INSTALLATION GUIDE

Post.Office™

v|3.0

Software.com™

THE INTERNET INFRASTRUCTURE COMPANY™

version 3.0 r0421

Table of Contents

Preface

Welcome to Post.Office!

The *Post.Office Installation Guide* tells you how to prepare for the installation of your mail server and guides you through the installation process. Once the software has been installed this book can be set aside in favor of the remaining Post.Office manuals. Those manuals, the *Administration Guide, List Owner's Guide,* and *User's Guide,* provide the operational instructions required for day-to-day running of your mail server.

Structure of the Manual

This manual is organized by function. Operations are presented in order of probable use, but feel free to review the information in whatever manner you desire - even skip sections if the content is familiar.

Chapter 1 provides an introduction to E-mail. It includes brief discussions on the software components involved in e-mail transmission and explains the role that mail servers, such as Post.Office, play in the process.

Chapter 2 describes pre-installation considerations. Installing Post.Office is easy - five minutes and you're finished. But preparing for installation requires thoughtful planning. We'll tell you what you need to know and suggest standard configuration options for common system requirements.

Chapters 3 and 4 provide installation instructions for Windows NT and UNIX, respectively. Just follow the simple steps and you'll be up and running in no time.

Chapter 5 wraps it up and points you in the right direction. And that's all, folks!

Style and Conventions

Consistency is the key. In order to make this manual as easy to use as Post.Office, we've adopted the following conventions:

Icons

Occasionally, an icon will appear in the left margin. Each icon has a specific meaning. The paragraphs that follow identify the icons and their intended use.

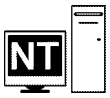
Note: *Notes alert you to information of special interest or provide clarification on the use of a particular Post.Office feature. Notes supplement standard content and are not required reading.*

Warning! Warnings contain critical information. Typical warnings include cautions about maintaining system security and avoiding overburdening your mail server. Failure to read a warning may have serious consequences.

Hint: *As you may have guessed, the helpful hints suggest ways to make your life easier. The tips are based on suggestions from other Post.Office users, including the Software.com "Postmistress."*

Security Feature: The security features of Post.Office (and there are many!) are highlighted by the appearance of a lock. Look for the locks when reviewing the security aspects of your mail server installation.

UNIX: Certain comments and instructions apply to UNIX users only. The UNIX computer icon provides a simple means of recognizing such items. Post.Office users whose system is installed on Windows NT should ignore these discussions.



Windows NT: Certain comments and instructions apply to Windows NT users only. The NT icon marks the discussion of such items. Any comments associated with the NT icon can be safely ignored by UNIX users.

Terminology and Type

- Fields and forms are referenced by their proper names.
- Literal entries (commands and such) appear in `monospaced` type.
- **Links** are underlined and in boldface.
- Important new terms appear in *italics*.
- Variable names appear in *`monospaced italics`*.
- Optional entries appear in [square brackets].

Standard Examples

Generic Term	Standard Examples	Meaning in this Manual
domain	software.com	a partial domain name (host name excluded)
host.domain	sparky.software.com	a fully qualified domain name (with host name included[1])
user@domain	john.doe@software.com	a sample user's E-mail address
list@domain list@host.domain	biking@software.com biking@sparky.software.com	a mailing list address; the address to which messages are submitted

1 Host names often involve a theme such as colors, animals, or cities. We've used common pet names as the theme for our sample hosts.

Generic Term	Standard Examples	Meaning in this Manual
		for posting
list-request@domain	biking-request@software.com	a mailing list request address; the address to which commands and requests for subscription or unsubscription are sent.
owner-list@domain	owner-biking@software.com	the list owner alias address; the address used to correspond with the mailing list owner

Questions and Comments

Copies of this manual can be obtained by anonymous FTP to ftp.software.com or from our web site at http://www.software.com. If you can't find an answer to your question in the manual, check the list of Frequently Asked Questions (FAQ), also located on our web site at http://www.software.com.

To suggest improvements or provide feedback on the content of this manual, send E-mail to Post.Office.Manual@Software.com

Legal Notices

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this documentation, and Software.com was aware of a trademark claim, the designations have been printed in initial caps or all caps.

Post.Office and Software.com are trademarks of Software.com, Inc.

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The MD5 Message-Digest algorithm

The MD5 Message-Digest algorithm used in Post.Office is ©1991-92 RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

The Regular Expression Routines

The Regular Expression Routines used in Post.Office are © 1992-94 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

The Regents of the University of California Copyright

Post.Office includes software that is © 1990, 1993, 1994. The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Olson.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Re-distributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Re-distributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ‘‘AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1

Understanding E-mail and the DNS

The Domain Name System (DNS) plays a huge role in the successful installation of any Internet-based mail server. To emphasize this point we decided to address DNS records right up front. If you are already familiar with the workings of the DNS feel free to skip to the next chapter for a discussion of additional items to be considered before installing your Post.Office mail server. If the DNS is new to you, or you'd like a refresher on the topic, you've come to the right place.

1.1 The Domain Name System (DNS)

The Domain Name System (DNS) is a distributed system for sharing information about computers (and other things). It is organized in a hierarchical structure with root domains (like Acme.com) at the top of the hierarchy and subdomains nested within those root domains.

The DNS is a fundamental part of the Internet and, therefore, Internet mail. It is managed by DNS servers which store records containing domain information (i.e. Fully Qualified Domain Names and the related TCP/IP addresses).

1.1.1 Fully Qualified Domain Names

A Fully Qualified Domain Name (FQDN) is the unique name that identifies a specific Internet location. FQDNs consist of two or more sections, separated by dots. Each section is a string of letters or numbers without spaces, usually a recognizable word or abbreviation. The order of the sections in an FQDN is significant. As you move from left to right each section represents a more general level in the Domain Name System (DNS) hierarchy.

For example, let's assume you're installing Post.Office on a computer named *yourPC* and you work for the Acme company. The FQDN for your site would be structured as follows:

```
yourPC.Acme.com
```

Hosts and Domains

With reference to Post.Office, the FQDN is further defined as consisting of two parts: the host and the domain. The host is the first (leftmost) section of the FQDN and typically corresponds to the name of the computer. The domain is the remainder of the FQDN and often tells you something about where the computer is located (e.g., at Acme's corporate headquarters).

In the example above *yourPC* is the host, and *Acme.com* is the domain.

Alternatively, if your FQDN had been `yourPC.MainOffice.Acme.com`, then your host would still be *yourPC*, but your domain would be *MainOffice.Acme.com.*

Note: *The term FQDN is universally understood, but the terms host and domain are not so clearly defined. We will use them consistently as described above, but be forewarned that they may appear in other texts with slightly different meanings.*

Determining Your Machine's Internet Domain Name

If you are currently on the Internet, a Fully Qualified Domain Name (FQDN) has already been established for your machine. Check the TCP/IP configuration files on your machine to identify your FQDN and its component parts (the host and Internet domain names) then note them for future reference.

If you are not yet hooked up to the Internet, you may not yet have a domain established. You will need to get a registered Internet domain as part of your Internet package when you get Internet access.

If you will be handling local mail only (i.e., you are not hooked up to the Internet and have no plans be) you will still need to designate a domain name, but it can be any name of your choosing and you do not need to register it.

Registering a Domain

All "root" domains, that is domains such as *Acme.com*, are obtained from InterNIC. InterNIC is the organization in charge of giving out and keeping track of all root domains on the Internet. To establish your root domain contact InterNIC directly at: `http://InterNIC.net/`

You can also get a domain from your Internet Service Provider (ISP). If you follow this course, your ISP may maintain your "MX" records for you, making your E-mail system configuration that much easier.

1.1.2 The Role of DNS Servers

A DNS server (sometimes called a nameserver) is a program that answers questions about the DNS. Like all else on the Internet, DNS servers are set up in a distributed hierarchical fashion, so that the oodles of nameservers on the Internet all have a share in the job: every nameserver is in charge of knowing only where a small chunk of the Internet is.

DNS servers do a good deal more than just answer queries from E-mail servers, but those tasks are not important as far as Post.Office is concerned. From a mail server's perspective, DNS servers answer requests from hosts regarding:

- identification of mail server hosts (e.g., what Internet host is supporting mail for the domain `Acme.com`?)

- Fully Qualified Domain Name resolution (e.g., what is the TCP/IP address for `Acme.com`'s mail server?)
- TCP/IP address resolution (e.g., what is the name for the address 192.17.254.0?)

Simply put, a nameserver helps a mail server such as Post.Office convert the Internet domain name in an E-mail address into a TCP/IP address. Once Post.Office knows another computer's TCP/IP address, it is able to contact it and forward messages to it.

1.2 How the DNS Routes E-mail

The following example (which again assumes a computer name of *yourPC* and a company name of *Acme*) illustrates the functioning of the DNS. Let's say Jane Doe wants to send an E-mail message to a user in your domain (e.g. `user@Acme.com`).

At the top level, on the Internet backbone, there is a gargantuan server that knows the location of every DNS server containing domain information for *.com (* being a wildcard). The mail server on Jane's host (this could be another copy of Post.Office) asks Jane's host to query the backbone server for information about the domain `Acme.com`. The backbone server responds that the domain is handled by a DNS server located on the host *nameserverhost.Acme.com.*

Jane's host then asks the DNS server on *nameserverhost.Acme.com* for information about the domain `Acme.com`. The DNS nameserver on *nameserverhost.Acme.com* receives the request, checks its records, and sends a response to Jane's host. The information in the response (the "MX" and "A" records) indicates that all mail for the domain `Acme.com` should be directed to the host *yourPC.Acme.com*. In addition, the TCP/IP address for *yourPC.Acme.com* is provided.

With this TCP/IP address, Jane's host can direct the message to *yourPC.Acme.com*, where it will be received by your Post.Office and delivered to `user@Acme.com`.

Note: *If you do not expect to be part of the Internet or receive Internet mail, local "hosts" files can be used instead of a DNS server to resolve names and TCP/IP addresses. Since this is not our recommended configuration, our documentation does not refer to these examples.*

1.2.1 MX and A Records

In order to receive E-mail from the Internet, either "A" records" or "MX" and "A" records" are required. "MX" and "A" records tell E-mail servers on the Internet how to route E-mail. ("A" records have other purposes as well, but we're only dealing with E-mail here.) You need to set up these records so that other mail servers can find your Post.Office host and forward E-mail to it.

Mail servers such as Post.Office use "A" records to convert host names into IP addresses. "MX" records are used to convert domains that do not point to any particular host into a

Fully Qualified Domain Name, or to route messages for one host to a different host that is running a mail server. (This feature is significant as it allows you to use E-mail addresses that do not include the name of your host.)

1.2.2 Establishing MX and A Records for Your Host

"MX" and "A" records should be entered in the primary nameserver for your domain. All DNS queries regarding your domain are directed to that nameserver. Your primary nameserver uses the "MX" and "A" records that you've set up within it to tell querying computers how to route the mail to your Post.Office host.

If your ISP maintains your DNS records for you, they should be able to help you figure out how to set up correct records for your Post.Office host.

Setting up an A record

Setting up "A" records is simple; you make an entry in your DNS server that resolves your Post.Office host's FQDN to its TCP/IP number. If you plan on including your host's name on all the E-mail addresses in your system, setting up an "A" record is all you need to make sure that other computers on the Internet will be able to forward E-mail to you. "A" records look like this:

```
host.yourdomain.      your_host's_IP_number(##.##.###.##)
```

The "A" record for our example would look like:

```
myPC.Acme.com.     IN  A  123.45.6.78
```

Setting up MX records

If you are going to use E-mail addresses that do not include your host's fully qualified domain name (in other words, if you plan to use host name hiding), you will need to establish "MX" records in your DNS server in addition to your "A" records. The "MX" records will instruct querying computers to forward all messages for your domain (Acme.com) to your Post.Office host (yourPC.Acme.com).

"MX" records are the recommended form of DNS entry for mail service. All mail servers look for "MX" records first in their search to identify an external mail host. In addition, "MX" records support the concept of priority. Priority rankings enable you to identify backup mail servers by inserting additional records in your DNS nameserver.

The figure below illustrates how "MX" records should be set up, both for your Post.Office host's domain as well as for any virtual domains that you may want to set up.


```
MX records: yourdomain.      IN  MX  10  host.yourdomain.
                             IN  MX  20  FQDN_of_backup_host

A records: host.yourdomain. IN  your_host's_IP_Number(###.##...)
```

Figure 1-1 Sample DNS Configuration for your host's Domain

A virtual domain is any domain besides the host's domain for which you configure Post.Office to receive messages (you can set up as many virtual domains as you like). We refer to such domains as virtual domains since there need not be any physical hosts in these domains.

```
MX records:  virtualdomain.  IN  MX  10  host.yourdomain.
                             IN  MX  20  FQDN_of_backup_host

A records: host.yourdomain.  IN  A  your_host's_IP_Number(###.##...)
A records: virtualdomain.    IN  A  your_host's_IP_Number(###.##...)
```

Figure 1-2 DNS Configuration for any "virtual domain"

Simple "MX" records for our sample company might look like this:

```
Acme.com.         IN  MX  10  myPC.Acme.com.
                  IN  MX  20  backupPC.ISP.net.

myPC.Acme.com.    IN   A  123.45.6.78
```

The first two lines are the "MX" records for `acme.com`. They provide information about how to handle any messages addressed to acme.com (the addresses *jane.doe@acme.com* and *john.deer@acme.com*, for example). Without "MX" records, messages to addresses such as this would not be deliverable since they do not include a host name (an "A" record will suffice but there will be no backup if myPC is down).

In this case, the "MX" records specify that E-mail for acme.com should be sent to yourPC. The record also specifies that if this fails, (for example, if yourPC is down), mail should be sent to backupPC.ISP.net, where it will be queued until yourPC is available again. Mail servers will send messages to yourPC rather than backupPC whenever possible because of yourPC's lower value (10 rather than 20) compared to backupPC.

Note: *You should never use someone as your backup without their consent, so remember to get permission first.*

The last line is an "A" record, which you should include since some older mail software does not understand "MX" records. The "A" record points directly to the IP number for the host yourPC.

In order for these "MX" records to work, there will of course need to be "A" records for both yourPC and backupPC. The "A" record for yourPC is shown above, while the "A" record for backupPC is maintained by "ISP", the folks who are kind enough to provide a backup for yourPC.

1.2.3 Consequences of Improper Configuration of DNS Records

The ability to send mail, but not receive it is a likely indication that your DNS records are misconfigured. The successful sending of mail simply reflects that the recipient's DNS records are in order. If mail can't find its way back to you, it's probably because you have an error in the records identifying your mail server to the DNS. Be sure to check your DNS records carefully if you suspect this is your situation.

2

Setting Up Your E-mail Network

This chapter provides a rough blueprint of how to successfully set up even the most complicated E-mail network. It includes a check list of things you should consider when setting up your E-mail network, discusses the tools used with Post.Office to take care of addressing and routing, and provides several example configurations that cover the most common situations and should spark ideas on how to approach your own solution. If you are already familiar with the topics described above, you can, of course, skip ahead to Chapters 3 and 4, which cover pre-installation planning and the actual installation for Windows NT and UNIX, respectively.

2.1 Safety First: Setting up a Secure Mail Server

The subject of security can be divided it into two themes: System Security and Mail Account Security. System security is concerned with the protection of the computer system on which Post.Office is operating. This includes services on the machine which are unrelated to Post.Office as well as the configuration information which is required for Post.Office operation. Mail account security relates to the protection of the information in the Post.Office databases which is relevant to the user's and Postmaster's mail accounts. Topics pertinent to these themes that are covered in this chapter include:

- Run-time Permissions
- Directory, Registry, & Program Owners
- Web Form Security
- E-mail Forms and Form Requests
- Message Security

2.1.1 System Security

The Post.Office approach to system security is to carefully isolate Post.Office from the remainder of the system. Sites which are concerned with the security of their machines are urged for this reason to create a special user account and group during the installation process.

During the installation of Post.Office, you will assign an account and group on the machine for the mail system to operate as. The account's permissions are intentionally limited to only those necessary to operate Post.Office. On most installations, this account should be for the Post.Office system only. (Sites which are not connected to external mail

sources may choose the built-in system account.) The Post.Office account (and group) permissions provide a significant share of the system security afforded by Post.Office.

Windows NT Run-Time Permissions

With no exceptions, the executable code which comprises Post.Office is run under the Post.Office user account (and permissions) and cannot gain access to the host system beyond what is required for the mail system.

The Post.Office service, known as the Dispatcher, is the module which controls the overall operation of the mail system as well as permissions for the other Post.Office modules. As the dispatcher‘s main role in Post.Office is the management of the tasks necessary for the mail delivery, it does not actually communicate with any users or other machines. This module operates secured with administrator access and can be interrupted only by an administrator or a server-operator.

UNIX Run-Time Permissions

With one exception (discussed below) the daemon portion of Post.Office is the only module allowed to use root permissions during run-time. The majority of the executable code which comprises Post.Office is run under the MTA user account and group and cannot gain access to the host system beyond what is required for the mail system.

The Post.Office daemon, known as the *Dispatcher*, is the module which controls the overall operation of the mail system as well as permissions for the other Post.Office modules. As the dispatcher’s main role in Post.Office is the management of the tasks necessary for the mail delivery it does not actually communicate with any users or other machines.

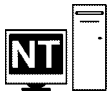
The dispatcher initially runs with the root (or super-user) permissions when Post.Office is started in order to carry out initialization of the network connections[2]. Immediately following necessary initialization, and prior to accepting or processing any messages, the dispatcher irrevocably releases the root permission and hence takes only the permissions set up for the Post.Office system during installation.

Thus, all special privileges are dropped and only the MTA users privileges are retained during normal operation. All other (with the exception below) network and local Post.Office modules are run by the dispatcher with these limited permissions.

2 UNIX only allows 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 thus requiring root permission for these services.

Warning! There is one exception to the rule of limited permissions: a utility module which works with UNIX-Deliver to create a mail drop file. Due to the ownership requirements of the UNIX mail drop file (the owner is the person who is receiving the incoming mail and the group is usually the mail group) it is necessary for there to be a special program which is able to create an empty file with the proper permissions allowing access for both the mail system (to deposit mail) and the user (to pick up mail from the file). This module (owner is root) runs with the set user id bit set in its permissions which allows it to assume the permission for the root account. The source code for this module is available for inspection and modification upon request.

Directory, Registry, & Program Owners in Windows NT



There are several directory trees which Post.Office uses in normal operation. The executable service (Post.Office.exe) lives in the Program directory while the Post.Office library (Post.Office.dll) is stored separately. The Spooling directory contains account and configuration information (SMTP-Accept, POP3-Server, etc.). Mail is stored in the Mailbox directory. The default permissions for each of these files/directory trees are designed to allow proper operation of the Post.Office modules while providing a secure envelope for the host system running Post.Office.

The owner and permissions on these files/directories as established by the installation program are as follows:

Directory Tree	Owner	Permission
\win32app\Post.Office (the Program directory)	Administrator	Post.Office (RX) Administrator(Full)
\winnt\system32 (the Post.Office library file)	Everyone	Read
\winnt\system32\spool\Post.Office (the Spooling Directory)	Administrator	Post.Office (Full)(Full) Administrator(Full)
\winnt\system32\spool\Post.Office\mailbox (the Mailbox directory)	Post.Office	Post.Office (Full)(Full)

The registry entries for Post.Office are stored in the

`HKEY_LOCAL_MACHINE\SOFTWARE\Software.com\Post.Office`

tree. The owner of this tree is the Administrator and the default permissions allow only the Administrators and Post.Office users full control.

Directory, Registry, & Program Owners in UNIX

There are three directory trees which Post.Office uses in normal operation: the executable, Post.Office, and mailbox directories. The permissions for each of these directory trees are designed to allow proper operation of the Post.Office modules while providing a secure envelope for the host system running Post.Office.

The owner and group for these directories are as follows:

Directory Tree	Owner	Group
Program	root[3]	MTA
Spooling	MTA	MTA
Mailbox	MTA	MTA

2.1.2 Mail Account Security

This section describes various Post.Office features which are used to protect the configuration of your account database (by controlling carefully the issuing and processing of remote configuration forms) as well as to protect the delivery of E-mail to users with Post.Office accounts.

Account Information

Fields on the Account Data form which are relevant to account security are illustrated in the two examples below. The fields to be discussed include: Mail Account Password, NT Logon Password, NT Username, and Internet Address, as well as delivery information and account security parameters. Fields not related to our discussion have been omitted for the sake of clarity (with the exception of the Account Name field which was included so we can keep a handle on things).

These hypothetical accounts will be used throughout the section to demonstrate how the security features of the Post.Office Managers work.

3 The executable modules of Post.Office are owned by root to prevent any other user from modifying the files (including the MTA user).


```
===== GENERAL ACCOUNT INFORMATION ================================

User's-Real-Name:      [Jane Doe]

Mail-Account-Password: [Sur+Fer!]

  Use-NT-Logon-Password: [] ("yes" or "no" to use their NT password)
      NT-Username:       []  (domain\user or simply user)

----- E-MAIL ADDRESSING INFORMATION -- INTERNET (SMTP Channel) -----

Internet-Addresses:    [Jane.Doe@Software.com])
                       [jane@Software.com]
                       [doej@Software.com]

----- LOCAL DELIVERY INFORMATION ----------------------------------

POP3-Delivery:         [POP]
      POP-Login-Name:  [Jdoe]

Forwarding-Addresses: [Bill.Zoom@software.com]

----- ACCOUNT SECURITY PARAMETERS -- ** Optional ** ---------------

Account-Locked:               [no]

General-Access-Restrictions:  [sparky.software.com]
                              [199.17.234.0]
```

Figure 2-1 These selections from Jane Doe's Account Data form show the fields which are relevant to our discussion on security.

```
===== GENERAL ACCOUNT INFORMATION ================================

User's-Real-Name:         [Support Account]
Mail-Account-Password:    [Friendly'nCourteous*##!!]

---- E-MAIL ADDRESSING INFORMATION -- INTERNET (SMTP Channel) ------

Internet-Addresses:       [Support@Software.com]

----- LOCAL DELIVERY INFORMATION ----------------------------------

Forwarding-Addresses:     [jane.doe@software.com]
                          []

----- ACCOUNT SECURITY PARAMETERS -- ** Optional ** ---------------

General-Access-Restrictions:   [sparky.software.com]
                               [199.17.234.0]
```

Figure 2-2 These fields, taken from the "support@software.com" Account Data form, are those fields which are relevant to the Post.Office security features discussed forthwith.

Web Form Security

The WWW-Server will answer web (WWW) client queries on the port number assigned during the installation (typically port 80 or 81). Upon connection to the Post.Office WWW-Server, there is a three step authentication procedure enforced on all initial web requests:

- **Initial Connection -** The calling web client's IP address is checked against the global web access domain list (this is on the System Security form under the Limit Configuration via Web forms field). If the list is empty, or the list contains a specific or wildcard match for the client's address, the WWW-Server issues the Authentication Form to the client. If the list is not empty and the web client does not match any of the entries, the WWW-Server responds with an error and the connection is immediately terminated.
- **Authentication Form** - The Authentication form prompts the user to enter their E-mail address and appropriate password. The password is not echoed on the users screen. After the user has entered both fields and selected the "Authenticate" button, the form information is delivered to the WWW-Server for verification.
    - If the E-mail address matches an existing account's E-mail address, the account's access restriction entry is checked to verify that access is allowed from the web client's IP number. If the account's access restriction entries preclude the web client's IP number, a message will be returned to the web client explaining this.
    - If the web client's IP address is allowed, the submitted password is checked against the account's password. If the passwords do not match, an access denied message is returned to the WWW client. If the passwords do match, the WWW-Server creates an access token for the session and returns this along with a web form (a user will get their Individual Account Information form, and a Postmaster will get a List of Accounts form).
    - Currently the authentication information is sent to the WWW-Server in an unencrypted form and may be monitored if there is physical access to your network by others or your web session is over a public network.
- **Access Token** - Access tokens are created with a time stamp and the web client IP address. The tokens are encoded into all further communications with the web client (in the URL). The token's time stamp is used to limit the time period for which an issued token is valid. The time limit is under the Postmaster's control (the time period may be set using the System Security form) with a default of 5 minutes. The token time stamp is reset with each form request or form submission so there is no time limit on a web session, only on the time between form request/submissions. In addition, the token is only valid for the web client's IP address and cannot be transferred to another machine (to switch to a different machine the user must re-submit an Authentication form from the other machine).

E-mail Forms and Form Requests

The safeguards which relate to remote configuration of forms and form requests are account determination, access restrictions, and passwords (passwords are not used for a form request, only in the forms themselves). These safeguards apply to issuing and processing forms such as the Account Data form and the Individual Account Information forms.[4]

Account Determination

Post.Office makes a determination of who is requesting or sending in a form by looking at the "From:" header line on the envelope of the mail message which contains the form (or request).

This address is compared to the addresses in the account database. For example, Post.Office may receive a form request in the envelope below:

```
To: <Accounts@software.com>
From: <Jane.Doe@Software.com>
------------------------------------------------------------------------

To: Accounts
From: Jane.Doe@Software.com
Subject: I want some information forms
------------------------------------------------------------------------

  Info <Jane.Doe@Software.com>
  Info <Support@software.com>
```

Figure 2-3 A typical mail message containing a form request from Jane Doe. The first two lines make up the electronic envelope which contains the message. The balance of the illustration contains the message itself: the headers followed by the body. Note that Post.Office makes its account determination based on the information contained in the envelope (bold), not the message headers.[5]

Post.Office compares the address "`Jane.Doe@Software.com`" (on the envelope) to the SMTP addresses in its account database. This address in this database may be associated either with the Internet Address field (as is the case in Figure 2-1) or with the Delivery field (as in Figure 2-2). In this manner, Post.Office ascertains that Jane Doe has access to two accounts: her own (as `Jane.Doe@Software.com` is an Internet Address for her account) and the support account (as `Jane.Doe@Software.com` is in the Delivery list for the support account). Since she is not Postmaster , the only form to which she has access is the Individual Account Information form which she is requesting.[6]

---

4 The safeguards discussed here apply equally to configuration forms.

5 If you are not familiar with the role of envelopes in E-mail, they are briefly discussed in Chapter 1.

6 Of course, access to the form is not everything, Unless Jane has the account passwords for the two accounts, she will be unable to make any changes. Thus the Postmaster has the option of directing all E-mail addressed to "`support@software.com`" to her without giving her the options of changing the account by withholding the password.

Had Post.Office's search revealed that Jane was also listed in the Delivery field of the Postmaster account, she would then also have access to that account, and, as a result, to the whole Post.Office system and any other form she might want; however, if she had "spoofed" her From address, she would still not be able to get a form as covered in the next section.

Note that Jane has Bill.Zoom@Software.Com listed as a forwarding address in her account delivery information. This means that Bill winds up getting any messages which are sent to support (through Jane and then on to Bill). However Bill, whose address is not listed in any field of the support account, has no access to the information for that account.[7]

Once account determination has been carried out, Post.Office then consults access restrictions to verify that Jane is allowed to do what she wants from where she is doing it.

Access Restrictions

```
User's-Real-Name:          [Jane Doe]

Access-Restrictions:       [sparky.software.com]
                           [199.17.234.0]
```

Figure 2-4 Jane Doe's access restrictions, taken from her Account Data form.

Once Post.Office has determined who is sending a form or a form request (we continue with the example from the previous section of Jane, who is requesting some information forms), Post.Office verifies that the domain portion of the From: address (software.com, highlighted above in Figure 2-3) listed on the envelope of the message is within the correct access restriction list for the account (Figure 2-4 above).

Post.Office compares this address to Jane's access restriction. If the address includes the phrase software.com or is located on a host with a 199.17.234.0 IP address ("0" acts as a wildcard), the request is approved, and Jane will get the Individual Account Information form for her accounts.

The form is then delivered to Jane's account as listed in the Post.Office account database, not to the "From" address on the form request. Thus, if Jane uses POP delivery for her account, she will still have to retrieve the message from the Post.Office host and provide her POP login and password -- yet another security hurdle.

In this case she will get two forms: one for her personal account and one for the support account, as per the account determination discussed above and in line with her request.

When forms are submitted there is one additional step: password verification.

---

7 This is relevant, for example, if the Postmaster goes on vacation and puts Bill in charge of things. Bill must be listed in the delivery field of the Postmaster account in order to get Postmaster privileges. Alternatively, Bill can be listed in the delivery field of whoever currently has Postmaster privileges, and receive all mail addressed to Postmaster but not have power to change the system.

Note: *A domain literal (used in the Access Restrictions list - i.e. 199.17.234.0) is more secure than a domain name (such as "software.com"), so if it is the same to you, stick to the numbers, particularly with key accounts such as the Postmaster account.*[8]

However in some cases (when there is no DNS server or host file entry), domain literals are not allowed by the managers as the envelope from address on a form request or a form submission (i.e. if Jane sent mail as Jane.Doe@[199.17.234.2] the manager would reject the mail even if 199.17.234.2 was within software.com).

Passwords and Form IDs

Once Jane submits her Individual Account Information form, having made the changes she wanted, Post.Office compares the password on the form to the password stored in the account database and verifies that it is an exact match (recall that Post.Office has already made an account determination as well as verified the access restrictions).

Post.Office also verifies that the form that is sent is the same form as it sent out. It does this by verifying that the form bears the correct form ID at the bottom (the part that says not to touch). However, if you are using E-mail forms and want to be able to use forms interchangeably on different hosts, you can specify that each host have the same E-mail form security enhancement password, which is specified on the System Security form. This password is mixed with other information and mangled through an encryption algorithm to create the unique form identifiers.

8 In the Domain Name System there are two basic types of requests: a forward request (or Address Record) and a reverse request (or Pointer record). The forward request takes a name (rome.sales.software.com) and finds the authoritative nameserver for the domain "sales.software.com" (which in this case is Troy.Software.com), and asks for the IP number (which would be 198.17.234.88, if it existed).

Inversely, a reverse lookup starts with an IP number (198.17.234.88), finds the authoritative domain name server (which may not be Troy.Software.com depending on the setup) for the IP Address (this gets complicated because sometimes it is authoritative for 128.11.x.y, sometimes 198.17.234.x, and sometimes even 10.w.x.y) and asks for the host name (rome.sales.software.com).

Security comes in because while the forward queries are almost certainty correct and you trustworthy, while the reverse is not true. An example illustrates the point;

If I am authoritative for software.com all requests with regards to software.com will come to me and I will give the answer. If Bad.Boy@Hacker.org is authoritative for 199.11.11.0 and he makes up a reverse record of 199.11.11.4 -> rome.software.com the reverse query of 199.11.11.4 from anyone (including a computer in my domain of software.com) will result in rome.software.com. I have no control over that.

How does this relate to access domains you are now asking?

Answer: if an access domain for the `Post.Office` program on Rome reads "software.com", and using the above scenario, Bad Boy's mail from 199.11.11.4 will be considered to originate from rome.software.com and thus will pass the access domains test. If however the access domain reads 198.17.234.0, Bad Boy's address (199.11.11.4) will not. Thus domain literals (i.e. numbers) are more secure than names because all they involve is forward lookups (is @rome.software.com in 198.17.234.0?). The drawback of domain literals is that they are not as flexible as domain names.

Every mail account in Post.Office has a password which is initially set up by the administrator and is under the control of the account user. A one-way encryption (MD5) is applied to the password when it is stored in the account database to insure secrecy. That way, if someone gets their hands on the account database, they still don't know any of the passwords and won't be able to do any excessively destructive things. The account password is used to control access to both the account's mail (in the case of a remote delivery like POP3) and to account information (via the Individual Account Information form).

Passwords are arbitrarily long strings of characters, their length limited only by your patience and the fact that they must be confined to a single line on a form. Post.Office passwords are case senSiTive. Additionally Post.Office enforces a minimum password length of 6 characters to help prevent users from making poor choices.

Postmaster Account Password

In addition to being a normal account which receives incoming messages, the Postmaster account (through its password) plays a crucial role in controlling the message transport system configuration and account information. *The Postmaster password is one of several important security filters for the administration of the message system and it should be appropriately protected*.[9]

Locked Accounts

The Postmaster can "Lock" Post.Office mail accounts to prevent access to the account information and prevent delivery of mail via POP. This is accomplished by requesting the Account Data form for the appropriate account and placing the word "yes" in Lock-Account field.

When an account is locked the prior password remains with the account but all access requiring a password for the account is denied until the lock is removed by the Postmaster. The lock on an account is removed simply by entering the word "no" in the Lock-Account field of the E-Mail Account form or by clicking on the No button in response to the "Lock Account?" question asked on the Account Data web form.

Message Security

Message security concerns the protection of user and system E-mail from eavesdropping or interception. Post.Office protects user messages using the POP mailbox.

POP3 Remote Message Pick up

When a user selects POP3 delivery, messages are stored in a sub-directory of the mailbox (as chosen during installation). The owner and group of the mailbox directory are given

9 For this reason we strongly recommend you not use the Postmaster password over unprotected networks outside your local network such as across the Internet at large. Most sites are comfortable administering things across their internal network within their domain, but restrict access via access domains from the Internet at large.

only MTA permissions to secure access from individuals or programs on the system running Post.Office.

Access to messages via POP3 is controlled by the Access Restriction and Account Password fields.

For example, when Jane Doe checks her mail, she must do so from a host whose address includes either the phrase "software.com" or "199.17.234.0" (where "0" is a wildcard).[10] Unless she meets this condition and enters the correct password for her account, access to her messages will be denied.

Additionally, she must know the POP login for the account which may be completely unrelated to any of her E-mail addresses, if desired.

Warning! Users should be wary of using their passwords on public networks such as the Internet. Eavesdropping is fairly easy, and amazingly enough there are people who are bored enough to think your mail may be interesting enough to warrant the effort of snooping out your password. The best bet is to keep your access restrictions limited to within your organization which you should protect via your network routing set up or your firewall. That way, you operate completely within a secure network which protects you from the evil lurking beyond your kingdom(ain) walls. If you desire or need to access your mail from a remote host across a public network, it is best to still have an access restriction in your account which is limited to your domain, and simply add the specific host or set of hosts you will use outside your domain. Access restrictions provide a powerful security enhancement even across public networks when applied judiciously.

2.2 Other Issues to Consider

Security should be one of the primary concerns in establishing your mail server, but it is by no means the only issue. This section is a check list of key items to review when thinking about how to set up your E-mail network. This is not a formula. Rather, it is a list of things you should keep in mind as you decide how many machines you need and how to configure Post.Office on each machine so that they work together harmoniously.

System Load

The load put on a machine running Post.Office, or any MTA, is directly proportional to the volume of mail that goes through the system. The volume obviously increases as the number of users increases, and as Post.Office is set up to handle more mail domains (since that means there are more users). To reduce the impact of mail on a single machine you may want to distribute users among several machines.

10 See discussion of access domains, above.

You should be particularly mindful of the potential burden imposed by mailing lists. Such lists are a great convenience, but if left unregulated can lead to trouble. Our advice: start small and only increase list limits as required.

Addressing Conventions

Post.Office will let you assign any valid address[11] to an account. You may want to choose a convention for user addresses (such as *First.Lastname@mail_domain*[12]). Regardless of the convention you choose, you must set up the DNS so that mail with the addresses you use will be delivered to your network.

If you want addresses to exclude hostnames of specific computers, you will need to follow the instructions for hostname hiding discussed a little farther on.

User Access to E-mail

Post.Office allows users to access their E-mail via the network using POP3 remote mail access protocol. The Post.Office POP3 server provides ease of administration, fast performance, and strong security. Program delivery is also available, which allows users to have their mail delivered to a program which will then process it efficiently (this is mainly for users with a large volume of E-mail).

Post.Office also allows UNIX users to log into the server and retrieve mail using software that reads their UNIX spool file (e.g. `/var/spool/mail/`*username*). For users who want mail and don't otherwise need a login account, the best option is to set them up with a POP account in Post.Office which they can access from a remote PC or workstation. Users that have UNIX login accounts most likely use mail software that accesses their maildrop directly. However if POP-aware software is available, some users may prefer to have a POP account set up for them.

If you have a number of users that only use POP to retrieve their mail, it may be beneficial to set up a dedicated mail server machine for this purpose. The benefits of such a "sealed server" are ease of administration, improved performance, and improved security.

Connectivity to the Internet

There are three levels of Internet connectivity: fully connected, intermittently connected, and not connected. How you set up your E-mail network depends on the category you fit into.

Fully and intermittently connected sites are similar. Since intermittently connected sites are not reachable at all times throughout the day, it is especially important that MX records are set up to redirect incoming mail to an alternate host while not connected. Such

---

11 A valid address is one that conforms to RFC 821 specifications.

12 The first.lastname format for addresses can cause problems if you have two users with the same, or similar, name, since all E-mail addresses must be unique.

sites often connect to the Internet using SL/IP or PPP to a network provider who acts as a backup mail exchanger.

Unconnected sites that use Post.Office on a private TCP/IP network for mail may or may not have a mail gateway to the Internet or other network such as UUCP or BITNET. Post.Office can be set up to deliver all non-local mail to the gateway machine which will pass it to the Internet or other network. Such a setup is very similar to having a firewall (discussed below).

Firewall Configuration

If your site is behind an Internet firewall you will need to do some extra things to allow mail to flow into and out of your network. Since other machines on the Internet can not directly contact any of your hosts except for the firewall, all incoming mail must be routed to the firewall with MX records. All outgoing mail needs to be sent to the firewall which will forward it to its final destination. The details of setting up Post.Office in an environment with a firewall are discussed in Section 2.4.

Use of Proxy Servers

Post.Office relies on UDP packets for internal communication. Proxy servers can filter UDP packets. For this reason, Post.Office should not be installed on a proxy server with this filter in place.

2.3 Addressing and Routing with Post.Office

Addressing and routing are fundamental concerns when setting up your network, from assigning addresses to accounts to setting up alias, routing tables and MX records on other hosts. Various ways of handling addressing and routing are discussed below, and will reappear frequently in the examples discussed in Section 2.4.

2.3.1 Account Addresses

Post.Office account addresses are very powerful. Any number of addresses can be assigned to an account. These addresses are used to determine if a piece of incoming mail should be delivered to the account. Accounts can be configured to rewrite the "From:" header of outgoing mail to list the account's official address. These features can be used to assign arbitrary addresses (such as `first.lastname`) to each user and/or to implement hostname hiding, which is discussed later in this chapter.

It is trivial to handle several domains on a single machine -- simply assign the addresses to the desired accounts and Post.Office will recognize them. Addresses within one domain are independent of any other domain. For example, an account with the address <joe@some.domain> can be different from an account with the address <joe@another.domain> with no confusion.

2.3.2 Local Mail Domains

The list of Local-Mail-Domains (LMD) is used to tell Post.Office that it alone knows every recipient in those domains. Post.Office will never attempt to deliver a message to these domains using a network protocol such as SMTP. If a message arrives for a recipient in one of the listed LMD's, Post.Office first attempts to find an account or channel alias for the recipient. If that fails, Post.Office will return an error report to the sender rather than attempt to forward it to the domain. This feature is used primarily to prevent people from attempting to deliver mail to PCs or other computers that are not running a mail server, or when several domains are being served by a single mail server running Post.Office.

2.3.3 Channel Aliases

Channel aliases are a simple address-rewriting way to redirect mail. A channel alias consists of two pieces of information, an incoming address and an outgoing address. Whenever a piece of mail arrives containing the incoming address of one of the channel aliases, the matching address is replaced with the outgoing address. The mail is then redirected to its new destination, generally to a different machine.

2.3.4 Mail Routing Table

The Mail Routing-Table (MRT) provides a way to redirect mail based on the domain to which it is being sent. Each entry in the MRT consists of a pattern and a domain. Before sending a message, the destination domain is compared against the patterns in the table. If a match is found, the destination host is replaced by the domain corresponding to the pattern that matched. (Note: no addresses are rewritten; the mail is just sent off to a different host.) This feature is useful for sites behind a firewall, or ones that have gateways to other networks such as UUCP or BITNET.

2.3.5 MX Records in the DNS

Mail exchanger (MX) records in the DNS provide a way to tell the outside world how to route mail to your domain(s). For each mail domain you can specify the hosts that should be contacted when attempting to deliver a message to the domain, along with the order they should be tried. The basic use for MX records is to specify one or more "third-party" machines that collect mail during temporary network outages. This is a must for poorly connected sites who use SL/IP or PPP to access the Internet and are only connected a few hours per day.

For sites that reside behind an Internet firewall, MX records are used to direct all incoming mail to the firewall machine (since no other machines are reachable). The firewall then relays the mail to its final destination on the internal network.

A very similar situation exists for sites that have domain-based E-mail addresses requiring one or more mail hubs. MX records channel all incoming mail into the hubs which then relay the messages to their final destinations.

MX records also enable the creation of "virtual domains" that have no machines connected to the Internet, yet are accessible via E-mail. A network provider will often set this up for a customer who has registered a domain name. The network provider advertises MX records for the virtual domain that point to their own mail servers, and the mail is delivered to the virtual domain, for example over a UUCP connection, or by some other method.

2.4 Sample Setups

In this section, several scenarios are presented which cover most typical setups. Your exact situation may not be covered exactly by one of the examples, but ideas can be pulled from the various examples as suits your situation to get your site set up correctly.

Each example describes what is being accomplished and then explains how to set up Post.Office to achieve the desired effect. The first two examples cover the basic types of addressing (host- and domain-based) and the last two deal with issues unrelated to user addressing, and therefore build on the first two examples.

2.4.1 The Basic Setup

The basic setup is used in a new, small scale (less than 50 users) installation. Sites that have minimal special requirements for Post.Office should build on the basic setup model. (If you implemented a domain-based addressing scheme using your current mail server software, skip to the next section which covers hostname hiding.)

Scenario:

- All machines are directly connected to the Internet.
- Users send and receive mail addressed from/to a single specific computer.
- User addresses are based on some combination of their real name.
- Users use POP3 mail clients (e.g. Beyond Mail, Z-mail, Eudora) that access their mailbox.
- Each machine acts independently; messages are sent and received directly to/from other machines on the Internet.

Network Diagram:

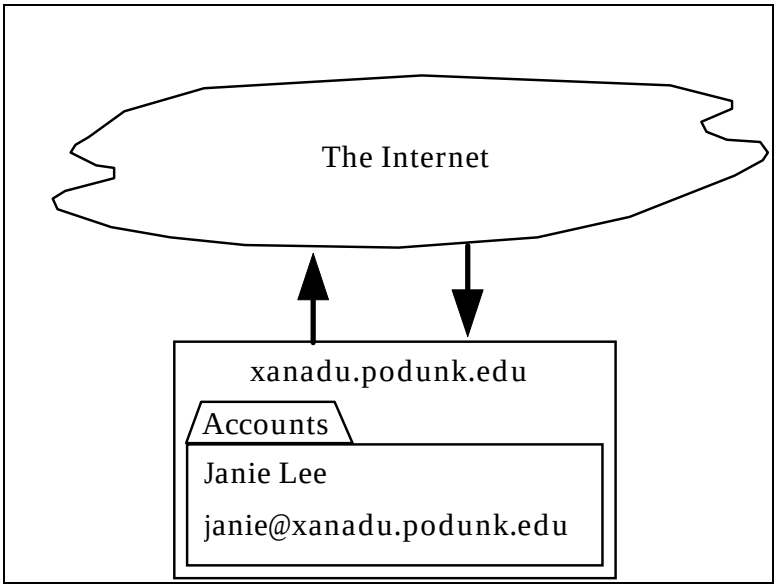


Figure 2-5 Janie's address is `Janie@xanadu.podunk.edu`.

Special UNIX installation instructions:

When running the installation program, you will be asked if you want all existing users to be added to the account database. You definitely want to let it do this since it will save you a lot of work and get you very close to your original sendmail setup. The only major task it does not do is wade through your aliases file and users' `.forward` files.

When asked if you want users to receive mail addressed to the domain in addition to the host, you MUST answer "no" (the default) or users' outgoing mail will have a domain-based return address and "From:" header, which will not be usable unless the instructions for Hostname Hiding are followed (see the next example for these instructions).

MX records:

Each machine may have MX records that point to itself, and optionally to one or more backup hosts. MX records are not necessary in this scenario since each computer has an A (address) record. When MX records are set up, they may look like this:

```
xanadu.podunk.edu.        IN  A  123.45.6.78

                          IN MX  10 xanadu.podunk.edu.
                          IN MX  20 hub.podunk.edu.
```

Janie's account:

This example shows how Janie's account is set up in this situation. Users on the machine xanadu.podunk.edu have their mail delivered to their POP3 mailbox. Since Post.Office rewrites Janie's "From:" header on outgoing mail, she is sure that recipients will be able to reply to her messages.


```
User's-Real-Name:          [Janie Lee]
Internet-Addresses:        [janie@xanadu.podunk.edu]
From-Address-Rewrite:      [comment]
POP3-Delivery:             [yes]
    POP-Login-Name:        [janie]
```

Figure 2-6 Janie's account form settings. Only relevant fields are shown.

Local Mail Domains:

None are needed (local machine is always implicitly on the list).

Mail Routing Table:

No entries are needed, but they can be added if you want. See other examples for uses of the Mail-Routing-Table.

2.4.2 Hostname Hiding

Hostname hiding refers to the practice of having domain-based E-mail addresses which do not contain the name of a particular host. This effect can be achieved almost as easily as Janie's setup. You will need one or more machines, commonly called mail *hubs*, to process all incoming mail and distribute the messages to the particular *client* computer that houses a user's account. Of course you can set up hostname hiding even if you only have one machine acting as both hub and client.

Scenario:

- All machines are directly connected to the Internet.
- Users send and receive mail addressed from/to their domain (or sub-domain).
- Mail hub(s) are required to forward incoming mail to client machine(s).
- ***UNIX only*** - User addresses are based on their login ID.
- ***UNIX only*** - Users use typical mail utilities that access their maildrop file (e.g. `/var/mail/`*`login_name`*) such as `mailx`.

Network Diagram:

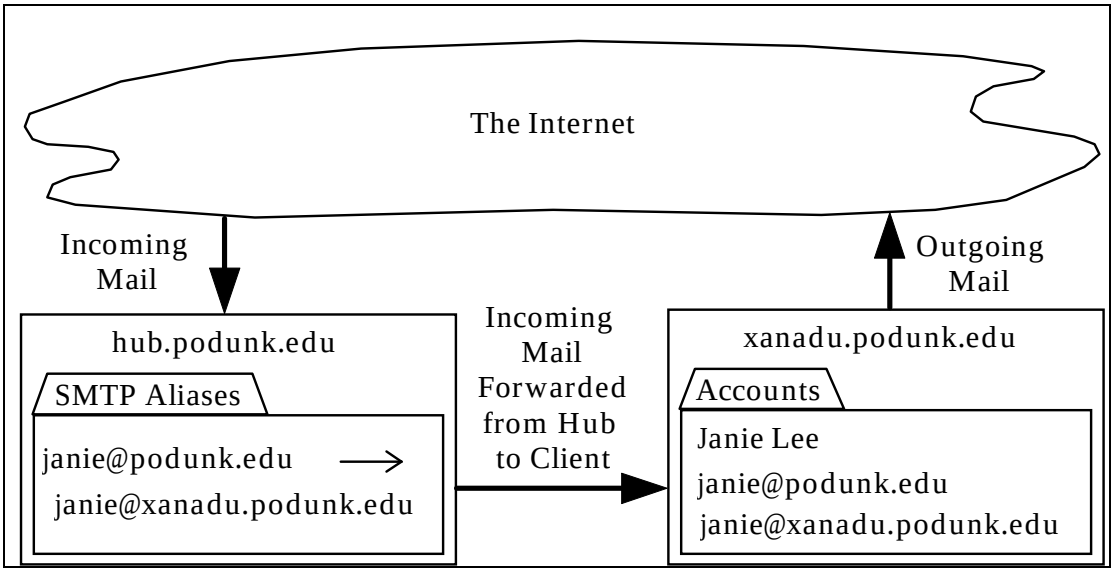


Figure 2-7 All messages for the domain podunk.edu go through the hub machine. On the hub host, Janie has an SMTP channel alias [<janie@podunk.edu><janie@xanadu.podunk.edu>] that points to Xanadu.

Special UNIX installation instructions:

When running the installation program, you will be asked if you want all existing users to be added to the account database. You definitely want to let it do this since it will save you a lot of work and get you very close to your original sendmail setup. The only major task it does not do is wade through your aliases file and users' `.forward` files.

When asked if you want users to receive mail addressed to the domain in addition to the host, you should answer "yes" so that users' outgoing mail will have a domain-based return address and "From:" header. Note that this only applies to accounts created by the installation program -- you must manually configure new accounts as shown below.

MX records:

There MUST be MX records for your domain, or mail addressed to your domain will not be deliverable. The MX records should point to each of your hub machines, most likely with equal preference. Backup mail exchangers are recommended and should have lower preference (higher number). Your MX records should look similar to this example:

```
podunk.edu.         IN MX  10 hub.podunk.edu.
                    IN MX  20 mx1.backup.net.
```

Hint: *Some existing (old) mail software does not understand MX records, so it is often a good idea to add an A record for your domain. The address should be that of one of your mail hubs.*

User Accounts:

This example shows how Janie's account is set up on a client machine supporting hostname hiding. Each user on the machine `xanadu.podunk.edu` has their mail delivered to their POP3 mailbox and their addresses are based on their first name. It is important that both the domain-based and host-based addresses are present in each account so that mail can flow into and out of the system correctly. It is equally important that each user have a From-Address-Rewrite specified, so Post.Office will rewrite their "From:" headers on outgoing mail to include their primary (first in the list) address.

```
User's-Real-Name:          [Janie Lee]
Internet-Addresses:        [janie@podunk.edu]
                           [janie@xanadu.podunk.edu]
From-Address-Rewrite:      [comment]
POP3-Delivery:             [yes]
   POP-Login-Name:         [janie]
```

Figure 2-8 Janie's account set up for hostname hiding.

Channel Aliases

Each hub needs to have a list of channel aliases for every user that can receive mail addressed to the domain. The aliases need to redirect mail to the specific machines that hold users' accounts. In the above example, the required channel alias (on the "SMTP Aliases" form) is:

```
Aliases:          [<janie@podunk.edu> <janie@xanadu.podunk.edu>]
```

Figure 2-9 Janie's channel alias on the SMTP Aliases form.

Note: *If you set up a single machine for E-mail for your domain, it acts as both the client and the hub without the need for channel aliases; however, each account should still contain both forms of addresses so that finger programs will work correctly (not to mention that this will also save you a lot of work if you ever expand to multiple machines).*

Local Mail Domains:

Each hub MUST list the domain, since it knows where every account is located. If this is missing, the Postmaster will see lots of "MX loop" error messages. A loop exists when the highest preference mail exchanger for a domain tries to forward a message to the domain and realizes it would send it to itself.

No client machine should need any entries.

Mail Routing Table:

No entries needed, but may be added as desired. The next two examples illustrate the use of the mail routing table.

2.4.3 Behind a 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 users of the Internet since it allows no direct connections to any internal machines, and relies on proxy servers or other trusted programs to carry communication across the divide.

A firewall introduces complexity to the delivery of mail between outside organizations. Since the firewall prevents direct connections between internal and external hosts, mail needs to be routed through the firewall in both directions. This is handled with a combination of MX records and the SMTP mail routing table for incoming and outgoing mail respectively.

Scenario:

- Local network is protected from the Internet by a firewall machine.
- Users have either host- or domain-based addresses as desired – see previous examples for specifics on how to do this.

Network Diagram:

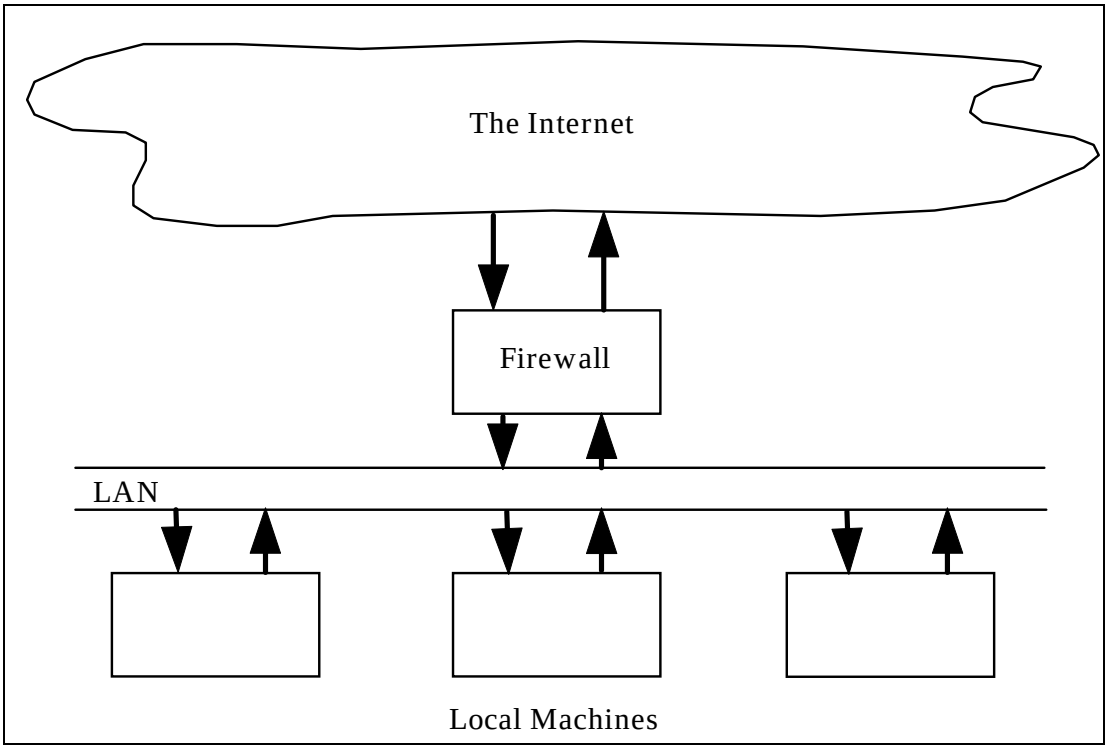


Figure 2-10 Diagram of a firewall scenario.

Special installation instructions:

Follow the instructions for either host-based or domain-based addressing provided in the first two scenarios.

If Post.Office is installed on the firewall itself and domain-based addresses are to be used, the firewall can act as the mail hub and should include a complete list of channel aliases for distributing mail to internal hosts.

MX records:

If you have a single DNS server on the firewall machine that answers requests from both internal and external hosts, your MX records for a host should point to the host first, then the firewall, and then any backup sites on the Internet (outside your network):

```
xanadu.podunk.edu.  IN MX  10 xanadu.podunk.edu.
                    IN MX  20 firewall.podunk.edu.
                    IN MX  40 provider.net.
```

For sites that hide their hostnames, MX records are needed for the domain as usual. These should point to the mail hub(s) first, then the firewall, and then to any backup sites.

Another option is to run two DNS servers -- one on the firewall for outside hosts and one on an internal machine for internal use only. The external DNS server (the one on the firewall) can be set up to give out very little information about the network. In fact, it can be set up with a wildcard MX record that says to just send all mail for any host in the domain to the firewall. Here's an example accomplishing that:

```
podunk.edu.  IN  A  123.45.6.78   ; for dumb mailers
             IN MX  20 firewall.podunk.edu.
             IN MX  40 provider.net.
```

The internal DNS server should contain the detailed information about the internal network and all internal hosts should be configured to use that server in preference to the external server.

Mail Routing Table

The firewall machine should not need any explicit routes since it can directly contact any internal or external machine.

Since the firewall is the only machine capable of delivering outgoing mail, you should set up every other machine with a default route to the firewall. A default route by itself will send **all** mail, including internal mail, to the firewall, so you need to also have entries in the table for your local domain that override the default. This example accomplishes that:

```
Mail-Routing-Table:      [podunk.edu:*]
                         [*.podunk.edu:*]
                         [*:firewall.podunk.edu]
```

Figure 2-11 Mail routing table for a firewall scenario.

Recall that a "*" after the colon means to send directly to the matching host (actually to one of its mail exchangers -- the Mail Routing Table entry does not override MX routing). Thus any mail destined for a host in the `podunk.edu` domain will be delivered directly to podunk and any other mail will be sent to the firewall which then forwards it to its destination.

2.4.4 Intermittently Connected Site

An “Intermittently Connected Site” is one that lacks continuous connectivity to the Internet, yet uses TCP/IP for communication. Typically these are sites that have a dialup connection to an Internet Provider and use either SL/IP or PPP to carry their packets over a phone line. Such sites are usually only “connected” for a few hours per day, or less. As such, they have some special requirements which are addressed here.

Such sites typically want to be able to connect up to the Internet, receive all their incoming mail, send all their outgoing mail, and then disconnect. For this to work, the site needs to have all their mail collect at a single location, such as their Internet provider, while they’re not connected. Similarly they would like all outgoing mail delivered efficiently to minimize connect time. For best efficiency, it can all be dumped to an external site such as the Internet provider who then forwards the messages to their final destinations. These two concepts are discussed in this section.

Scenario:

- Local network is seldom connected to the Internet
- When connected, all machines have direct access to the Internet
- Users have either host- or domain-based addresses as desired -- see previous examples for specifics on this

Network Diagram:

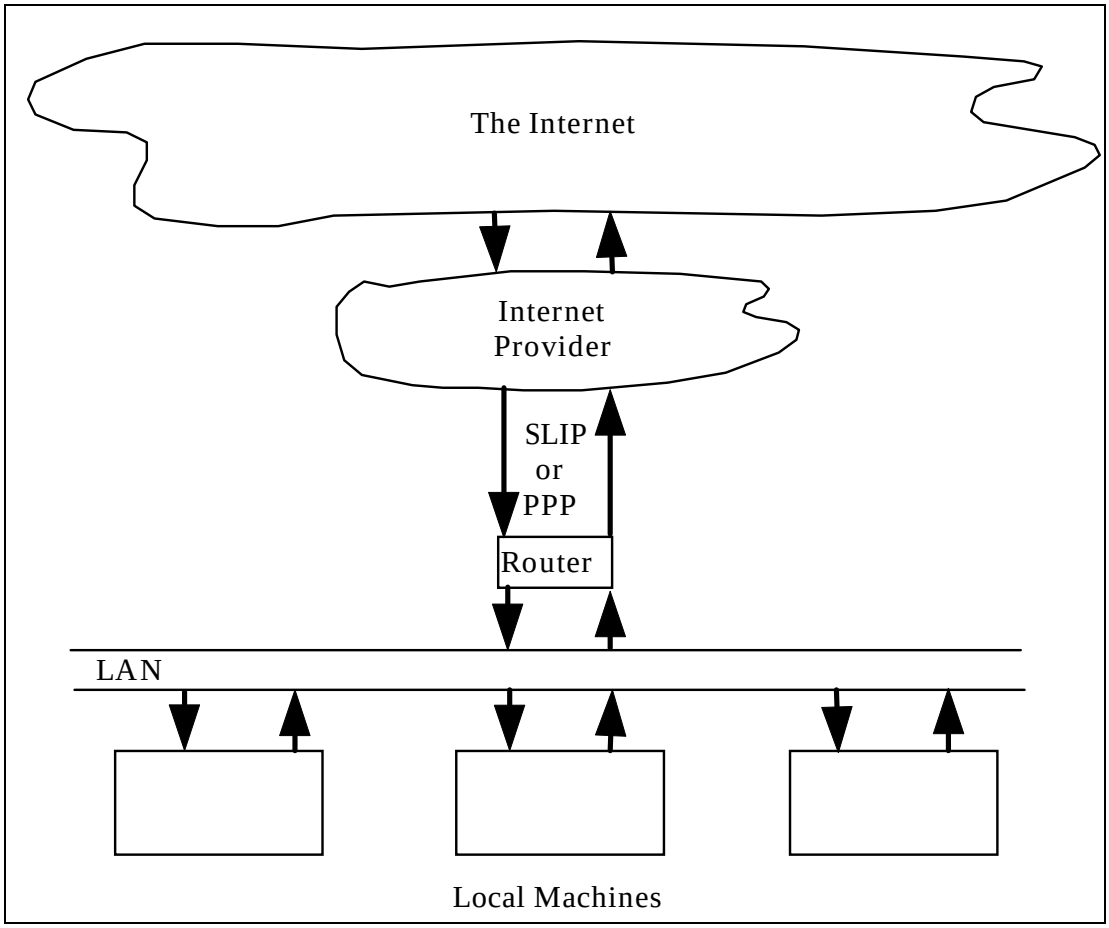


Figure 2-12 Typical setup for an intermittently connected site.

Special installation instructions:

None. Follow the installation instructions for either host-based or domain-based addressing provided in the first two scenarios.

MX records:

Each machine should have MX records that point to itself first, and then to one or more backup hosts. The Internet provider should have the lowest preference (highest number) of all mail exchangers since it should be used only in the case where the dialup connection is down. For example:

```
xanadu.podunk.edu. IN A     123.45.6.78

                   IN MX 10 xanadu.podunk.edu.
                   IN MX 20 hub.podunk.edu.
                   IN MX 40 provider.net.
In this scenario, the number of extra mail exchangers on the
“inside” should be small to minimize the impact on outside hosts
that try to send you mail while your network is not connected.
```


Mail Routing Table:

To achieve the most efficient delivery of outgoing mail, you should set up a default route to a single well-connected site (make sure you have an agreement with the other site before you set this up!) such as your Internet provider. A default route by itself will send **all** mail, including internal mail, to the default machine, so you need to also have entries in the table for your local domain that override the default. This example accomplishes that:

```
Mail-Routing-Table:       [podunk.edu:*]
                          [*.podunk.edu:*]
                          [*:provider.net]
```

Figure 2-13 Mail routing table for an intermittently connected site.

Recall that a "`*`" after the colon means to send directly to the matching host (actually to one of its mail exchangers -- the MRT does not override MX routing). Thus any mail destined for a host in the `podunk.edu` domain will be delivered directly to podunk and any other mail will be sent to the Internet provider who then forwards the mail to its proper destinations.

Retrieving Messages From an Intermittently Connected Site

Messages can be retrieved from the backup host by telneting to the SMTP port and using the "qsnd" command.

3

Installing Post.Office on Windows NT

In order to install Post.Office, you must verify that all system requirements are met, complete the pre-installation planning discussed in Section 3.2, and then follow the installation instructions outlined in Section 3.3. Section 3.3 includes a reference to the FAQ (Frequently Asked Questions) as a place to turn for additional information, and concludes with de-installation instructions should the need arise.

If you are setting up a mail system for the first time or are thinking about re-configuring you mail system and are not clear on what your options are, you should review Chapter 2 for illustrations of some of the more common messaging system configurations.

3.1 System Requirements

Hardware Requirements:

- Windows NT Workstation or Server.
- An Intel compatible 486 or Pentium processor, or a Digital Alpha AXP RISC processor. (Multiprocessors are supported.)
- 32 Mg RAM minimum (assuming no other major services are running on the machine hosting Post.Office). 64 Mg RAM recommended.
- An NTFS formatted hard drive is required. Installation of Post.Office on FAT partitions is not supported.

Note: *Exact requirements for processor speed, memory, hardware, and hard drive space are highly site-specific and depend mainly on the number of mail accounts maintained on the machine and the volume and size of mail and attachments.*

Software Requirements:

- Post.Office must be installed on a host running Windows NT version 3.51, for which you must install Service Pack 4. Windows NT version 4.0 is also supported. Before installing, please refer to the Technical Support section of the Software.com web site (http://www.software.com) and check out the latest information on the Service Pack awareness page.
- Post.Office will only work on a TCP/IP network. You must have TCP/IP installed on your host.

- If you are connected to the Internet, you will need a DNS server which lists your site's "A" and MX records. If you are not connecting to the Internet you can use either DNS or the HOSTS file for name resolution within your local network.
- A web browser (e.g., Netscape) is required.
- Mail Client with Post Office Protocol version 3 mail pickup (POP3) e.g. Z-mail, Eudora, Beyond Mail, etc.

3.2 Pre-Installation Planning

This section outlines a strategy for installing Post.Office. As you go through it, a checklist (a series of tables, actually) is provided for you to fill out with your choice of parameters. Completing this checklist will make the installation process flow smoothly.

Further assistance is available via Simple Online Support (SOS), a web tool designed to help prepare you for installation and guide you through the Setup process. SOS should be launched prior to installation and can be accessed by pointing a browser at the location: `http://www.software.com/tech/sos/po-install.htm`

The SOS screens list all pre-installation requirements for Post.Office and provide detailed instructions to assist you in meeting those requirements. Once all pre-installation conditions have been met, the SOS display can be positioned to one side of the screen and the Setup installation program launched. The two programs (SOS and Setup) are designed to be used simultaneously with information in one explaining entry fields in the other.

What to do with your Current Mail System

Since you are about to replace your current mail system with the Post.Office system, any existing services/programs you may have which perform as an SMTP mail server, POP3 Server, or finger service must be shutdown.

Choosing the Post.Office Account

Every process running under Windows NT operates with the privileges of an account. This can be a local account or, if you are using NT Server, a part of a domain. (On a workstation use a local account; on a non-primary server you may opt for either a local or global account; on a domain controller you must choose a global account.)

The Post.Office account will be created automatically as part of the installation process. You may choose to use another account, but that practice is discouraged. *In particular, you should not use the System account for security reasons.*

If you do choose to use another account you will need to setup the local account, and group, and insure over time that they are not deleted as Post.Office will not be able to run if its account is disabled.

Note: *If you choose to create a new user via the NT User Manager the following conditions must be met. The user must be the sole member of its group and have the right to "Log on as a Service" in addition to the following attributes:*

- User Must Change Password At Next Logon - no (off)
- User Cannot Change Password - yes (on)
- Password Never Expires - yes (on)
- Account Disabled - no (off)

Also, you will need to note the Username and Password that you select for this NT User account as you will need them when you run the Setup program.

Again, it is *highly* recommended that you allow the account and group to be established for you during installation.

Determining Use of Advanced Features

Two of the features available in Post.Office version 3.0 require that additional rights be granted to the Post.Office user. Those features are Program Delivery and the option to link an NT system password to a Post.Office mail account to be used in place of the standard Post.Office password. Please review the descriptions below to determine *before* installation if these are features you wish to activate.

Optional Linking of NT Logon Passwords to Post.Office Accounts

Office offers NT users the ability to use their NT logon password instead of their standard Post.Office password when accessing the Post.Office system to configure their account or retrieve their mail. Their Post.Office password still exists and is maintained independent of the NT password, but it is not used by the Post.Office system if this feature is selected. Instead, Post.Office always verifies and then utilizes the user's NT Username Logon Password as the user's Post.Office Account Password.

Note: *Installations which take advantage of this feature frequently define the user's NT Logon Name to be the same as their Post.Office POP3 Logon Name.*

This feature requires that special rights be assigned to the NT user responsible for running Post.Office (the one created at installation) and to those NT users who wish to use their NT logon password as their Post.Office password. Password integration will NOT work unless these required rights have been assigned.

Optional Use of NT Program Deliver

Version 3.0 of Post.Office also offers NT users the ability to deliver mail to a program (for archiving, special handling, etc.). This feature is described in the *Post.Office Administration Guide*, but for installation it is sufficient to note that if this feature is to be used, the Post.Office service account must have (in addition to the basic "Logon as a service" right required of any Post.Office service account) the following advanced users

rights (also required for using the password of an associated NT account as the mail password):

- Act as part of the operating system
- Increase quotas
- Replace a process level token

Hint: *The simple solution? These rights will automatically be granted to either a created service account, or an existing one, if the "Use Advanced Features" option is selected in the Post.Office installation program (SETUP.EXE). Otherwise, they can be enabled (or disabled) at any time using User Manager.*

Note: *You will still need to assign the right to "Log on Locally" to the NT usernames associated with the those individuals who wish to integrate their NT and Post.Office passwords, but that can be done after the mail server is installed.*

Your Registration Information

If you have already purchased a license for Post.Office you will have a license number. Entry of that number will be required before the installation software will run. If you are installing the free 10 user version of Post.Office, you will need to use the word "trial" in the registration information section.

Your DNS Domain

Most sites installing Post.Office will already be connected to the Internet and have a registered Internet domain name[13]. During the installation you will be asked for the domain name of the computer on which you are installing the system. This may be your organization's domain name, or possibly a subdomain. For example, if you were installing Post.Office on a machine named emile.math.ucsb.edu, the domain name you would specify is math.ucsb.edu.[14]

Note: *Refer to Chapter 2 in this Installation Guide and the discussion in SOS (`http://www.software.com/tech/sos/po-install.htm`) for additional information about domain names.*

13 An Internet domain name has nothing to do with an NT domain. For more on the Internet Domain Name System (DNS), you might want to check out some of the books in appendix E, which is a bibliography of sorts.

14 If you are not familiar with the DNS, or how to obtain a registered domain name, you may want to take a look at appendix B, which is a bibliography of topical reference material which may help you orient yourself with the terminology, protocols, and bureaucracy of the Net.

Postmaster Password

You will be prompted for a Postmaster password. This password is required to perform maintenance of the mail accounts or Post.Office configuration. Please make a careful note of your choice as it is difficult to recover from a lost Postmaster password.

Postmaster Password:	

Locations of Programs and Working Directories

Post.Office is broken up into three major parts: the executable modules, the mail processing center (or spooling directory), and the message store (or user mailboxes). The locations for each of these directories can be customized during the installation.

Note: *For simplicity's sake it is recommended that you store the Post.Office modules in the default directory locations.*

The contents of each directory are referenced below. After installation you can review the locations of these directories at any time by referring to the display in the Licensing/Configuration Form.

The Executables Directory - The executable modules that constitute Post.Office are all located in a single directory tree. Typically this directory will be in /win32app (depending on your conventions).

The Spooling Directory - The Spooling Directory is a directory where mail is processed. All incoming mail is temporarily stored in the Spooling Directory and remains there until it is either successfully delivered or returned.

Generally mail resides in the Spooling directory for only a few seconds as it is routed to its destination; however, if a message is destined for a remote computer that is temporarily unreachable, the message can remain queued up in the Post Office for several days, depending on how the system is configured. Typically the `system` partition is used for such storage in the directory \WINNT\System32\spool.

Make sure you put the Spooling Directory in a place that gets backed up regularly since it also contains mail messages which are in transit.

The Mailbox Directory

The Mailbox directory is where mail is stored for users that retrieve their messages via the network using the Post Office Protocol (POP3).

The amount of storage needed for this directory depends on the number of users that use POP3, the volume of mail they receive, and whether they leave their mail on the server or download it to their PC or workstation.

Warning! Do not utilize network drives for storage on a mail server because you would not want your partitions to be unavailable if for some reason your remote host was not accessible but your mail server was functioning.

Effect on Your Existing Mail System

Post.Office replaces your current mail transport agent. It does not, however, replace any mail user agent software you are using[15]. Since Post.Office is designed to be upwardly compatible with your existing mail infrastructure, all POP3 compatible user agents should continue to operate normally when Post.Office is installed as the mail server.

The Role of the Postmaster

During installation you will have to appoint a Postmaster. Anybody listed as a recipient of mail addressed to <postmaster@your.domain> is considered a Postmaster.

Each Postmaster is able to configure the mail system parameters, add, modify, and delete mail accounts, and set up automatic reply accounts. Since none of these tasks require administrator privileges, the system administrator can safely appoint someone else to the position of mail administrator, thus reducing the system administrator workload.

Postmasters interact with the mail system by sending it forms E-mail or a Web Browser. Thus the Postmaster doesn't even have to be a local user of a machine to be able to configure it. In fact all configuration and account changes for an entire E-mail network can be handled from a remote site.

Postmaster and Other Passwords

There will be three different passwords used in the installation section: the *local account password*, the *Postmaster password*, and your personal mail *account password*. **Each of these should be different for security reasons.**

The *local account password* is used by the Service Control Program (in Windows NT) to login the Post.Office service and give it access rights on the machine it is running.

The *Postmaster password* will be used by Post.Office to verify any administrative actions such as creating a new mail account.

Your *mail account password* is the password assigned to your personal E-Mail account and allows you to retrieve your mail (as it is also your POP password) and make any changes to your personal E-mail account (like going on vacation).

Record your passwords in the table below for ease of reference.

Local Account Password:	
Postmaster Password:	
Your Mail Account Password:	

15 Mail user agent software is the software you use to read and write E-mail, as opposed to message transport agents (such as Post.Office), which deliver and hold messages for user agents.

Impact of Migration for Mail System Users

Typically, when Post.Office opens an account for a user that user automatically receives a message from Post.Office called the **Greeting message**. The idea of the greeting message is to welcome the user to their account and provide them with basic account information (see Figure 3-1 below). Thus, one consequence of installation will be that all the users on your host will get this message:


```
To: You@Your.domain
From: Account-Manager<>
Reply-To: Account-Manager<>
Subject: Form: Greeting

MIME-Version: 1.0

Information

An electronic mail account has just been opened for you. This
account is configured as indicated below. Make sure you note your
password and safeguard it since this is the only time it will be
sent to you. See the instructions below the account summary for
information on how to make changes to your mail account as well as
for explanations about each of the fields.

Your-Name:              [your name here]
   (Note: your name is sometimes referred to as your account name)

Internet-Addresses:     [your address@your.domain]

Finger-Information:     [Tell the world how happy you are]
                        [about Post.Office]

======================================================================

 Here's some information about changing your account:

Only the system administrator can change your name or addresses. If
you want to change your password or your finger information, you can
do so with a World Wide Web browser (such as NCSA Mosaic), or via
E-mail. You simply fill out a form indicating the desired changes
and submit the form to the mail system.

To request the Individual Account Information form:

via the Web:      connect to http://

via E-mail:       You can get the E-mail form to modify your
                  account by simply replying to this message
                  and sending it in, or
                  send a new message To: <Accounts@your.domain>
                  with the word "Information" as the message body
                  like this:

                            To: Accounts@your.domain

                            Information

After receiving the Information Form, make the appropriate changes
to the form (use the "Reply" feature of your mail client if you are
using the E-mail interface), put in your password, and submit the
form. If you don't receive an error message, the changes have been
accepted.

======================================================================

                ....(full form is not shown)
```

Figure 3-1 This is the Greeting message which is sent to new users to orient them to how to get the most use out of Post.Office.

Note: *There is a mechanism for disabling the automatic delivery of a Greeting message. Post-installation, this option can be controlled via the selection made on the System Configuration form.*

Checking the Permissions for the Systems Directories

To insure that the Post.Office installation program is able to give the proper permissions to the Post.Office system, it is necessary that the owner of the System directories be the Administrators.

You can easily check that this is the case with the File-Manager: Select the system directory (/WINNT or /WINNT35 or /windows depending on your specific installation) and select Permissions... under the Security menu item. **The directory owner must be Administrators for the install to proceed.** If this is not the case, you will need to take ownership of the directory, sub-directory and files within, as one of the administrators (this is not a step to take lightly so please review the on-line help and additional manuals to be sure that you understand this operation).

3.3 Installing Post.Office

Now that you are prepared you are ready to begin this step-by-step guide to installing Post.Office. If you haven't gone through the previous section and planned for the installation, please do so now. A good plan at the start will make the installation run smoothly.

3.3.1 The Installation Process

The Post.Office system is distributed in a self-extracting compressed-file format which is common for Windows NT software. Follow the steps outlined below to extract the Setup package and install Post.Office on your system.

1. If you have not already done so, open the Simple Online Support (SOS) tool by launching your browser and pointing it to:

   `http://www.software.com/tech/sos/po-install.htm`

   This tool provides detailed information on pre-installation requirements, the installation process, and related topics such as proper configuration of DNS records.

2. Verify that all pre-installation requirements have been met.

3. Locate the Post.Office software package that was downloaded from the Software.com web site (http://www.software.com), obtained via ftp from the Software.com ftp site (the ftp/public/software directory), or delivered directly on CD.

4. Verify that you are logged on properly. If you are on a workstation or backup domain server you must be logged on as the Administrator of your host machine before

running Setup.exe. Only if you are on a primary domain controller can you log in as the Administrator of your domain.

5. Double-click on the Post.Office ".exe" file. The package will self extract and the Setup program will be launched. (The Setup program occupies only half your screen. This was done deliberately to allow for simultaneous display of SOS).
6. Respond as prompted to complete the installation process (making entries via Installshield and then the web interface) using SOS to guide you through each step.

That's it! The system should be up and running. Now you can start exploring the variety of features in Post.Office.

3.3.2 Checking to See if Installation Worked

Maybe you're wondering if everything is working. You can double check this by initiating a finger query at a DOS prompt:

```
> finger postmaster@your.hostname
```

You should see this:

```
[hostname]
Account Name: Mail Administrator
Email address: Postmaster@your.hostname
----------
mail system administrator.
```

Which means Post.Office is up and running, faithfully serving your E-mail needs.

Alternatively, you could locate the Post.Office applet icon in the Control Panel, double-click on it, and then click on the Status button to verify that the service is running.

3.3.3 Common Installation Mishaps

Please see the Post.Office FAQ for answers to the most commonly encountered installation mishaps. It can be found on our web site at http://www.software.com.

3.4 Installing a New License Number

As your mail system grows you may need to install a new license number reflecting the purchase of additional mail accounts. To enter your new license number, simply re-run the Post.Office installation package. While running through its initial checks the program will note that Post.Office is already installed and offer you the option to update your license or serial number. Choose this update option and proceed as instructed, entering your new license number when prompted.

Note: *This is a non-destructive procedure that will update your license number but make no other changes. All of your accounts and configuration information will remain intact.*

3.5 De-installation

We are confident that you will be entirely satisfied with Post.Office. However, if you do want to remove it from your system, you can do so quickly and easily by following the instructions provided in the section below. But before you remove Post.Office from your system, we would encourage you to contact customer support at Support@Software.com to discuss a solution to your problem.

Note: *Since Post.Office runs as a service, you can easily disable it by selecting it and turning it off, without removing the program from your system.*

Removing Post.Office

The Setup program can be used to remove the Post.Office service if it is executed anytime after the initial installation. It will automatically detect if there is currently an installed Post.Office MTA service and verify that you want to remove it.

If you select the De-Install option the Setup program will stop the service (if it is currently running) and remove it from the services list, then it will remove the executables and the registry entries.

To completely remove the Post.Office system, you will need to manually delete the working directory located in the spool sub-directory of the system root, by default:

```
WINNT\System32\spool\Post.Office
```

The de-installation process will have re-assigned full control permissions to the administrator so removal can be accomplished with ease.

Note: *If you are de-installing with the intention to reinstall, you may need to reboot your server between operations.*

4

Installing Post.Office on UNIX

In order to install Post.Office, you must verify that all system requirements are met, complete the pre-installation planning discussed in Section 4.2, and then follow the installation instructions outlined in Section 4.3. Section 4.3 includes a reference to the FAQ (Frequently Asked Questions) as a place to turn for additional information, and concludes with de-installation instructions should the need arise.

If you are setting up a mail system for the first time or are thinking about re-configuring you mail system and are not clear on what your options are, you should review Chapter 2, Setting up your E-mail Network, for illustrations of some of the more common messaging system configurations.

4.1 System Requirements

Sites must be able to resolve host names through either Domain Name Service (DNS) or /etc/hosts. If you are connecting to the Internet you'll need Domain Name Service with MX records. This can be managed at the local site or by your Internet Service Provider If you are not connecting to the Internet you can use either DNS or the /etc/hosts file for name resolution within your local network. In addition you'll need:

- WWW Browser (e.g., Netscape)
- A mail client that is MIME aware (i.e. Pine, MH, etc.)

Note: *Exact requirements for processor speed, memory, hardware, and hard drive space are highly site specific and depend mainly on the number of mail accounts maintained on the machine, and the volume and size of mail and attachments.*

4.2 Pre-Installation Planning

This section will help you plan a strategy for installing Post.Office. A checklist is provided for you to use as a means of recording the options you select. To install Post.Office you will need to create a new user and group for the mail system, and decide where to install each of the parts of the system. The following sections explain each of the decisions you will make, and offer suggestions for optimum performance and security.

If you are planning to install Post.Office on several machines or your site has some special needs, please review the preplanning discussions in Chapter 2 before installing Post.Office. It covers setting up Post.Office in a distributed (multi-host) environment

including such topics as domain-based addressing (hostname hiding), mail exchangers, and firewalls.

4.2.1 Establish What Mail System You Already Have

Since you are about to replace your current mail system, you probably already know which one you have. Most likely you are running *sendmail*, since it is included with the majority of UNIX-based operating systems. A quick way to find out which mail server is running on your machine is to connect to the mail port and check the greeting line. Here is a sample *telnet* session that does this:

```
% telnet localhost 25
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
220 rome.software.com Sendmail 5.0/SMI-SVR4 ready ....
quit
221 rome.software.com closing connection
Connection closed by foreign host
%
```

In this example, the mail server running on the local machine is a version of sendmail. If you are not running *sendmail* on your machine, some of the installation process may be different than what you find in this chapter since it is assumed that that is what you are replacing.

If by chance you are not running any mail server, the telnet session will generate the following error message:

```
% telnet localhost 25
Trying 127.0.0.1 ...
telnet: connect: Connection refused
telnet> quit
%
```

If you are not running a mail system, it's a good thing you're installing Post.Office.

4.2.2 Your DNS Domain

Most sites installing Post.Office are already connected to the Internet and have a registered domain name. During the installation you will be asked for the domain name of the computer on which you are installing the system. This may be your organization's domain name, or possibly a subdomain. For example, if you were installing Post.Office on a machine named `emile.math.ucsb.edu`, the domain name you would specify is `math.ucsb.edu`.

4.2.3 Setup User and Group for Post.Office

One of the important security features of Post.Office is that the system runs as a non-privileged user. Before installing the system, you should create a new user called mta. All Post.Office programs run as this user so the system does not have privileged access to sensitive files. The primary group of this new user (also called mta) should be newly created and have no members since any member of the group can read mail stored in the queue or in users' POP3 mailboxes. Specifically, the *mail* group should be avoided since it is used by the UNIX mail system.[16]

	Suggestion	Your choice
User Name	mta	
Group name	mta	

4.2.4 Locations of Programs and Working Directories

Post.Office is divided into three major parts: the executable programs, the mail processing center, and the message store (or user mailboxes). The locations for each of these directories can be customized during the installation.

Note: *For simplicity's sake it is recommended that you store the Post.Office modules in the default directory locations. These default locations will be suggested automatically by the installation program.*

Warning! Always install Post.Office into an empty directory, and never use NFS mounted directories for any part of the system.

The Spooling Directory

The Post.Office Spooling directory is a directory where mail is processed. All incoming mail is stored in the Spooling directory and remains there until it is either successfully delivered or returned. Often mail resides in the Spooling directory for only a few seconds as it is routed to its destination; however, if a message is destined for a remote computer that is temporarily unreachable, the message can remain queued up in the Spooling directory for several days, depending on how the system is configured. Typically the `/var` partition is used for such storage.

Make sure you put the Spooling directory in a place that gets backed up regularly since it also contains all the configuration information and the account database. The default location for this file is: `/var/spool/post.office`

16 Several security problems have arisen with `/usr/bin/mail` and `/usr/bin/mailx`, which could possibly be exploited by a user to obtain mail group permissions. As long as `Post.Office` is installed with a different group, it is safe from this problem.

The Mailbox Directory

The *mailbox* directory is where mail is stored for users that retrieve their messages via the network using the Post Office Protocol (POP3). The amount of storage needed for this directory depends on the number of users that use POP3, the volume of mail they receive, and whether they leave their mail on the server or download it to their PC or workstation. The mailbox directory may require less storage than a traditional UNIX mail directory since only one copy of a message is kept regardless of the number of recipients.

This directory should also be backed up regularly since it contains users' mail. The default location for this file is: `/var/spool/mailbox`

The Executables Directory

The executable programs that constitute Post.Office are all located in a single directory tree. This directory should not be located on the disk that also houses the Spooling directory. Typically this directory will be in either `/opt` or `/usr/local` depending on your conventions.

Warning! We feel that it is not a good idea to utilize network drives for storage on a mail server because you would not want your partitions to be unavailable if for some reason your remote host was not accessible but your mail server was functioning. You do not have to follow this recommendation, but you should be aware of the risks should you choose to use this type of configuration.

4.2.5 Changes to Existing Files and Services

Because Post.Office replaces services you already have, the installation process will alter some system files. The number of modifications is small and each is described in this section.

Effect on Your Existing Mail System

Post.Office replaces your current mail transport agent such as sendmail or smail. It does not, however, replace any mail client software you are using[17]. Since Post.Office is designed to be upwardly compatible with your existing mail infrastructure, all mail clients should continue to operate normally when Post.Office is installed as the mail server.

Notes Regarding sendmail Replacement

Post.Office is designed to be a drop-in replacement for sendmail in most installations (see appendix F for a discussion of compatibility). In order to be upwardly compatible, there is a replacement sendmail program provided with the system that emulates much of

17 Mail user agent software is the software you use to read and write E-mail, as opposed to message transport agents (such as post.office), which deliver and hold messages for user agents.

sendmail's functionality. The sendmail replacement is discussed at length in the sendmail compatibility appendix.

When Post.Office is installed, the sendmail executable on your machine is saved as `sendmail.bak` and a symbolic link is put in its place that points to the replacement program. This design choice lets you continue to run software that uses sendmail to deliver mail, etc. without modification. Also if there is a reason you want to disable Post.Office and enable sendmail, simply remove the symbolic link and rename `sendmail.bak` as `sendmail`. You then need to shutdown Post.Office and start up sendmail.

Note: *UUCP is not supported in Post.Office; the sendmail replacement has enough knowledge of UUCP to convert simple !-addresses to domain addresses, but delivery via UUCP is not implemented. As an example, host1!host2!user is rewritten as user%host2@host1 which then gets sent off to host1.*

As a sendmail administrator, you have probably learned to do things like maintain the *aliases database*, set up UNIX accounts for each mail user, configure `.forward` files, and perhaps even modify the `sendmail.cf` file to rewrite addresses or do some customized routing. With Post.Office you don't have to do any of this; all alias and delivery information is kept in an internal account database, and address rewriting is all but eliminated.

The changes in the way things are done will simplify your job as a mail administrator so you can concentrate on setting up accounts rather than debugging configuration files. To find out everything you can do with mail accounts in Post.Office, please see the operations chapters which follow.

Effect on Other Files and Services

In addition to the mail transport agent, Post.Office contains a POP3 server, and a finger server. These are integrated into a single system rather than being a collection of individual services.

Finger

Typically UNIX workstations are shipped with a finger server that runs under *inetd* (the Internet daemon) and gets its information from `/etc/passwd` and each user's `.project` and `.plan` files. The installation process will disable the finger server by editing your `inetd.conf` file, and then resetting the inetd process (by sending it a HUP signal). At the same time every user's project and plan files will be loaded into the account database. This is the only time these files will be accessed; the finger server always pulls user information out of the Post.Office account database. Users will be able to change their finger information using the *information form*, which allows them to make limited changes to their account information.

Post Office Protocol version 3 (POP3)

If you have a POP3 server running on your machine, it is most likely a local customization since POP3 doesn't usually come as part of a stock UNIX system. The available POP3 servers read users' maildrop files which are typically located in `/var/spool/mail` or `/var/mail`. In Post.Office, users that retrieve their mail via POP3 have their mail stored in a special part of the system called the *message store* (the mailbox directory). This design choice eliminated the need to parse the various formats of UNIX maildrop files, removed the requirement that each mail recipient have a UNIX login account, and allowed for several other efficiencies. The one drawback with this design is that a user can not easily alternate between reading mail via POP3 and via standard UNIX mail programs.

If your POP3 server is launched by inetd as is the finger server, then it will also be disabled in the `inetd.conf` file. However, if it is a standalone daemon process, disabling it requires a bit of your help. First the daemon has to be killed, and then the commands in the boot script which starts it up have to be disabled.

4.2.6 The Role of the Postmaster

During installation you will have to choose who the Postmaster is going to be. On UNIX systems running sendmail, the *Postmaster* or *mail administrator* is usually the same person as the system administrator. Mostly this is due to the fact that root privileges are required to make any changes to a sendmail-based mail system. Activities that require root privileges include adding and removing UNIX accounts, and editing the `aliases` and `sendmail.cf` files. Without being able to perform all of these tasks, you would be severely constrained in your ability to administer the mail system.

Fortunately with Post.Office none of the equivalent tasks require root permission. Instead, anybody listed as a recipient of mail addressed to `<postmaster@your.domain>` is considered a Postmaster (you can also grant Postmaster privileges via the web[18] by giving people the Postmaster password and having them log on as "Postmaster").

Having Postmaster privileges in Post.Office is similar to having root privileges for administering sendmail. Each Postmaster is able to configure mail system parameters, add, modify, and delete mail accounts, and set up automatic replies. Since none of these tasks require root privileges, the system administrator can safely appoint someone else to the position of mail administrator, thus reducing the system administrator workload.

Postmasters interact with the mail system either by sending it mail or logging on to the Post.Office host with a web browser. The Postmaster does not have to be a local user of a machine to be able to configure it. In fact all configuration and account changes for an entire E-mail network can be handled from a remote site.

---

18 *Web* is used as an acronym for world wide web throughout this manual.

4.2.7 Impact of Migration for Mail System Users

Typically there are three methods used to access mail on a UNIX machine: accessing the maildrop file directly, using a POP3 server, or using an IMAP (Internet message access protocol) server.

Note: *The method of choice is established on a user by user basis via the Account Data form or Individual Account Information form.*

The first method is probably the most common since all standard programs such as `mail` and `mailx` read the maildrop file directly. Users who access their mail this way will not have to change what they do.

Those users who access their mail via POP3 exclusively will need to make a few changes if their account is currently set up to deliver their mail to the message store. If they do not, their mail will collect in their UNIX maildrop file until the necessary corrections are made (note that no mail will be lost).

IMAP is probably the least common of the three methods since it is a new technology, though similar to POP3. Post.Office does not currently contain an IMAP server so you can continue to run your own if you have one. It will access users' maildrop files as it always has.

If any users regularly switch between POP3 and other access methods, they may find that the switch to Post.Office requires them to rethink how they collect their mail. Either they will have to choose a single method of mail access, have messages sent to both their UNIX maildrop and the Post.Office message store, or switch the delivery method in their account between UNIX and POP3 as their needs dictate. Users who opt to change regularly between the two deliveries will find that the Individual Account Information form allows them to do so quickly and easily, either via E-mail or by using the web.

Note: *When switching between UNIX and POP deliveries, any accumulated mail will remain where it was and appear to be "lost" when using the new type of access. This occurs because the POP server does not read the UNIX mail spool file for users' mail and vice versa. Users who experience problems as a result should select both delivery methods concurrently so that they have their full set of messages available to them however they check their mail. (This will of course result in a somewhat awkward duplication).*

Creating New User Accounts

Post.Office will automatically create new E-mail accounts for everyone with UNIX accounts on the host it is installed on, if you so choose. (Recall that Post.Office accounts

are not linked in any way to UNIX accounts, except that during installation Post.Office will automatically open accounts for all users with UNIX accounts, if you want it to).[19]

Every time Post.Office opens an account for a user, that user will receive a message from Post.Office called the *Greeting message.* The idea of the Greeting message is to welcome the user to their account and provide them with basic account information (see below). Thus one consequence of installation may be that all the users on your host will get this message:

19 Accounts which are not created this way during installation must be made using the *account form*, which is discussed in excruciating detail in the next few chapters. It's not actually a big deal, but you get a lot of options which sometimes come in handy. Thus the detail. The account form itself actually includes fairly comprehensive information on how to use it, and chapter 4 shows you how to get it by sending an E-mail message to `Post.Office.`


```
To: You@Your.domain
From: Account-Manager<>
Reply-To: Account-Manager<>
Subject: Form: Greeting

MIME-Version: 1.0

Information

An electronic mail account has just been opened for you. This
account is configured as indicated below. Make sure you note your
password and safeguard it since this is the only time it will be
sent to you. See the instructions below the account summary for
information on how to make changes to your mail account as well as
for explanations about each of the fields.

Your-Name:              [your name here]
   (Note: your name is sometimes referred to as your account name)

Internet-Addresses:     [your address@your.domain]

Finger-Information:     [Tell the world how happy you are]
                        [about Post.Office]

======================================================================

 Here's some information about changing your account:

Only the system administrator can change your name or addresses. If
you want to change your password or your finger information, you can
do so with a World Wide Web browser (such as NCSA Mosaic), or via
E-mail. You simply fill out a form indicating the desired changes
and submit the form to the mail system.

To request the Individual Account Information form:

via the Web:      connect to http://

via E-mail:       You can get the E-mail form to modify your
                  account by simply replying to this message
                  and sending it in, or
                  send a new message To: <Accounts@your.domain>
                  with the word "Information" as the message body
                  like this:

                            To: Accounts@your.domain

                            Information

After receiving the Information Form, make the appropriate changes
to the form (use the "Reply" feature of your mail client if you are
using the E-mail interface), put in your password, and submit the
form. If you don't receive an error message, the changes have been
accepted.

======================================================================

                ....(full form is not shown)
```

Figure 4-1: This is the Greeting message which is sent to new users to orient them to how to get the most use out of Post.Office.

4.3 Installing Post.Office

Now that you're ready, here is a step-by-step guide to installing Post.Office. If you haven't gone through the previous section and planned for the installation, please do so now. A good plan at the start will make the installation run smoothly.

4.3.1 The Installation Process

Installation instructions vary slightly from platform to platform. Please refer to the appropriate section below for specific installation instructions on Solaris, or the instructions applicable to all other UNIX platforms.

Solaris Installation Instructions

1. Log on as root.

2a. Create a new group with a unique id (mta being the recommended choice)

2b. Create a new user with no special privileges using the group id established in the last operation. (Post.Office will run as this user.)

3a. If your software was delivered on CD: mount the CD on your computer and change directory to the location containing the Post.Office files or your particular operating system/platform.

3b. If you downloaded the software from our ftp or web site: uncompress the file you downloaded into a temporary directory and expand the resulting archive file to create the Post.Office package (SCOM-MTA) by typing:

```
cd /var/tmp
uncompress PO30-solaris2.4.tar.Z
tar xvpf PO30-solaris2.4.tar
```

4. Install the new package by typing:

```
pkgadd -d . SCOM-MTA
```

5. Run the Post.Office configuration program:

```
/opt/post.office/Setup
```

Several questions will be asked during the installation, but you already know the answers since you went through the "pre-installation planning". This shuts down your existing mail and finger services, sets up mail accounts, and starts up the Post.Office system. If at any time you quit out of the program, you can run it again later to finish the installation process.

When the program is finished, it will start Post.Office for you.

Installation Instructions for all Other UNIX Platforms

1. Log on as root.

2a. Create a new group with a unique id (mta being the recommended choice)

2b. Create a new user with no special privileges using the group id established in the last operation. (Post.Office will run as this user.)

3a. If your software was delivered on CD: mount the CD on your computer and change directory to the location containing the Post.Office files or your particular operating system/platform.

3b. If you downloaded the software from our ftp or web site: uncompress the file you downloaded into a temporary directory, expand the resulting archive file, and then change to the newly created Post.Office directory by typing:

```
cd /var/tmp
uncompress PO30-<platform>.tar.Z
tar xvpf PO30-<platform>.tar
cd Post.Office
```

4. Install Post.Office by typing:

```
./installpo
```

Several questions will be asked during the installation, but you already know the answers since you went through the “pre-installation planning”. This shuts down your existing mail and finger services, sets up mail accounts, and starts up the Post.Office system. If at any time you quit out of the program, you can run it again later to finish the installation process.

The flowchart below (Figure 4-2) outlines the steps taken by the Post.Office installation program.

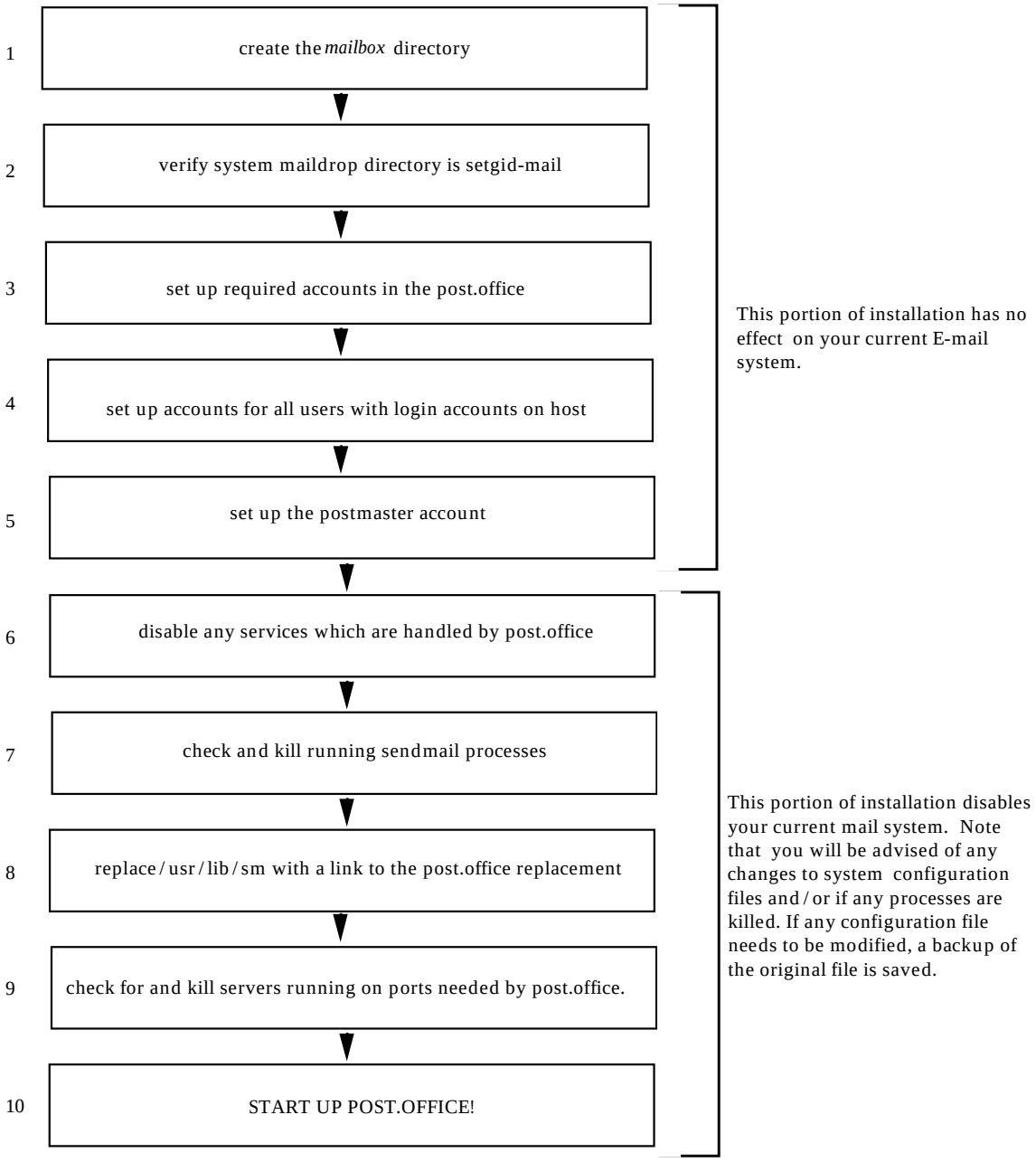


Figure 4-2: Installation Flowchart

The above flowchart illustrates the steps taken by the Post.Office installation program.

1. The mailbox directory is used to store messages for users who access their mail via POP3.
2. The install program will offer to set this permission bit for you.
3. These are a few special accounts (described in the operations portion of the manual) which are required for operation.
4. If you select this option, a summary of the created accounts will be mailed to you at the end of installation.

5. The Postmaster Account is the account which allows you to configure and oversee the operation of the Post.Office system. See operations chapters for details.
6. The installation program checks the configuration file of *inetd* to see if it is set up to handle any of the services in Post.Office; it will disable them by editing the `inetd.conf` file and resetting the *inetd* process.
7. You should be aware by now that you are replacing sendmail with Post.Office. If not, go back to pre-installation planning and make sure that you know what you are doing.
8. This link is set up so that the Post.Office sendmail replacement program can be run, for example by other programs that use sendmail commands to carry out certain tasks. See Appendix F for details.
9. This is necessary so that Post.Office can monitor, for example, the SMTP and POP3 ports.
10. You're done!

4.3.2 Finishing Up

When you're done with `installpo`, it may tell you that some things still need to be taken care of. If so, write them down and perform the tasks when you get a chance. In any case, the system should be running so you can start exploring the variety of features of Post.Office.

4.3.3 Common Installation Mishaps

Please see the Post.Office FAQ for answers to the most commonly encountered installation mishaps. It can be found on our web site at http://www.software.com.

Rerunning Install

If you quit out of the `installpo` program before it is finished, you can simply rerun it later to complete the installation process. The Post.Office system will not be started until you explicitly tell `installpo` to start it, and it will warn you if any problems need to be taken care of before the system can be started.

4.4 Installing a New License Number

As your mail system grows you may need to install a new license number reflecting the purchase of additional mail accounts. To enter your new license number, you will need to re-run the Setup portion of the installation program. To do so…

1. Change directory to the location in which the `Setup` program is stored. If you originally installed Post.Office using the default locations, it will be found in either /opt/post.office (Solaris 2 users), or /usr/local/post.office (all other UNIX users).

2. Type `./Setup` to re-run the Setup portion of the installation program. This will allow you to modify certain configuration information including your Post.Office license number.
3. Respond as desired to the options presented being sure to enter the new license number where appropriate. Post.Office will use the new number to replace the old one.

Note: *This is a non-destructive procedure that will update your license number but make no other changes. All of your accounts and configuration information will remain intact.*

4.5 De-installation

Although it is believed that you will be completely satisfied with Post.Office, if you want to remove it from your system, this section will tell you what to do.

Things To Check

Before removing Post.Office from your system, check that there is no deferred mail waiting to be delivered. The queue form can be used to check this, as well as to deliver the queued mail.

Also if you have any users retrieving their mail via POP3, their mailboxes may contain unread mail. Removing Post.Office from your system won't delete this stored mail, but it will be hidden from the users since only the Post.Office POP3 server is able to access the mail.

Removing Post.Office in Solaris

Removing Post.Office is fairly simple since it is installed as a package. Once you are satisfied that no undelivered mail is still in the system (see previous section), follow these instructions:

As root:

1. Remove the Post.Office MTA Package using the pkgrm utility:

   ```
   #pkgrm SCOM-MTA
   ```

   If you haven't already done this you might need to remove the original install package: `#rm -rf /var/spool/pkg/SCOM-MTA`

2. Replace sendmail in /usr/lib:

   ```
   #cd /usr/lib; #ls -lF sendmail* (sendmail should be a link)
   rm sendmail; mv sendmail.bak sendmail
   ```

3. Edit `/etc/inted.conf` (removing the # (Comments) in front of the services that were originally disabled for Post.Office); i.e., finger

4. Reset the inetd process:

```
kill  -HUP  inetd_process_number
```

5. Remove the postoffice directory:

```
rm  -rf  postoffice_directory
```

(the default is /opt/post.office)

6. Remove the mailbox directory:

```
rm  -rf  mailbox_directory
```

(the default is /var/spool/mailbox)

7. Remove the config directory:

```
rm  -rf  postoffice
```

(the default is /var/spool/post.office)

Removing Post.Office in All Other UNIX Platforms

Here are the instructions for PERMANENTLY removing Post.Office on Sun OS4.

1. Look at the file /etc/post.office.conf: cat /etc/post.office.conf
2. Shutdown Post.Office: /usr/local/post.office/post.office shutdown
3. Remove each of the listed directories and their contents:

```
rm -rf /usr/local/post.office
rm -rf /var/spool/post.office
rm -rf /var/spool/mailbox
```

4. Remove the /etc/post.office.conf file:

```
rm /etc/post.office.conf
```

5. To re-enable sendmail:

```
cd /usr/lib
```

(check that sendmail is a link before removing)

```
ls -l sendmail
rm sendmail
mv sendmail.bak sendmail
```


5

What Happens Next

Assuming everything went well, you're now ready to access the Post.Office mail server and begin adding accounts. But before you do, review the next section which discusses the differences between Post.Office accounts and the intended use of each type.

5.1 Understanding Accounts

The installation program you just ran helped you to set up Postmaster and personal accounts. This section's purpose is to ensure that you understand the function of the different accounts so that you can get the most out of them.

5.1.1 The Postmaster Account

The purpose of the Postmaster Account is:

- To define who is given access to Post.Office configuration and operation.
- To define the individual or individuals who are responsible for day to day supervision of the mail system.

These two purposes are closely related. However they are not identical.

The first point asserts that when you are Postmaster, you have the keys to the car (note that you can have as many sets of keys as you like). The reason that you and perhaps a few other Postmaster cronies are given the "keys" to the system is less to create an E-mail nomenclature then to establish strict security controls over who has access to the system. If there are too many Postmasters, or the Postmaster Account becomes public domain, then you are short-circuiting one of the primary security mechanisms of your mail system.

You will use your position as Postmaster to set up new accounts, make configuration changes to the system, and take care of any errors that occur. You will find that in most cases, too many cooks can spoil the batter. In general, your mail system will function better if only one or a few people are entrusted with mapping out and implementing an E-mail game plan.

The algorithm for who is a Postmaster is simple: anybody who's E-mail address is listed in the Postmaster Account delivery field is a Postmaster. You do not need to have an account on the Post.Office host in order to be a Postmaster.

The second purpose of the Postmaster Account is that it identifies the responsible party or parties for all E-mail related questions.

The Postmaster is responsible for dealing with any errors which crop up. For example, most frequently this will mean invalid addresses. The Postmaster has to decide whether messages with such addresses should be returned to their sender or forwarded to a user on the system. The Postmaster is also the person most often turned to when folks outside your E-mail network have a question about how to contact someone in your organization, or other E-mail related questions. It is conventional that every domain support the "postmaster@domain" address, so that the outside world can have a contact on your network.

Warning! The Postmaster Account is not a personal E-mail account. Even if you are a Postmaster, you should have a personal account to which all your personal correspondence should be addressed. You should then include the address for your personal account in the delivery field of the Postmaster Account, so that you will have Postmaster privileges on the host and be able to access both E-mail and web forms.

5.1.2 Personal Accounts

The purpose of a personal account is to give an individual access to E-mail. In some cases accounts can also be used to deliver mail to a program or to automatically distribute information (using the auto-reply utility).

Thus every Postmaster should have a personal E-mail account in order to have access to E-mail in addition to access to Post.Office E-mail forms.

Users who have personal accounts on a host can receive mail through that host, as well take advantage of other features such as having their addresses re-written on outgoing messages, having finger queries answered, and advising correspondents when they are on vacation (using the auto-reply utility).

5.2 Where to Go Now

You can now proceed to the *Administration Guide* to learn how to run the system.

Index