No other options have any effect. All other options, even invalid ones, are ignored.

Appendix

C

Program delivery

This appendix explains how to set up the Messaging Server to deliver incoming messages to external programs.

Note Program delivery is currently available only on the Unix platform. This feature is disabled by default and must be enabled before it can be used.

Here's what you'll read about in this appendix:

- "About program delivery" on page 93
- "Program delivery terminology" on page 94
- "Trusted and untrusted operating modes" on page 96
- "Configuring for program deliveries" on page 98

About program delivery

You can configure each account in the Messaging Server to do a variety of things with messages it receives. Usually this involves putting the message in a mailbox, forwarding it somewhere else, or generating an automatic response. To accommodate the needs of advanced users who want tighter control over

the handling of their mail or to create autonomous services such as a file server, Netscape Messaging Server offers the ability to deliver mail to external programs that can carry out these additional tasks.

When you set up program delivery for an account, a custom program will be run whenever mail arrives for that account. The Messaging Server starts the program as if it were logged in to the host as the recipient of the mail, and the mail is handed over to the program. The following two examples describe situations in which program deliveries are helpful.

Program delivery can be used to help sort mail. If you receive a great deal of email, you might want to consider using a mail filter. In this type of program delivery, messages are delivered to the filtering program as they arrive. The mail filter scans each message to determine into which of several mailboxes it should be put, and then delivers it there.

An automatic filter can usually sort messages based on the sender or the topic of the message.

Program delivery can also be used as an email file server. Some sites have a lot of information that they wish to make publicly available. The most common way to share files on the Internet is to make them available through the File Transfer Protocol (FTP) or the World Wide Web (WWW).

Many people, however, have only email access to the Internet and can't benefit from such services. You can make files available to these people with a file server that can send documents in response to received email requests. A request sent to your typical email file server consists of one or more commands such as this:

```
SEND /documents/internet/rfc/rfc0822.txt
```

Program delivery terminology

The following terms are used throughout this section:

- **Setuid-root program:** A program that acquires root permissions when it is run. Such programs need more permissions than those of the user who executes them to perform certain tasks. Setuid programs can be identified by an *s* as the user-execute permission in the output of `ls -l`, as shown here:

```
-r-s--x--- 1 root mta 70064 Feb 17 10:32 Program-Deliver
```

- **Controlling user:** The Unix user for whom a command is executed. This is the user specified in the Unix LoginName field of an account. Before running a command, the program delivery module of the Messaging Server relinquishes its root permission and acquires the permissions of the controlling user (using the `setuid(2)` system call).

- **Restricted environment:** Many programs (especially shells such as `/bin/sh` and so on) use information from environment variables to modify their behavior. To avoid the possibility of security problems, the only environment variables passed to an external program are TZ (time zone information), AGENT= the Messaging Server (for compatibility with sendmail), and sometimes PATH.

- **Trusted program:** When running the Messaging Server in an untrusted environment, you can designate a collection of programs as *trusted*. Such programs are believed to function properly even if run by someone with malicious intent. Trusted programs typically consist of mail filters, distribution list software, automatic responders, and the like.

- **Trusted program directory:** The program delivery module looks for trusted programs in a special directory known as the *trusted program directory*. (Its location is `<server root>/bin/mail/server/trusted` and cannot be changed.) Any executable file (or a hard or soft link to an executable) in this directory is considered to be a trusted program. When the program delivery module runs a trusted program, it ignores the path specified in the user's account and executes the one found in this directory. This allows the system administrator to specify the exact executable files that the program delivery feature will run. For example, if users want to set up a program delivery that notifies them whenever new mail arrives, they can specify it in their account as

  ```
  /usr/local/bin/new_mail
  ```

  ```
  /home/user3/bin/new_mail
  ```

  or simply as

  ```
  new_mail
  ```

  and the trusted version of the `new_mail` program found in the trusted program directory will be executed. The details of how to set up the trusted program directory are included later in this appendix.

- **Valid shell:** Before running a program as a controlling user, the login shell of the user is checked against the list of valid shells found in `/etc/shells`. The `/etc/shells` file is simply a list of shells, one per line, that can be used to log into the system. If this file is missing or empty, the user's shell is checked against the following default list:

  ```
  /bin/sh   /usr/bin/sh
  /bin/csh  /usr/bin/csh
  /bin/ksh  /usr/bin/ksh
  ```

  The Messaging Server therefore won't run commands for users who aren't normally allowed to log in and type the commands themselves.

Trusted and untrusted operating modes

The program delivery module in the Messaging Server can operate in one of two modes, either trusted or untrusted, depending on the level of security desired. The module determines which operating mode to use by checking for programs in the trusted program directory.

If no programs are found, the system operates in trusted mode and lets users run any command on the system. If at least one file is in the trusted program directory, the system runs in untrusted mode and restricts users to running only the trusted programs. Only the system administrator (that is, root) of the machine is allowed to add or remove trusted programs, so the untrusted mode is very secure. Regardless of how accounts are set up, because the trusted programs are the only programs on the system that the mail delivery module will run, the security vulnerability of a system running the Messaging Server is limited to this small collection of programs.

The system administrator will ensure that each trusted program is well understood and known to be safe. In particular, programs that interpret their input as a sequence of commands (such as shells like `sh` and `csh` or scripting languages like perl and tclsh) are not usually set up as trusted programs.

The following algorithm is used to deliver mail to a user with a valid shell when the Messaging Server is set up in untrusted mode:

1. The Messaging Server sets up a restricted environment consisting of only the variables TZ and AGENT.
2. The Messaging Server permanently gives up root permissions by changing to those of the controlling user (using `setuid(2)`).
3. The Messaging Server switches to the controlling user's home directory if possible (it remains in `/tmp` if a failure occurs).
4. The Messaging Server performs two checks—one to make sure there are no special characters in the command and one to ensure that the program to run is a trusted program. (The special characters are $ ^ & ( ) | ` ; < > CR and LF. So, for example, you won't be able to run two programs connected by a pipe when you're using the Messaging Server delivery in untrusted mode.)
5. The Messaging Server runs the trusted program (using `execve(2)`) without invoking a shell such as `/bin/sh`.
6. The Messaging Server feeds the message to the running program.
7. If the program exits abnormally or produces any output, an error message is generated.

As server administrator, you are less likely to run the program delivery module in trusted mode. This is because trusted mode bypasses some of the security systems that systems administrators use. For example, in trusted mode users can set up accounts with improper system permissions, because they can assign an arbitrary Unix login to any account. Such an account could then be used to run commands as the assigned user, provided the user has a valid shell. Trusted mode can also open the doors to system invasion via the Internet.

When using trusted mode, you and the system administrator can take precautions that minimize the risks. First, set up the Messaging Server to run in the untrusted mode by default; this is done by adding selected programs to the trusted program directory. Second, set up special accounts such as bin, sys, adm, and so forth with shells that aren't valid for delivering mail to programs. (Note that leaving the shell field blank doesn't accomplish this because a default of `/bin/sh` is assumed.) In the trusted mode, it's especially important not to override the checking of valid shells in `/etc/shells`.

The following algorithm is used by the Messaging Server when delivering mail through the program delivery facility to a user with a valid shell:

1. The Messaging Server sets up a restricted environment consisting of only the variables TZ, PATH, and AGENT.
2. The Messaging Server permanently gives up root permissions by changing to those of the controlling user (using `setuid(2)`).
3. The Messaging Server switches to the controlling user's home directory if possible (it remains in `/tmp` if a failure occurs).
4. The Messaging Server runs `/bin/sh` with the command line specified in the account.
5. The Messaging Server feeds the message to the running program.
6. If the program exits abnormally or produces any output, it generates an error message.

Configuring for program deliveries

The following instructions explain the steps that must be performed to enable program deliveries. Server administrators and system administrators must work together to complete these steps. Because of the security issues involved, the program delivery module is disabled by default and must be activated explicitly by the system administrator.

The commands shown in the examples assume that the executable programs have been installed in `/opt/NscpMail`. In the executable directory are several subdirectories, including `local/` and `trusted/`, where the program delivery module and the trusted program directory, respectively, are located.

Enabling the program delivery module

The program delivery module is activated by performing two simple steps as root. The resulting mode of operation is the trusted mode, so further configuration is required to set up the untrusted mode (which is highly recommended for most situations) with a list of trusted programs.

Removing the NO-PROGRAM-DELIVERIES file

Whenever the program delivery module finds a file in the trusted program directory named No Program Deliveries, it refuses to deliver mail to any program. If a mail user attempts to deliver mail to a program (by setting the option on the Account or Information form), the Messaging Server generates an error message to the "postmaster."

You or the system administrator must remove this file for program deliveries to work.

```
cd /usr/netscape/suitespot/trusted
rm NO-PROGRAM-DELIVERIES
```

Note The filename must be typed exactly as shown in all capital letters and with dashes.

The program delivery module

To run programs as a controlling user, the program delivery module needs to be setuid-root. This step probably must be completed by your system administrator. If the setuid-root permission bit isn't set, messages destined for users' programs are deferred until either the setuid bit is enabled or the maximum queue time expires and the message is returned to the sender.

```
cd /usr/netscape/suitespot/local
chmod u+s Program-Deliver
```

Setting up the trusted program directory

If you want to set up the Messaging Server to run in the more secure untrusted mode, you must set up some trusted programs. To do this, you or the system administrator must copy each program to the trusted program directory or create a link in the directory to the program. This short example shows one way to set up a program called mail-filter as a trusted program:

```
cd /usr/netscape/suitespot/trusted
ln -s /usr/bin/mail-filter mail-filter
```

Note It's important to remember that programs that interpret their input as a sequence of commands to execute (such as `sh`, `tclsh`, or `perl`) should not be set up as trusted programs. However, some scripts that run under such programs can be considered safe after careful inspection.

Setting up the list of valid shells

If you want to allow users with login shells other than `sh`, `csh`, or `ksh` to use the program delivery feature, you need to set up `/etc/shells`. Your system administrator may wish to perform this task. Note that if you're creating the `/etc/shells` file for the first time, you need to include entries for any of the six default shells that you want to allow. Here's an example of a possible `/etc/shells` file:

```
% cat /etc/shells
/bin/csh
/bin/ksh
/bin/tcsh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/tcsh
%
```

Disabling the program delivery module

You or your system administrator can disable the program delivery module by replacing the No Program Deliveries file. As long as this file remains in the trusted program directory, the Messaging Server will not deliver any mail to programs.

```
cd /usr/netscape/suitespot/trusted
touch NO-PROGRAM-DELIVERIES
```

Note Type the filename exactly as shown (in all capital letters with dashes: NO-PROGRAM-DELIVERIES) to disable the program delivery feature.

Program deliveries through the New User form

The server administrator sets up program deliveries by using the Mail User Information section of the New User form, in the Administration Server's Users & Groups menu. To do this, you will need a Unix login that has a valid shell. One or more programs should be listed in the trusted program directory.

Note The program delivery facility is disabled by default, so you or the system administrator must turn it on before setting up any program deliveries.

This section assumes that you've already set up an account. To implement program delivery, you should select program delivery as a delivery option in the Mail User Information portion of the New User form.

The command-line argument in the Program Deliveries field should indicate a program that is listed in the trusted program directory, unless the module is configured in trusted mode. In untrusted mode, you can't use characters in the command that have special meaning to a shell.

The Unix LoginName field must be a valid Unix login name.

Program deliveries and the Unix form

The Unix form, which is available from the Messaging Server's System Settings menu of forms, provides settings related to program delivery.

Note Because program delivery is available only on Unix systems, Windows NT users will not be able to access this form.

The "Interface to the Unix mail system" section of the Unix form allows the server administrator to specify the local mail delivery program used onsite. The "program delivery options" section allows the server administrator or system administrator to further define the security of the program delivery module. Netscape Messaging Server, by default, will not allow a mail program to be run as root, even if it is specified in the Unix login for the account. For program delivery, the Messaging Server allows for a "safe" account, one that is not a member of any group and has no access to user directories, that will be considered the default ID for a user with root permissions.

System administrators can create an isolated account, with no access to sensitive directories or groups, and server administrators or system administrators can specify that user ID and group ID in this section. If the Messaging Server is asked to deliver mail for a root user, these default user and group IDs are used.

Appendix

D

Command-line operations and utilities

This appendix provides information on how to operate certain Netscape Messaging Server 3.0 functions from the Unix command line. It also presents a variety of command-line utilities that you can use with Netscape Messaging Server 3.0.

Command-line operations

The Unix version of the Messaging Server provides certain operations that you can perform from the command line: starting up and shutting down the system and checking and delivering the mail queue.

Note For utilities that you can run from the command line, see "Command-line utilities" later in this appendix for more information.

Starting the system

Once installed, the Messaging Server normally starts up when the computer is turned on and runs continuously until the computer is shut down. (The startup script uses `usr/lib/sendmail -bd` to start the Messaging Server in daemon mode.) If for some reason you need to manually start the system, type the following command:

```
NscpMail start
```

The specific path to the command depends on where the system is installed. Default Unix installations are in the directory `/etc/NscpMail`.

Shutting down the system

The Messaging Server is usually shut down automatically with boot scripts. If it's necessary to manually shut down the program, use the following command:

```
NscpMail shutdown
```

Wait five to ten seconds. (Use the `ps` command to find the `NscpMail` process, if it still exists.)

```
% kill -9 <PID-Of-NscpMail-Server>
```

Checking the mail queue

To check the mail queue, type `mailq` at a command prompt. If there are no queued messages, that fact will be reported:

```
% mailq

Mail queue is empty.

%
```

If there are queued messages, each host that has queued messages waiting to be delivered will be listed, along with the number of pending deliveries. For example, output might look like this:

```
% mailq


       Queued Messages    Destination Host
       ---------------    ----------------
              2           math.csusj.edu
              3           expertelligence.com
%
```

In this example, five messages are waiting for delivery. Delivering all of them should require two connections to other machines because the Messaging Server attempts to deliver all queued mail for a host before disconnecting.

Delivering mail in the queue

The queue is automatically processed at regular intervals, so you normally never need to deliver the queue manually. Of course, you can use the Queue form to process the queue; however, if you want to process the entire queue manually at the command line, use the `processq` command:

```
/usr/lib/processq
```

To attempt to deliver all queued mail for a specific host, use this command:

```
/usr/lib/processq hostname
```

The *hostname* can be the full name of the host as reported by `mailq`, or any pattern contained in the name. If the pattern matches more than one hostname, each match will have its queue processed.

Command-line utilities

The following sections describe a variety of command line utilities that you can use with Messaging Server 3.0.

CheckPO

The CheckPO command line utility checks a message store for message inconsistencies, searches for "orphaned" mailboxes, and fixes message corruptions if needed.

Synopsis

```
CheckPO [-h] [-u userid | -p maildrop] [-f] [-d filename | -m filename]
[-l filename] object
```

Description

The CheckPO utility will detect inconsistencies in the Netscape Messaging Server 3.0's post office. Message inconsistency could be caused by restoring files from backup, or program bugs, or file corruptions, or by accidently removing a mailbox without using a proper tool.

Also, because of LDAP, users' mail attributes can be changed independently from the Messaging Server's operations. Consequently, a physical mailbox can become “orphaned” (that is, mail is no longer delivered/retrieved to/from the mailbox) when the owner's mailhost or maildrop path is changed via LDAP.

Note The user who runs this utility must have system administrator's privileges.

Important The Messaging Server must be stopped before CheckPO can be run.

The utility expects one parameter specifying the post office's object that the tool will check for inconsistency. The following are valid values for the object parameter:

- mailbox
- message
- all

This parameter is not case-sensitive; that is, the value can be in mixed cases. When “mailbox” is specified, the utility will check for orphaned mailboxes. When “message” is specified, the utility will check for inconsistencies in all messages. When “all” is specified, the utility will check for both orphaned mailboxes and inconsistencies in all messages.

Options

There are several options that can be specified with the CheckPO utility:

-h

When this option is specified, a detailed description of the utility will be displayed.

-u userid

When this option is specified, the utility will perform its tasks for the user specified by the userid. The userid is the id that a user uses to logon to post office. This value is used to map to a physical mailbox in this message store.

If either “mailbox” or “all” is specified, the utility will search for any mailbox in the current mailhost that matches the userid. When found, the utility will check if the mailbox is orphaned or not. That is, the utility will check if the owner of the mailbox exists in the directory, still has the same mailhost, and if the user's

messaging store path is the same as the mailbox's current path. If this option and the -p option are not specified, the default behavior is to check all mailboxes in the message store.

If either “message” or “all” is specified, the utility will scan all messages in the mailbox that matches the userid and check for inconsistencies such as:

- A reference message points to a single copy message that does not exist.
- A zero size message (could be a reference message or the single copy message, or a non-single-copy message).
- Missing back link file.
- A reference message file name does not exist in the back link file.
- Mismatched reference count of a single copy message.
- A message that does not have a message header.

If this option and the -p option are not specified, the default behavior is to scan all messages in all mailboxes in the post office.

Note This option cannot be used in conjunction with the -p option.

-p maildrop

When this option is specified, the utility will perform its tasks within the specified maildrop path. A maildrop is the physical path on the system where a group of mailboxes are located. There is always a default maildrop which is specified during installation. The administrator also has the option of specifying a different message store path for each user via the Administration Server interface.

If either “mailbox” or “all” is specified, for each mailbox that is in the specified maildrop path, the utility will check if its owner exists in the directory, still has the same mailhost, and if the messaging store path attribute is the same as the mailbox's current path. If this option and the -u option are not specified, the default behavior is to check all mailboxes in all of the post office's maildrop paths.

If either “message” or “all” is specified, the utility will scan all messages in all mailboxes within the specified maildrop path and check for inconsistencies such as:

- A reference message points to a single copy message that does not exist.
- A zero size message (could be a reference message or the single copy message, or a non-single-copy message).
- Missing back link file.
- A reference message file name does not exist in the back link file.
- Mistach reference count of a single copy message.
- A message that does not have a message header.

If this option and the -u option are not specified, the default behavior is to scan all messages in allmailboxes in the post office.

Note This option cannot be used in conjunction with the -u option.

-f

When this option is specified with either “message” or “all”, the utility will attempt to fix any message inconsistency it finds by deleting corrupted files, adjusting reference count...etc.If this option is not specified, the utility will only generate a report of the inconsistencies.

The utility will never attempt to fix orphaned mailbox problems. Hence, this option will be ignored if the object is “mailbox”.

-d filename

When this option is specified, the utility will output a DelMbx command for each of the orphaned mailbox that it locates into the file specified by the filename. Later, the administrator can turn this file into a script file and run the commands to delete the orphaned mailboxes. If this option and the -m option are not specified, the default behavior is to write the DelMbx commands to standard output.

If the object is “message”, this option will be ignored.

Note This option cannot be used in conjunction with the -m option.

-m filename

When this option is specified, the utility will output a MoveUser command and a DelMbx command for each of the orphaned mailbox that it locates into the file specified by the filename. Later, the administrator can turn this file into a script file and run the commands to move the orphaned mailboxes to new mailhosts or maildrop paths. The MoveUser command will copy the contents of the mailbox (all messages and folders) from the old mailhost's location to the new mailhost's location or from the old maildrop path to the new maildrop path. Since the MoveUser does not remove the old mailbox, the DelMbx command is issued to cleanup the old mailbox. Together, the MoveUser command and the DelMbx command constitute the move mailbox action.

If the owner of a mailbox cannot be found in the directory or the owner's mailhost cannot be determined, the utility will output only the DelMbx command to delete the orphaned mailbox, even though -m is specified since there is no destination that the mailbox can be moved to.

If this option and the -d option are not specified, the default behavior is to write the commands to standard output. If the object is “message”, this option will be ignored.

Note This option cannot be used in conjunction with the -d option.

-l filename

If this option is specified, all log messages will be written to the file specified by the filename. Log messages consists of all error messages, reports of message inconsistencies and orphaned mailboxes, as well as some other information messages. If this option is not specified, the default behavior is to write the log messages to standard output.

DelMbx

The DelMbx command line utility deletes a user mailbox when the mailbox is no longer in use.

Synopsis

```
DelMbx [mailbox path]
```

where `mailbox path` is the full path name of the mailbox directory.

Description

This utility will scan all the messages in the designated directory and delete all messages, and the message reference count will be adjusted correctly. All files and sub directories are deleted in the process.

Important Use this utility instead of the operating system command rm -r directory. Because of the single-copy message feature in Messaging Server 3.0, the reference count will become corrupted, and the master copy message never gets deleted.

MoveUser

The MoveUser command line utility moves messages in users' mailboxes from one Messaging Server to another.

Synopsis

```
MoveUser-s srcmailhost -x proxyuser -p password -u uid -o srcmaildrop
-m destmaildrop [-l ldapurl -D bindDN -w bindpassword [-f localB path]]
[options]
```

Description

When user accounts are moved from one Messaging Server to another, it is also necessary to move user's mailboxes (folders) from one server to the other. This utility moves messages in a user's mailbox from one server to the other. It also updates entries in the associated LDAP Directory Server to reflect the user's new mailhostname and message store path. This utility makes use of Netscape's PROXYAUTH extensions IMAP4 protocol.

There are several arguments that can be used with the MoveUser utility:

Argument	Explanation
-l ldapurl	ldap://<hostname>:<port>/ <base_dn>?<attributes>?<scope>?<filter>
-D bindDN	bind dn
-w password	bind password (for simple authentication)
-u uid	uid for the user whose mailbox needs to be moved Not to be used with -l option
-s srcmailhost	source Messaging Server
-x proxyuser	ProxyAuthUser for source Messaging Server
-p password	password for ProxyAuthUser of srcmailhost
-d destmailhost	destination Messaging Server
-a proxyuser	ProxyAuthServer for destmailhost
-v password	password for ProxyAuthUser on destmailhost
-o scrmaildrop	message store path on srcmailhost
-m destmaildrop	message store path for destmailhost
-h	display usage information

Requirement

In /etc/netscape.mail.conf file, on a 3.0 server there should be an entry as follows:

```
ProxyAuthUser="authorized user"
```

“Authorized user” may be the administrator of the Messaging Server.The utility uses this name and access permission to gain access to mailboxes for all users.

Components of LDAP URL

LDAP URLs have the following syntax:

```
ldap://<hostname>:<port>/<base_dn>?<attributes>?<scope>?<filter>
```

Component	Explanation
<hostname>	Name of the LDAP Directory Server
<port>	Port number for the LDAP Directory Server. If no port is specified, standard LDAP port (389) is used.
<base_dn>	Distinguished name of an entry in the directory. This component is required.
<attributes>	The attributes to be returned. If no attributes are specified, all attributes are returned.
<scope>	Scope of search. base retrieves information only on the distinguished name (<base_dn>) specified in the URL. one retrieves information one level below the <base_dn>. The base entry is not included. sub retrieves information on all entries below the <base_dn>. Base entry is included in this scope.
<filter>	Search filter to apply to entries within specified scope of search. If no filter is specified, (objectclass=*) is used.

bindDN

Specifies the distinguished name with which to authenticate to the server. The value must be a DN recognized by the Directory Server, and it must also have the authority to modify the entries.

bindDN password

Specifies the password associated with the bind DN.

Examples

Following are some examples of how to use the MoveUser utility:

To move all users from host1 to host2, based on account information in LDAP:

```
MoveUser -l "ldap://your.domain.com:389
```

```
ou=development,o=writable,c=us?mail?one?(mailhost=host1.domain)" -D
"cn=Directory Manager," -w password -s host1 -x administrator -p
password -d host2 -a administrator -v password -o /var/mail/spool/
mailbox -m /nsmail/mail/spool/mailbox
```

To move one user from host1 to host2, based on account information in LDAP:

```
MoveUser -l "ldap://your.domain.com:389/
ou=development,o=writable,c=us?mail?one?(uid=user)"-D "cn=Directory
Manager," -w password -s host1 -x administrator -p password -d host2 -a
administrator -v password -o /var/mail/spool/mailbox -m /nsmail/mail/
spool/mailbox
```

To move group of user from host1 to host2, based on account information in LDAP:

```
MoveUser -l "ldap://your.domain.com:389/
ou=development,o=writable,c=us?mail?one?(&(mailhost=host1.domain)(uid=s
*))" -D "cn=Directory Manager," -w password -s host1 -x administrator -
p password -d host2 -a administrator -v password -o /var/mail/spool/
mailbox -m /nsmail/mail/spool/mailbox
```

In this example, note `(uid=s*)`. This indicates move all users with uid starting with `s`.

To move one user's mailboxes from host1 to host2 when the uid is specified (for use with the CheckPO utility):

```
MoveUser -u uid -s host1 -x administrator -p password -d host2 -a
administrator -v password -o /var/mail/spool/mailbox -m /nsmail/mail/
spool/mailbox
```

MTA-migrate

This section provides instructions for MTA-migrate utility for migrating users from MTA-Accounts in a 2.x Mail Server to Messaging Server 3.0. The MTA-migrate utility

- migrates users found in MTA-Account in 2.x Mail Server database to an LDAP Directory server or to a local directory used in 3.0 Mail Server.
- migrates users' mailboxes from 2.x to 3.0 Mailbox directory.

Table D.1 MTA-migrate options.

Option	Explanation	Example
-b basedn	Base dn for migration If not specified, the base dn used in the Administration Server is used as the default.	-b "o=Ace Industry, c=US"
-n	Previews what would be migrated in LDIF but doesn't actually migrate.	
-D binddn	bind dn	-D "cn=Directory Manager, o=Ace Industry, c=US"
-w passwd	bind password (for simple authentication	-w password
-f format	Optional distinguished name format string Format parameters: %uid, %cn, %mailhost, %basedn	f "cn=%cn, %basedn" -f "cn=%cn (%uid), %basedn" -f "uid=%uid, %basedn" -f "mail=%uid@%mailhost, %basedn" -f "uid=%uid at %mailhost, %basedn"
-h host	LDAP Directory Server hostname If not specified, the LDAP hostname used in the Administration Server is used as the default.	-h heman
-p port	Port on LDAP Directory Server If not specified, he LDAP port number used in the Administration Server is used as the default.	-p 400
-u	Puts uid in dn to avoid duplicate cn	
-P postmtr	Mail group or person (The default is mail group.)	-P mailgroup
-x mbx	Skips migration of mailboxes. Only migrates users to the LDAP Directory Server or the local directory database If not specified, the program migrates both users and their mailboxes.	
-x dir	Skips migration of directory. Only migrates mailboxes. If not specified, the program migrates both users and their mailboxes.	

Table D.1 MTA-migrate options.

Option	Explanation	Example
-l	Sets up the LdapAccounts environment variable. (The default is no.) Use this option carefully. This option is not required for migration from 2.x to 3.x Messaging Servers. By default, LdapAccouts is set to "no" in migration. If "-l yes" is used in the program, migration will takes place from 3.x to 3.x Messaging Servers.	-l yes
-O postoffice	Specifies the 2.x post office directory if different from the post office directory in 3.0	-O /var/spool/postoffice.2x
-M mailbox	Specifies the 2.x mailbox directory if different from the mailbox directory in 3.0	-M /var/spool/mailbox.2x
-C cfgfile	Uses the local directory database described by cfgfile.	-C /usr/netscape/suitespot/userdb/ldap/config/lcache.conf
-H	Displays usage information.	

Migration to an LDAP Directory Server

The following options allow you to specify the LDAP Directory Server that your MTA-Accounts are migrated to.

-D binddn

Specifies the distinguished name used to authenticate to the server. The value must be a DN recognized by the Directory Server, and it must also have the authority to modify the entries under the given basedn. If -D and -w parameters are not specified, default is binding as anonymous person.

-w bindpw

Specifies the password associated with the distinguished name specified in the -D option. If -w is not specified in command line option, user will be prompted for password if -D option is used in the command line.

-h host

Specifies the name of the host on which the LDAP Directory Server is running. If -h parameter is not specified, default is using the settings in Administration Server. If Administration Server is not installed, default is localhost.

-p port

Specifies the port number that the LDAP Directory Server uses. If -p parameter is not specified, default is using the settings in Administration Server. If Administration Server is not installed, default is 389.

Migration to a Local directory database

MTA-migrate can work with a local directory database. The -C parameter is specific for migration to a local directory database; all other options remain the same for the local directory database.

-C cfgfile

Specifies the complete file name of the configuration file for Local DB such as

```
/usr/netscape/suitespot/userdb/ldap/config/lcache.conf.
```

Preview mode in MTA-migrate

-n

Allows user to preview the migration results in LDIF file. Once this option is used, MTA-migrate will merely display the migration results in LDIF file format. It will not migrate any user accounts or mailboxes.

Essentially, output of MTA-migrate, when used with -n option, can be used with the LDAP command line tool ldapmodify. For example,

```
MTA-migrate -b "ou=demo, o=Ace Industry, c=US" -D "cn=Directory Manager,
o=Ace

Industry, c=US" -w password -n >testrun

ldapmodify -D "cn=Directory Manager, o=Ace Industry, c=US" -w password -
f testrun -c
```

A proper distinguished name and password are required for ldapmodify to authenticate with the LDAP Directory Server for modification privilege.

Customization of distinguished name

By default, MTA-migrate will choose to format the distinguished name as follows:

```
n=John Smith, ou=People, o=Ace Industry, c=US
```

You can use the following options to customize the distinguished name in migration.

-u

Formats the distinguished name by adding (uid) to the distinguished name:

```
n=John Smith (jsmith), ou=People, o=Ace Industry, c=US
```

-f format

You can use the optional -f parameter to format the distinguished name according to uid, cn, mailhost, and basedn

Table D.2 -f formats.

Format	Example
-f "cn=%cn, %basedn"	cn=John Smith, ou=People, o=Ace Industry, c=US
-f "cn=%cn (%uid), %basedn"	cn=John Smith (jsmith), ou=People, o=Ace Industry, c=US
-f "uid=%uid, %basedn"	uid=jsmith, ou=People, o=Ace Industry, c=US
-f "mail=%uid@%mailhost, %basedn"	mail=jsmith@my.host.com, ou=People, o=Ace Industry, c=US
-f "uid=%uid at %mailhost, %basedn"	uid=jsmith at my.host.com, ou=People, o=Ace Industry, c=US

Migration from 2.x post office

-O postoffice

Specifies the directory for 2.x post office if different from 3.0 post office. This option is required if a 3.0 post office is installed in a directory different from the 2.x post office directory

Migration from 2.x mailbox

-M mailbox

Specifies the directory for 2.x mailbox if different from 3.0 mailbox. This option is required if 3.0 mailbox resides in a directory different from the 2.x mailbox directory.

Migration of Postmaster By default, MTA-migrate will migrate Postmaster as a mailGroup in 3.0 MailServer.

-P person

Specifies migration of Postmaster as a person. This will preserve all the forwarding addresses and mail delivery options for Postmaster as a person as in 2.x MTA-Accounts.

-P mailgroup

Specifies migration of Postmaster as a mailGroup. This will include all the forwarding addresses to Postmaster in the member list of a mailgroup. All the forwarding addresses will be created in rfc822MailMember of a mailGroup objectClass.

Migration in stages

-x mbx

This option allows the program to skip the migration of mailboxes. This option is useful when you want to migrate the 2.x user accounts to an LDAP Directory Server or a local directory database without upgrading the 2.x mailboxes.

-x dir

This option allows the program to skip the migration of user accounts to an LDAP Directory Server or a local directory database. This option is useful when you want to migrate mailboxes without creating LDAP accounts. This assumes that you have manually created the LDAP accounts and that they contain all the mail attributes required by the Messaging Server.

MTA-migrate examples

```
MTA-migrate -D "cn=Directory Manager, o=Ace Industry, c=US" -w password
```

This example migrates 2.x accounts to the LDAP Directory Server with port number and base dn settings specified in the Administration Server.

```
MTA-migrate -b "ou=People ,o=Ace Industry, c=US" -D "cn=Directory
Manager, o=Ace Industry, c=US" -w password
```

Similar to the first example, this example migrates 2.x accounts to the specified basedn "ou=People, o=Ace Industry, c=US"

```
MTA-migrate -D "cn=Directory Manager, o=Ace Industry, c=US" -w password
-O /var/spool/postoffice.2x -M /var/spool/mailbox.2x
```

This example migrates accounts found in `/var/spool/postoffice.2x` with mailboxes specified in `/var/spool/mailbox.2x` to the LDAP Directory Server with settings specified in the Administration Server.

```
MTA-migrate -C "/usr/netscape/suitespot/userdb/ldap/configlcache.conf"
-O /var/spool/postoffice.2x -M /var/spool/mailbox.2x
```

Similar to the previous example, this example migrates 2.x accounts to a local directory database.

Glossary

access domain This security measure limits access to certain Messaging Server operations from within a specified domain. For example, an access domain can be used to limit where mail for an account can be collected.

account All information relating to sorting incoming messages is held in accounts. Accounts specify which addresses the Messaging Server should accept messages for and what it should do with those messages once they are accepted. Every user who gets messages through the Messaging Server has an account.

address The information in an email message that determines where and how the message must be sent. Addresses are found both on message headers and on message envelopes.

addressing protocol The addressing rules that make email possible. SMTP is the most widely used protocol on the Internet. Other protocols include X.400 and UUCP.

alternate address A secondary address for an account, generally a variation on the primary address. In some cases it is convenient to have more than one address for a single account.

AutoReply utility This Messaging Server feature automatically responds to messages sent to accounts with the AutoReply feature activated. Every account in the Messaging Server can be configured to automatically reply to incoming messages. There are three AutoReply modes available: reply, echo, and vacation. Reply mode sends back an automatic reply to every message sent to a specific address. Echo mode does the same thing but also includes the text of the original incoming message. Vacation mode, which is the only mode users can set up on their own, is used to let senders know that the mail recipient is unavailable.

body Email messages consist of an envelope, a header, and a body. Although headers and envelopes must follow a standard format, the body of the message has a content determined by the sender—the body can contain text, graphics, or even multimedia.

daemon program Unix programs that run in the background, independent of a terminal, and perform a function whenever necessary. Daemons usually run with root privileges and perform very specialized functions. Common examples of daemon programs are mail handlers, license servers, and print daemons.

dispatcher This is the daemon or service component of the Messaging Server. The dispatcher initiates all the Messaging Server processes and monitors ports for incoming messages and finger queries.

Domain Name System (DNS) The DNS is the addressing protocol that allows the Internet network's computers to find each other. Email addresses are based on DNS addresses. Every computer (and user) in a network using the DNS has a unique address. You need DNS to run your mail system. You can provide this service internally by running a DNS server, or your Internet provider can supply this service to you as part of your Internet connection.

echo Like the reply setting of the AutoReply feature, echo sends a copy of the AutoReply message specified for an account to anyone who contacts that account. The original message is sent along with the reply message.

envelopes Email messages are stored in electronic "envelopes" while they are being moved from place to place by various email programs. Envelopes are used only by programs; users see only the header and body of a message.

error handler This module handles all the Messaging Server errors. It issues error messages and processes error action forms after the postmaster fills them out.

error message The Messaging Server generates error messages in a number of situations, notably when it gets an email message that it can't handle. One type of error message, the Error-Handler Action form, requires you to resolve the error. This form contains fields that you must fill out and return to the error handler. Others error messages, called notification errors, are for informational purposes only.

field Forms consist of fields. Fields are parameters that you can (and sometimes must) specify to configure the Messaging Server. Usually, fields are multiple choice, with the options listed adjacent to the field or described nearby (as in email forms) or selectable from a scrolling menu or buttons (as in web forms). The fields in forms correspond to fields in the account and configuration databases.

finger service A rudimentary directory service you can use to "finger" an email address. The Messaging Server answers finger queries with any information placed in the Finger Information field. Server administrators can make all sorts of information available this way. Such information typically includes phone numbers and street addresses.

firewall An Internet firewall provides security for a site by restricting or preventing access to internal machines by outside computers. A typical firewall is safe from hostile Internet users because it allows no direct connections to internal machines and relies on proxy servers or other trusted programs to carry communication across the wall.

form Forms are specialized web documents used to configure and administer the Messaging Server. Forms are composed of fields, where specific instructions to the Messaging Server are entered. Although most forms are only for the system and server administrators, users can use the Information form to change certain aspects of their accounts.

Greeting form The Greeting form is usually sent to users when an account is created for them. This form acts as confirmation of the new account and verification of its contents. The Greeting form also instructs users on how to change information related to their mail account. During installation, system administrators have the option of deciding whether to send Greeting forms to users.

header The portion of an email message that precedes the body of the message. Headers contain information useful to email programs and users trying to make sense of the message: they tell whom the message is for, who sent it, when it was sent, and what it is about. Headers must be written strictly according to the SMTP protocol so that email programs can read them.

hostname hiding The practice of having domain-based email addresses that don't contain the name of a particular host.

hub, mail A single host that acts as a hub for the system. When two networks are separated by a firewall, for example, the firewall computer often acts as a mail hub.

IMAP4 Internet Message Access Protocol Version 4 (IMAP4) allows users to be disconnected from the main messaging system and still be able to process their mail. The IMAP specification allows for administrative control for these disconnected users and for the resynchronization of the users' message store once they reconnect to the messaging system.

intermittently connected site	A site that doesn't have a continuous connection to the Internet, yet uses TCP/IP for communication. These sites are usually "connected" only a few hours per day.
LDAP	Lightweight Directory Access Protocol (LDAP) is a simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of user and group account management across Netscape SuiteSpot servers.
mail client	Mail clients are the programs that help users send and receive email. This is the part of the various networks and mail programs that users have the most contact with. Mail clients create and submit messages for delivery, check for new incoming mail, and accept and organize incoming mail.
mail exchange (MX) record	A list of hosts that accept mail for a domain and tell how to contact a domain. MX records are required to get mail to a disconnected host or to a system that is down, as well as to "distribute load" (give several hosts the same preference value). MX records are part of the DNS.
mail queue	For various reasons beyond its control, the Messaging Server is sometimes unable to deliver messages immediately and must wait before attempting delivery again. During this wait, undelivered messages are stored in the mail queue.
mailbox directory	Messages stored for POP3 or IMAP4 delivery are held in the mailbox directory.
message	The fundamental unit of email, a message consists of a header and a body and is often contained in an envelope while it is in transit from the sender to the recipient.
message transfer agent (MTA)	Programs, such as the Messaging Server, that exchange email with other MTAs and accept and deliver messages to mail clients.
MIME (Multi-purpose Internet Mail Extension)	Multipurpose Internet Mail Extension (MIME) is a protocol you can use to include multimedia in email messages by appending the multimedia file in the message. Because not all mail clients support MIME, you should make sure that the message recipient has a MIME-enabled mail client.
MTA	See message transfer agent.
MX records	See mail exchange record.
password	One building block in the security features of the Messaging Server. Passwords are required to process forms and to retrieve messages through POP3.

POP3 The Post Office Protocol Version 3 (POP3) delivery method doesn't require the message transfer agent to have access to the user's mailbox directory. This is an advantage in a networked environment, where often the mail client and the message transfer agent are on different computers.

postmaster By convention, an account used to communicate with the person (or people) responsible for maintaining a Messaging Server.

reply (AutoReply feature) This AutoReply feature automatically replies to anyone who sends a message to an account with the reply feature activated. The reply message can be anything from a few words to bulky multimedia attachments.

reply (mail client feature) Most mail clients have a reply feature that lets you automatically return a message to its sender along with any modifications you'd like to make. Use this feature to return email forms to the Messaging Server.

sendmail This is currently the most common MTA used on Unix machines. In most applications, the Messaging Server can be used as a dropin replacement for sendmail.

SMTP Simple Mail Transfer Protocol (SMTP) is the email protocol most commonly used by the Internet. It is implemented by the Messaging Server SMTP channel.

SMTP channel alias SMTP channel aliases are designed to handle incoming messages that are forwarded to another mail transfer agent located on another address (for example, for an address that has no local delivery). SMTP channel aliases are specific to the SMTP channel. Whenever a message enters the Messaging Server destined for one of the listed SMTP channel aliases, the address is immediately rewritten and the message delivered to the new address at a remote host.

SMTP Mail Routing table Provides a way to redirect mail based on the domain to which it is being sent. Each entry in the SMTP Mail Routing table consists of a pattern and a domain. Before sending a message, the destination domain is compared to the patterns in the table. If a match is found, the destination host is replaced by the domain corresponding to the pattern that matched.

SNMP Simple Network Management Protocol (SNMP) is a network protocol that allows administrators to monitor server processes remotely on SNMP-compatible servers through the use of SNMP station software.

TCP/IP TCP/IP (Transmission Control Protocol/Internet Protocol) is the protocol suite that underlies much Internet activity, such as the SMTP protocol.

user Short for computer user. In this manual, this word is also used to distinguish persons using the Messaging Server system (users) from the postmaster and system administrator.

UUCP (Unix to Unix Copy Protocol) An older Unix email addressing protocol still employed in some legacy mail systems.

vacation You can use this AutoReply feature to tell people that you'll be away from your email for a while. It automatically sends everyone who contacts you one (and only one) message.

Index

Symbols

* (asterisk)
  wildcard used in mail routing tables 44
'Quota Exceeded' Message field 39

A

about the Mail Group Information form 29
about the Mail User Information form 24
accept agents, in message channels 75
access domains
  algorithm to limit and verify 56
  security and 55
  See also finger access domains, domains
  setting up 56
Access Domains field 26
accessing the Administration Server 21
Account form
  program delivery and 101
Account Handler
  logging 66
Account handler 40
account handler 48, 80
Account Manager
  logging 66
accounts 22
  group 28
  mail 49
  MTA group 54
  MTA user 54
accounts managing 24
accounts, user 24
address
  Internet Protocol (IP) 48
Address Completion Domain field 46
address completion, for mail with no domain 46
addresses
  "bad" 46
  incomplete, security and 55
  Internet Protocol 56
  IP 56
  verifying 43
Addresses for Forward Delivery field 40
Administration Server 20
Administration server
  accessing 21
agent
  deliver 75
  routing 75
agents
  accept 75
algorithm
  to determine if client can access server 56
  to limit and verify access domains 56
alias
  mail 30
  SMTP channel 40–??, 41, 44
aliases
  compatibility with sendmail 84
  creating 40–??
  mail 30
  SMTP channel 40–??, 41, 44
Allowed Sender Domains field 32
Allowed Senders field 33
alternate email addresses (group) 30
Alternate Email Addresses field (group) 30
Alternate Email Addresses field (user) 25
Always Defer Delivery field 43

API, plug-in 14
architecture
  AutoReply utility 81
  directory service role in 82
  dispatcher role in 72
  major components of 71
  message transport agent (MTA) role in 73
  Messaging Server 71
  top-level depiction of (figure) 72
authentication 12
Auto-reply 72
AutoReply Handler
  logging 66
Auto-Reply Mode field 27
Auto-Reply Text field 28
AutoReply utility 81

B

backslash 17

C

CC recipients 31
channel
  local delivery 73, 77
  message 73
  SMTP 73, 75
CheckPO 105
cluster size 50
command line
  checking mail queue via 104
  startng the system 103
command line utilites
  CheckPO 105
command line utilities 105
Command-line operations 103
command-line operations (UNIX only) ??–105
command-line refererence for sendmail 88
command-line utilites
  MoveUser 110
command-line utilities
  DelMbx 109
  MTA-migrate 113
configuration
  system ??–46
configuration database 71
Configuration Manager
  logging 66
configuring
  DNS 31
controlling user, in program delivery 95
conventions 15
  naming 16
  pathname 17
  slash 17
  typeface 17
conventions used in this guide 15

D

daemon 54, 71
database
  directory 82
  module configuration 73
default
  echo reply message, creating 39
  information reply message 39
  log-file value 65
  mail routes 44
  number of running processes 48
  vacation message, creating 38
Default Echo-Mode Reply Message field 39
Default Max Concurrent Network Servers field 48
Default Reply-Mode Reply Message field 39
Default User Disk Quota field 49
Default Vacation-Mode Reply Message field 38
deleting the mailbox 109
deliver agent 75
deliver agent, in message channel 75
delivery

IMAP4 78
POP3 78
program 79
Unxi 79
delivery options
Unix 50
Delivery Options field 50
Delivery Options fields 26
Delivery status notification 13
DelMbx 109
directory databases 82
directory entries 22, 40
and email accounts 22
Directory Server 20, 40, 72, 82
directory services 72, 82
disk quota 49
Disk Quota Exceeded error 46
Disk Quota Exceeded field 45
disk space 49
dispatcher 54, 71, 72
defined 54
logging 66
role in architecture 72
DNS 25, 44, 48, 57
DNS configuration 31
Do nothing option 65
domain 46, 47, 48, 68
domain name
fully-qualified 26, 31
domain name service 25
domains 32
changing 46
completing for received mail 46
list of local 47

E

echo reply message, default 39
email accounts 22, 24
and directory entries 22
email addresses
alternate (user) 25
primary (user) 24
encryption 12, 53
entries
directory 40
group 40
user 40
user and group 40
error actions
specifying 45
Error Handler
logging 66
error handler 81
error messages 67
Max Hops Exceeded 45
notification messages 67
overview 67
processing 67, 69
routing through error handler 81
Unknown Local Account 45
Error-Handler Action form 67, 68, 69
errors
Disk Quota Exceeded 46
Max Hops Exceeded 46
Unknown Local Account 45
executable directory
permissions and 55

F

Fidonet gateway, routing to 44
field
List of CC Recipients 31
Message Store Path 26
fields
'Quota Exceeded' Message 39
Access Domains 26
Address Completion Domain 46
Addresses for Forward Delivery 40
Allowed Sender Domains 32

Allowed Senders 33
Alternate Email Addresses (group) 30
alternate email addresses (user) 25
Always Defer Delivery 43
Auto-Reply Mode 27
Auto-Reply Text 28
Default Echo-Mode Reply Message 39
Default Max Concurrent Network Servers 48
Default Reply-Mode Reply Message 39
Default User Disk Quota 49
Default Vacation-Mode Reply Message 38
Delivery Options 26, 50
Disk Quota Exceeded 45
Forward Delivery 27
LDAP Criteria for Generating CC List 31
Local Mail Delivery Program 50
Local Mail Domains 47
Log Directory 65
Lookup Client Machine Names 48
Mail Quota 26
Max Hops Exceeded 45
Maximum Message Size 32
Maximum MTA Hops 43
Maximum MTA Hops Exceeded 45
Maximum Queue Time 47
Messaging Server 50
Messaging Server (group) 31
Messaging Server (user) 26
Minimum Free Disk Space 49
Personal Description 28
primary email address (group) 29
Primary Email Address (User) 24
primary email address (user) 24
Program Delivery 27
Queue Processing Interval 47
Queued Mail Processing Interval 43
Recommended Account Management URL for Mail Users 49
Rejection Notice 33
Send Errors To 30
SMTP Mail Routing Table 44
UNIX Delivery 27
Unknown Local Account 43, 45
Verify each recipient's address 43

file delivery, compatibility with sendmail 85
finger 48
finger queries
  for host, messages in response to 38
Finger Server
  logging 66
finger service 82
finger services 82
firewalls
  default routes and 44
  message rerouting and 44
form
  SMTP Aliases 42
format for SMTP mail routing table 44
forms
  configuring mail server with 13
  creating default ??–28
  Error-Handler Action 67, 68, 69
  List of Queued Mail 64
  Logging Preferences 50–??, 64, 65–66
  Mail Group Information 28
  Mail User Information 24, 50
  Message Stores 50
  Security 57, 58
  Single Copy On/Off 49
  SMTP Aliases 41
  SMTP Channel 42–46
  SMTP Channel Aliases 40–??
  SMTP Channel Options 42–??
  SNMP Configuration 62, 63
  SNMP Subagent Control 63
  System 46–??
  System Configuration 43, ??–46
  Unix Mail 50
Forward Delivery 40
Forward Delivery field 27
forward slash 17
FQDN 26, 31
fully-qualified domain name 26, 31

G

glossary 121–??
group account 54
group accounts
  managing 28

H

handler
  account 80
handlers 73
hiding the hostname in addresses 25
hostname 25, 46, 57
hostname hiding 25
  address completion and 46

I

IMAP
  Delivery 26
IMAP authentication 12
IMAP encryption 12
IMAP Server
  logging 66
IMAP server
  log files for 66
IMAP4 48, 49
  login 57
IMAP4 delivery 78
information reply message, default 39
intermittently connected sites
  queuing mail for 43
Internet Protocol (IP) address 48
Internet Protocol address 56
IP address 48, 56

L

LDAP 12, 20, 31, 40, 82
LDAP criteria 32
LDAP Criteria for Generating CC List field 31
LDAP filter 32
LDAP lookup 44
Lightweight Directory Access Protocol 12, 20
List of CC Recipients field 31
List of Queued Mail form 64
local delivery channel 73, 77
local delivery channels
  POP3 message delivery and 78
  program delivery (UNIX) and 79
  role in architecture 77
  UNIX message delivery and 79
Local Mail Delivery Program field 50
local mail domains (LMDs)
  list of, in System form 47
Local Mail Domains field 47
Log Directory field 65
log file
  default value of 65
  moving 65
  viewing 67
Logging Preferences form 64
  fields for 50–??, 65–66
login name 57
  Unix 27
logs
  server 64
Lookup Client Machine Names field 48

M

mail accounts 49
mail alias 30
mail aliases 30
mail forwarding
  compatibility with sendmail 84
Mail Group Information form 28
  about 29
mail loops, preventing 43

mail queue 43
  checking 64
  checking via command line 87, 104
  checking with sendmail 87
  configuring 46
  delivering via command line (UNIX) 105
  for intermittently connected sites 43
  processing 64
  specifying attempted-delivery intervals 47
  specifying message time in queue 47
Mail Quota field 26
mail routing 40, 42, 44
mail routing tables (MRTs)
  defaults used in 44
  specifying in SMTP Channel form 44
mail server
  architecture of 71–82
  compatibility with sendmail ??–92
mail server daemon 54
Mail User Information form 24, 50
mail users 49
mailbox
  deleting 109
Mailbox Deliver
  logging 66
mailbox directory
  permissions and 55
mailboxes
  moving 110
maildrop file 54
  permissions and 54
mailing lists
  compatibility with sendmail 86
mailq command 87, 104
manager
  Messaging Server 22
Managing group accounts 28
managing user accounts 24
master agent, SNMP 64
Max Hops Exceeded error 46
Max Hops Exceeded field 45
Maximum Message Size field 32
Maximum MTA Hops Exceeded field 45
Maximum MTA Hops field 43
Maximum Queue Time field 47
mesage channel
  components of 74
message "hops" 43
message channel 73
message channels
  role in architecture 74
message queue 47
  processing 64
Message quotas 13
message size 32
message store
  single copy 49
Message Store Path field 26
message store, single copy 13
Message Stores form 50
message transfer agent 71, 73, 75
  error handler 81
  handlers in 79
message transport agents (MTAs)
  account handler and 80
  components of 73
  local delivery channels in 77
  message channels in 74
  role in architecture 73
MessageHostName 31
messages
  notification 67
  transferring from one channel to another 76
messages, error 67
Messaging Server
  daemon 54
  finger service 82
  manager 22
  security 53
  service 54

Messaging Server architecture 71
Messaging Server dispatcher
  logging 66
Messaging Server field 50
Messaging Server field (group) 31
Messaging Server field (user) 26
Messaging Server manager, using 22
Minimum Free Disk Space field 49
Minimum Message Size option 50
module configuration database 73
module configuration database, database
  module configuration 71
MoveUser 110
moving user's mailboxes 110
MTA 71, 73, 75
  error handler 81
  handlers in 79
MTA user account and group 54
MTA-migrate 113
MX records 44

N

name lookup, on connecting client
      machines 48
naming conventions 16
Netscape Mail Server
  architecture of 71–82
  compatibility with sendmail ??–92
Netscape servers
  acessing the Administration Server 21
  Administration 20
  Directory 20, 40
network management, remote 13
NIS 44
No Program Deliveries file, removing for
      program deliveries 99
notification messages 67
notification, delivery status 13
NscpMail command 103
NscpMail shutdown command 104

O

option
  Do nothing 65
options
  Minimum Message Size 50
  Select the Expire 65
  Select the Process 65

P

password 57
pathname conventions 17
permissions 53
Personal Description field 28
plug-in API 14
POP
  Delivery 26
POP (Post Office Protocol) delivery 78
POP/IMAP Delivery 26
POP3 48, 49, 54
  login 57
POP3 delivery 78
POP3 Server
  logging 66
POP3 server
  log files for 66
port operations 103–105
postmaster 67
postoffice directory
  permissions and 55
primary address, defined 24, 29
Primary Email Address (group) 29
Primary Email Address field (group) 29
Primary Email Address field (user) 24
processes, default number of running 48

processing error messages 69
processing the queue 43
processq command 105
Program Deliver
  logging 66
Program delivery 79
program delivery
  compatibility with sendmail 85
  configuring for 98
  defined 79
  setting up via Account form (postmaster) 101
  terms related to 94
Program Delivery field 27
program-delivery module, disabling 100

Q

Queue Processing Interval field 47
queue, message 47
queue, processing 43
queued mail 64
  processing 64
Queued Mail Processing Interval field 43
queued messages 64
  processing 64
quota, disk 49
quotas
  message 13

R

Recommended Account Management URL for Mail Users field 49
Rejection Notice field 33
remote configuration and management 13
Remote network management 13
reports
  server 64
  The View Logs 67
Required 33
restricted environment, in program delivery 95
routing agent 75
routing agents, in message channels 75
routing, mail 40, 42, 44
runtime permissions, security and 53, 54

S

security
  access domains and 55
  domain names vs. IP addresses 56
  finger service and 82
  of system 53–??
  runtime permissions and 54
Security form
  configuring security options with 57, 58
security forms 53
security options, configuring with Security form 57, 58
Select the Expire option 65
Select the Process option 65
Send Errors To field 30
sendmail
  alternate names for 88
  checking mail queue with 87
  command-line compatibility 86
  command-line reference 88
  functional compatibility 83
  options 91
  sending mail with sendmail replacement 86
  starting server with sendmail replacement 87
Server Administration page, using 21
server logs 64
server logs and reports 64
server reports 64
servers
  accessing the Administration Server 21
  Administration 20
  Directory 20, 40, 72, 82
service 54
Setting up an SMTP channel alias 41

setuid-root program, in program delivery 94
shutting down system 104
shutting down system via the Unix command-line 104
SIMAP4 Server
  logging 66
Simple Mail Transfer Protocol 12, 73
Simple Mail Transfer Protocol (SMTP) channel
  as example of message channel 75
Simple Network Management Protocol 13
Single copy message store 13
single copy message store 49
Single Copy On/Off form 49
slash conventions 17
SMTP 12, 48, 54, 73
SMTP Accept
  logging 66
SMTP Aliases form 41
SMTP channel 40, 42–??, 73, 75
  channel aliases and 40
SMTP channel aAliases 44
SMTP channel alias 40–??, 41
  setting up 41
SMTP channel aliases 40–??, 41
  setting up 41
SMTP Channel Aliases form 40–??
SMTP Channel form ??–46
  fields for ??–46
SMTP Channel Options form 42–??
SMTP Deliver
  logging 66
SMTP Mail Routing table 42
SMTP mail routing table
  format 44
SMTP Mail Routing Table field 44
SMTP Router
  logging 66
SMTP, compatibility between sendmail and mail server 84
SNMP 13
SNMP Configuration form 62, 63
SNMP master agent 64
SNMP Master Agent Control form
  forms
    SNMP Master Agent Control 64
SNMP subagent
  restarting 64
SNMP Subagent Control form 63
SNMP subagent log 64
starting
  Administration server 20
starting and stopping the Administration Server 20
Starting the system via the Unix command line 103
status, delivery 13
stopping
  Administration Server 20
superuser 54
Synopsis 105
System Configruation form ??–46
system configuration ??–46
System Configuration form 43
System form 46–??
system security 53
system settings 37

T

The components of a message channel 74
The SMTP Aliases form 42
trusted program, in program delivery 95
trusted-program directory
  in program delivery 95
  setting up for program delivery 99
typeface conventions 17

U

UNIX
  command-line operations for ??–105
  delivering queued mail 105
  message delivery 79
  starting system via command-line 103
Unix
  checking mail queue via command line 104
  command-line 104
Unix command line 103
Unix Deliver
  logging 66
Unix delivery 50, 79
UNIX Delivery field 27
Unix delivery options 50
UNIX delivery, enabling via Account form 27
Unix login name 27
Unix mail 27
Unix Mail form 50
UNIX maildrop file
  permissions and 54
Unknown Local Account error 45
Unknown Local Account field 43, 45
URL 49
user account 54
user accounts 24
user and group entries 40
user and group forms 23
user forms
  working with
    group forms
      working with 23
using the Messaging Server manager 22
using the Server Administration page 21
utilities
  CheckPO 105
  command line 105
  DelMbx 109
  MoveUser 110
  MTA-migrate 113
UUCP gateway 44
UUCP gateway, routing to 44

V

vacation message, default 38
valid shells, in program delivery 96, 100
Verify each recipient's address field 43
verifying addresses 43
View Logs report 67

W

working with user and group forms 23