3

3A contains introductory reference information which will help you set up a distributed E−mail network.

Section 3B covers pre−installation planning and installing `post.office`.

NT PLATFORM

3A: SETTING UP YOUR E−MAIL NETWORK

3B: INSTALLATION

3.A.0 SETTING UP YOUR ENTIRE E–MAIL NETWORK

The purpose of the first part of this chapter (3A) is to provide a rough blueprint of how to successfully set up even the most complicated E–mail network.

- 3.A.1 is a check list of things you should consider when setting up your E–mail network.
- 3.A.2 discusses the tools used with **`post.office`** to take care of addressing and routing. These include account addresses, aliases, and mail routing facilities.
- 3.A.3 concludes with several example configurations that cover the most common situations and should spark ideas on how to approach your own solution.

Note: If you are already familiar with the material covered in section 3A, you can of course skip ahead to section 3B, which covers pre–installation planning and the installation itself.

You may run across some ground which you are not familiar with that you would like to know more about before configuring your system. You may find useful reference information in the sources we list in appendix B, *References*.

3.A.1 THINGS TO CONSIDER WHEN DESIGNING YOUR NETWORK

This section is a check list of key issues to review in thinking about how you're setting 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.

ADDRESSING

`post.office` will let you assign any valid address to an account. You may want to choose a convention for user addresses (such as *First.Lastname*@*mail_domain*). 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.

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 in.

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 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 a firewalled environment are discussed in section 3.A.3.

3.A.2 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 bellow, and will reappear frequently in the examples discussed in section 3.A.3.

ACCOUNT ADDRESSES

`post.office` account addresses are very powerful. Any number of addresses (aliases) can be assigned to an account, which 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@some.other.domain>` with no confusion.

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 PC's 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`.

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.

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.

MX RECORDS IN THE DNS

Mail exchanger (MX) records in the Domain Name System 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.

3.A.3 EXAMPLE 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.

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. Pegasus, Zmail, Eudora) that access their mailbox.
- Each machine acts independently; messages are sent and received directly to/from other machines on the Internet.

Network Diagram:

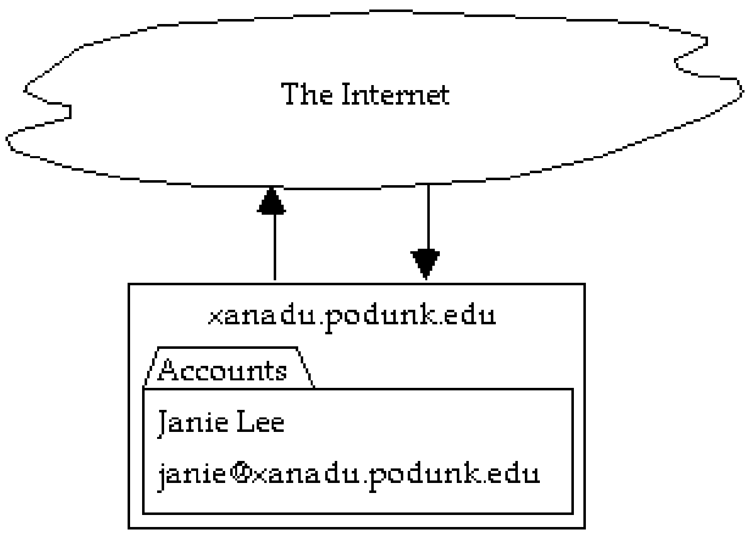

Figure 3.A.3a: Janie's address is `Janie@xanadu.podunk.edu.`

MX records:

- Each machine may have MX records that point to itself, and optionally to one or more backup hosts. MX records are not really 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 3.A.3b: 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.

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).

Network Diagram:

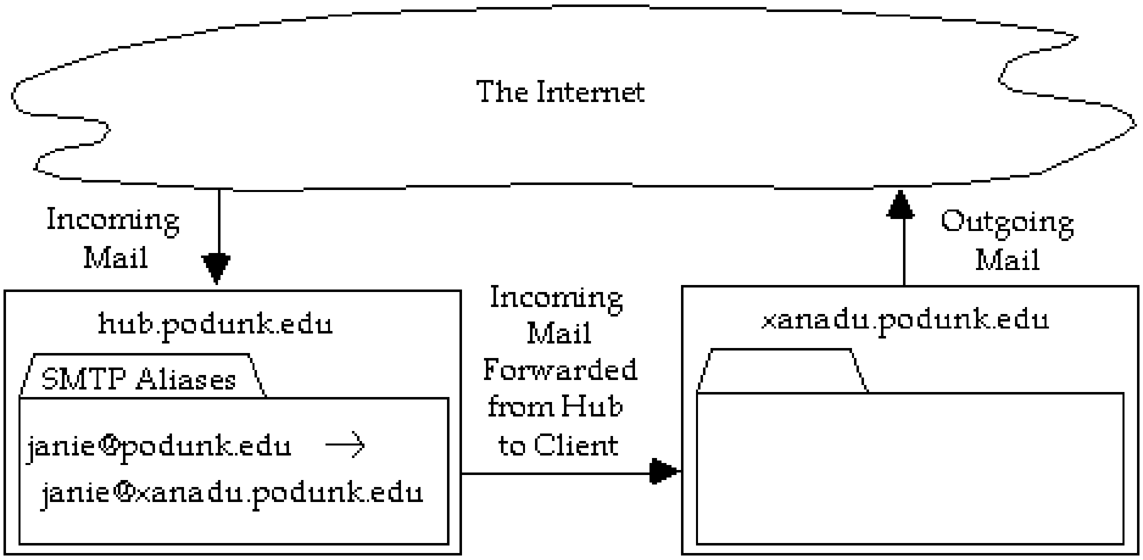

Figure 3.A.3c: All messages for the domain `podunk.edu` go through the hub machine. On the hub host, Janie has an SMTP channel alias [<janie@podunk.edu><janie@xanadu.podunk.edu>] that points to Xanadu.

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.

- Each client machine should have MX records that point to itself, and optionally to one or more backup hosts (usually the hub machines). For example:

```
xanadu.podunk.edu.        IN  A   123.45.6.78
                          IN MX   10 xanadu.podunk.edu.
                          IN MX   20 hub.podunk.edu.
```

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 3.A.3d: 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 3.A.3e: 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 uses of the mail routing table.

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:

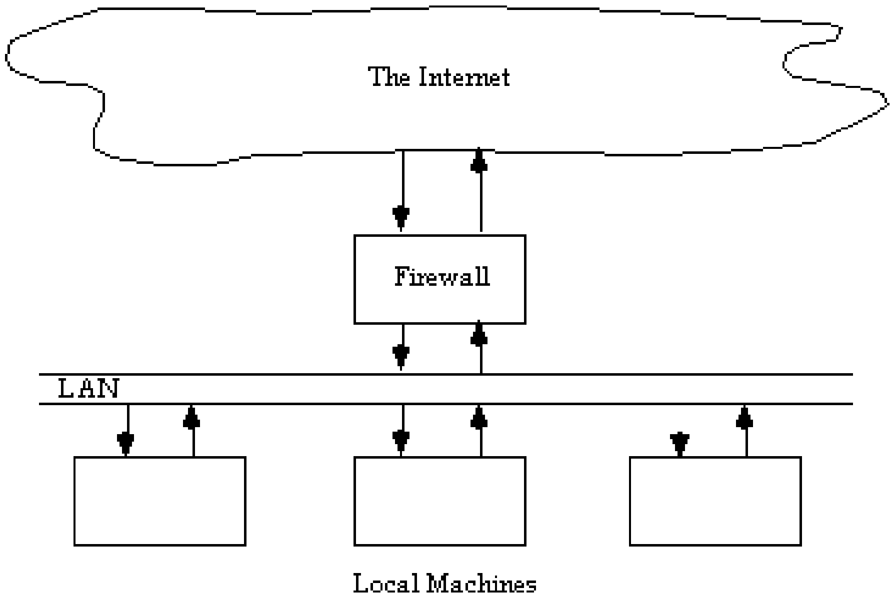

Figure 3.A.3f: Diagram of a firewall scenario.

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.
*                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 3.A.3g: 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 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 firewall which then forwards it to its destination.

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:

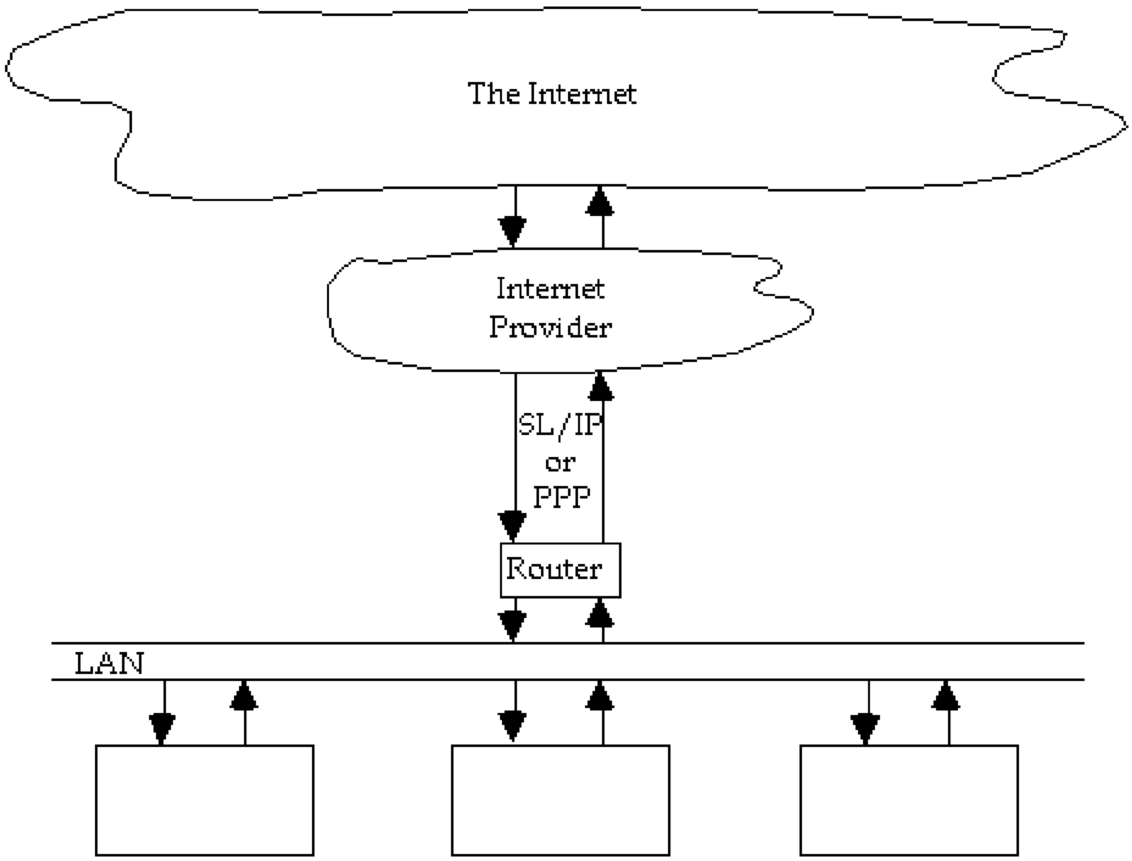

Figure 3.A.3g: Typical setup for an intermittently connected site.

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 3.A.3h: 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. See chapter 6 for details.

3.B.0 INSTALLATION INSTRUCTIONS (WINDOWS NT VERSION)

In order to install `post.office`, you must:

- 1. Go through section 3.B.2, *Pre−Installation Planning*,, to make sure that you are ready to install the program.
- 2. Follow instructions set out in section 3.B.3: *Installing* **`post.office`**.
- 3B includes a section to assist you with common installation mishaps (3.B.4) and concludes with de−installation instructions should the need arise (3.B.5).

Note: 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 may want to have a peek at the first section of this chapter: 3A, *Setting up your E−mail network***, which illustrates some of the more common messaging system configurations.**

3.B.1 SYSTEM REQUIREMENS

- Intel Platform (minimum 486/33) running Windows NT 3.5 (both Server and Workstation are O.K.)
- NTFS Formatted Hard Drive Recommended. FAT Formatted system partitions are supported but not recommended (Long filenames are required).
- Mail Client with Post Office Protocol version 3 mail pickup (POP3) e.g. Zmail, Eudora, Pegasus, etc.
- WWW Browser (e.g. Mosaic or Netscape).

3.B.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.

When installing `post.office` you are urged to create a new account and group for the mail system. You must also decide where to install each of the parts of the system. The following sections cover these decisions and offer suggestions for optimum performance and security.

3.B.2.1 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.

3.B.2.2 THE SYSTEM DRIVE PARTITION FORMAT

An NTFS formatted hard drive is **highly** recommended. `post.office` will run on FAT partitions but you lose tremendous security features and power failure/disk crash recovery capability.

3.B.2.3 SETTING UP A NT–LOGIN ACCOUNT FOR `POST.OFFICE`

How you set up your login account for `post.office` has a strong impact on how secure your system is. Please read this section carefully.

We strongly recommend the use of a new account and group other than the built–in *System* **account for sites connecting to the Internet.**

DECIDING WHAT KIND OF ACCOUNT TO USE

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` service can operate using the privileges of the built–in *System* account or as any local account which is pre–configured (prior to running the installation program) on the machine. This decision is primarily a security consideration.

The advantage of using an account other than the built–in *System* **account is that the default installation of `post.office` will setup permissions which will not allow other processes or accounts to access any of the `post.office` directories/files or registry information (additionally the `post.office` service will be unable to read/modify/delete any system or user files).**

The only disadvantage of using an account other than *System* is that 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.

USING THE BUILT−IN SYSTEM ACCOUNT

If you choose to use the system account, you may skip the remainder of this section and proceed with section 3.B.2.4. When prompted for the system account please use "System" (with an uppercase S).

CREATING AN NT ACCOUNT AND GROUP FOR THE SERVICE

You must use the User Manager (as an administrator) to create an account and group for the service (`post.office)` to use during normal operation. The new account and group should be specifically for the `post.office` service and should have no other members or groups.

Note: the account must have *User Cannot Change Password*, and *Password Never Expires* checked and must **not** have *User Must Change Password* at next login checked.

NT Workstation installation notes:

You will be creating a local user and group. If the workstation is also part of an NT Domain, we suggest that you use a local user and local group (specific to the workstation, not a member of the NT Domain). Be sure to include only the `post.office` user in the new group and that the `post.office` user has membership in only the new `post.office` group.

NT Server notes:

We suggest that you use a global user/global group for the `post.office` service account. After creating the `post.office` user and group, be sure to:

set the `post.office` group to be the primary group for the `post.office` user: under the user properties/Groups button, select the `post.office` group on the left hand side and click the "Set Primary Groups" button.

remove the domain users group from the list of groups for the `post.office` user (it is added by the user manager by default).

Suggestion Your Choice

Account Name`post.office`

Account Password

Group Namepost.office−group

Setting up `post.office` as a service

You must also give the account the *logon as a service* privilege. This is accomplished while still in the User Manager program:

Under the Policies menu, select the User Rights option. There is a click box titled "Show Advanced User Rights" which must be checked. Under the scroll bar titled "Right:" choose "Log on as a Service" and you must add the account name (chosen above) which you created for the mail system to this privilege list. You will need to select the "Add..." button, then select "Show Users", select the `post.office` user account (it will be near the bottom of the list), and click the "Add" button.

3.B.2.4 YOUR REGISTRATION INFORMATION

If you have already purchased a license for `post.office` you will have a license number. If you are installing `post.office` and have not yet made the commitment to purchase the license, you will need to use the word "trial" in the registration information section and your software will operate normally with a 45 day period. After the trial period has expired, `post.office` will operated normally (footnote) but you will be in violation of the trial license agreement.

License Number:

3.B.2.5 YOUR DNS DOMAIN

Most sites installing `post.office` will already be connected to the Internet and have a registered Internet 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`.

Domain Name:

3.B.2.6 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:

3.B.2.7 LOCATIONS OF PROGRAMS AND WORKING DIRECTORIES

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

Note: It is not a good idea to use remote or network mounted directories for any part of the system.

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).

SuggestionYour Choice

Executables`/win32app`

THE `POST.OFFICE` DIRECTORY

The *post.office* is a directory where mail is processed. All incoming mail is stored in the postoffice and remains there until it is either successfully delivered or returned.

Generally mail resides in the postoffice 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 postoffice for several days, depending on how the system is configured. Typically the `system` partition is used for such storage in the directory \winnt(35)\system32\spool.

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

SuggestionYour Choice

Postoffice`/winnt/system32/spool`

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.

This directory should be backed up regularly since it contains users' mail.

SuggestionYour Choice

Mailbox`/winnt/system32/spool/post.office`

3.B.2.8 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. Since `post.office` is designed to be upwardly compatible with your existing mail infrastructure, all POP3 UAs should continue to operate normally when `post.office` is installed as the MTA.

3.B.2.9 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. Chapters 5 and 6 contain all of the information necessary to remotely configure `post.office`.

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* (created when you created an account for `post.office`) 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).

Local Account Password:

Postmaster Password:

your Mail Account Password:

3.B.2.10 IMPACT OF MIGRATION FOR MAIL SYSTEM USERS

Every time `post.office` opens an account for a user, that user will receive a message from `post.office` called the *greeting form.* The idea of the greeting form is to welcome the user to their account and let them know how to change their password and other select account information (see figure 3.B.1.7a 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)

    Mail-Account-Password:  [your secret here]

    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 user 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.
=========================================================================
Here is an explanation of each of the fields shown for your account:
Your-Name
...  (full form is not shown)
```

Figure 3.B.2.7a: This is the greeting form which is sent to new users to orient them to how to get the most use out of post.office.

3.B.2.11 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.B.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.B.3.1 THE INSTALLATION PROCESS

There are three main steps to installing `post.office`. First the software is unpacked (you receive it as a compressed file), then it is installed on the system. Finally a special program is run to initialize the mail system and set up accounts.

UNPACKING **POST.OFFICE**

The `post.office` system is distributed in compressed−file format which is common for Windows NT software. When uncompressed (use your WinZipNT or equivalent program), the result is a *setup package* which is fairly typical of the software written for the Windows NT operating system. The package contents need to end up in a temporary directory so that `post.office` can be installed. When the installation is finished you can remove the temporary directory.

RUNNING INSTALL

After loading the package onto your computer and unpacking it, you need to run the `setup.exe` program. To do so, from a DOS prompt:

Change directories to the temporary directory where you unpacked the package:

```
c:\temp> cd \temp\post.office
```

Execute the install program:

```
c:\temp\post.office> setup.exe
```

You will be asked the questions which you have already answered in the pre−installation planning section you just completed (above).

If at any time you quit out of the `setup` program, you can run it again later to finish the installation process.

FINISHING UP

When you're done with `setup`, 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`.

3.B.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.

3.B.3.3 POSTMASTER AND PERSONAL 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.

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 are less to create an E–mail nomenclatura 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.

Note that 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.

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 the postmaster(s) should have a personal E−mail account in order to have access to E−mail as well as to be able to have 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).

3.B.3.4 WHERE TO GO NOW

You can now proceed to the operations chapters (chapters 4, 5 & 6) to learn how to run the system. But first, please note section 3.B.4.2 below (regarding changing the Postmaster account) since you may find it useful someday. We've also included below a brief section on setting up postmaster and personal accounts to orient you before you plunge into the nitty gritty of operations.

3.B.4 COMMON INSTALLATION MISHAPS

What you should do if you have to abort install half−way or end up without a valid postmaster.

3.B.4.1 RERUNNING INSTALL

If you quit out of the `setup` program before it is finished, you *can* simply rerun it later to complete the installation process. This can be done by following the instructions in section 3.B.5.1 "Removal of the directories". After this is completed rerun the *Setup* program and installation will be completed properly.

The `post.office` system will not be started until you explicitly tell `setup` to start it, and it will warn you if any problems need to be taken care of before the system can be started.

3.B.4.2 CHANGING THE POSTMASTER ACCOUNT

It is possible to accidentally configure `post.office` so that there are no valid postmasters. If this happens, the system will not allow further configuration changes, in other words there will be no way to fix the problem with the postmaster account. If this occurs, contact Technical Support at Software.com (Support@Software.com, 805−882−2470 voice, or 805−882−2473 fax).

3.B.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.

Before you remove `post.office` from your system, we welcome you to contact customer support at Support@Software.com or by telephone at 805−882−2470 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.

3.B.5.1 REMOVING POST.OFFICE

The *setup* program will remove the service if it is executed anytime after the first 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 answer yes to the prompt, the install program will stop the service (if it is currently running), remove it from the services list, remove the registry entries, and delete all exectuables.

All that will remain is the `post.office` spool directory − which could contain mail messages. The setup program will have re−assigned ownership to the administrator and given it full control permissions. Therefore, it is a simple task to delete this directory if desired.