SunLink® X.400 8.0.2 Administrator's Guide

SunSoft
A Sun Microsystems, Inc. Business
2550 Garcia Avenue
Mountain View, CA 94043
U.S.A.

Part No: 801-4956-11
Revision A, November 1994

Contents

Figures

Tables

Preface

Purpose and Audience

This manual explains how to configure and use the SunLink X.400 8.0.2 Message Handling System to exchange electronic messages with other mail systems that conform to CCITT X.400 MHS recommendations. It is intended for system administrators who are familiar with the Solaris environment.

SunLink X.400 8.0.2 implements an X.400 Message Transfer Agent (MTA) to transfer electronic messages between host machines and an X.400/SMTP gateway that handles the exchange of electronic messages between UNIX mail applications (for example, `mailtool`) and the X.400 domain. This manual provides an overview of SunLink X.400 8.0.2, a detailed description of the OPEN LOOK® graphical user interface (`x400tool`) used to configure and maintain the components of your message transfer system, and troubleshooting information to help you locate and diagnose problems with your configuration.

SunLink X.400 8.0.2 is one of a suite of applications delivered as part of the SunLink OSI release. You must install and configure the SunLink OSI Communications Platform (stack) in order to use SunLink X.400 8.0.2. Refer to the *Installing and Licensing SunLink OSI* and the *SunLink OSI 8.0.2 Communication Platform Administrator's Guide* for detailed instructions.

Chapter Summary

Chapter 1, "Introducing SunLink X.400 8.0.2," provides an overview of the SunLink X.400 8.0.2 Message Handling System and describes each of its component parts in detail.

Chapter 2, "Starting and Using x400tool," describes how to start the OPEN LOOK graphical user interface for SunLink X.400 8.0.2 (`x400tool`) and provides an overview of how to use it to configure and maintain SunLink X.400 8.0.2.

Chapter 3, "Configuring Your Local MTA," describes how to use `x400tool` to set up your local Message Transfer Agent (MTA).

Chapter 4, "Configuring an X.400/SMTP(MIME) Gateway," describes how to use `x400tool` to set up an X.400/SMTP gateway to exchange electronic messages between the UNIX mail domain and the X.400 domain.

Chapter 5, "Adding Remote MTA Information," describes how to use `x400tool` to add remote Message Transfer Agents (MTAs) to your message handling system. These are the message transfer agents with which your local MTA will be able to communicate directly.

Chapter 6, "Adding Third-Party Agents," describes how to use `x400tool` to manage third-party user agents (UAs) and P1 users.

Chapter 7, "Routing Between Agents," describes how to use `x400tool` to modify the default routing tables to handle complex routing between agents.

Chapter 8, "Sending and Receiving UNIX Mail," describes how to use UNIX mail applications to send and receive UNIX mail messages through the X.400/SMTP gateway.

Chapter 9, "Managing Your Message Transfer System," describes how to use `x400tool` to maintain your message handling system and to gather information about the current state of its component parts.

Chapter 10, "Error Messages,"contains information to help you diagnose and resolve problems with your message handling system.

Appendix A, "Technical Specification and Conformance Information," contains a detailed technical specification for SunLink X.400 8.0.2, including a description of the CCITT X.400 MHS recommendations to which it conforms and the specific features that are implemented.

Appendix B, "Customizing sendmail for SunLink X.400 8.0.2," describes how to modify the default `sendmail` configuration file (`sendmail.cf`) to add information for routing UNIX mail through the X.400/SMTP(MIME) gateway.

Product Documentation

The documents in the SunLink X.400 8.0.2 document set are:

- *Installing and Licensing SunLink X.400 8.0.2*
  (Part No. 804-4669)
- *SunLink X.400 8.0.2 Administrator's Guide*
  (Part No. 801-4956)
- *X/Open Electronic Messaging (X.400) API*
  (Part No. 801-4957)
- *X/Open CAE Specification OSI-Abstract-Data Manipulation (XOM) API*
  (Part No. 802-1311)

Since you must install and configure the SunLink OSI Communications Platform (stack) before installing SunLink X.400 8.0.2, you will also need:

- *Installing and Licensing SunLink OSI*
  (Part No. 804-4666)
- *SunLink OSI 8.0.2 Communication Platform Administrator's Guide*
  (Part No. 801-4975)

New Features in This Release

The main features that have been added for this release are:

- Can be installed on both SPARC and x86 systems running Solaris.
- Address conversion—tests how the gateway converts X.400 and UNIX addresses.
- Message Queue Access—allows access between the MTA and non-XAPIA applications via message queues.
- Reliable Transfer Service—provides a choice of 1984 or 1988 RTS version.
- The SunLink X.400 documentation set is now available on-line with Answerbook.

What Typographic Changes Mean

The following table describes the typographic changes used in this book.

Table P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output, or step in a procedure	`machine_name% su` `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type `rm` *filename.*
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide.* These are called *class* options. You *must* be root to do this.

Boxes:

```
Contain text that represents listings, part of a
configuration file, or program output.
```

Boxes are also used to represent interactive sessions. For example:

```
% df -k /usr
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t3d0s6     155015  103090   36424    74%    /usr
```

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

Table P-2 Shell Prompts

Shell	Prompt
C shell prompt	`prompt%`
C shell superuser prompt	`prompt#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	#

Valid Characters

The following characters must not be used for any of the names describing MTAs, user agents, or gateways:

Invalid Characters	Description
@	“at” symbol
/	Forward slash
\	Backslash
#	Hash or pound sign
	Space
->	Tab

MTA names can be up to and including 32 characters long; user agent and P1 user agent names can be up to and including 16 characters long.

Introducing SunLink X.400 8.0.2 1

This chapter provides an overview of the SunLink X.400 8.0.2 Message Handling System and introduces the terminology used to describe each of its components. It also includes a list of the requirements for running SunLink X.400 8.0.2.

CCITT X.400 MHS Recommendations

The CCITT X.400 MHS recommendations specify a method of exchanging electronic messages between diverse systems based upon the principles of the OSI reference model. SunLink X.400 8.0.2 implements the 1988 revision of these recommendations, and provides a graphical user interface to configure and maintain the various components of your message handling system.

The complete CCITT 1988 X.400 recommendations are located in the *CCITT Blue Book: Data Communications Networks Message Handling Systems Recommendations X.400—X.420 (Volume VIII, Fascicle VIII.7) November 1988.*

1

X.400 Message Handling System

Figure 1-1 shows the components of a typical X.400 Message Handling System. This system is used to transfer electronic messages from one end-user (the *originator*) to another (the *recipient*).

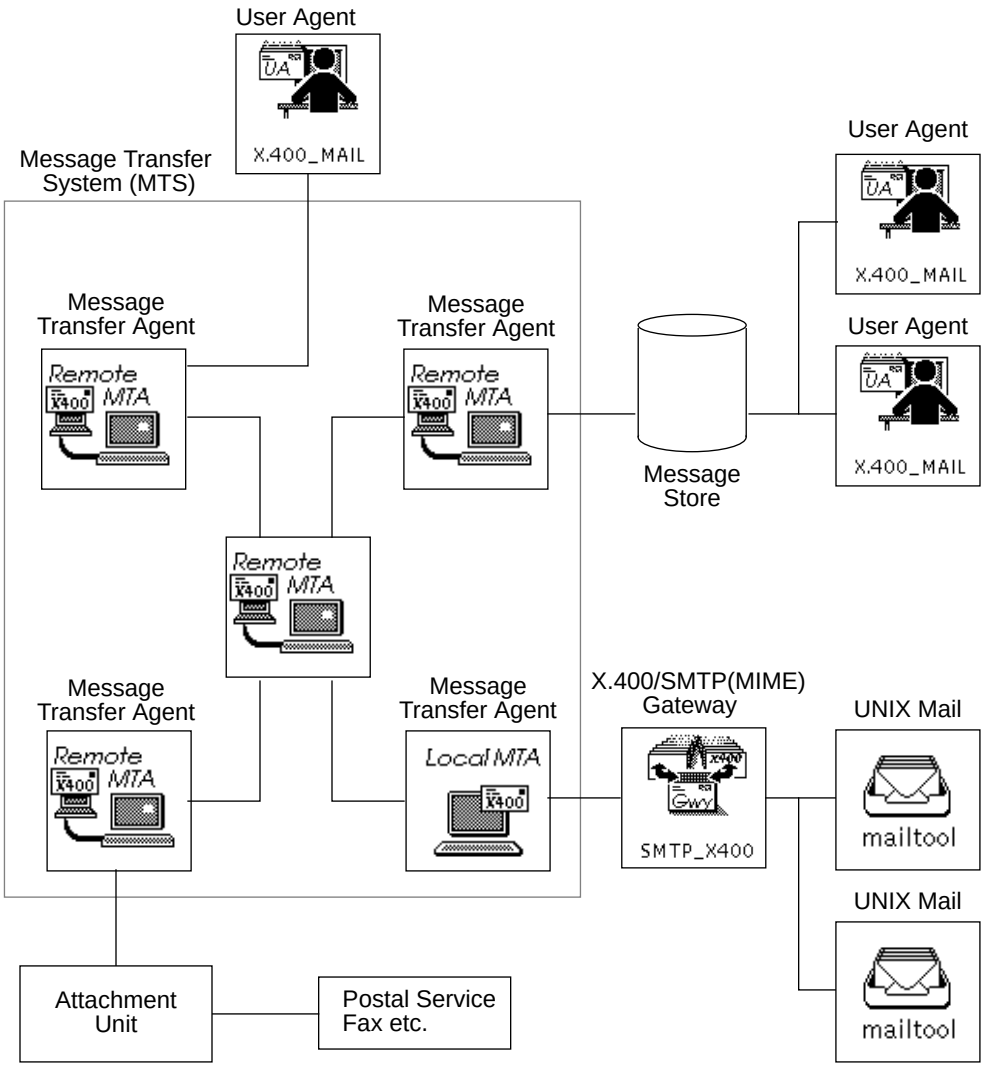


Figure 1-1 The X.400 Message Transfer System Model

The basic parts of the X.400 Message Handling System are:

- **Message Transfer System (MTS)**
  The message transfer system (MTS) handles the exchange of electronic messages between remote end-systems. It consists of one or more message transfer agents (MTAs) that relay messages from the originator to the recipient.

- **Message Transfer Agents (MTA)**
  Message transfer agents (MTAs) handle the reliable routing and relaying of electronic messages within the message transfer system (MTS). Your local MTA is the MTA running on your local machine. Remote MTAs are the message transfer agents with which your local MTA can communicate directly.

Note – The terms MTS and MTA are not considered as equivalents.

- **User Agents (UA)**
  User agents (UAs) handle the submission and delivery of electronic messages. They provide the direct interface between end-users (application processes) and the message transfer system (MTS).

- **Message Gateways**
  Message gateways handle the translation of electronic message formats between dissimilar mail systems—for example, between UNIX mail and X.400 mail.

- **Attachment Units (AU)**
  Attachment units (AUs) provide the direct interface between other communication systems (such as fax or postal services) and the message transfer system (MTS).

- **Message Store (MS)**
  The message store (MS) is used to store and retrieve electronic messages for user agents (UAs) that are not continuously available.

Note that all of the above components may reside on the same system.

The SunLink X.400 8.0.2 provides a message transfer agent (MTA) and the ability to add third-part user agents to link to the same message transfer system. An X.400/SMTP(MIME) message gateway and a messaging toolkit (containing application programming interfaces) are also provided.

1

The X.400 MHS Model

The way in which electronic messages are exchanged between end-users is often related to the components of the postal service. This model compares the content of the message to a letter, the service used to transport the message to an envelope, and the MTA to a postal sorting-office.

The basic components of the X.400 message handling system are:

- **Message Transfer Protocol (P1)**
  The message transfer protocol defines the structure used to transport an electronic message (the “envelope”) between end-users. It includes the addresses of both the originator and the recipient of the message.
- **Interpersonal Messaging Protocol (P2)**
  The interpersonal messaging protocols define the content of the message (the “letter”). An interpersonal message consists of a *header* that contains information about the message (for example, originator and recipient addresses, date, subject) and *body* parts that contain the content of the letter (for example, text (IA5), voice, G3 fax).

Figure 1-2 shows these components of the X.400 MHS model compared to their equivalents within the postal service.

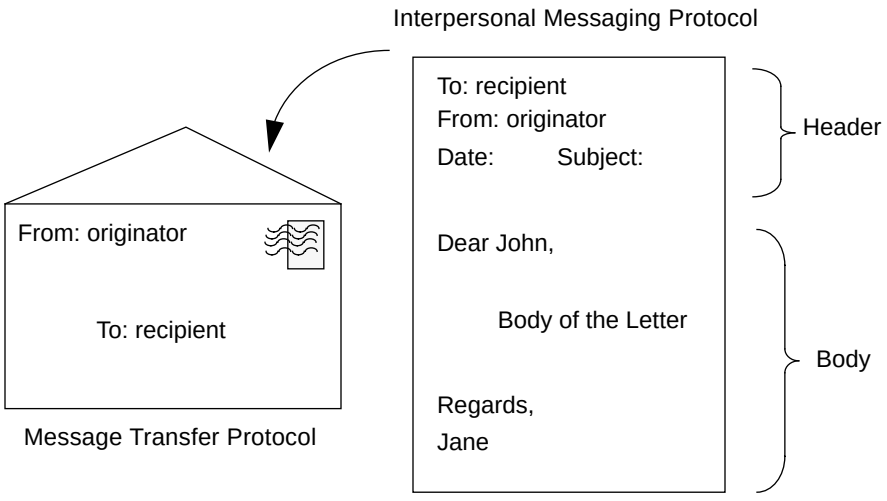


Figure 1-2 Message Transfer Protocol and Message Content

Figure 1-3 shows the way in which X.400 messages are exchanged between end-users.

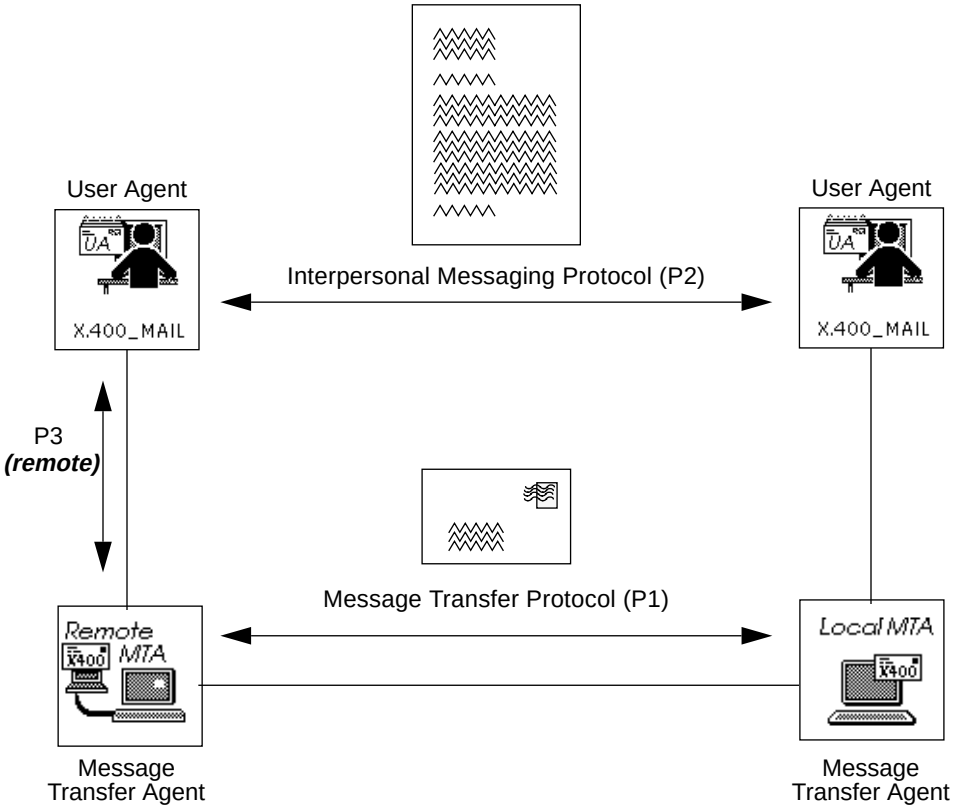


Figure 1-3 Exchanging Messages Between End-Users

SunLink X.400 8.0.2 also supports the exchange of EDI messages as defined by X.435. This protocol defines a wide range of electronic commercial communications. For example, a “bill” (or invoice) that is exchanged between end-users. This might be a message consisting of a *header* that contains information about the message (for example, originator and recipient addresses, date, subject) and a *body* that contains the content of the bill (for example, an EDIFACT, X.121, or ASCII message).

Refer to the CCITT X.435 Recommendation and the *X/Open Electronic Messaging (X.400) API* for more information on EDI messaging.

1

X.400 Management Domains

The purpose of the X.400 MHS recommendations is to create a global X.400 domain within which communicating systems throughout the world can exchange electronic messages. This global X.400 domain is divided into countries and each country is further divided into *management domains*—that is, one or more MTAs (and any associated UAs) governed by a given controlling organization.

Management domains are divided into *administrative management domains* (ADMD) and *private management domains* (PRMD):

- An ADMD is controlled by an administration (for example, a national Postal Telegraph and Telephone (PTT) Agency or a non-national organization).
- A PRMD is controlled by any other type of organization (for example, a privately-owned company).

An ADMD (such as ATLAS or MCIMAIL) is often divided into PRMDs. In general, the ADMD handles all messages that are either exchanged between PRMDs or exchanged across international boundaries; however, since the ADMD charges for its services and since not all PRMDs are controlled by an ADMD, there are exceptions to this rule.

Each MTA is assigned a *global domain identifier* that specifies the country, the ADMD, and (optionally) the PRMD in which the MTA is located as shown in Figure 1-4. This is the minimum information required to identify a given MTA.

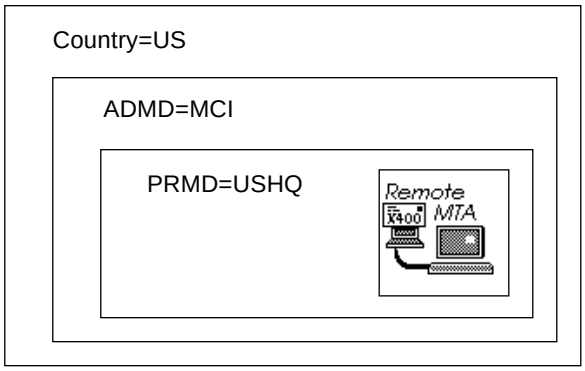


Figure 1-4 The Global Domain Identifier for an MTA

X.400 Addressing

An X.400 address (an originator/recipient address or O/R address) specifies the information needed to deliver a message to an end-user. It is analogous to the address used to direct a letter within the postal service.

An O/R address consists of a list of *attributes* that describe the end-user (or a distribution list in the case of multiple end-users) and locate that end-user within the global X.400 domain. These attributes are defined by recommendation X.402 and are generally divided into the four categories shown in Table 1-1.

Table 1-1 Attribute Categories

Attribute Type	
Personal Attributes	Attributes that describe the end-user (for example, surname, given name)
Organizational Attributes	Attributes that describe the organization to which the end-user belongs (for example, organization name, organizational unit)
Architectural Attributes	Attributes that describe the environment to which the organization belongs (for example, PRMD, X.121 address)
Geographical Attributes	Attributes that describe the physical location of the end-user (for example, country, postal code)

Domain-defined attributes are attributes that fall outside the scope of the CCITT recommendations. These attributes are interpreted only within the confines of the domain in which they are defined, but are transmitted as part of the address in the same way as standard attributes. SunLink X.400 8.0.2 supports both standard and domain-defined attributes.

In a text representation (for example, for addressing within UNIX mail) each attribute is represented by a code (or key) to which an appropriate value is assigned. Table 1-2 on page 8 lists the standard attribute keys and a description of each attribute as defined by the 1988 revision of X.402. Keys may be represented in uppercase or lowercase. Attribute values may be represented in printable text format (TXT), teletext format (TLTX), or numeric format (NUM) as indicated. (Note that the SunLink X.400/SMTP(MIME) gateway does not support teletext format O/R addresses.)

Table 1-2 Standard Attribute Keys

Attribute Key	Attribute Description	TXT	TLXT	NUM
ADMD	administration domain name	X		X
CN	common name	X	X	
C	country name	X		X
X121	network address			X
UA-ID	numeric user identifier			X
O	organization name	X	X	
OU or OU<*num*>	organizational unit name (<*num*>=1-4)	X	X	
PN	personal name	X	X	
S	surname (mandatory)	X	X	
G	given name	X	X	
I	initials	X	X	
GQ	generation qualifier	X	X	
PRMD	private domain name	X		X
T-ID	terminal identifier	X		
T-TYPE	terminal type	X		
PD_SERVICE	physical delivery service name	X		
PD-C	physical delivery country name	X		X
PD-CODE	physical delivery postal code	X		X
PD-EXT-ADDRESS	physical delivery extension address components	X	X	
PD-OFFICE	physical delivery office name	X	X	
PD-OFFICE-NUM	physical delivery office number	X	X	
PD-PN	physical delivery personal name	X	X	
PD-O	physical delivery organization name	X	X	
PD-ADDRESS	physical delivery unformatted postal address	X	X	
PD-STREET	physical delivery postal street address	X	X	
PD-BOX	physical delivery postal box address	X	X	
PD-RESTANTE	physical delivery poste restante address	X	X	
PD-UNIQUE	physical delivery unique postal name	X	X	
PD-LOCAL	physical delivery local postal attributes	X	X	
NET-NUM	extended network address	X	X	
DD<*num*>	domain defined attribute	X	X	X

Note that the personal-name attribute has four component attributes (given-name, surname, initials, generation-qualifier) of which only the surname is mandatory.

Representing O/R Addresses

There are two notations used for representing O/R addresses in a text format (O/R addresses are encoded for transmission). Of these, the more widely accepted notation separates the component attributes by a slash (/) character.

By convention, O/R names are often represented in an order similar to that used for postal addresses as shown in the example in Figure 1-5; however, there are actually very few restrictions to the order in which attributes appear in the address.

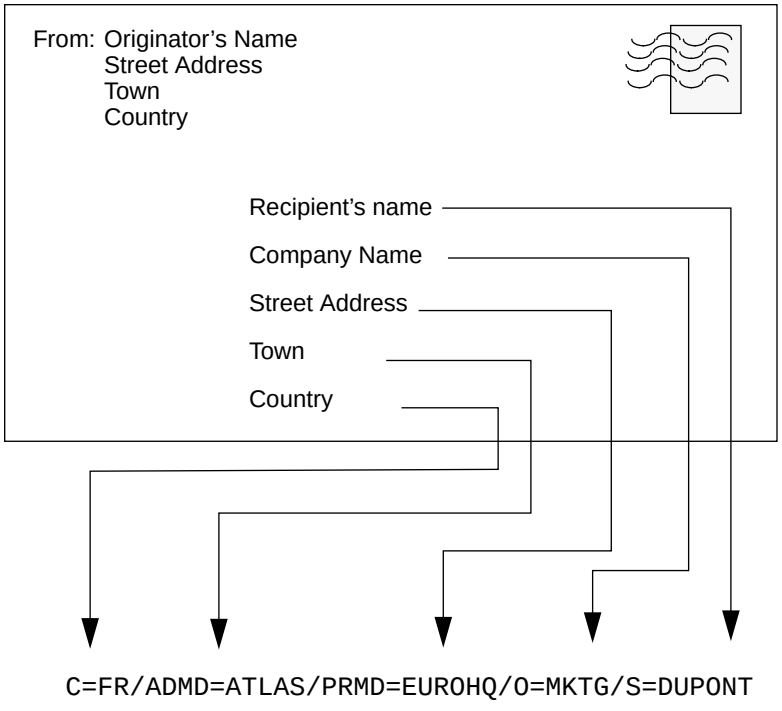


Figure 1-5 O/R Address Conventions

A less common notation separates the component attributes by a semicolon (;). Using this notation, the address shown in Figure 1-5 becomes:

```
S=DUPONT;O=MKTG;PRMD=EUROHQ;ADMD=ATLAS;C=FR;
```

O/R addresses are divided into four types:

- Mnemonic O/R Address
- Numeric O/R Address
- Terminal O/R Address
- Postal O/R Address

1. **Mnemonic O/R Address**
   This is the most common type of O/R address. It identifies the user and the administrative domain within which the user is located. By definition, all attributes are assigned text (or teletext) format values. A mnemonic O/R address consists of the following component attributes:

   - One country-name (C) and one administration-domain-name (ADMD), which may be assigned a blank space as a value. This identifies the ADMD within which the user is located.
   - A combination of attributes selected from the following list:
     private-domain-name (PRMD)
     organization-name (O)
     organizational-unit-names (OU)
     common-name (CN)
     personal-name (PN)
     surname (S) — mandatory
     given-name (G)
     initials (I)
     generation-qualifier (GQ)
   - Optionally, one or more domain-defined attributes (DD).

Note that you can have up to four organizational unit (OU) names in a mnemonic O/R address. If you use organizational unit names, the order of the attributes can be important. You can use either numbered organizational unit names (OU1, OU2, etc.):

```
/S=DUPONT/OU1=PROD/OU2=FCAST/O=MKTG/PRMD=EUROHQ/ADMD=ATLAS/C=FR/
```

or unnumbered organizational unit names (OU) which are interpreted in the order in which they appear, numbered from the side nearest the country code:

```
/S=DUPONT/OU=FCAST/OU=PROD/O=MKTG/PRMD=EUROHQ/ADMD=ATLAS/C=FR/
or
/C=FR/ADMD=ATLAS/PRMD=EUROHQ/O=MKTG/OU=PROD/OU=FCAST/S=DUPONT/
```

2. **Numeric O/R Address**
   A numeric O/R address identifies the user and the ADMD within which the user is located using numeric attributes only. It consists of the following component attributes:

   - One country-name (C) and one administration-domain-name (ADMD), both of which must be assigned numeric values. This identifies the ADMD within which the user is located.
   - One numeric-user-identifier (UA-ID) and (optionally) a private-domain-name (PRMD).
   - Optionally, one or more numeric domain-defined attributes (DD).

3. **Terminal O/R Address**
   A terminal O/R address identifies a user by means of a network address and some other optional information. It consists of the following component attributes:

   - One network address (X.121).
   - Optionally, a terminal-identifier (T-ID).
   - Optionally, one country-name (C) *and* one administration-domain-name (ADMD). Both attributes must be defined. This identifies the ADMD through which the terminal is accessed.
   - Optionally, only when the country-name and administration-domain-name are present, one private-domain-name (PRMD).
   - Optionally, only when the country-name and administration-domain-name are present, one or more domain-defined attributes (DD).

4. **Postal O/R Address**
   A postal O/R address identifies the user by means of the user's postal address (street address, postal code, etc.) and is used to physically deliver a message to a user.

Postal O/R addresses are not directly applicable to SunLink X.400 8.0.2 and physical-delivery attributes are not supported by `x400tool`. Although SunLink X.400 8.0.2 supports messages that present a postal O/R address, it does not base any of its routing decisions on the physical-delivery attributes.

The X.400 recommendations specify a *formatted* postal O/R address that is composed of several attributes:

- One country-name (C) and one administration-domain-name (ADMD). This identifies the ADMD within which the user is located.
- One physical-delivery-country-name (PD-C) and one physical-delivery-postal-code (PD-CODE) that identify the physical (geographical) location at which the user takes delivery of the message.
- Optionally, a combination of attributes from the following list:
  - private-domain-name (PRMD)
  - physical-delivery-service-name (PD-SERVICE)
  - physical-delivery-personal-name (PD-PN)
  - physical-delivery-office-name (PD-OFFICE)
  - physical-delivery-office-number (PD-OFFICE-NUM)
  - physical-delivery-organization-name (PD-O)
  - physical-delivery-unformatted-postal-address (PD-ADDRESS)
  - physical-delivery-postal street-address (PD-STREET)
  - physical-delivery-postal-box-address (PD-BOX)
  - physical-delivery-unique-postal-name (PD-UNIQUE)
  - physical-delivery-local-postal-attributes (PD-LOCAL)
  - physical-delivery-poste-restante-address (PD-RESTANTE)

Refer to Chapter 8, “Sending and Receiving UNIX Mail” for a detailed description of how to use X.400 O/R addresses when sending messages using UNIX mail applications such as `mail` or `mailtool`.

Routing Messages in the X.400 Domain

An MTA functions like a traditional postal service sorting-office—sorting the messages for delivery, based on the recipient address.

When it receives a message, the MTA compares the list of attributes in the O/R address against the entries in its local routing table. If the O/R address (or part of the O/R address) matches one of the entries, the message is forwarded to the agent associated with the matching entry.

This can be any one of the recognized components (remote MTA, local user agent, or message gateway) in the message transfer system.

Figure 1-6 illustrates the behavior of an MTA compared to a sorting office. Refer to Chapter 7, “Routing Between Agents” for detailed instructions on defining entries in the routing table used by your local MTA.

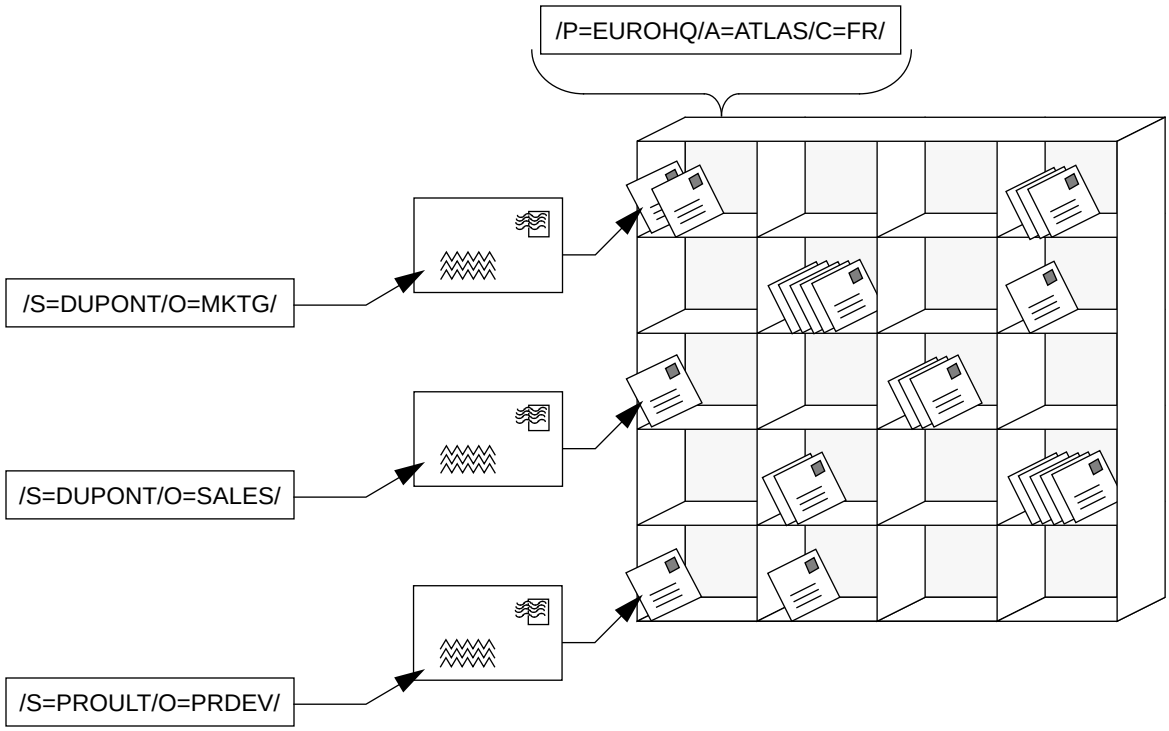


Figure 1-6 The MTA as a Postal Service Sorting Office

X.400/SMTP(MIME) Gateway

One of the features of SunLink X.400 8.0.2 is an X.400/SMTP(MIME) gateway which handles the exchange of mail messages between UNIX mail systems that conform to RFC 822 (such as `mailtool`) and the X.400 domain.

The X.400/SMTP(MIME) gateway maps RFC 822 addresses and service elements to equivalent X.400 addresses and service elements, and adds any additional information required to route messages across the global X.400 domain. It provides support for the transfer of MIME (Multipurpose Internet Mail Extensions) attachments as defined by RFC 1341, and incorporates Sun-specific mail features such as international character set and Sun multimedia attachment support.

Routing Messages in the UNIX Mail Domain

This section provides an overview of UNIX mail handling services and routing in the UNIX mail domain. Refer to Chapter 8, “Understanding Mail Services”, in the your Solaris *Setting Up User Accounts, Printers, and Mail* document for a detailed description of the UNIX mail system.

The routing of messages within the UNIX mail domain is handled by the `sendmail` daemon as shown in Figure 1-7.

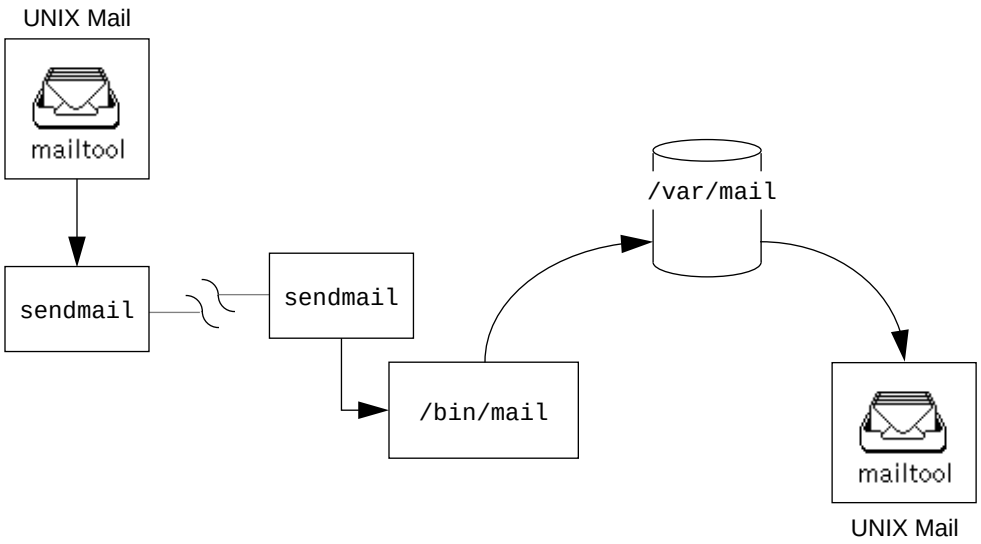


Figure 1-7 Routing Messages in the UNIX Mail Domain

When sendmail receives a message (from either a local UNIX mail application or from a remote sendmail daemon) it expands and parses the recipient address using the information in its local configuration file (sendmail.cf).

- If the message cannot be delivered locally, the message is relayed between sendmail daemons based on the recipient address and the information in the NIS database (or the local /etc/hosts if NIS is not running).
- If the message can be delivered locally, sendmail calls the program /bin/mail which writes the message into the recipient's mailbox (/var/mail/<*username*>). From the mailbox, the message can be retrieved with a UNIX mail application such as mailtool.

Routing Messages from UNIX Mail to X.400

Your X.400/SMTP(MIME) gateway provides an interface between the sendmail daemon (which routes electronic mail in the UNIX mail domain) and your local MTA (which routes electronic mail in the X.400 domain).

Each X.400/SMTP(MIME) gateway is identified by a *pseudo host name* which is an alias for the machine on which the gateway is running. This alias must be entered in the NIS database (or in /etc/hosts if NIS is not running). It must also be registered in the local configuration file (sendmail.cf) for the sendmail daemon running on the same machine as the gateway. (Note that the local sendmail.cf is modified automatically with a default pseudo host name—x400-gate when SunLink X.400 8.0.2 is installed.)

Routing messages between the UNIX mail domain and the X.400 mail domain occurs in two distinct steps:

1. **Routing the message to the machine on which the gateway is running.** When sendmail receives a message (from either a local UNIX mail application or from a remote sendmail daemon) it expands and parses the recipient address, using the information in its local configuration file (sendmail.cf). If the message cannot be delivered locally, it is relayed between sendmail daemons based on the recipient address and the pseudo host name located in the NIS database (or the local /etc/hosts if NIS is not running) until it reaches the machine on which the gateway is located.

2. **Routing the message to the gateway running on the machine.**
   The `sendmail` daemon running on the same machine as the gateway recognizes the message based on the pseudo host name entered in its local configuration file (`sendmail.cf`). As a result, it calls the X.400 mailer program `osix400mail` in place of the UNIX mailer program `/bin/mail`.

Instead of writing the message directly into the recipient's mailbox, the X.400 mailer `osix400mail` writes the message into a product-specific spool directory (`/var/SUNWconn/OSIROOT/mhs/spool`) where it can be accessed and parsed by the X.400/SMTP(MIME) gateway. The X.400/SMTP(MIME) gateway translates UNIX address and message elements into X.400 equivalents and passes the outgoing message to the local MTA for delivery across the X.400 domain. Figure 1-8 shows how outgoing messages are routed from the UNIX mail domain to the X.400 mail domain through the X.400/SMTP(MIME) gateway.

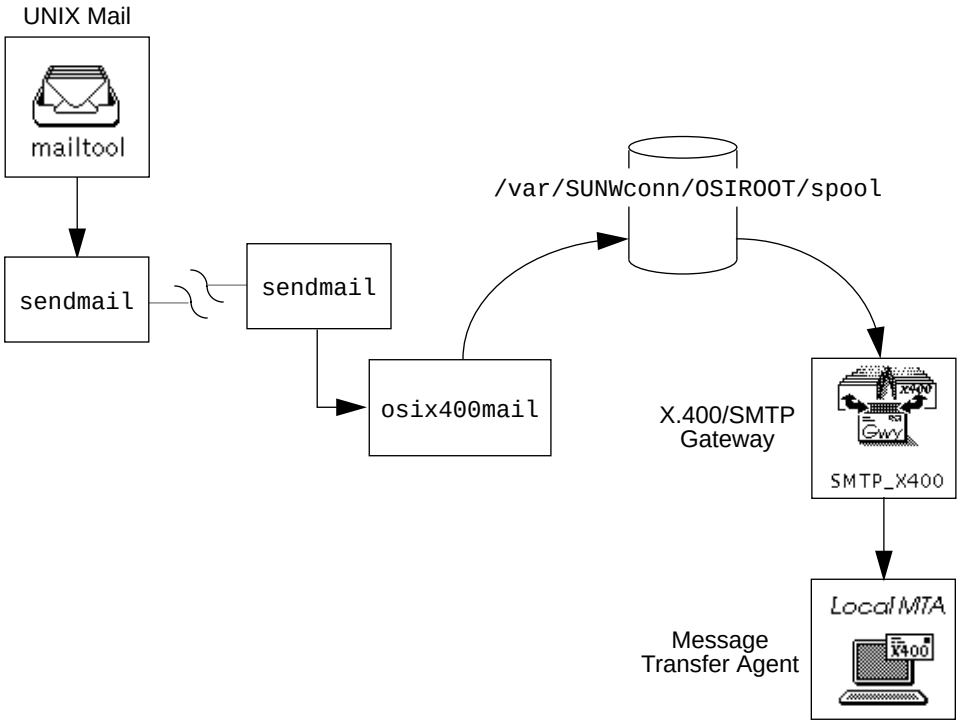


Figure 1-8 Routing Mail from UNIX Mail to X.400 Mail

Routing Messages from X.400 to UNIX Mail

When the X.400/SMTP(MIME) gateway receives an incoming message from the local MTA, it converts the X.400 address and message elements into UNIX mail equivalents. It passes the message directly to the local `sendmail` daemon, which handles the routing in the UNIX mail domain based on the information in its local configuration file and the NIS database.

When the message reaches the machine on which the mailbox for the recipient is located, the `sendmail` daemon calls the UNIX mailer program `/bin/mail`. This writes the message into the recipient's mailbox from where it can be retrieved using a UNIX mail application (such as `mailtool`).

Figure 1-9 shows how incoming messages are routed from the X.400 mail domain to the UNIX mail domain through the X.400/SMTP(MIME) gateway.

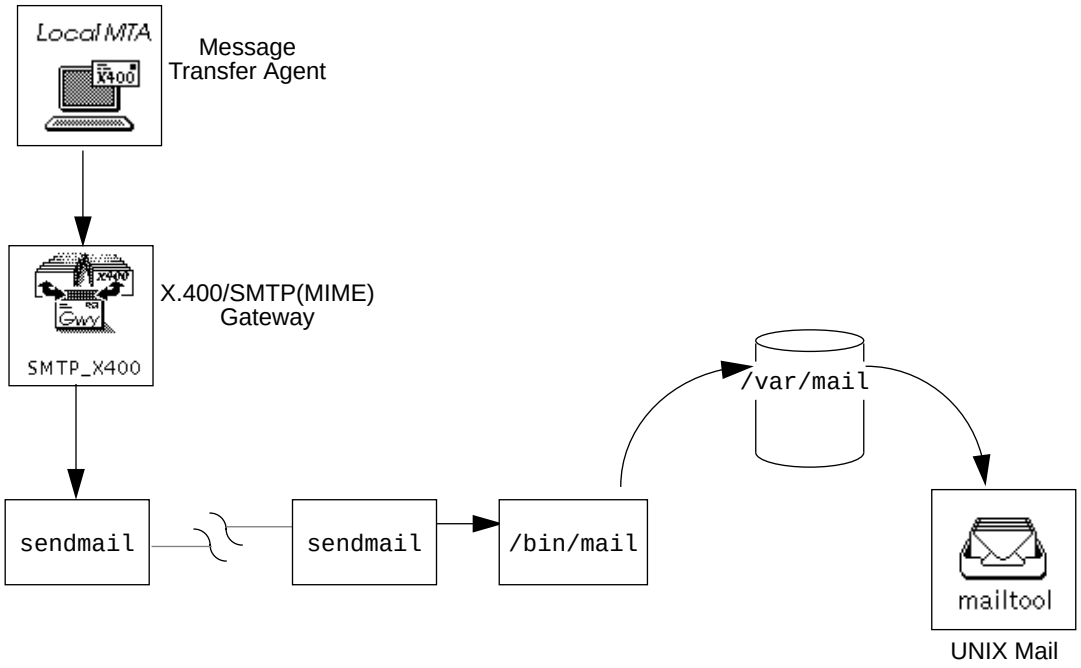


Figure 1-9 Routing Messages from X.400 Mail to UNIX Mail

1

Addressing Mail to the X.400/SMTP(MIME) Gateway

A UNIX mail address contains the name of the recipient and the name of the machine to which the message must be delivered. Addresses used to direct mail the UNIX mail domain are usually of the form:

```
<local_address>@<domain_address>
```

Where <*local_address*> is the local address of the recipient and <*domain_address*> specifies the location of the local address within the global UNIX mail domain. Refer to Chapter 8, “Understanding Mail Services”, in your Solaris *Setting Up User Accounts, Printers, and Mail* document for a more detailed description of UNIX mail addressing.

To address mail to a recipient through the X.400/SMTP(MIME) gateway, you need to specify the local address of the recipient and the domain address of the gateway.

The complete domain address for the X.400/SMTP(MIME) gateway is comprised of the pseudo host name (alias) assigned to the gateway, and the domain address of the UNIX mail domain in which the gateway is located.

For example:

To address mail to a recipient John Smith through an X.400/SMTP(MIME) gateway with a pseudo host name `x400-gate`, located in the domain `Division.Company.COM`:

```
jsmith@x400-gate.Division.Company.COM
```

When you address mail to a recipient within the same UNIX mail domain, you need only specify the pseudo host name:

```
jsmith@x400-gate
```

You can also address mail to the recipient using X.400-style addressing. In this case, you provide the X.400 O/R address as the local address and you still specify the pseudo host name as the domain address for the gateway.

The `sendmail` daemon routes the message to the gateway based on the pseudo host name and the X.400/SMTP(MIME) gateway does not need to translate the X.400-style address.

For example:

To address mail to the same recipient using his X.400 O/R address:

```
/G=john/S=smith/PRMD=PRMD_gnb/ADMD=ATLAS/C=FR/@x400-gate
```

Refer to Chapter 8, "Sending and Receiving UNIX Mail" for more detailed instructions on addressing mail messages to the X.400 domain from within UNIX mail applications such as `mail` and `mailtool`.

Supported Mail Headers

The X.400/SMTP(MIME) gateway also translates the mail headers that are used to carry additional information and to modify the behavior of the mail delivery system on a per-message basis—for example, to mark the message for urgent delivery or to request a delivery report. It supports all the mail headers specified within RFC 822, and additional headers specified in RFC 987 and RFC 1327. Headers are mapped according to the rules defined in RFC 1327.

Table 1-3 lists some of the most commonly used mail headers that can be used to set X.400 flags in messages sent through the X.400/SMTP(MIME) gateway. Refer to Chapter 8, "Sending and Receiving UNIX Mail" for a complete list of the supported headers and detailed instructions on how to set mail headers from within UNIX mail applications such as `mail` and `mailtool`.

Table 1-3 Supported Mail Headers

Header	**Usage**
Bcc (blind carbon copy)	recipient address
Cc (carbon copy)	recipient address
Conversion	true/false
Conversion-with-loss	true/false
Delivery-Report	always/never/audited/non-delivery
Disclose-Recipient	true/ false

Table 1-3 Supported Mail Headers

Header	Usage
Expiry-Date	RFC 822 format date
Importance	low / high / routine
Priority	low / urgent / normal
Receipt-Notification	always / non-receipt / never
Reply-to	originator address
Sender	originator address
Sensitivity	personal / private / confidential / non-sensitive
Subject	string
To	recipient address

System Requirements for Running SunLink X.400 8.0.2

In order to configure and run SunLink X.400 8.0.2, you must have the following software installed on your system:

1. **SunOS 5.4 operating system, or a later version.**
   The Solaris 2.4 environment includes the SunOS 5.4 operating system. To check the version of the operating system on your machine, type:

```
hostname% showrev
```

   Check that the operating system is 5.4 or later:

```
Hostname: scratchit
Hostid:  1234f567
Release:  5.4
Kernel architecture:  sun4m
Application architecture:  sparc
Hardware provider:  Sun_Microsystems
Domain:  XYZ.DIV.Company.COM
Kernel version:  SunOS 5.4 generic. July 1994
```

2. **OpenWindows 3.1 or later, and in particular the file `cetables` which is used by the X.400/SMTP(MIME) gateway.**
   You need to run OpenWindows in order to configure SunLink X.400 8.0.2 (there is no command-line interface). To check that the file `cetables` is available on your machine:

```
hostname% ls $OPENWINHOME/lib/cetables/cetables
/usr/openwin/lib/cetables/cetables
```

3. **If you want to be able to use the X.400/SMTP(MIME) gateway you must have the `sendmail` daemon installed and running on your system.**
   The sendmail daemon is used by UNIX mail applications such as `mail` and `mailtool`. To check that the sendmail daemon is running on your system, type:

```
hostname% ps -ef | grep sendmail
<pid>  <timestamp> /usr/lib/sendmail -bd -q1h
```

4. **The `sendmail` daemon uses the configuration file `sendmail.cf`. This file is modified automatically when you install the SunLink X.400 8.0.2 software; however, if `sendmail.cf` does not exist, or if you have a customized version of the file, the modification will fail.**
   Refer to Appendix B, “Customizing sendmail for SunLink X.400 8.0.2” for detailed instructions of how to add the necessary modifications manually.

1

Starting and Using `x400tool` 2

This chapter provides a summary of the steps required for configuring your machine as a message transfer agent (MTA) and X.400/SMTP (MIME) gateway. It describes how to start the OPEN LOOK graphical user interface for SunLink X.400 8.0.2 (`x400tool`) and introduces its primary components.

This chapter assumes that you have already installed and configured the SunLink OSI Communications Platform (stack) and installed the product packages associated with SunLink X.400 8.0.2. See the *Installing and Licensing SunLink OSI* and the *SunLink OSI Communication Platform Administrator's Guide* for detailed instructions.

You should read Chapter 1, "Introducing SunLink X.400 8.0.2", which introduces the terms and concepts presented throughout this manual, before starting to use `x400tool`.

2

Summary of Steps

1. **Ensure that you have installed the software and licenses for the SunLink OSI Communications Platform (stack). Configure and start the stack.**
   Starting the stack allows you to test each component of your configuration as you set it up. Refer to the *Installing and Licensing SunLink OSI* and the *SunLink OSI Communication Platform Administrator's Guide* for detailed instructions.

2. **Ensure that you have installed the software and licenses for the SunLink X.400 8.0.2. Start the processes for SunLink X.400 8.0.2.**
   You will not be able to start `x400tool` unless these processes are running. Refer to "Starting x400tool on Your Local Machine" on page 26.

3. **Become superuser and start `x400tool`.**
   Refer to "Starting x400tool on Your Local Machine" on page 26 and "Starting x400tool on a Remote Machine" on page 27 in this chapter for detailed instructions.

4. **Use `x400tool` to configure your local MTA.**
   For a minimum configuration you must provide a name for your local MTA and specify its local domain identifier. Refer to Chapter 3, "Configuring Your Local MTA" for detailed instructions.

5. **Use `x400tool` to configure your X.400/SMTP (MIME) gateway.**
   If you want to communicate with the X.400 domain with UNIX mail applications, you must configure a message gateway that will handle the translation of UNIX mail addresses and service elements. Refer to Chapter 4, "Configuring an X.400/SMTP(MIME) Gateway" for detailed instructions.

6. **Use `x400tool` to add remote MTAs to your message transfer system (MTS).**
   This identifies each of the remote MTAs with which your local MTA can communicate directly. You should test the connections to each remote MTA as you add it to your network. Refer to Chapter 5, "Adding Remote MTA Information" for detailed instructions.

7. **Use `x400tool` to add any third-party user agents or P1 user agents to your message transfer system (MTS).**
   A user agent is not provided with the default configuration provided with SunLink X.400 8.0.2; however, you can develop your own user agents and P1 user agents (via XAPIA or message queue access), and add these to the same message transfer system. Refer to Chapter 6, "Adding Third-Party Agents" for detailed instructions.

8. **Use `x400tool` to modify the routing table for your local MTA, if required.**
   When you add agents to the message transfer system there are default entries made in the local routing table; however, you may need to modify these entries to improve the efficiency of the routing algorithm. Refer to Chapter 7, "Routing Between Agents" for detailed instructions.

9. **Use `mail` or `mailtool` to send messages across your message transfer system (MTS).**
   Your message transfer system is now be configured and ready for daily use. Chapter 8, "Sending and Receiving UNIX Mail" provides an overview of how to use UNIX mail applications such as `mail` and `mailtool` to send and receive mail across the X.400 domain.

10. **Use `x400tool` to manage and maintain your message transfer system (MTS).**
    Once you have configured and tested your message transfer system, you can also use `x400tool` to open and close MTAs and to recover status information about the transfer of messages. Refer to Chapter 9, "Managing Your Message Transfer System" for detailed instructions.

Note – Throughout this manual, it is assumed that you accepted the default base directory (`/opt`) for the SunLink X.400 8.0.2 executable program files when you installed the software. If this is not the case, you will need to replace `/opt` in the example commands with the true base directory for your system.

For convenience, before using `x400tool` you should modify the local environment variables to add the following definitions:

```
$PATH       /opt/SUNWconn/bin

$MANPATH    /opt/SUNWconn/man

$HELPPATH   /opt/SUNWconn/mhs/lib/locale/C
```

When you have set these variables, you can access on-line help information by pressing the Help key on your keyboard. This book plus *X/Open Electronic Messaging (X.400) API* and *X/Open CAE Specification OSI-Abstract-Data Manipulation (XOM) API* are available on-line if you have installed the Answerbook supplied with the CD-ROM. *Installing and Licensing SunLink X.400 8.0.2* describes how to install Answerbook.

Starting `x400tool` *on Your Local Machine*

The OPEN LOOK graphical user interface for SunLink X.400 8.0.2 is called `x400tool`. It is used to configure and maintain your message transfer system.

To start and use `x400tool`:

1. **Log in as `root` or become `superuser`, if you have not done so already.**
   To help protect your message transfer system from unauthorized modification, you must always possess superuser privileges in order to run `x400tool`.

```
hostname% su
Password: <your superuser password>
hostname#
```

2. **Ensure that you have started the SunLink X.400 8.0.2 processes.**
   This allows you to test each of the connections from your local MTA as you set them up. If you rebooted your machine after you installed the product packages for SunLink X.400 8.0.2 then these processes should already be started. You can verify this by typing:

```
# ps -ef |grep osi
root <pid>  <timestamp>   osismtpx400 osismtpx400 osismtpx400
root <pid>  <timestamp>   osimta osimta osimta
root <pid>  <timestamp>   osix400mqa osix400mqa osix400mqa
... other osi processes
root <pid>  <timestamp>   grep osi
```

If the SunLink X.400 8.0.2 processes are not running, you can start them manually by using `osistart`:

```
hostname# /opt/SUNWconn/bin/osistart osimta osix400mqa osismtpx400
```

Use the `-v` option (verbose) to obtain trace information during the startup.

3. **Start `x400tool` by typing:**

```
hostname# /opt/SUNWconn/bin/x400tool &
```

Starting `x400tool` *on a Remote Machine*

If you want to use `x400tool` to configure a remote machine as an MTA you can start `x400tool` remotely so that it displays on the monitor of your local machine.

Note – Remember that although you are running `x400tool` remotely, you are still configuring the remote machine as your local MTA.

To start `x400tool` remotely:

1. **On your *local* machine, disable access restrictions for the remote machine so you are able to display `x400tool` on your local monitor.**

```
localhost% $OPENWINHOME/bin/xhost + <remotehost>
```

2. **Log in to the remote machine as root or superuser.**

```
localhost% rlogin <remotehost>
Password: <your password>
remotehost% su
remotehost% <superuser password of the remote host>
remotehost#
```

3. **On the *remote* machine, check that SunLink X.400 8.0.2 is running. Start these processes manually if required.**

```
remotehost# /opt/SUNWconn/bin/osistart osimta osix400mqa osismtpx400
```

Use the -v option (verbose) to obtain trace information during the startup.

4. **On the *remote* machine, start** `x400tool` **so that it displays on your local monitor.**

```
remotehost# /opt/SUNWconn/bin/x400tool -display <localhost>:0 &
```

Using `x400tool`

When you start `x400tool` you will see a map of the current message transfer system. An icon will appear representing each component (local MTA, remote MTAs, user agents) of your system.

If this is the first time you started `x400tool` on your machine, you will see two icons: one that represents your (unconfigured) local MTA; another that represents an (unconfigured) X.400/SMTP gateway. Figure 2-1 shows the main window as it appears when you start `x400tool` for the first time.

To modify the configuration of any of the components in your message transfer system, double-click SELECT on its icon to activate the associated configuration window.

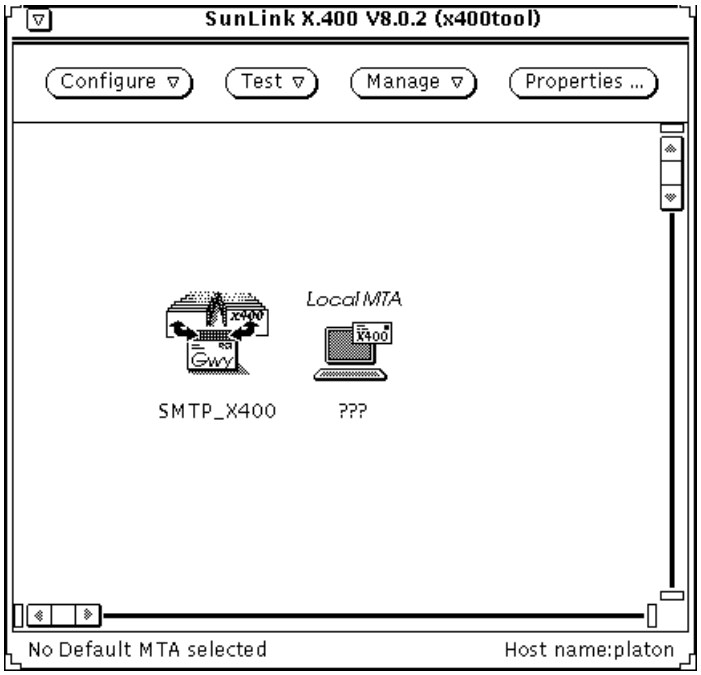


Figure 2-1 `x400tool`: Main Window

The message transfer system map has three pull-down menus that can be used to modify, test, and manage the system. Figure 2-2 shows these three pull-down menus:

- The **Configure** menu is used to modify the configuration for the currently selected agent. It also contains options used to backup and restore the configuration for your message transfer system.
- The **Test** menu is used to check the associations between agents and the routing of electronic messages throughout your message transfer system. There is also an option to check the conversion of addresses made by the gateway.
- The **Manage** menu is used to maintain the elements of your message transfer system and to recover status information.

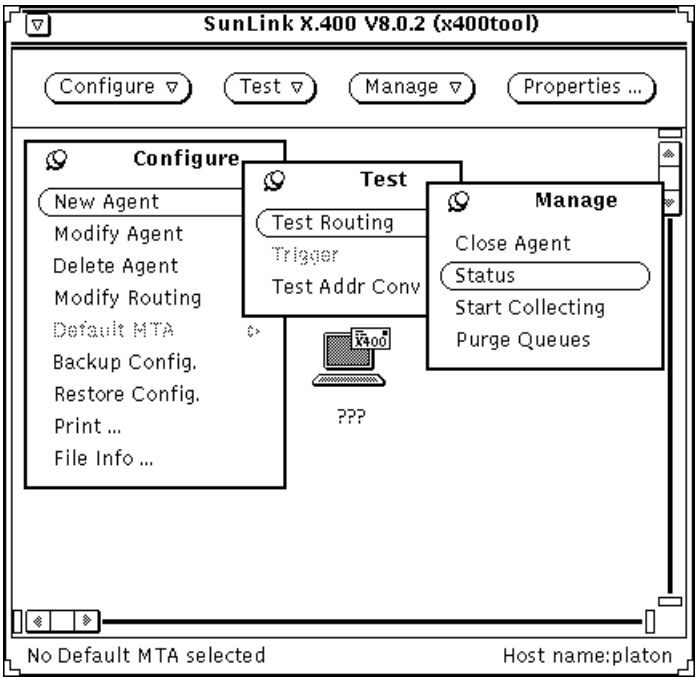


Figure 2-2 `x400tool`: Pull-Down Menus

Changing the Tool Properties

Properties ...

The tool Properties affect the way in which `x400tool` operates. The Properties window in shown in Figure 2-3.

1. **Click SELECT on the Properties... button to activate the Tool Properties window.**

2. **Click SELECT on either Automatic or Manual to set the refresh mechanism for the `x400tool` status windows.**
   Refer to “Displaying Status Information” on page 131 for a detailed description of the `x400tool` status windows used for viewing the current status of the various elements in your message transfer system.

- If you choose Automatic, the status windows are refreshed automatically at intervals specified by the value Interval. Click SELECT on the slider to set a value for the interval, or type a value and press Return.

- If you choose Manual, you must use the “Refresh” button on each status window to update the display every time you want to see the most recent information.

Apply

3. **Click SELECT on Apply, Reset, or Default.**
   The default value is 20 seconds.

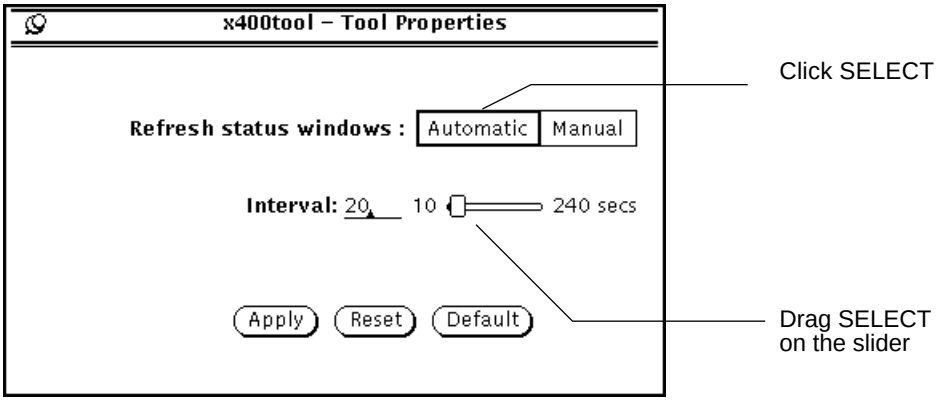


Figure 2-3 `x400tool`: Changing the Tool Properties

Configure ▽ *Backing Up Your Configuration*

The Backup Config item is used to save your current configuration to a set of files. By default, configuration files are saved in the directory `/var/SUNWconn/OSIROOT/mhs/conf`, but you can specify an alternative location. The configuration is saved under a number of files identified by the same file prefix. The file <*prefix*>`.mhscf` defines the name and location of all other configuration files. You specify a prefix to identify the configuration when you backup the files.

The configuration that is displayed when you start `x400tool` for the first time is saved under `/var/SUNWconn/OSIROOT/mhs/conf/master.mhscf`.

1. **Press MENU on the Configure menu button and drag the pointer to the Backup Config item. Release MENU to activate the file selection window.**

2. **Choose a directory and enter the prefix for your backup configuration.**
   If you do not append `.mhscf` to your prefix this will be added automatically when you save your configuration.
3. **Click SELECT on Backup to save your configuration to file.**

Configure ▽ *Restoring an Existing Configuration*

The Restore Config item is used to load an existing configuration from file. You can use this facility to restore the master configuration:

```
/var/SUNWconn/OSIROOT/mhs/conf/master.mhscf
```

1. **Press MENU on the Configure menu button and drag the pointer to the Restore Config item. Release MENU to activate the file selection window.**
2. **Choose a directory and select an existing configuration.**
   Only files that are appended with `.mhscf` are displayed. When you select a file called <*prefix*>.mhscf, all of the configuration files that start with this prefix will be loaded.
3. **Click SELECT on Restore to load the contents of the configuration files.**

Configure ▽ *Printing Your Configuration*

The Print option is used to format and print the current configuration. You can print to any local printer or to a file.

1. **Press MENU on the Configure menu button and drag the pointer to the Print item. Release MENU to activate the print selection window.**
2. **Choose the name of a printer from the pull-down menu, or specify the name of a file.**
   If there are no printers configured for your system, then you can only print to a file.
3. **Click SELECT on Print to print the configuration.**

Configure ▽ *Using* `x400tool` *Files*

Several files are associated with SunLink X.400 8.0.2. These files can be divided into three categories:

- Configuration files that define the components of your message transfer system. By default, configuration files are located under the directory `/var/SUNWconn/OSIROOT/mhs/conf`.
- Spool or log files that contain a record of all transactions that occur in your message transfer system. By default, log files are located under the directory `/var/SUNWconn/OSIROOT/spool`.
- Work files used by the processes associated with your message transfer system. By default, work files are also located under the directory `/var/SUNWconn/OSIROOT/spool`.

If these files become too large, for example, if the queue of messages becomes very long, you should use symbolic links to another directory where there is more room. That is, symbolically link the original spool file to disk space outside your own home directory, so that your own system is not affected by a large message queue. You must ensure that any directories that are symbolically linked have the correct access rights.

Caution – Do not delete the files in your spool directory. Use the "purge" option (see "Purging the Mail Queues" on page 139) to remove unwanted messages completely.

To display the location of the files associated with your current configuration:

1. **Press MENU on the Configure menu button and drag the pointer to the File Info item. Release MENU to activate the Current Configuration window.**
   This displays the short view (summary) of the base directories in which the configuration, log, and work files are located.
2. **Click SELECT on Full View to display a complete list of the files associated with your current configuration.**

2

Table 2-1 contains a complete list of the SunLink X.400 8.0.2 configuration, spool, and log files:

Table 2-1 SunLink X.400 8.0.2 Configuration and Spool Files

File Name	Description
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf`	Defines the name and location of all other configuration files
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.text`	Text version of the MTS configuration. The other configuration files can be regenerated from this file using `x400_genconf`.
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.mta`	Defines the remote MTAs recognized by the local MTA.
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.luag`	Defines the user agents recognized by the local MTA.
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.x121`	Identifies the default MTA and lists the X.121 prefixes supported by the local MTA (not configurable).
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.orname`	Routing table for the local MTA.
`/var/SUNWconn/OSIROOT/mhs/conf/<`*prefix*`>.mhscf.alternate`	Defines the alternate recipients for user agents.
`/var/SUNWconn/OSIROOT/mhs/conf/journal.fmt`	Specifies the format of the messages printed in the journal file. Do not edit this file.
`/var/SUNWconn/OSIROOT/mhs/conf/rfc1148*.bin`	Binary mapping tables for addresses used by the X.400/SMTP gateway.
`/var/SUNWconn/OSIROOT/mhs/conf/rfc1148*`	Corresponding text files for the mapping tables.
`/var/SUNWconn/OSIROOT/mhs/conf/*cache`	Cache files, used by the gateway to optimize address conversion.
`/var/SUNWconn/OSIROOT/spool/billing1`	Binary format billing files. Alternated with `billing2`.
`/var/SUNWconn/OSIROOT/spool/billing2`	Binary format billing files. Alternated with `billing1`.
`/var/SUNWconn/OSIROOT/spool/billing.tmp`	Temporary billing file (internal use).
`/var/SUNWconn/OSIROOT/spool/msg`	Queue of messages to be sent/received. Do not delete this file.[1]
`/var/SUNWconn/OSIROOT/spool/journal1`	Journal of events. Alternates with `journal2`.
`/var/SUNWconn/OSIROOT/spool/journal2`	Journal of events. Alternates with `journal1`.

Table 2-1 SunLink X.400 8.0.2 Configuration and Spool Files

File Name	Description
/var/SUNWconn/OSIROOT/spool/T00000*	File used by the local MTA for initial reference to the message queue.
/var/SUNWconn/OSIROOT/spool/f00000*	Temporary files used to store messages if the message is larger than the size of the record in the message database.
/var/SUNWconn/OSIROOT/spool/p00000*	Temporary files used to store messages if the message is larger than the size of the record in the message database.
/var/SUNWconn/OSIROOT/spool/xomfil*	Temporary files used by the XAPIA library.
/var/SUNWconn/OSIROOT/spool/<*P1username*>/in_queue	Message queue access file for incoming messages.
/var/SUNWconn/OSIROOT/spool/<*P1username*>/out_queue	Message queue access file for outgoing messages.
/var/SUNWconn/OSIROOT/conf/<*process*>.init	Messages sent to the specified process during initialization.
/var/SUNWconn/OSIROOT/conf/<*process*>.msg	Messages returned by the specified process during initialization.
/var/SUNWconn/OSIROOT/conf/xom.ini	Configuration file used by the XAPIA library.
/var/SUNWconn/OSIROOT/conf/xmh.ini	Configuration file used by the XAPIA library.
/var/SUNWconn/OSIROOT/conf/osiam_op.data	Binary file containing a record of all running OSIAM and gateway processes.
/var/SUNWconn/osinet/osilogd.log	Log file, contains logged messages, events, errors, and trace information.

1. The message queue file (msg) can become large and may create problems for your system if stored in /var. You can create a symbolic link to another directory where this large file size would not cause a problem. Make sure that this linked directory allows full access rights, for example, by using chmod 777.

2

Configuring Your Local MTA 3

This chapter describes how to use `x400tool` to specify the global domain identifier for your local message transfer agent (MTA) and how to set advanced configuration features, if required. It assumes that you have already started `x400tool` and are familiar with its menu system. Refer to Chapter 2, “Starting and Using x400tool” for detailed instructions.

Your local MTA handles the routing and relaying of electronic messages between user agents (application programs) and remote MTAs. It is the hub through which all messages pass through your local message transfer system. Your local MTA is only able to communicate directly with the other agents defined within your message transfer system map.

When you start `x400tool` for the first time your message transfer system map shows a default configuration for your local MTA. You must modify this default configuration to add specific information for your own local MTA.

3

Basic Configuration

For a minimum configuration you must specify a name and a global domain identifier for your local MTA. In most cases, this will be sufficient to provide your local MTA with a unique identity within the global X.400 domain.

Specifying Your Local MTA Name

The local MTA name is used to identify the local MTA and is the name on which remote MTAs will base the acceptance of an association request when access control is enabled. It is not part of the X.400 address and is not used for routing messages.

You must give this name to other system administrators who want to add your local MTA to their message transfer systems.

To specify your local MTA name:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Type the name assigned to your local MTA on the Name input line.**
   You must enter a name of 16 characters or less.

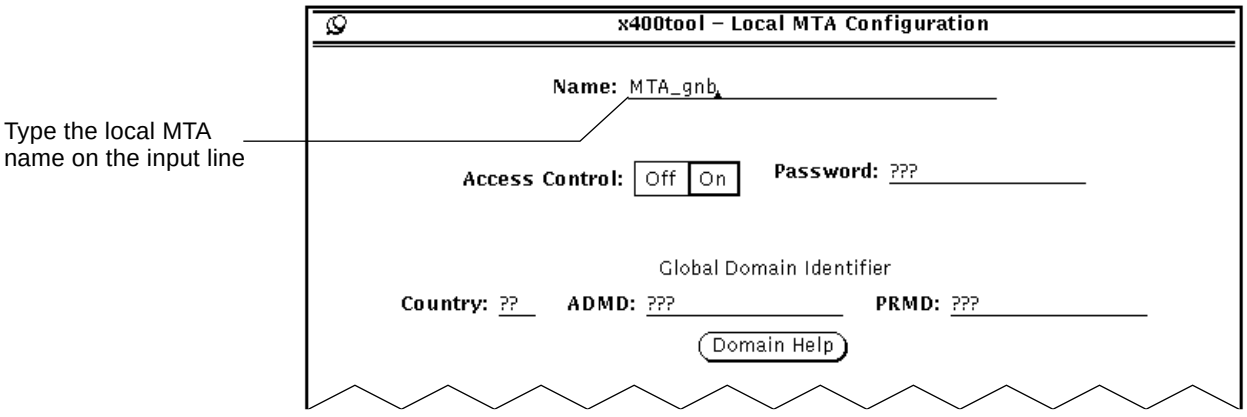


Figure 3-1 Specifying Your Local MTA Name

Setting an Access Control Password

The access control mechanism used to identify the message source is dependent upon the configuration of the both the local MTA *and* the remote MTA. Access control must be enabled or disabled for each remote MTA.

- The remote MTA configuration determines whether access control is enabled. See "Enabling and Disabling Access Control" on page 82 for detailed instructions.
- The local MTA configuration determines what is transmitted when access control is enabled. Access control can be based on the name of the initiating MTA only, or on the name *and* password of the initiating MTA.

The access control algorithm is summarized in Table 3-1. Note that this algorithm can be further modified by setting the advanced security parameters discussed in "Tuning the Security Options" on page 52.

Table 3-1 Access Control Algorithm

Local MTA	Remote MTA	Access Control
Access control OFF	Access control OFF	Access control DISABLED
Access control OFF	Access control ON	Local MTA name and null password
Access control ON	Access control OFF	Access control DISABLED
Access control ON	Access control ON	Local MTA name and true password

By default, the local MTA access control is set `ON`. Passwords must not contain more than 64 characters and must not contain spaces. If you do not set a password, a null password is transmitted.

You must give this password to other system administrators who want to add your local MTA to their message transfer systems.

To set your access control password:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT to disable or enable access restrictions, and enter a password (if required) as shown in Figure 3-2 on page 40.**
   If you set a password, it will be sent to all remote MTAs that have access control enabled.

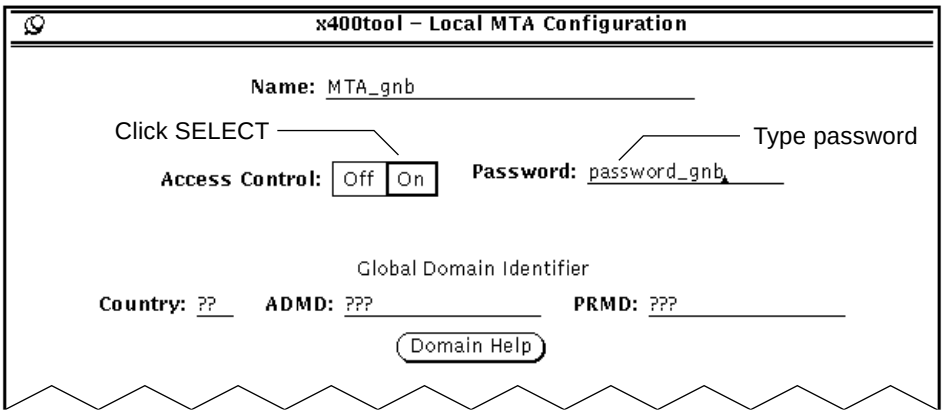


Figure 3-2 Setting an Access Control Password for the Local MTA

Specifying Your Global Domain Identifier

The global domain identifier locates your local MTA within the global X.400 domain. It consists of a country code, an ADMD, and an optional PRMD. Refer to “X.400 Management Domains” on page 6 for a more detailed description of the global domain identifier.

You must give this global domain identifier to other system administrators who want to add your local MTA to their message transfer systems.

To specify the global domain identifier for the local MTA:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Enter the global domain identifier for your local MTA as shown in Figure 3-3 on page 41.**

- Type a country code and PRMD. If necessary use the domain help to locate this information. If your local MTA does not require an ADMD in its X.400 address, enter a space on the ADMD input line.
- Type your PRMD on the input line. If your local MTA is not part of a PRMD, you can leave a null PRMD entry. Do not insert a space.

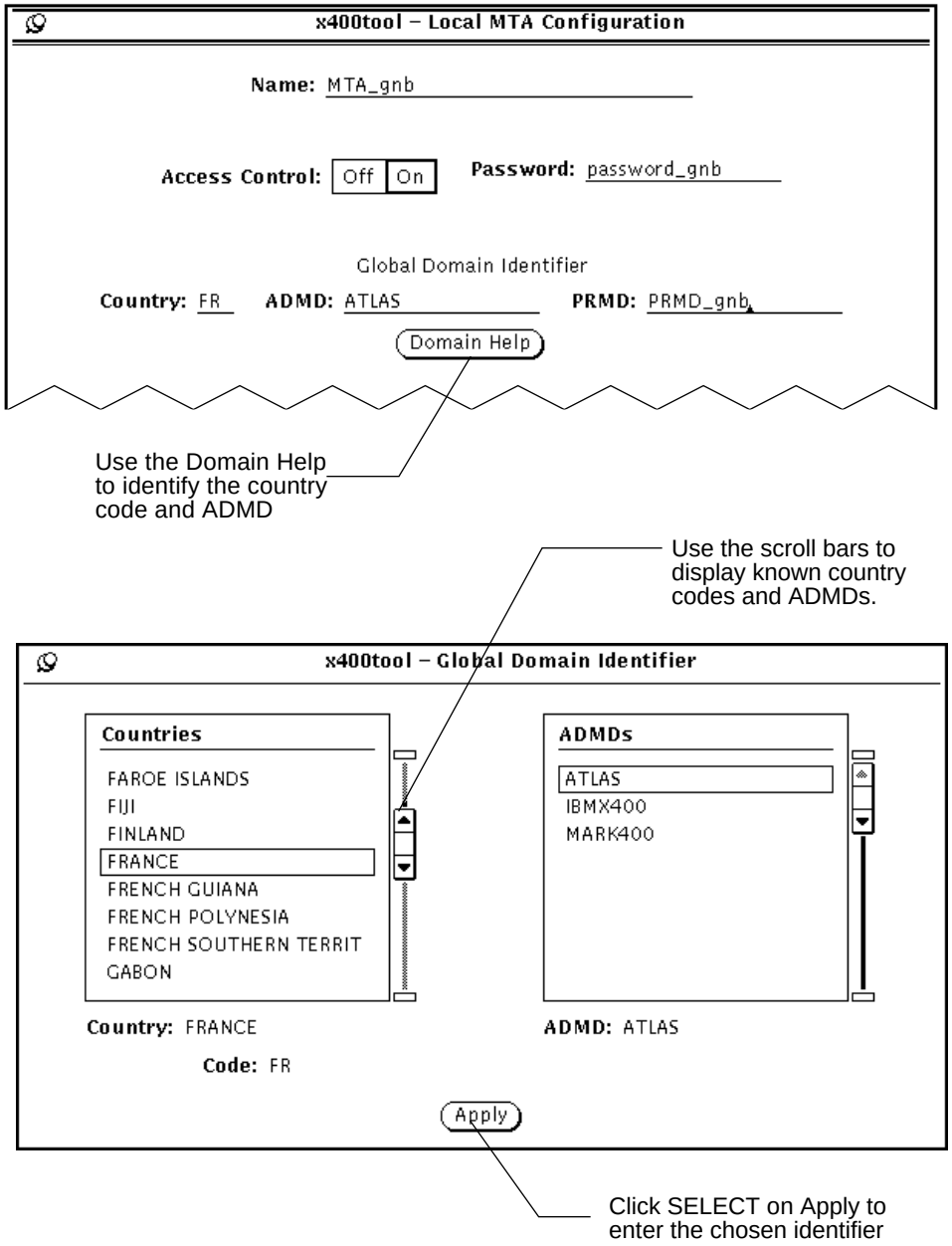


Figure 3-3 Specifying the Global Domain Identifier for the Local MTA

3

OSI Addressing Information

The Local MTA Configuration window displays the OSI addresses by which the local MTA can be reached.

Note – This information is based on the running stack configuration and cannot be modified from within `x400tool`. (Refer to the *SunLink OSI Communication Platform Administrator's Guide* for detailed instructions on how to configure your stack.)

You must give the OSI address of your local MTA to other system administrators who want to add it to their message transfer systems.

The local MTA can be attached to the X.400 domain through four network interfaces:

- X.25 (for X.25 1980)
- TCP/IP (RFC 1006)
- LLC1 (LAN—for example, Ethernet)
- CONS (for X.25 1984)

The OSI address for your local MTA is dependent on how your machine is physically connected to the OSI network. Your local MTA may be reached through multiple network connections; however, each remote MTA will recognize only one connection. If you want to communicate through multiple network connections you must define multiple remote MTAs—at least one remote MTA for each network connection.

This scrolling-list displays the sub-network connection that is configured in the OSI stack configuration and indicates the transport layer connection. Note that for X.25 1980 connections, the network address is an X.121 network address, and for CONS X.25 1984 connections, the network address is an NSAP address.

For example:

If your local MTA is attached to the X.400 domain through an X.25 (1980) interface and a TCP/IP (RFC 1006) interface, follow these steps:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**

2. **Choose** `X.25 - Service Access Point 62` **from the scrolling-list.**
   The information displayed is recovered from the running stack configuration. You must give this OSI address to system administrators who want to connect to your local MTA over the X.25 interface.

3. **Choose** `TCP/IP - Service Access Point 262` **from the scrolling-list.**
   The information displayed is recovered from the running stack configuration. You must give this OSI address to system administrators who want to connect to your local MTA over the TCP/IP interface.

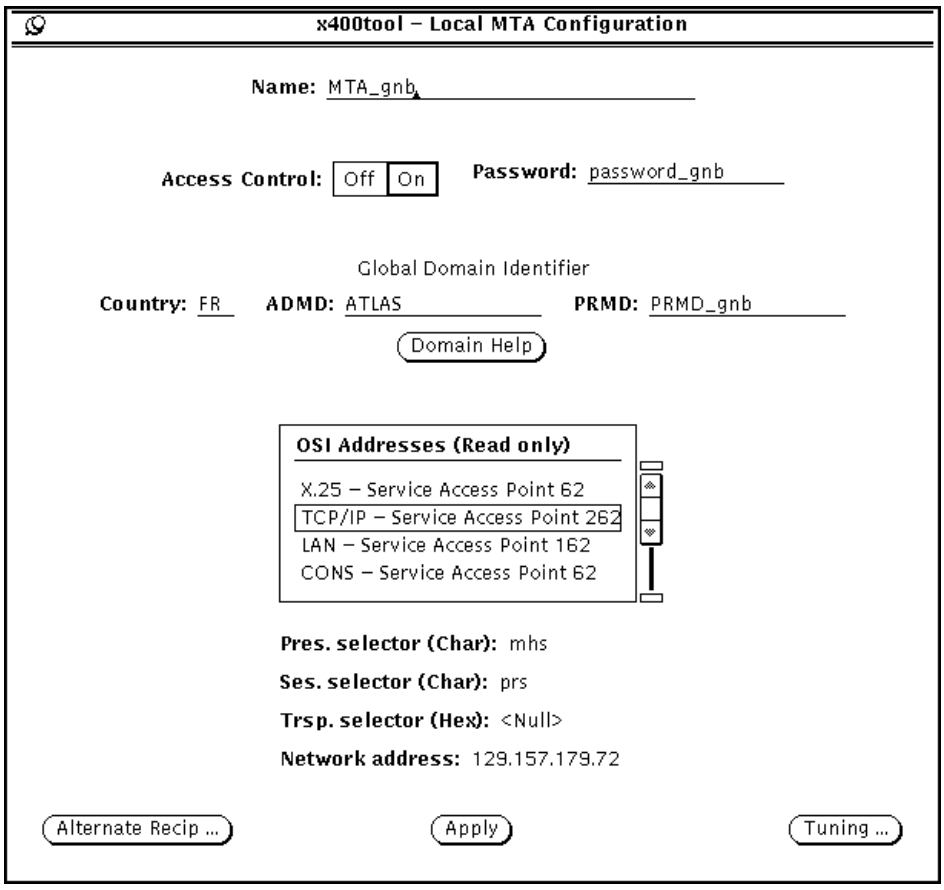
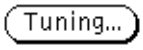


Figure 3-4 OSI Addressing Information for the Local MTA

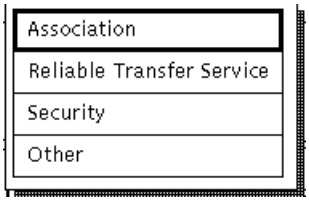
Once you have completed the basic configuration steps described in this section, apply your local MTA configuration by clicking SELECT on the Apply button.

Advanced Configuration

The advanced configuration options for your local MTA are used to define the relationship between the local MTA and the remote MTAs in the local message transfer system. In particular, they are used to set the thresholds at which certain events occur. These features are optional and your local MTA should operate correctly using the default values for these parameters.



Tuning the Basic Association Options



An association is like a connection between two MTAs. Once an association is established, it is maintained until either there are no more messages waiting to be exchanged between the two MTAs, or one of the predefined thresholds is reached.

To modify the basic behavior of associations between your local MTA and the remote MTAs in your message transfer system, follow these steps:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Tuning... button.**
3. **Press and drag MENU on the Tuning pull-down menu, and release MENU over the Association item.**
4. **Press and drag SELECT on the sliders to change the thresholds and time-outs as shown in Figure 3-6 on page 46.**
   You can also type the values directly on the input line for each option.

Basic Association Options

The local MTA is able to open associations as required until a set (non-configurable) maximum number is reached. As the total number of current associations approaches this limit, the local MTA enters a *shortage condition*.

Your local MTA reacts to a shortage condition by trying to share its resources equally between the other agents in the message transfer system as shown in Figure 3-5. During a shortage condition, the local MTA closes associations automatically when the *sent data* or *sent messages* thresholds are reached.

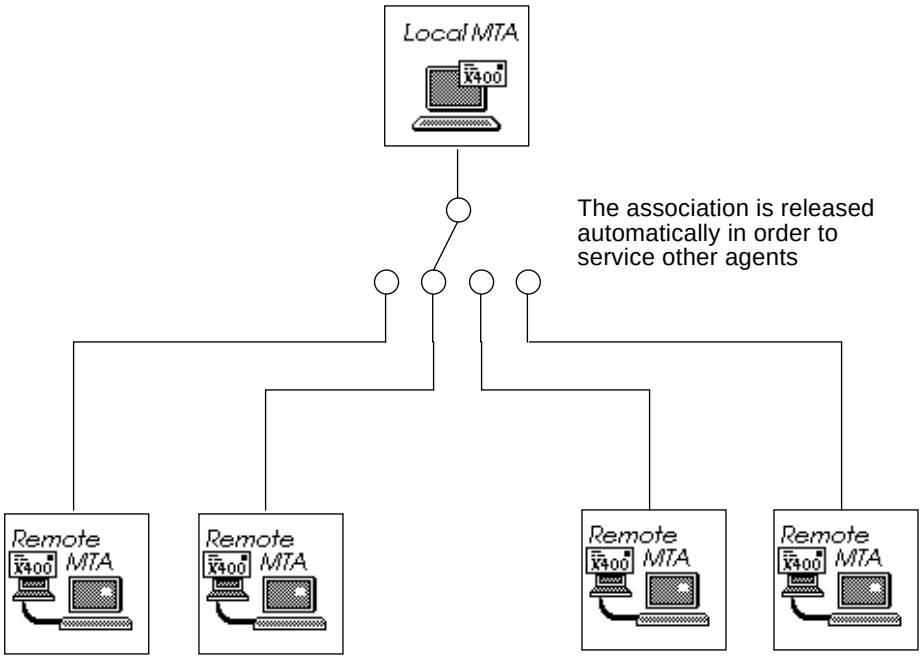


Figure 3-5 Resource Sharing During a Shortage Condition

Sent Data Threshold: Defines the maximum quantity (in *10 Kbytes) of data sent over a single association before the association is closed automatically. This threshold is applied only when there is a high demand for associations (shortage condition).

Sent Message Threshold: Defines the maximum number of messages sent over a single association before the association is closed automatically. This threshold is applied only when there is a high demand for associations (shortage condition).

Retry Connection Timeout: Defines the delay between a failed association attempt and the next retry.

Idle Association Timeout: Defines the maximum amount of time that an association is allowed to remain idle (no messages transmitted) before the association is closed automatically.

Recovery Attempts Delay: Defines the delay between a failed message delivery attempt and the start of the recovery process initiated by the local MTA (outgoing messages).

Association Retention Timeout: Defines the maximum delay permitted between a failed message delivery attempt and the start of the recovery process initiated by the remote MTA (incoming messages).

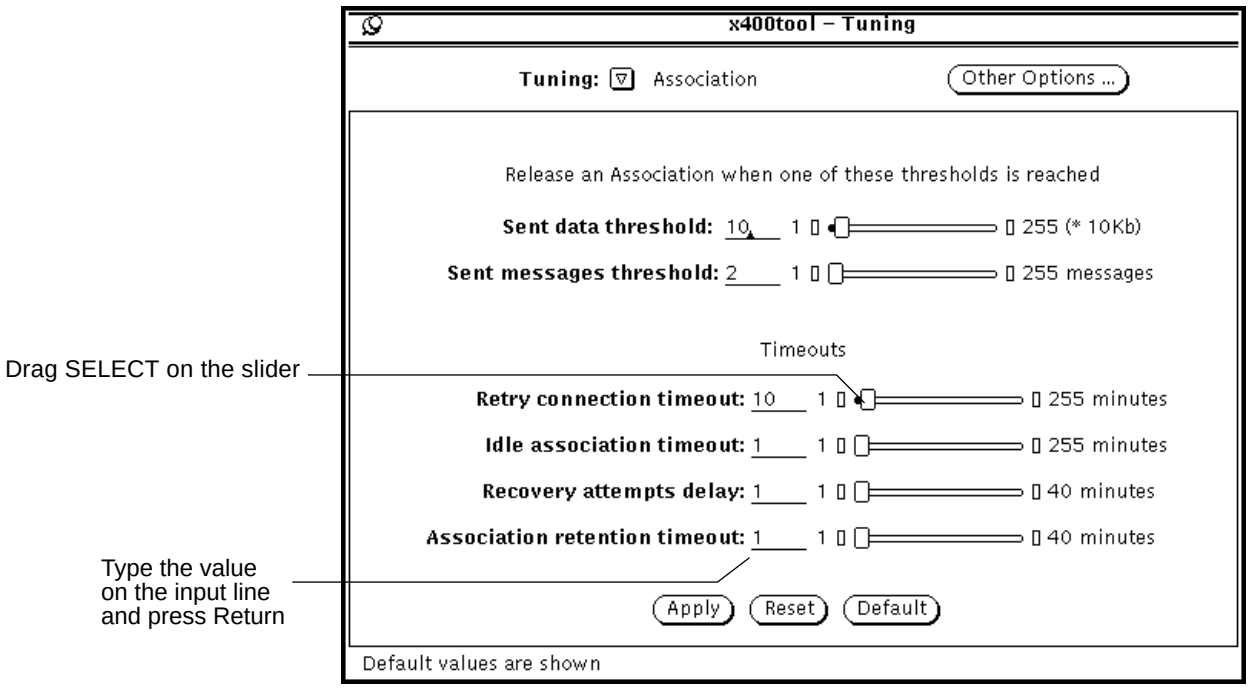


Figure 3-6 Tuning the Association Thresholds

Apply

Once you have finished tuning the basic association options described in this section, apply your configuration by clicking SELECT on the Apply button.

Tuning...

Tuning the Other Association Options

Other Options ...

There are three queues associated with each remote MTA defined in the message transfer system. Messages that are waiting to be sent to a remote MTA are placed in one of its queues according to the priority (non-urgent, normal, or urgent) assigned in the message header. (See “Defining a Custom Mail Header” on page 125 for instructions on assigning the priority to a message using `mailtool`.)

The Other Options are used to define the conditions under which the local MTA will open another association with a remote MTA. For outgoing messages, the local MTA bases its decision on the number of messages in each queue and the time that messages have spent in the queue.

You can also define the algorithm used to determine the priority assigned to a remote MTA when it requests an association for an incoming message. When the local MTA receives a number of simultaneous association requests it accepts the request from the remote MTA with the highest priority first.

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Tuning... button.**
3. **Press and drag MENU on the Tuning pull-down menu, and release MENU over the Association item.**
4. **Click SELECT on the Other Options... button.**
5. **Press and drag SELECT on the sliders to change the thresholds and the MTA priority as required.**
   You can also type the values directly on the input line for each option. In this case, you must press Return to enter each typed value into the database.

Association Thresholds Based On Number of Messages in the Queue

Urgent Messages: Defines the total number of messages that must be waiting in the urgent (high-priority) queue before an association is opened with the remote MTA.

Normal Messages: Defines the total number of messages that must be waiting in the normal (unspecified-priority) queue before an association is opened with the remote MTA.

Non-Urgent Messages: Defines the total number of messages that must be waiting in the non-urgent (low-priority) queue before an association is opened with the remote MTA.

Total Number of Messages: Defines the total number of messages that must be waiting in all three queues (urgent, normal, and non-urgent) before an association is opened with the remote MTA.

Figure 3-7 shows the default values assigned to these thresholds:

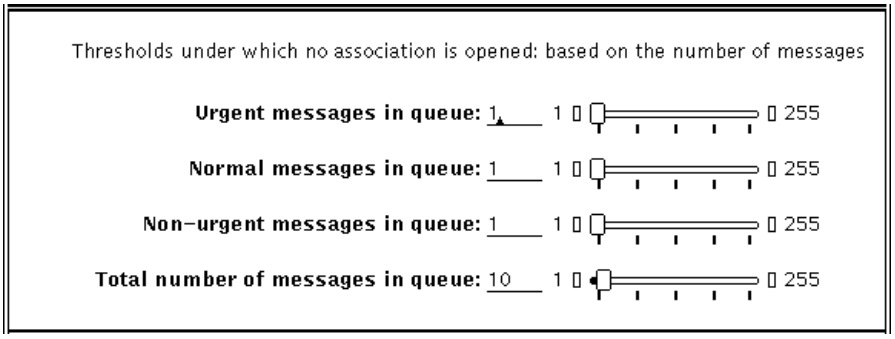


Figure 3-7 Association Thresholds Based On Number of Messages

Association Thresholds Based On Time Spent in the Queue

Timer Unit: Defines the multiplier used to determine the other thresholds in this category.

Urgent Queue Stay-Time: Defines the maximum time (stay-time *x* timer unit) that messages are allowed to spend in the urgent (high-priority) queue before an association is opened.

Normal Queue Stay-Time: Defines the maximum time (stay-time *x* timer unit) that messages are allowed to spend in the normal (unspecified-priority) queue before an association is opened.

Non-Urgent Queue Stay-Time: Defines the maximum time (stay-time *x* timer unit) that messages are allowed to spend in the non-urgent (low-priority) queue before an association is opened.

Figure 3-8 on page 49 shows the default values assigned to these thresholds:

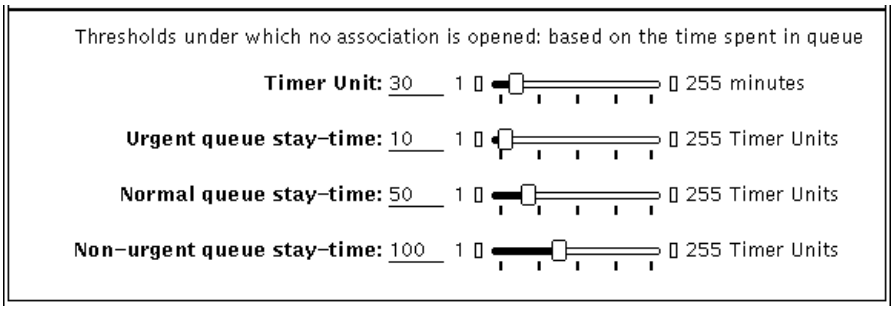


Figure 3-8 Association Thresholds Based On Time Spent in Queue

Remote MTA Association Priority Options

These options define the relative importance of the factors used to determine the priority assigned to a remote MTA when it requests an association. Three factors are considered, the number of messages waiting in the queue, the size of the messages, and the time the messages spend in the queue.

Number of Messages: Defines the multiplier applied to the number of messages waiting in the queue.

Size of Messages: Defines the multiplier applied to the size of the messages waiting in the queue.

Time Spent in Queue: Defines the multiplier applied to the time messages have spent in the queue.

Figure 3-9 shows the default values assigned to these options:

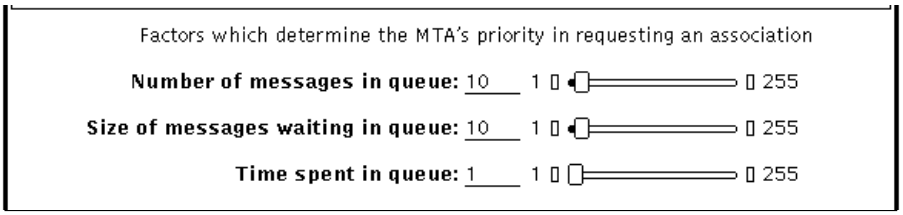
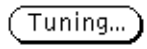
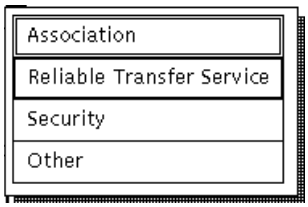


Figure 3-9 Remote MTA Association Priority

Once you have finished tuning the Other association options described in this section, apply your configuration by clicking SELECT on the Apply button.



Tuning the Reliable Transfer Service



The Reliable Transfer Service (RTS) is used to ensure the safe delivery of messages. To tune the reliable transfer service:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Tuning... button.**
3. **Press and drag MENU on the Tuning pull-down menu, and release MENU over the Reliable Transfer Service item.**
4. **Modify the Reliable Transfer Service options shown in Figure 3-10 on page 51.**

Reliable Transfer Service Options

RTS Inactivity Timeout: Defines the maximum delay allowed between the opening of an association and the start of activity. If no activity occurs within this specified delay, the association is closed automatically.

Checkpoint Size: Regular synchronization marks (or checkpoints) are normally sent during message transmission. This allows the RTS to recover broken messages from the last checkpoint received. The checkpoint size (the amount of data sent between checkpoints) is a negotiated parameter proposed by the association initiator.

- **Initiator Checkpoint Size:** Defines the checkpoint size proposed by your local MTA for outgoing messages.
- **Acceptor Checkpoint Size (if proposed=0):** Defines the checkpoint size for incoming messages if there is no checkpoint size proposed by the remote MTA.
  - If you set this value to 0, your local MTA will accept associations that do not use synchronization.
  - If you set this value to >0, then your local MTA will propose this checkpoint size to the remote MTA. The remote MTA may choose to reject the proposal.
- **Acceptor Checkpoint Size (if proposed>0):** Defines the maximum checkpoint size for incoming messages accepted by your local MTA. The checkpoint size proposed by the remote MTA will be used unless it exceeds this value.

Minor Synchronization: When minor synchronization is enabled, minor (intermediate) checkpoints are generated between the standard checkpoints.

- **Minor Sync. Window Size:** Defines the amount of data sent between minor checkpoints.

Required Session Version: Defines the session layer protocol version required by the local MTA for all incoming messages. This may be version 1 only, or both version 1 and 2. For sessions with a remote 1988 system, you should set this option to both version 1 and 2.

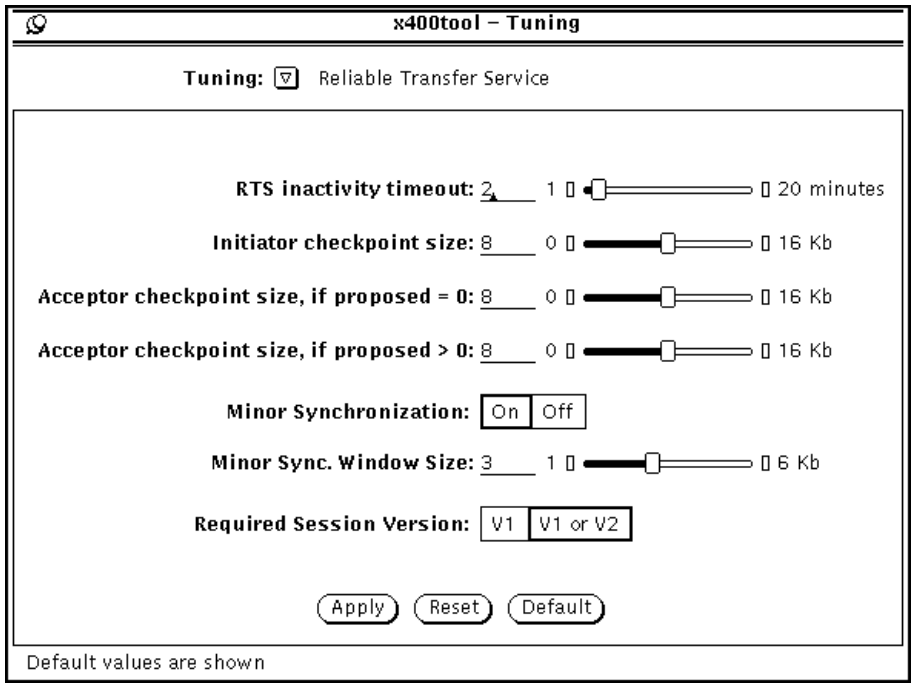
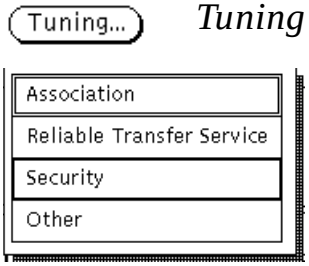


Figure 3-10 Tuning the Reliable Transfer Service

Apply

Once you have finished tuning the Reliable Transfer Service options described in this section, apply your configuration by clicking SELECT on the Apply button.



Tuning the Security Options

The security options are used to modify the basic access control mechanism. Refer to “Setting an Access Control Password” on page 39 and “Enabling and Disabling Access Control” on page 82 for detailed instructions on enabling and disabling access control for each remote MTA.

To tune the security options:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Tuning... button.**
3. **Press and drag MENU on the Tuning pull-down menu, and release MENU on the Security item.**
4. **Press and drag MENU on the MTA connection validation pull-down menu and release MENU over the desired validation system as shown in Figure 3-11.**
   This option determines which elements the local MTA uses to check the source of incoming messages during the association negotiation phase. The local MTA refuses associations that fail to provide the expected parameters.

   Check address: The local MTA checks the OSI address elements only.

   Check name: The local MTA checks the name only.

   Check address and name: The local MTA checks both the name and the OSI address elements.

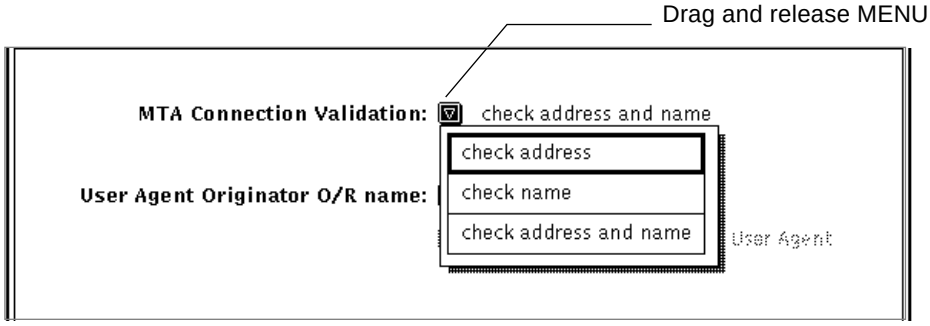


Figure 3-11 Setting the MTA Connection Validation

5. **Click SELECT on the check boxes to define the restrictions placed upon the originator/recipient (O/R name) that identifies the user agent that sent the incoming message.**
   When a message is submitted by a user agent, the local MTA verifies the originator O/R address and applies the routing algorithm defined by the entries in its routing table.

- If you check “must be local” then the originator O/R address must match an entry in the routing table used by the local MTA, and this entry must point to a local user agent.
- If you check “must belong to requesting agent” then the originator O/R address must match an entry in the routing table used by the local MTA. The matching entry must be associated with the user agent that submitted the message.

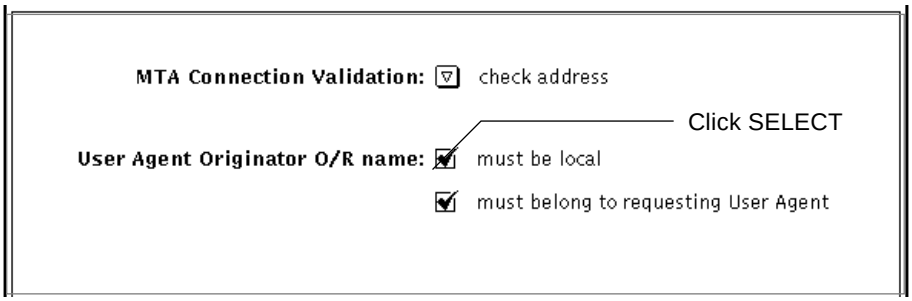
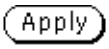
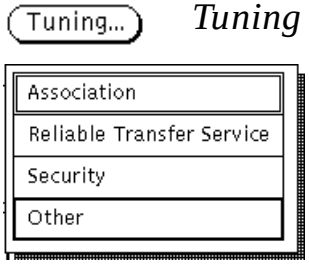


Figure 3-12 Specifying the Restrictions Placed on the O/R Name



Once you have finished tuning the Security options described in this section, apply your configuration by clicking SELECT on the Apply button.



Tuning the Other Options

The Other configuration options are used to define the type of report requested by the local MTA for outgoing messages, the time tolerance for trace information, and the congestion thresholds applied to the spool file system.

To tune the Other configuration options:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Tuning... button.**
3. **Press and drag MENU on the Tuning pull-down menu, and release MENU over the Other item.**
4. **Press and drag MENU on the Report Request pull-down menu and release MENU to define the type of report requested by outgoing messages as shown in Figure 3-13.**
   There are three types of reports that may be requested by a user agent when sending messages to the local MTA:

   Basic: Non-delivery report requested—unconfirmed delivery.

   Confirmed: Delivery and non-delivery reports requested.

   Audit and Confirmed: Delivery and non-delivery reports requested. Trace information for the delivered message is also requested.

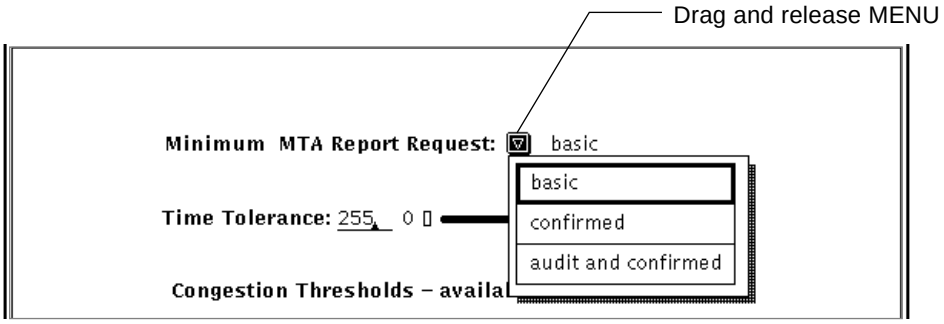


Figure 3-13 Defining the Report Request

5. **Drag SELECT on the slider (or type in the value on the input line) to define the Time Tolerance as shown in Figure 3-14.**
   This is the tolerance (error margin) applied to all timer values checked by the local MTA—for example, trace information. Altering this parameter can help accommodate problems that occur when MTAs that have their clock or time zone set incorrectly. Messages that claim to have been sent before they arrived are normally rejected as errors; however, you can increase the tolerance within which your local MTA will ignore this discrepancy.

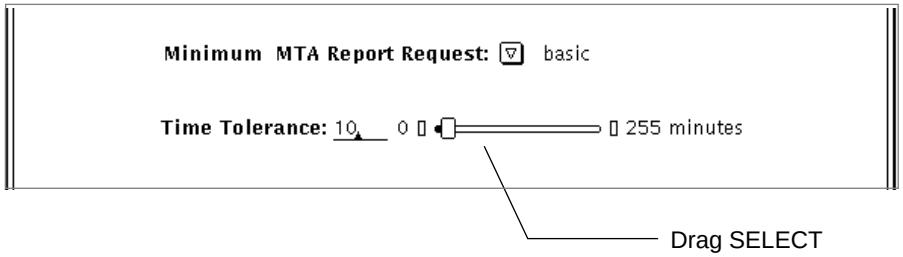


Figure 3-14 Defining the Timer Tolerance

6. **Click SELECT on the increment/decrement buttons (or type the value on the input line) to define the congestion thresholds as shown in Figure 3-15.**

   These thresholds determine whether your local MTA is in a normal, critical, or congested state. Depending on the amount of space remaining in your spool file system, your local MTA may refuse to accept further incoming messages. By default, your spool file system is located under `/var/SUNWconn/OSIROOT/spool`.

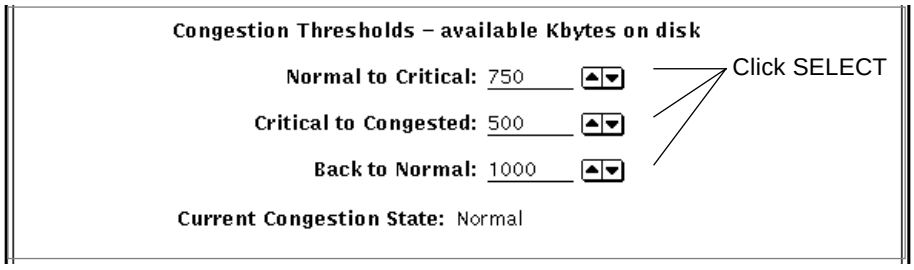


Figure 3-15 Tuning the Congestion Thresholds

Normal to Critical: Defines the disk space threshold (in Kbytes) at which your local MTA passes from a normal to a critical state. If you have less than this amount of disk space left in your spool file system, the situation is considered *critical* and the local MTA will limit the amount of incoming data.

Critical to Congested: Defines the disk space threshold (in Kbytes) at which your local MTA passes from a critical to a congested state. If you have less than this amount of disk space left in your spool file system, the situation is considered *congested* and the local MTA will refuse all incoming data.

Back to Normal: Defines the disk space threshold (in Kbytes) at which your local MTA passes from a critical or congested state, and returns to a normal state. You must have at least this amount of disk space left in your spool file system before your local MTA will lift the restrictions placed on incoming data.

When specifying values for these parameters, the relationship between the three thresholds should be:

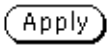
```
Back to Normal > Normal to Critical > Critical to Congested
```

Current Congestion State: Displays the current state of your spool file system.

Normal: All new incoming messages accepted.

Critical: No new incoming messages will be accepted. Incoming message transfers currently in progress will be accepted if possible.

Congested: No incoming messages will be accepted. Incoming message transfers currently in progress will be aborted.Once you have finished tuning the Other options described in this section, apply your configuration by clicking SELECT on the Apply button.



Specifying Alternate Recipients for User Agents

Note – This option is only applicable if you are adding third-party user agents (UAs) to your message transfer system. Refer to Chapter 6, "Adding Third-Party Agents" for detailed instructions.

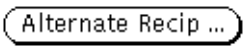
The Alternate Recipients window is used to define one or more alternate O/R addresses for each third-party user agents in your message transfer system. These O/R addresses are used by the local MTA in the event that it cannot route a message to the user agent defined by the O/R address contained in the message.

For example:

If the message contains a body part of a type that is not supported by the user agent specified by the O/R address in the message, the local MTA will forward the message to the alternate recipient address if one is defined.

Refer to "Defining the Alternate Recipient for a User Agent" on page 116 for detailed instructions on how to assign an alternate recipient for a given user agent by modifying the local routing table.

Creating a List of Alternate Recipients



You can define one or more alternate recipients for your local MTA. You must choose from this list of recognized addresses when you assign an alternate recipient for a third-party user agent. Refer to "Defining the Alternate Recipient for a User Agent" on page 116 for detailed instructions.

To create a list of alternate recipients:

1. **Double-click SELECT on the local MTA icon to activate the Local MTA Configuration window.**
2. **Click SELECT on the Alternate Recipients button to activate the Alternate Recipients window.**
3. **Type in the full O/R address of an alternate recipient.**
4. **Click SELECT on Add to create a new alternate recipient address in the list, or click SELECT on Update to modify the currently selected address.**

Figure 3-16 shows a list of alternate recipients for the local MTA. The alternate recipient is usually a system administrator, or someone charged with ensuring that the redirected message reaches its ultimate destination.

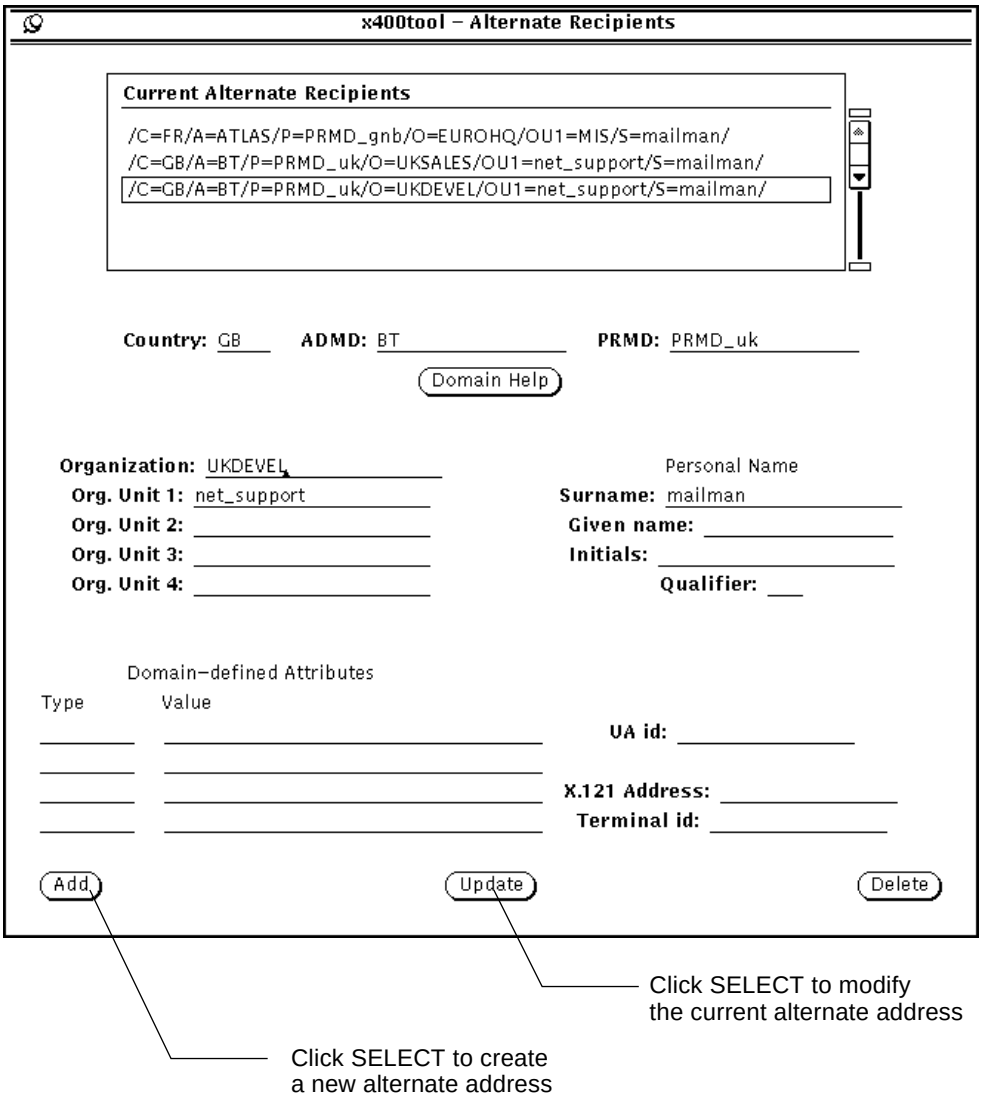
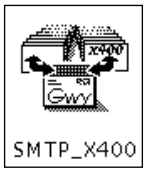


Figure 3-16 Creating a List of Alternate Recipients

Configuring an X.400/SMTP(MIME) Gateway 4

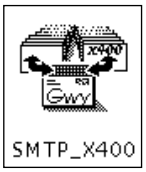


This chapter describes how to use `x400tool` to set up an X.400/SMTP(MIME) gateway to handle the exchange of messages between UNIX mail applications and the X.400 domain. It assumes that you have already set up your local message transfer agent (MTA) as described in Chapter 3, “Configuring Your Local MTA”.

The X.400/SMTP(MIME) gateway is provided as part of the SunLink X.400 8.0.2 and is an implementation of RFC1327. It maps UNIX mail (RFC 822) addresses and service elements to equivalent X.400 addresses and service elements, and adds any additional information required to route messages across the global X.400 domain. The X.400/SMTP(MIME) gateway can be configured to support MIME-compliant attachments. It incorporates features of Sun-specific mail, including international character set support and Sun multimedia attachments.

4

Basic Configuration



Note that there is an unconfigured X.400/SMTP(MIME) gateway in your message transfer system by default when you first start `x400tool`.

The X.400/SMTP(MIME) Configuration window is used to define how electronic messages are exchanged between UNIX mail applications (such as `mailtool`) and your local MTA. In particular, it is used to define the UNIX mail domain address and pseudo host name that will be used by the `sendmail` daemon to route UNIX mail messages to the X.400/SMTP(MIME) gateway.

Refer to "X.400/SMTP(MIME) Gateway" on page 13 for a detailed description of how the gateway works.

Determining Your Local UNIX Domain Address

Your UNIX mail domain address is roughly equivalent to an X.400 global domain identifier. It locates the machine on which your gateway is running within the global UNIX mail address space. A typical UNIX mail domain name looks like this:

```
Division.Company.COM
```

Your local UNIX mail domain address is defined within the `sendmail` configuration file (`/etc/mail/sendmail.cf`) located on your mail host (or on your mail server if you are remotely mounting your `/var/mail` directory).

A mail host is a machine that is designated as the primary mail machine on your network. This is the machine that receives mail from outside your local domain; it is also the machine that receives mail that the local domain cannot deliver.

A mail server is a machine that stores mailboxes for client machines (in `/var/mail`). When mailboxes are located on a mail server, messages are first delivered to the mail server, and not directly to the client machine.

Refer to Chapter 8, "Understanding Mail Services" in your Solaris *Setting Up User Accounts, Printers, and Mail* for a detailed description of the components of a UNIX mail system and the addresses used to route messages between them.

To determine the UNIX domain address for your local machine:

- **If** `/var/mail` **is mounted remotely, determine the name of your mail server**:

```
hostname% mount | grep spool
/tmp_mnt/var/spool/mail on <mail_server>:/var/spool/mail <datestamp>
```

  If `/var/mail` is mounted remotely, the mount point displayed with the name of the mail server (<*mail_server*>). This is where you will find your local UNIX domain address.

- **If your** `/var/mail` **is located on your own machine, determine the name of your mail host**.

```
hostname% ypmatch mailhost hosts
129.123.123.12  <mail_host> mailhost
```

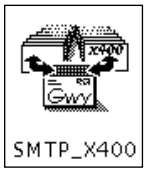
  The name of the mail host (<*mail_host*>) follows the IP address. This is where you will find your local UNIX domain address.

- **Look for your UNIX domain name in the** `sendmail` **configuration file on either your** *mail server* **(if your mailbox is mounted remotely) or on your** *mail host* **(if your mailbox is mounted locally)**.
  - On machines running Solaris 2.x, this file is called `/etc/mail/sendmail.cf`.
  - On machines running Solaris 1.x, this file is called `/etc/sendmail.cf`.

```
hostname% more /etc/mail/sendmail.cf | grep Dm
# appear in you mail headers, add a "Dm" line to define your domain name
# The Dm value is what is used in outgoing mail. The Cm values are
# accepted in incoming mail. By default Cm is set from Dm but you might
# DmCS.Podunk.COM
Dm<local_domain_address>
```

  Make a note of the local UNIX domain address (<*local_domain_address*>) in the last line of text. You will need to know this when configuring your gateway.

You can use `x400tool` to show you how this address is converted to an X.400 address in the gateway (see “Testing the X.400/SMTP(MIME) Gateway” on page 69).



Configuring the X.400/SMTP(MIME) Gateway

The X.400/SMTP(MIME) Configuration window shown in Figure 4-1 is used to define the way in which messages and addresses are mapped between UNIX mail and X.400 mail applications. It is also used to define the UNIX domain address and pseudo host name that `sendmail` uses for routing electronic messages to the gateway.

To configure the X.400/SMTP(MIME) gateway:

1. **Double-click SELECT on the SMTP_X400 icon to activate the X.400/SMTP Configuration window shown in Figure 4-1.**

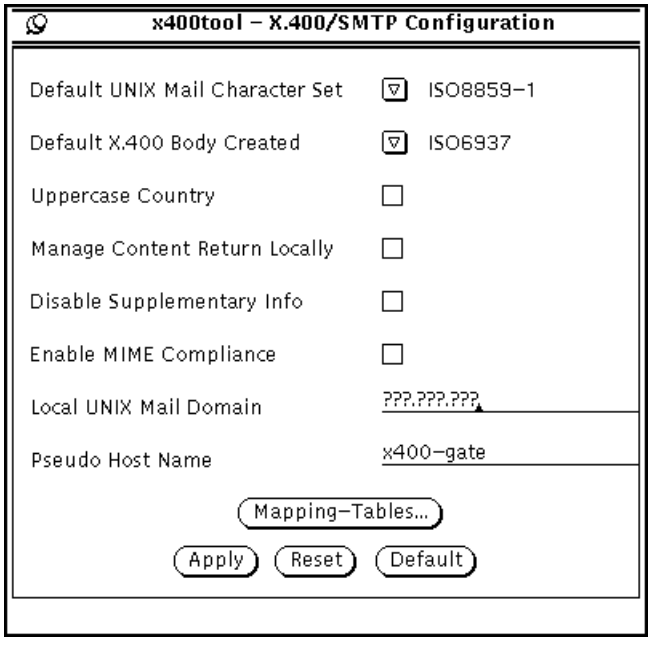
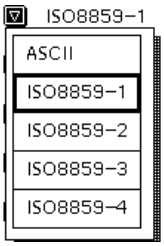
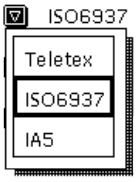


Figure 4-1 The X.400/SMTP Configuration Window





2. **Drag and release MENU to define the default character set that is used to map between UNIX mail and X.400 mail body parts (the content of the message).**
   Note that the ASCII character set does not support international (8-bit) characters. International characters are represented by the nearest ASCII (7-bit) character. The default value is ISO8859-1.

3. **Drag and release MENU to define the default body type created when a message that contains international characters is received from UNIX mail.**
   Under most circumstances, you should choose the default value of ISO6937 as the default body type. ISO6937 provides full IA5 (ASCII) and Teletext (T61, a subset of ASCII) character support, and also supports international (8-bit) characters. If ISO6937 is enabled, but the message does not contain 8-bit characters, an IA5 (7-bit) body part is created automatically.

4. **Click SELECT on Uppercase Country, as shown in Figure 4-2, to convert country codes contained in X.400 addresses to uppercase characters.**
   Some ADMDs (such as ATLAS in France) require that country codes always be in uppercase. If this option is enabled, the X.400/SMTP(MIME) gateway automatically converts any lowercase country codes to uppercase characters.

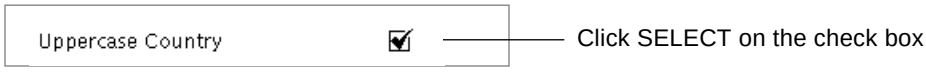


Figure 4-2 Enforcing Uppercase Country Codes

5. **Click SELECT on Manage Content Return Locally, as shown in Figure 4-3, to preserve the content of failed deliveries.**
   By default, your gateway requests negative-delivery reports and content return for the messages it sends to the message transfer system. The negative-delivery report normally contains the content of the original message; however, the only way to guarantee this is to set Manage Content Return Locally. This preserves a local copy of an outgoing message until a positive-delivery report is received.

Note – This facility can be costly, in terms of both disk space and network charges imposed by ADMDs. The file system used by the local MTA to spool messages can fill with local copies of outgoing messages that are only deleted when a positive-delivery report is received. In addition, you may be charged for the return of positive-delivery reports by some ADMDs.

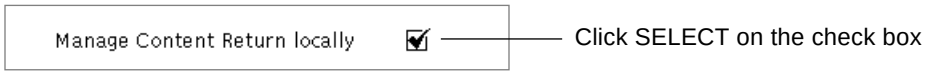


Figure 4-3 Enabling Local Content Return Management

6. **Click SELECT on Disable Supplementary Info, as shown in Figure 4-4, to prevent the gateway from providing supplementary information when it generates a non-delivery report.**
   The gateway provides the reason for the failed delivery (generated by `sendmail`) in a supplementary information field in the non-delivery report. Some ADMDs (such as ATLAS in France) do not support this field.

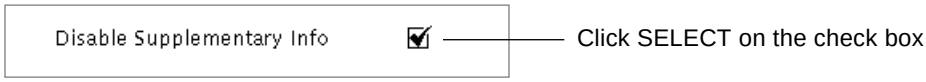


Figure 4-4 Disabling Supplementary Info

7. **Click SELECT on Enable MIME Compliance, as shown in Figure 4-5, if the gateway is to convert X.400 messages into MIME-compliant messages.**
   If this feature is enabled, incoming messages from the X.400 domain are converted to be MIME-compliant when they are output to UNIX mail.

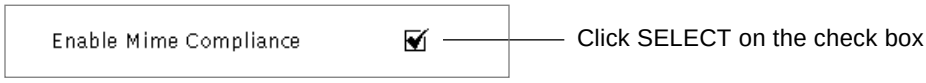


Figure 4-5 Enabling MIME Compliance

8. **Enter the local UNIX domain address for the gateway as shown in Figure 4-6.**
   This is the domain name that you recovered from the `sendmail.cf` file on your mail host or mail server. See "Determining Your Local UNIX Domain Address" on page 60 for detailed instructions.

Figure 4-6 Entering your UNIX Domain Name

9. **Enter the pseudo host name that will be used to route messages from UNIX mail applications to the gateway as shown in Figure 4-7.**
   Use the default pseudo name `x400-gate`, proposed by `x400tool`, or enter your own pseudo host name for the gateway. The UNIX mail daemon (`sendmail`) that runs on this machine will route all messages identified by the pseudo host name to the X.400/SMTP(MIME) gateway.

   The pseudo host name must be entered in the `/etc/hosts` file on your NIS server (or on your local machine if you are not running NIS) as an alias of the machine running the gateway. If you modify the default pseudo host name, the change must also be registered in the `sendmail.cf` file on your mail host (if `/var/mail` is located locally) or on your mail server (if `/var/mail` is located remotely).

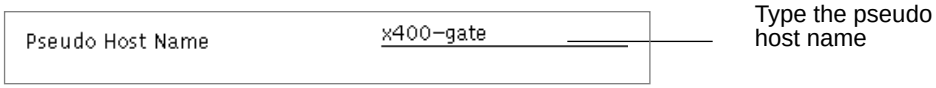
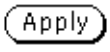


Figure 4-7 Entering the Pseudo Host Name



Once you have completed the basic configuration steps described in this section, apply your X.400/SMTP(MIME) gateway configuration by clicking SELECT on the Apply button.

If you modified the default pseudo host name you will see the message shown in Figure 4-8. It warns you that you must modify the `sendmail.cf` file on your local machine. Click SELECT on one of the buttons to modify this file or leave it unmodified. If you do not authorize `x400tool` to modify this file, you must edit it manually to change the pseudo host name for your gateway.

If you have a standard `sendmail.cf` file, then you can normally allow the `sendmail.cf` file to be changed automatically.

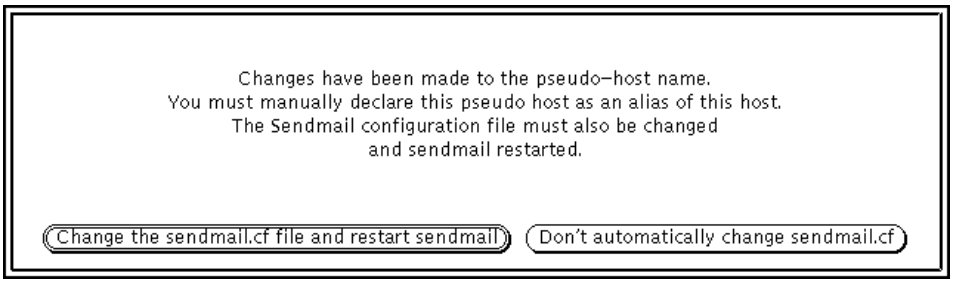


Figure 4-8 Modifying `sendmail.cf`

Adding the Pseudo Host Name to the NIS Database

The pseudo host name is an alias for the machine on which the gateway is running. To enter the pseudo host name into the name service (NIS, NIS+, DNS, etc.) database:

1. **Edit the `/etc/hosts` file on your NIS server (or on your local machine if you are not running NIS) and add the pseudo host name for the gateway.** This creates an alias for the machine on which the gateway is running. Add the pseudo host name to the line where the primary IP address and host name for your local machine is defined:

```
<IP address>  <localhost>  <pseudo hostname>
```

For example:

If the host name for your local machine (the machine on which the gateway is running) is `papyrus`, and you accepted the default pseudo host name proposed by `x400tool` (`x400-gate`), the entry in `/etc/hosts` would be:

```
<IP address> papyrus x400-gate
```

2. **If you are running NIS, you need to build a new NIS database that includes the pseudo host name for the gateway.**

```
hostname# cd /var/yp
hostname# make
```

3. **Verify that the pseudo host name for the gateway is registered in the Name Service database correctly by doing a** `ypmatch(1)`:

```
hostname# ypmatch <pseudo hostname> hosts
<IP address> <localhost> <pseudo hostname>
```

Modifying sendmail.cf

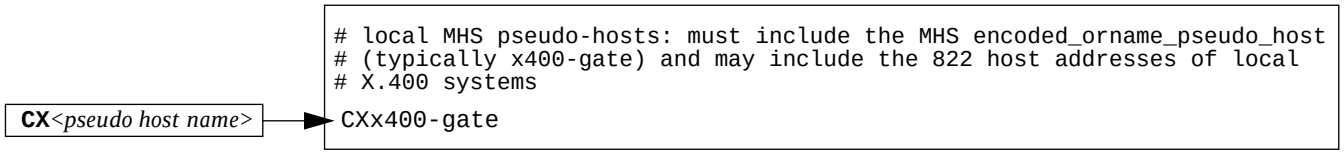
If you changed the default pseudo host name, you need to register this change in `/etc/mail/sendmail.cf` on your local machine. If you did not authorize `x400tool` to make this change, you must edit the file manually.

To modify `sendmail.cf`:

1. **Log in as root, or become superuser, and use a screen editor such as** `vi`**, to edit the file** `/etc/mail/sendmail`**.**

```
hostname# vi /etc/mail/sendmail.cf
```

2. **Search for the text string** `CXx400-gate` **and replace the default pseudo host name (the text after** `CX`**) with the pseudo host name you assigned for your gateway.**



3. **Save your modifications (overriding the read-only protection) and exit the screen editor.**

4. **Recover the process id (**<*pid*>**) for the** `sendmail` **daemon.**

```
hostname# ps -ef | grep sendmail
<owner> <pid> <timestamp> /usr/lib/sendmail -bd -q1h
```

5. **Kill the** `sendmail` **daemon and then restart it so that it uses the modified configuration file.**

```
hostname# kill -15 <pid>
hostname# /usr/lib/sendmail -bd -q1h
```

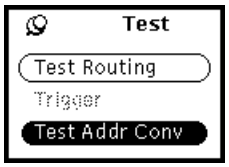
Refer to Appendix B, “Customizing sendmail for SunLink X.400 8.0.2” for a detailed description of how to modify `sendmail.cf` to support the gateway.

Testing the X.400/SMTP(MIME) Gateway

You can test that your gateway has been correctly configured in two stages:

- Check that the address is converted by the gateway in the way you expected it. Use the Address Conversion function on the Test pull-down menu.
- Send an electronic mail message to yourself, via the gateway.

Checking the Address Conversion



To ensure that the gateway translates your UNIX address to an X.400 address in the expected way, or that X.400 addresses are converted to correct UNIX addresses, you should check them with the Address Conversion option.

1. **Press and drag MENU down the Test menu and release it over the Test Addr Conv item.**
   The Test Address Conversion screen is displayed, as shown in Figure 4-9.

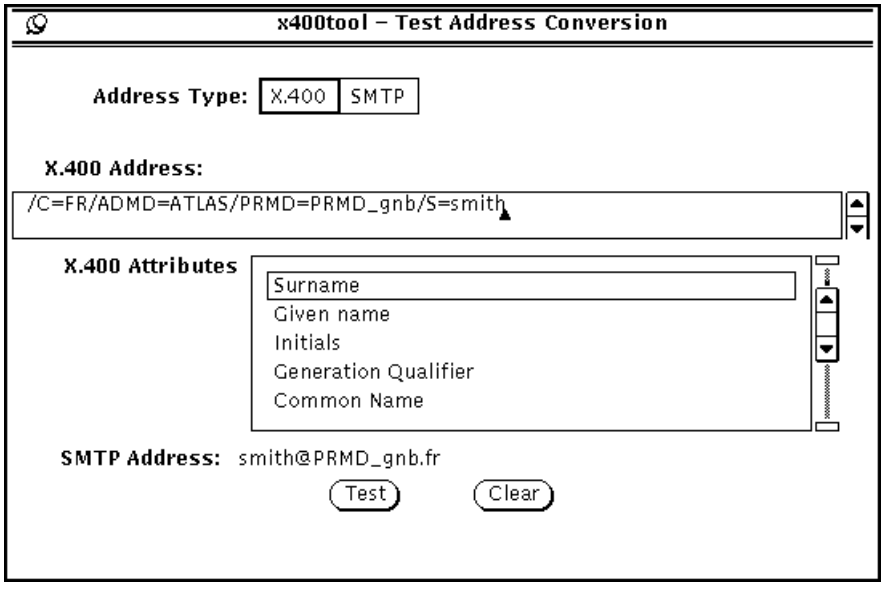


Figure 4-9 Test Address Conversion for Gateway

2. **Press SELECT on X.400 (for an address conversion from X.400 to UNIX), or SMTP (for an address conversion from UNIX to X.400).**

3. **Enter the address for which you want to see the result of the gateway conversion.**
   If you enter an X.400 address, the available components are displayed in the scroll list. Press SELECT to choose each component and then enter its value in the address field.

4. **When you have entered the complete address, press SELECT on Test to display the conversion that would be made in the gateway.**
   Note that the correct address conversion is only possible if you have configured the gateway. That is, if the address that you try to test is not a real or configured system, then the conversion result will include unknown characters. These characters are defined in RFC987 and RFC1327.

Sending a Test Message

When you are sure that the address is correct and that you have configured the gateway, you should test that it works by sending a message to yourself, via the gateway.

Send a message using your own UNIX mail address, specifying the gateway using the pseudo host name that you assigned to it. For example, if you assigned the default pseudo host name proposed by `x400tool` (`x400-gate`) then the address would be:

```
<recipient_name>@x400-gate
```

Figure 4-10 shows the `mailtool` compose window that is used to send a mail message to test the X400/SMTP gateway. The local UNIX mail address is the login name of the recipient (`jsmith`) and the UNIX mail domain address is the pseudo host name assigned to the gateway (`x400-gate`).

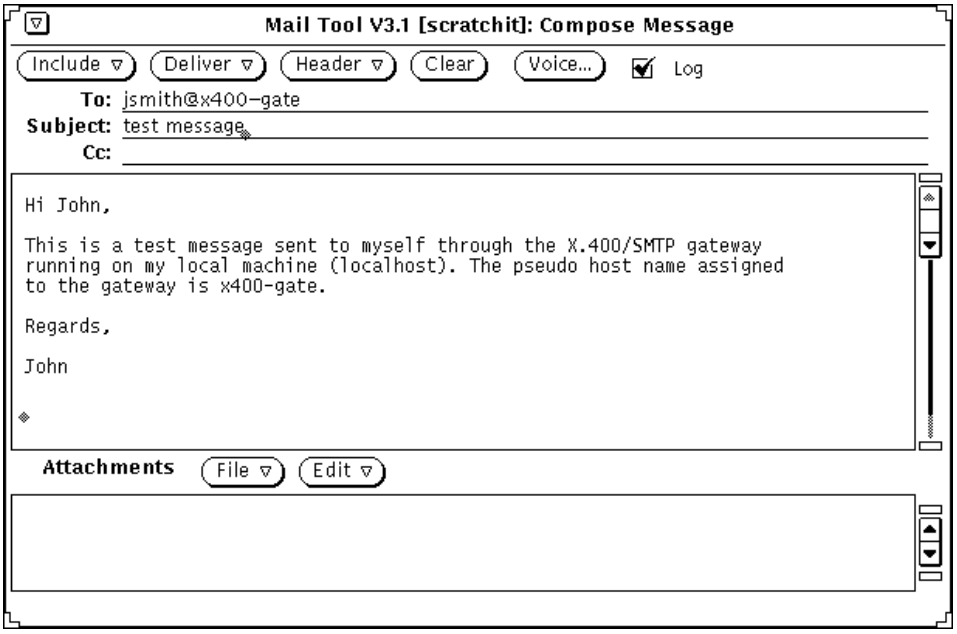


Figure 4-10 UNIX Mail Message Sent Through the Gateway

Figure 4-11 shows the UNIX mail message that was received through the X.400/SMTP(MIME) gateway. The full message header shows how the message is routed between systems and how the local UNIX mail address is converted into an equivalent X.400 O/R address.

Figure 4-11 UNIX Mail Message Received Through the Gateway

Modifying the Mapping Tables

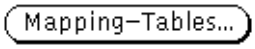
Caution – You should not modify the mapping tables supplied with SunLink X.400 8.0.2 other than under exceptional circumstances. Altering these mapping tables will affect the operation of your X.400/SMTP(MIME) gateway.

The X.400/SMTP(MIME) gateway translates SMTP (RFC 822) addresses and message elements to X.400 equivalents. This is done based on the mappings defined in RFC 1327 (superseding RFC 987 and RFC 1148) which provide for transparent conversion between UNIX mail and X.400 domains. In particular, the X.400/SMTP(MIME) gateway translates addresses using the standard mapping tables developed by the COSINE MHS project. These tables comply to RFC 1327 and are distributed globally under the auspices of the MHS Coordination Service.

There are three mapping tables:

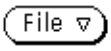
- **rfc1148-mapping1:** contains standard mappings between X.400 addresses and SMTP (RFC 822) addresses.
- **rfc1148-mapping2:** contains standard mappings between SMTP (RFC 822) addresses and X.400 addresses.
- **rfc1148-gate:** contains mappings for the default UNIX gateway that must be used if the domain is not defined in **rfc1148_mapping2**.

Using the Mapping Table Editor



To modify the standard mapping tables supplied with SunLink X.400 8.0.2:

1. **Double-click SELECT on the SMTP_X400 icon to activate the X.400/SMTP Configuration window.**
2. **Click SELECT on the Mapping Tables button to activate the Mapping Table Editor.**



3. **The Load Translation Table File window is displayed when you open this window. If this window is already open, then drag and release MENU on the File manu button to activate it. Choose one of the mapping tables from the list and click SELECT on Load.**
   Figure 4-12 shows the mapping table editor with a mapping table loaded.

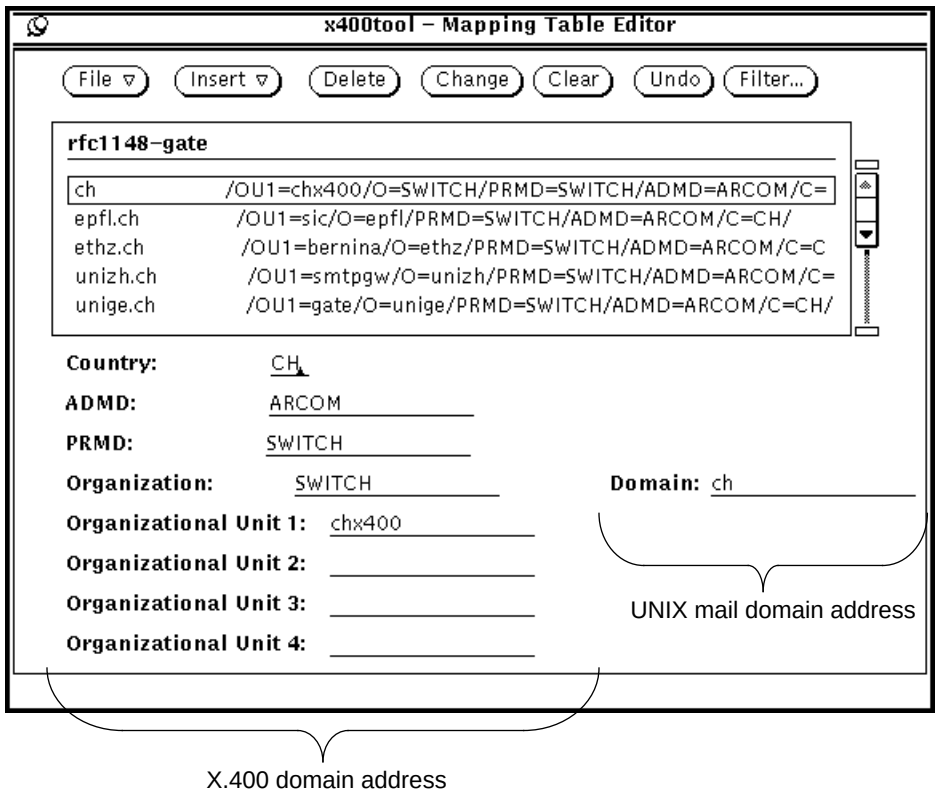


Figure 4-12 The Mapping Table Editor

4. **Click SELECT on the Filter button to activate the Filter window.**
   Use these options to limit the search so that the editor displays only a subset of all possible mappings. The filter can be a regular expression.

   For example:

   Set the Country filter `ON` and enter the appropriate country code for the X.400 domain in which you are interested—in the example shown in Figure 4-13 on page 75, `FR` for France was entered. Click SELECT on Apply to display the mappings associated with this country.

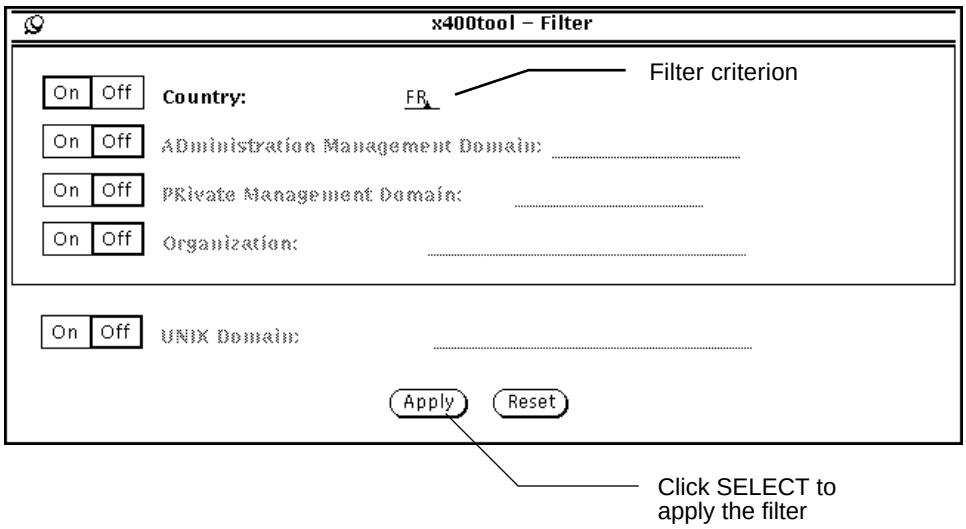


Figure 4-13 Mapping Editor Filter

You can use the mapping table editor to insert new mappings, change existing mappings, or delete entries from the mapping table.

The following options are associated with the Mapping Editor:

Insert: The Insert menu button is used to insert a new mapping into the table at the specified position:

- **Before:** inserts a new mapping immediately before the selected entry.
- **After:** inserts a new mapping immediately after the selected entry.
- **Top**: inserts a new mapping at the top of the table.
- **Bottom:** inserts a new mapping at the bottom of the table.

Delete: Removes the selected entry from the table.

Change: Modifies the selected entry with the new domain information.

Clear: Clears the domain information.

Undo: Reverses the last action taken.

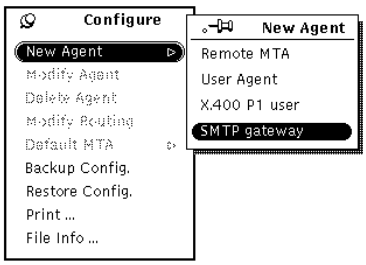
4

Replacing a Deleted X.400/SMTP(MIME) Gateway

There is an unconfigured X.400/SMTP(MIME) gateway in your message transfer system by default when you first start `x400tool`.

You can only have one X.400/SMTP(MIME) gateway in your message transfer system at any one time; however, if you delete the default gateway, you can replace it by adding a new agent.

Configure ▽ *Adding a New X.400 SMTP Gateway*



There is a default (unconfigured) X.400/SMTP(MIME) gateway in your message transfer system when you first start `x400tool`. You cannot add more than one X.400/SMTP(MIME) gateway to the message transfer system. If you delete the gateway, and later want to replace it:

1. **Press and drag MENU down and right to display the New Agent submenu.**
2. **Release MENU over the SMTP gateway item to add a new (unconfigured) X.400/SMTP gateway to your message transfer system.**
3. **Start the process `osismtpx400` by typing**:

```
hostname# /opt/SUNWconn/bin/osistart osismtpx400
```

4. **Configure the new gateway as described in "Basic Configuration" on page 60.**

Configuring Routes to the X.400/SMTP(MIME) Gateway

When you add a new X.400/SMTP(MIME) gateway to your message transfer system, `x400tool` attempts to create a default entry in the local routing table. This table is used by your local MTA to determine the forwarding address for each message that it receives. The default route for the X.400/SMTP(MIME) gateway is based upon the global domain identifier assigned to the local MTA.

If `x400tool` cannot create a default route (because, for example, an identical route already exists in the routing table) you will have to modify the routing table to add an entry that improves the granularity of the routing mechanism.

For example:

If you already have a remote MTA defined with the same global domain identifier, the local MTA will not create a default route for the X.400/SMTP(MIME) gateway. You must create a new entry in the routing table and add some discriminating attribute (organization name, organizational unit name, etc.) to the route so that your local MTA can forward messages correctly to both systems.

Refer to Chapter 7, “Routing Between Agents” for detailed instructions on how to modify default routing entries.

4

Adding Remote MTA Information 5

This chapter describes how to use `x400tool` to add information about remote message transfer agents (MTAs) to your local message transfer system. It assumes that you have already configured your local MTA as described in Chapter 3, “Configuring Your Local MTA”.

Remote message transfer agents (MTAs) handle the routing and relaying of electronic messages throughout the X.400 domain. Your local MTA can only communicate directly with remote MTAs that are added to your local message transfer system.

To add a remote MTA to your message transfer system, you need its name (and password, if applicable), global domain identifier, and OSI address. You must obtain this information from the system administrator who set it up.

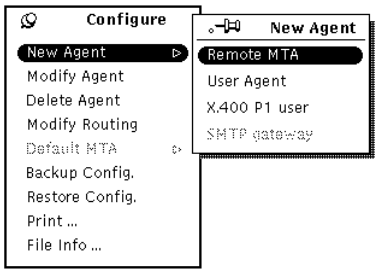
5

Basic Configuration

For a minimum configuration, you must assign a name for your remote MTA and specify its global domain identifier and OSI address. If you enable access control for this remote MTA, you must also specify its password if it has one.

You must obtain the information that is required to configure a remote MTA from the system administrator who set it up.

Configure ▽ *Adding a New Remote MTA*



To add a new remote MTA to your message transfer system:

1. **Press and drag MENU down and right to display the New Agent submenu.**
2. **Release MENU on the MTA item to add a new (unconfigured) remote MTA to your message transfer system as shown in Figure 5-1.**

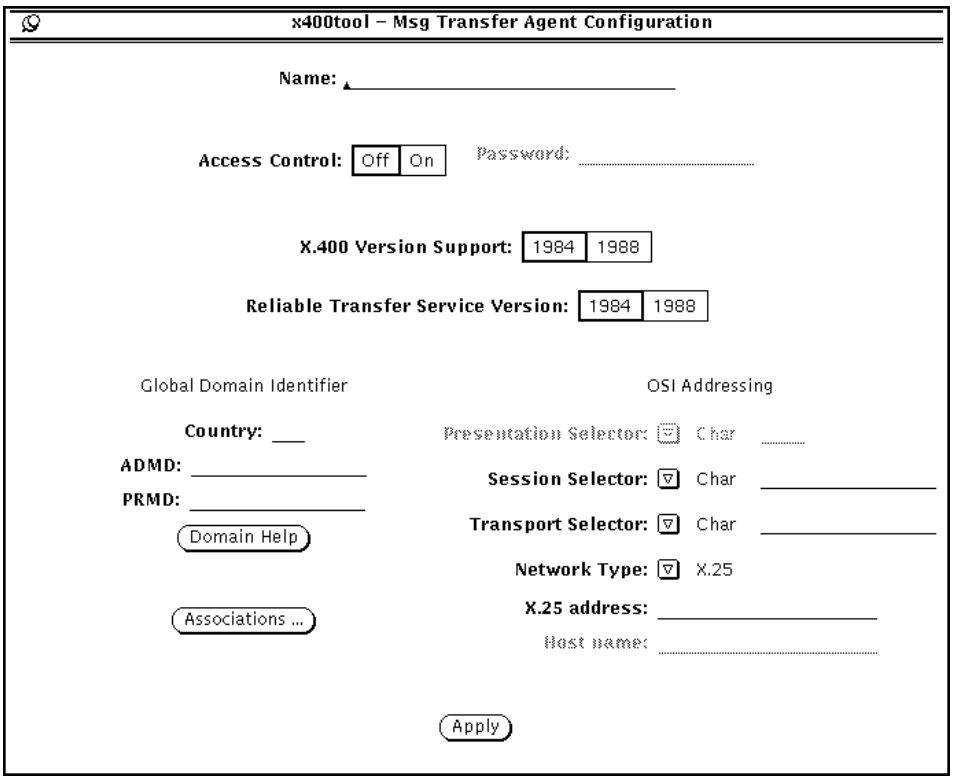


Figure 5-1 Remote MTA Configuration Window

Specifying the Remote MTA Name

The remote MTA name identifies the remote MTA within your message transfer system. It is not part of the X.400 address and is not used for routing messages.

You must obtain the name of the remote MTA from the system administrator who set it up.

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**

2. **Type the name assigned to this remote MTA on the Name input line as shown in Figure 5-2.**
   An unassigned (blank) MTA name will generate an error when you try to apply your remote MTA configuration. You cannot modify this name once your configuration is applied.

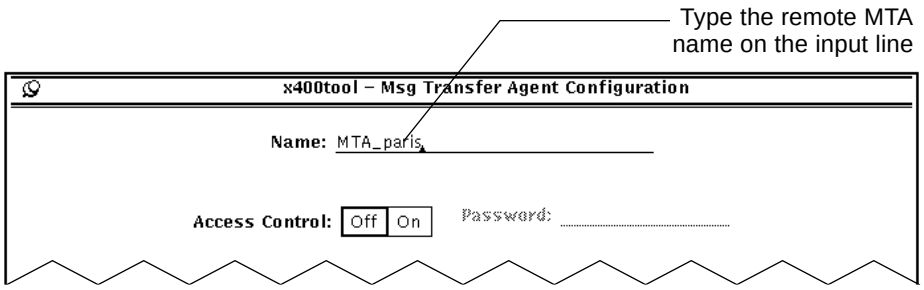


Figure 5-2 Specifying the Remote MTA Name

Enabling and Disabling Access Control

The access control mechanism is dependent upon the configuration of both the local and remote MTA. Access control is enabled for each remote MTA.

- The remote MTA configuration determines whether access control is enabled. *The system administrator responsible for the remote MTA must also enable access control and provide you with its password, if access control is required.*
- The local MTA configuration determines what is transmitted when remote access control is enabled. Access control can be based on the name of the initiating MTA only, or on the name *and* password of the initiating MTA. (Refer to “Setting an Access Control Password” on page 39 for detailed instructions on setting the password for your local MTA.)

The access control algorithm is summarized in Table 5-1. Note that this algorithm can be modified by setting the advanced security parameters discussed in “Tuning the Security Options” on page 52.

Table 5-1 Access Control Algorithm

Remote MTA	Access Control
Access control OFF	Access control DISABLED
Access control ON	Access control ENABLED

If you enable access control for a remote MTA, you must obtain its password from the system administrator who set it up.

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**
2. **Click SELECT to disable or enable access restriction, and enter a password (if required) as shown in Figure 5-3.**
   This is the password that the local MTA must receive from the remote MTA before it will accept an association for an incoming message.

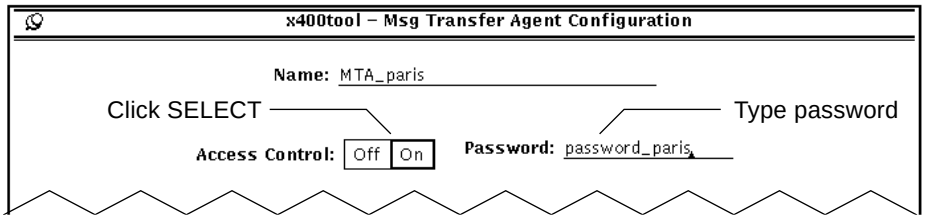


Figure 5-3 Enabling and Disabling Access Control for the Remote MTA

Specifying the Global Domain Identifier

The global domain identifier locates the remote MTA within the global X.400 domain. It consists of a country code, an ADMD, and an optional PRMD. Refer to “X.400 Management Domains” on page 6 for a more detailed description of the global domain identifier.

You must obtain the global domain identifier for the remote MTA from the system administrator who set it up.

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**

2. **Enter the global domain identifier for the remote MTA as shown in Figure 5-4.**

- Type a country code and ADMD. If necessary use the domain help to locate this information. If the address of the remote MTA does not require an ADMD, then insert a space.
- Type your PRMD on the input line. If the remote MTA is not part of a PRMD, you can leave a null PRMD entry. Do not insert a blank space.

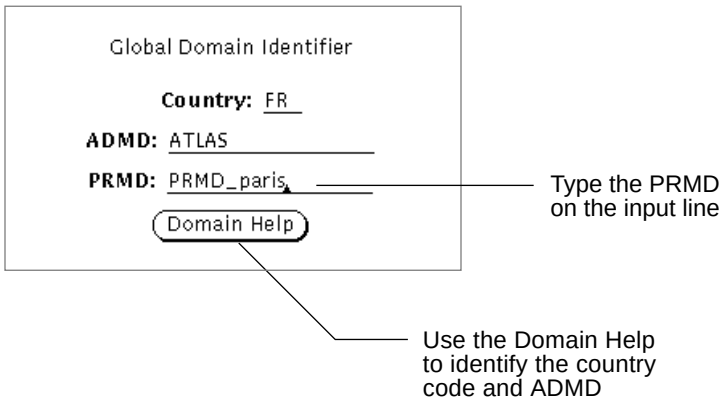


Figure 5-4 Specifying the Global Domain Identifier for a Remote MTA

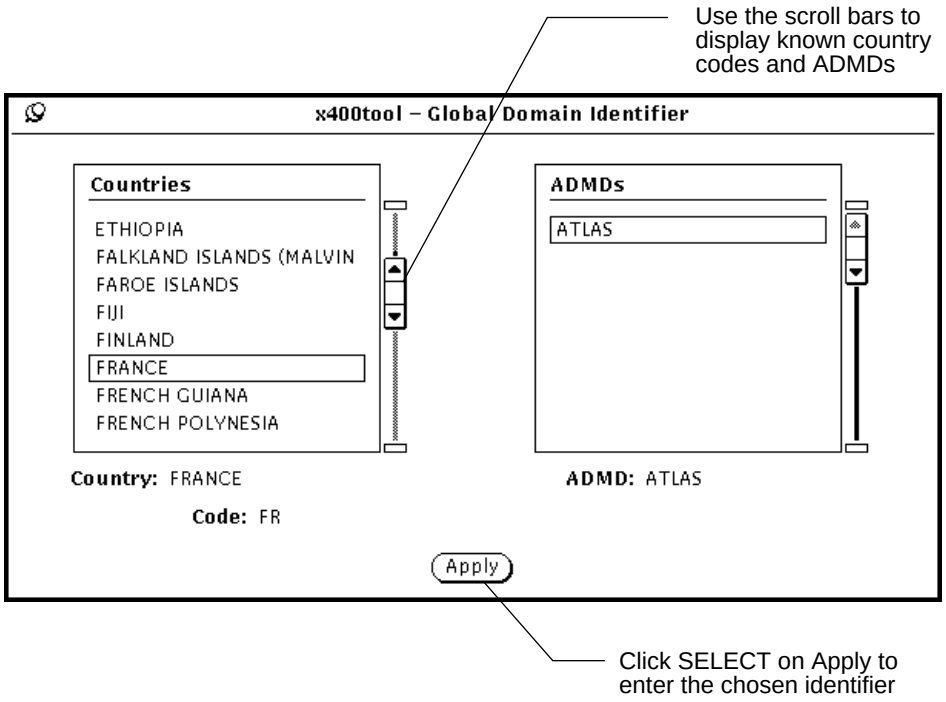


Figure 5-5 Using the Domain Help

Selecting X.400 Version Support

SunLink X.400 8.0.2 is an implementation of the 1988 version of the X.400 recommendations; however, it can exchange messages with systems that comply to the 1984 version. Complete use of the presentation layer, which also implies the use of OSI addresses up to the presentation layer, is a major feature introduced by the 1988 version.

- Choose 1984 X.400 Version Support if the remote MTA complies to the 1984 version. This disables the input line for the OSI presentation selector. This is the default option.
- Choose 1988 X.400 Version Support if the remote MTA complies to the 1988 version. This is the case if the remote MTA is running SunLink X.400 8.0.2. This enables the input line for the OSI presentation selector and the ability to select the Reliable Transfer Service version.

To choose the X.400 Version Support:

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**
2. **Click SELECT on 1984 or 1988 to select the X.400 Version Support.** This selection should agree with the configuration of the remote MTA.

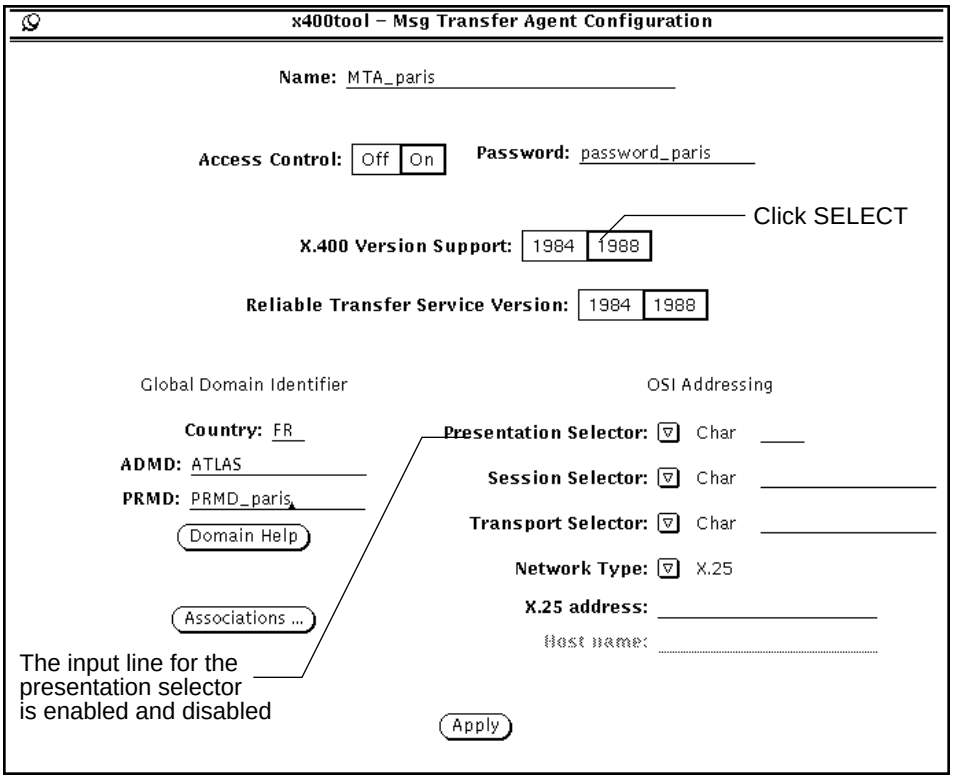


Figure 5-6 Selecting X.400 Version Support

Note – When you change the 1988 X.400 Version Support, the related number of associations will also change accordingly, if you have not previously altered them. You should verify that the number of associations is correct for your chosen version support. (See “Tuning the Remote MTA Associations Options” on page 90)

Selecting Reliable Transfer Service Version

The Reliable Transfer Service is used to ensure the safe delivery of messages. The RTS 1984 version interfaces directly with the session layer, whilst RTS 1988 interfaces with the presentation layer. You will not normally need to change this option. Check with your remote system administrator for the version of RTS.

To select the RTS version:

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**
2. **Click SELECT on 1984 or 1988 to select the Reliable Transfer Service Version.**
   If you have selected 1984 X.400 version support, then you cannot change this option. If you selected 1988 X.400 support, you can select RTS version 1984 or 1988.

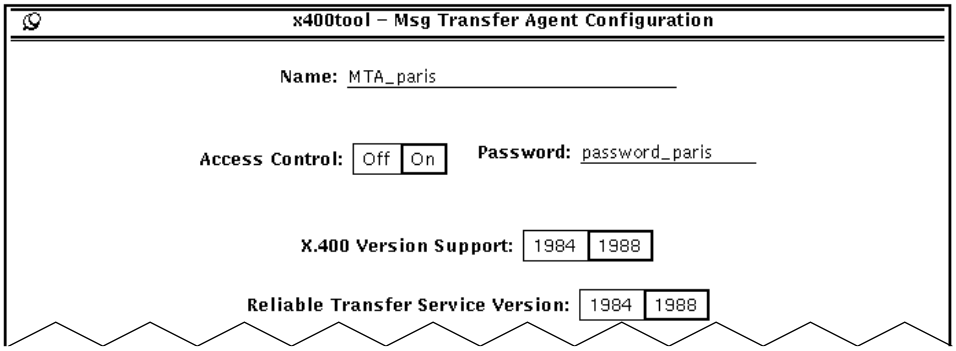
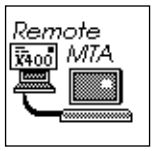


Figure 5-7 Selecting the RTS Version



Specifying the OSI Address

Your local MTA uses the OSI address to reach the remote MTA across the OSI network. It is dependent on how the remote MTA is physically attached to the OSI network.

You must obtain the OSI address for the remote MTA from the system administrator who set it up.

A remote MTA can be attached to the OSI network through the following network interfaces:

- X.25 (1980)
- TCP/IP (RFC 1006)
- LLC1 (LAN—for example, FDDI)
- CONS - X.25 1984

Each remote MTA can have only one OSI address. If the machine on which it resides has multiple network interfaces or multiple OSI addresses, you must define multiple remote MTAs—one remote MTA for each network interface.

You need to specify the sub-network connection configured for the remote MTA indicating the transport layer connection. Note that for X.25 1980 connections, the network address is an X.121 network address, and for CONS X.25 1984 connections, the network address is an NSAP address.

For example:

If the remote MTA uses different OSI addresses for incoming and outgoing messages you need to create two MTAs in your message transfer system. Your local MTA will send messages to one MTA and receive messages from the other.

To enter the components of the OSI address:

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**
2. **Drag MENU on the Network Type pull-down menu to choose the type of network interface used to attach the remote MTA to the OSI network as shown in Figure 5-8 on page 89.**

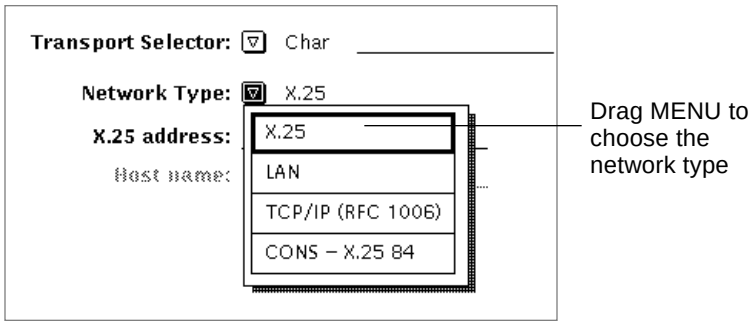


Figure 5-8 Choosing the Network Type

3. Drag MENU to select the address format for each selector as shown in Figure 5-9.
The elements of an OSI address can be entered in character format (char) or in hexadecimal format (hex).

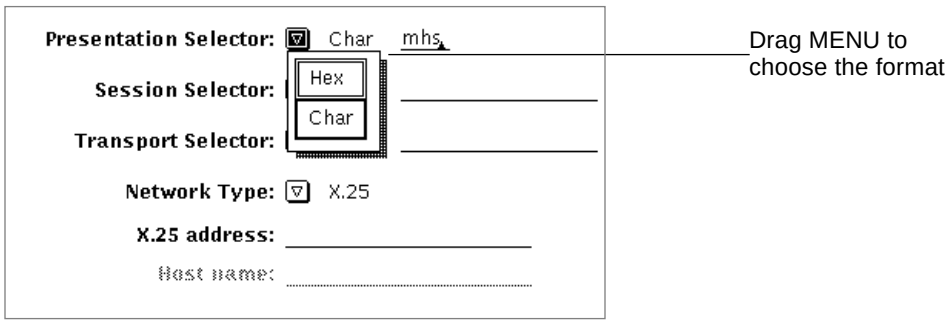


Figure 5-9 Choosing the Address Format

4. Enter each layer of the OSI address.
You must obtain the OSI address for the Remote MTA from the system administrator who set it up.

- For an OSI address for an X.25 interface, enter the *entire* X.25 address including the subaddress (without any internal prefixes) on the network address input line. The X.25 address is composed of decimal digits only.
- For an OSI address for a LAN interface, you can either enter the NSAP in character or hexadecimal.

- For an OSI address for a TCP/IP (RFC 1006) interface, you can enter either the network address in Internet format (dot notation) on the network address input line, or the host name that corresponds to this address on the host name input line. The network address is recovered from the NIS map using `gethostbyname`.

Apply

Once you have completed the basic configuration steps described in this section, apply your remote MTA configuration by clicking SELECT on the Apply button. This adds the remote MTA to your message transfer system and adds a default route to the routing table used by the local MTA (provided an identical route does not exist). The default route is based on the global domain identifier for the remote MTA. See "Configuring Routes to Remote MTAs" on page 94 for more information.

Tuning the Remote MTA Associations Options

Associations ...

The remote MTA Association Management options are used to restrict the number of simultaneous associations that are created between your local MTA and the remote MTA.

1. **Double-click SELECT on the remote MTA icon to activate the Remote MTA Configuration window.**
2. **Click SELECT on the Associations button to activate the Remote MTA Associations window.**
3. **Drag SELECT on the slider, or type the value directly on the input line.**

Remote MTA Association Management Options

Max. Local Associations: Defines the maximum number of simultaneous associations that your local MTA can open with the remote MTA (association initiated by the local MTA). Note that Two Way associations have priority over Monologue associations.

- **Two way:** Defines the maximum number of simultaneous associations that your local MTA can open with the remote MTA to send and receive messages.
- **Monologue:** Defines the maximum number of simultaneous associations that your local MTA can open with the remote MTA to send messages only.

Max. Remote Associations: Defines the maximum number of simultaneous associations that the remote MTA can open with your local MTA (association initiated by the remote MTA). Note that Two Way associations have priority over Monologue associations.

- **Two way:** Defines the maximum number of simultaneous associations that the remote MTA can open with your local MTA to send and receive messages.
- **Monologue:** Defines the maximum number of simultaneous associations that the remote MTA can open with your local MTA to send messages only.

Figure 5-10 shows the associations window.

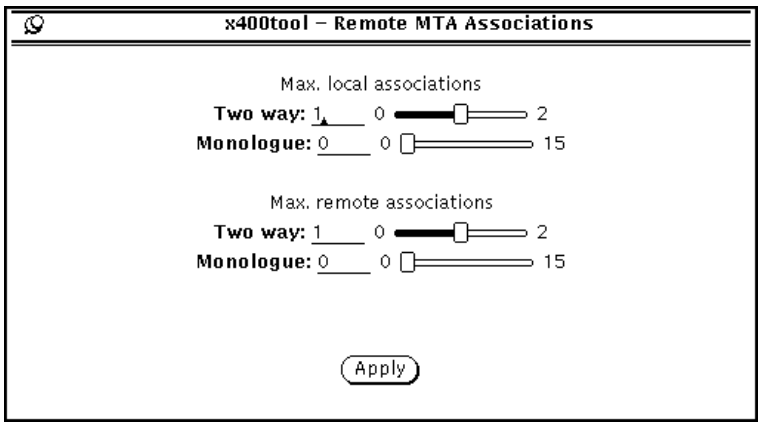


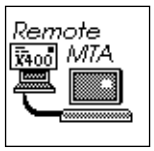
Figure 5-10 Tuning the Remote MTA Association Management Options

The table below shows the default settings for the associations:

	Local		Remote	
	Two-way	**Monologue**	**Two-way**	**Monologue**
1984	0	1	0	1
1988	1	0	1	0

Once you have completed the configuration steps described in this section, Apply your remote MTA configuration by clicking SELECT on the Apply button. Note that this will only take effect after you have also Applied the selections on the Remote MTA window to confirm the overall configuration.

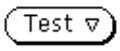
Testing the Associations



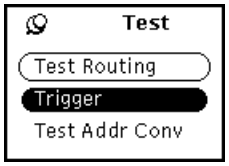
Once you add a remote MTA to your message transfer system, you can test the configuration with the *trigger* option. This tests whether your local MTA can reach the remote MTA across the OSI network. It does not test whether electronic messages are correctly routed to this MTA or whether they can be delivered to their ultimate recipient.

To use the trigger successfully, the following conditions must be met:

- The *remote* MTA defined in your local message transfer system must be defined as a *local* MTA in the remote message transfer system to which it belongs.
- The *local* MTA defined in your local message transfer system must be defined as a *remote* MTA in the remote message transfer system. It does not have to be open to respond to the trigger.
- The access control parameters must be set coherently between the local and remote MTAs in both message transfer systems.
- The remote MTA must be open. Highlight the remote MTA and press MENU on the Manage menu button and drag the pointer to the Open Agent item. Release MENU to open the remote MTA.



Using the Trigger to Test the Associations



The Trigger option is used to determine whether your local MTA can open an association with an MTA. It does not show whether messages are correctly routed.

To use the Trigger option:

1. **Click SELECT on the icon that corresponds to the remote MTA you want to test.**
2. **Press MENU on the Test menu button and drag the pointer to the Trigger item. Release MENU to activate the Trigger Remote MTA window.**

3. **Click SELECT on the Trigger button to test the association between your local MTA and the remote MTA as shown in Figure 5-11.**

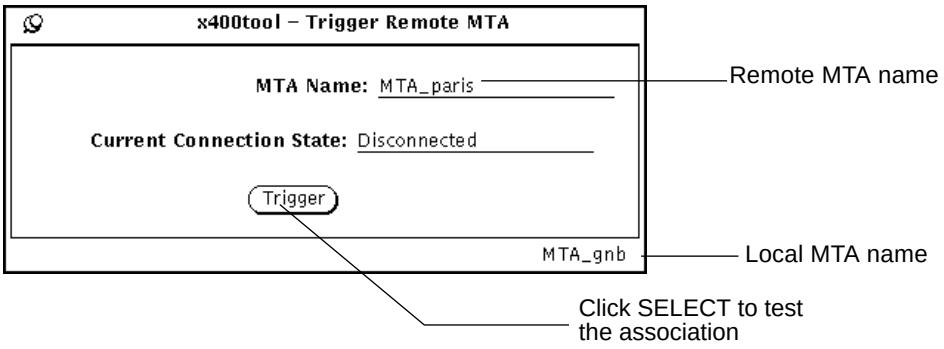


Figure 5-11 Using the Trigger

If the trigger is successful, the local MTA will open an association with the remote MTA and the current connection state will change to *connected* as shown in Figure 5-12. This shows that your remote MTA is configured correctly and will be able to receive electronic messages from your local MTA.

The association remains open for the time specified by the **Idle Association Timeout** for your local MTA. By default, this is one minute. (Refer to “Tuning the Basic Association Options” on page 44 for detailed instructions on how to alter this delay.)

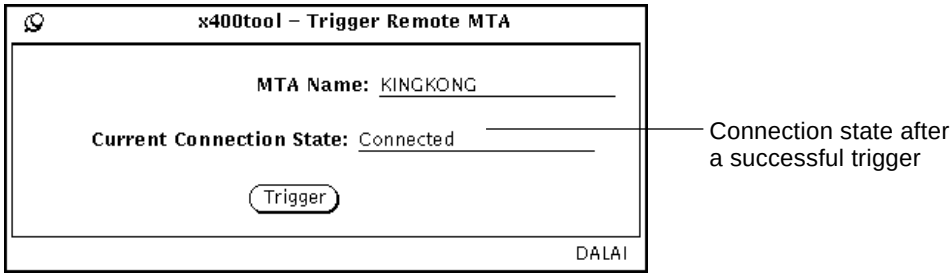
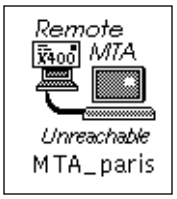


Figure 5-12 Successful Trigger Attempt



If the trigger is unsuccessful, the current connection state is marked as either *disconnected* or *unreachable*. If it is marked *unreachable*, as shown in Figure 5-13, then the icon for the remote MTA is also marked *unreachable* and the remote MTA is closed. It must be reopened before you can try another trigger attempt. Refer to “Opening and Closing Agents” on page 129 for detailed instructions on how to reopen a closed MTA.

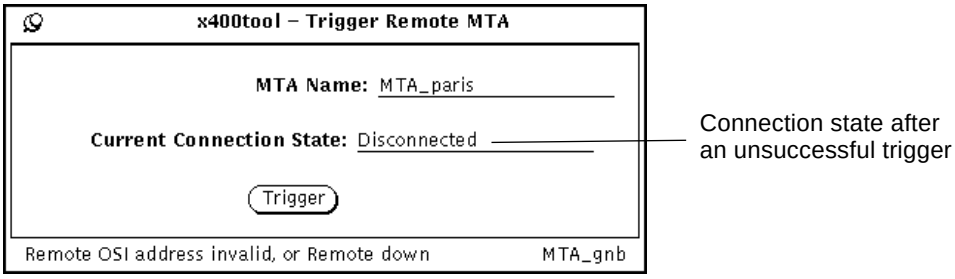


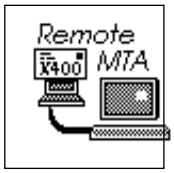
Figure 5-13 Unsuccessful Trigger Attempt

The probable cause of the unsuccessful trigger attempt is shown in the status bar at the bottom of the window. The most common causes of a failed trigger are:

Remote MTA refuses connection: This occurs if there is a problem with the access control mechanism (for example, passwords not set correctly) or if your local MTA is not included in the remote message transfer system.

Remote OSI address invalid: The local MTA was unable to reach the specified remote MTA with the OSI address elements provided. Check that you entered the correct OSI address. Use `osi_trace` to examine the connection attempt.

Configuring Routes to Remote MTAs



When you add a remote MTA to your message transfer system, `x400tool` attempts to create a default entry in the local routing table. This table is used by your local MTA to determine the forwarding address for each message that it receives. The default route for the remote MTA is based upon its global domain identifier.

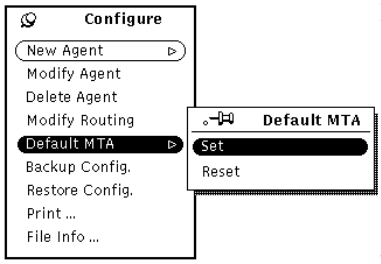
If `x400tool` cannot create a default route (because, for example, an identical route already exists in the routing table) you will have to modify the routing table to add an entry that improves the granularity of the routing mechanism.

For example:

If two remote MTAs are defined with the same global domain identifier, the local MTA will not create a default route for the second one. You must create a new entry in the routing table and add a discriminating attribute (organization name, organizational unit name, etc.) to the route so that your local MTA can forward messages correctly to both systems.

Refer to Chapter 7, “Routing Between Agents” for detailed instructions on how to modify default routing entries.

Configure ▽ *Setting a Default MTA*



If you define a default MTA (also called a “catch-all” MTA), then the local MTA uses it as the destination for all messages that it fails to route based on the entries in its routing table. This mechanism works efficiently for X.121 addresses and for a default MTA that has its domain name (Country, ADMD, and PRMD) as its route; however, you must take care when there are other MTAs in the message transfer system that route messages based on the organization name or other lower level attributes.

For example:

To route a message with the address `/C=FR/A=ATLAS/P=CORP/O=GRP/` to the default MTA in a message transfer system that includes a remote MTA with the route `/C=FR/A=ATLAS/P=CORP/O=MKTG/`, you must ensure that the default MTA has the domain name `/C=FR/A=ATLAS/P=CORP/` entered in its routing table.

Note – You must define a default MTA if you want to route messages based on an X.121 address only. The remote MTA that you choose for the default MTA must support routing decisions based on the X.121 address.

You can choose any of the remote MTAs in your message transfer system as the default MTA. Ideally, the default MTA should point to a public X.400 provider since they maintain comprehensive and up-to-date routing tables that increase the chance of the message reaching its ultimate destination.

To set a default MTA:

1. **Click SELECT on the icon that corresponds to the remote MTA that you want as your default MTA.**
2. **Press MENU on the Configure menu button and drag the pointer to the Default MTA item.**
3. **Activate the submenu and choose Set to configure the remote MTA as the default MTA.**

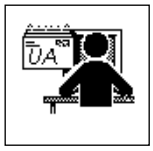
Note – If you reset a default MTA, so that it is no longer the default MTA, it will route messages as normal. That is, messages that match its default route will continue to be routed through it.

Adding Third-Party Agents 6

This chapter describes how to add third-party local or remote user agents (UAs) and X.400 MT (P1) users (for example, message gateways) to your message transfer system. It assumes that you have already defined your local message transfer agent (MTA) as described in Chapter 3, “Configuring Your Local MTA.”

Refer to the *X/Open Electronic Messaging (X.400) API* for detailed information regarding the development of X.400-compatible user agents and X.400 MT (P1) users using the Message Access (MA) and Message Transfer (MT) interfaces.

Adding and Configuring Third-Party User Agents

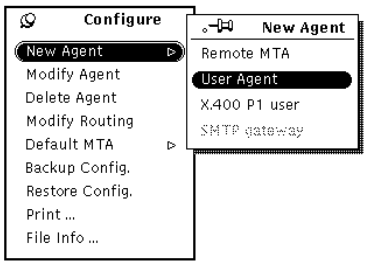


User agents (UAs) handle the submission and delivery of electronic messages. They provide the direct interface between end-users (application processes) and the message transfer system (MTS).

Native user agents are not supplied with the SunLink X.400 8.0.2; however, you can add a third-party user agent to your message transfer system by giving it an identifying name and specifying the body types and contents that it uses.

6

Configure ▽ *Adding a Third-Party User Agent*



To add a third-party user agent to your message transfer system:

1. **Press and drag MENU down and right to display the New Agent submenu.**
2. **Release MENU over the User Agent item to add a new (unconfigured) user agent to your message transfer system as shown in Figure 6-1.**

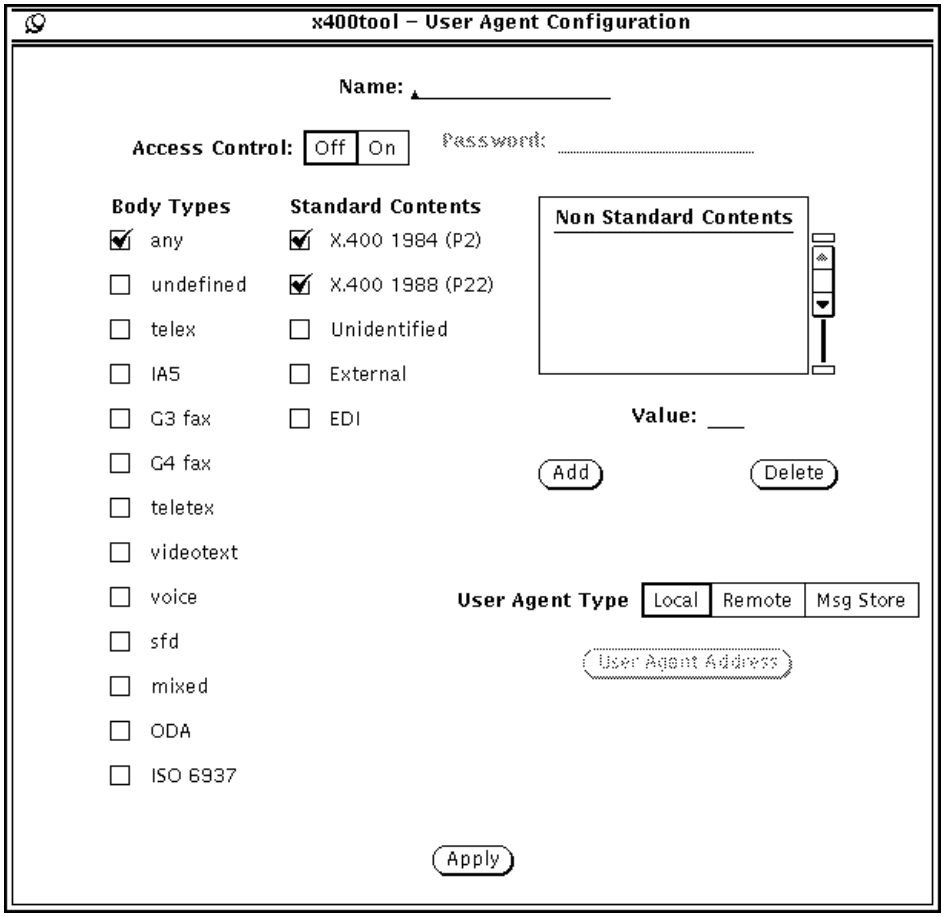


Figure 6-1 Adding a Third-Party User Agent

Specifying the User Agent Name

The user agent name locates the user agent within your message transfer system. It is not part of the X.400 address and is not used for routing messages; it is used as the client name in the `ma_open` function of the XAPIA message access (MA) interface.

1. **Double click SELECT on the user agent icon to activate the User Agent Configuration window.**
   Alternatively, you can use the Configure menu and select User Agent from the New Agent sub-menu.

2. **Type the name assigned to this user agent on the Name input line as shown in Figure 6-2.**
   An unassigned (blank) user name will generate an error when you apply your configuration. You cannot modify this name once it is applied.

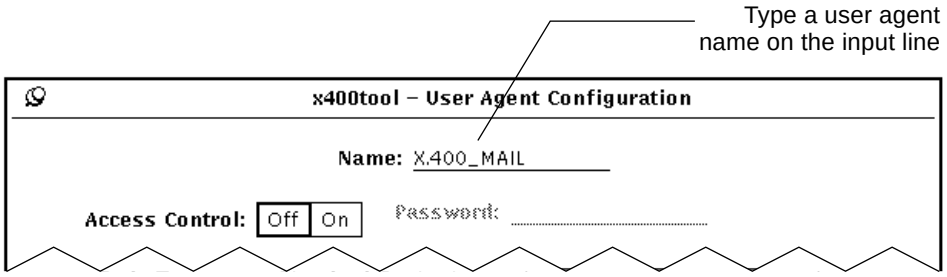
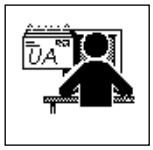


Figure 6-2 Specifying the User Agent Name



Enabling and Disabling Access Control

The access control mechanism is dependent upon the configuration of the both the user agent *and* its local MTA. Access control is enabled for each user agent if:

- The user agent configuration determines whether access control is enabled. If access control is enabled, then the local MTA will check the identity of the user agent sending the message before it will accept the connection.
- The local MTA configuration determines what is transmitted when access control is enabled. Access control can be based on the name of the initiating agent only, or on the name *and* password of the initiating agent.

Note that this algorithm can be further modified by setting the advanced security parameters for the local MTA as discussed in “Tuning the Security Options” on page 52.

1. **Double-click SELECT on the user agent icon to activate the User Agent Configuration window, if it is not already displayed.**
2. **Click SELECT to disable or enable access restriction, and enter a password (if required) as shown in Figure 6-3.**
   This is the password that the local MTA expects to receive from the user agent before it will accept an association for an outgoing message.

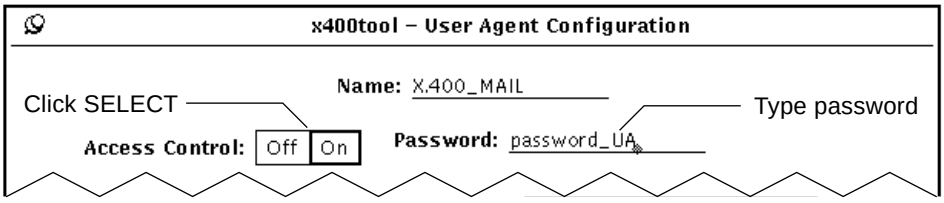
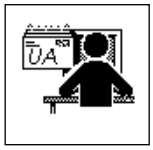


Figure 6-3 Enabling and Disabling Access Control for a User Agent



Specifying the Supported Body Types

The body types define the format in which the body parts of messages are transmitted. Body parts may be either binary data or text. An undefined body part is treated as binary data. You can prevent the local MTA from forwarding body parts that the user agent is unable to process by defining the specific body types that the user agent supports.

Note that the body type definition is only relevant if either X.400 1984 (P2) or X.400 1988 (P22) is selected as one of the supported standard content types. See “Specifying the Supported Standard Content Types” on page 102.

To specify the body types supported by the user agent:

1. **Double-click SELECT on the user agent icon to activate the User Agent Configuration window, if it is not already displayed.**
2. **Click SELECT on one or more of the check boxes associated with the body types supported by the user agent.**

The standard body types defined by the X.400 recommendations are:

any: Indicates that the user agent supports all possible body types (both binary data and text) and will accept messages with body parts of various formats.

undefined: Indicates that the user agent will accept a message including a binary data (bilaterally defined data) body part. Only supported by the 1984 version of the X.400 specifications.

telex: Indicates that the user agent will accept messages including a telex format body part.

IA5: Indicates that the user agent will accept messages including an IA5 (ASCII) text format body part.

G3 Fax: Indicates that the user agent will accept messages including a Group 3 (G3) fax format body part.

G4 Fax: Indicates that the user agent will accept messages including a Group 4 (G4) fax format body part.

teletext: Indicates that the user agent will accept messages including a teletext format body part as defined by T.61.

videotex: Indicates that the user agent will accept messages including a videotex format (as defined by T.100 and T.101) body part.

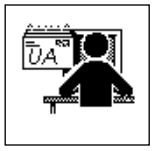
voice: Indicates that the user agent will accept messages including a voice body part.

sfd: Indicates that the user agent will accept messages including a Simple Format Document (SFD) as defined by the 1984 revision of the X.400 recommendations.

mixed: Indicates that the user agent will accept messages of a sort that can be processed by mixed-mode terminals (teletext and G4 fax).

ODA: Indicates that the user agent will accept messages conforming to Office Documentation Architecture standards. For example, this allows recognition of word-processor files.

ISO 6937: Indicates that the user agent will accept messages including full ASCII text plus additional features, such as accents. It is the equivalent of the teletext format.



Specifying the Supported Standard Content Types

You can prevent the local MTA from forwarding messages that the user agent is unable to process by specifying the content types that the user agent supports.

To specify the standard content types supported by the user agent:

1. **Double-click SELECT on the user agent icon to activate the User Agent Configuration window.**
2. **Click SELECT on the check boxes associated with the supported standard content types.**

The standard content types defined by the X.400 recommendations are:

X.400 1984 (P2): Standard content type 2. Indicates that the user agent will accept Interpersonal Messages (used to exchange electronic mail between end-users) conforming to the 1984 revision of the X.400 recommendations.

X.400 1988 (P22): Standard content type 22. Indicates that the user agent will accept Interpersonal Messages (used to exchange electronic mail between end-users) conforming to the 1988 revision of the X.400 recommendations.

Unidentified: Standard content type 0. Indicates that the user agent will accept messages of an unidentified (or unknown) content type. The user agent may or may not be able to process the message.

External: Standard content type 1. Indicates that the user agent will accept messages whose content type is not defined by the X.400 recommendations.

EDI: Standard content type 35. Indicates that the user agent will accept EDI messages (used to exchange billing information between end-users).

Specifying the Supported Non-Standard Content Types

You can also specify the non-standard content types (content types not defined by the X.400 recommendations) supported by your third-party user agent. These are used for end-to-end communication between user agents and rely upon proprietary encoding.

To specify the non-standard content types supported by the user agent:

1. **Double-click SELECT on the user agent icon to activate the User Agent Configuration window.**

2. **Type a numeric content type identifier on the Value input line as shown in Figure 6-4.**
   The code must be recognized as a content type by the user agent. Its value must not correspond to any of the standard content types, or any other non-standard types. The standard content types are:

   0: Unidentified

   1: External

   2: X.400 1984 (P2)

   22: X.400 1988 (P22)

   35: EDI

3. **Click SELECT on Add to place the non-standard content type in the scrolling-list.**

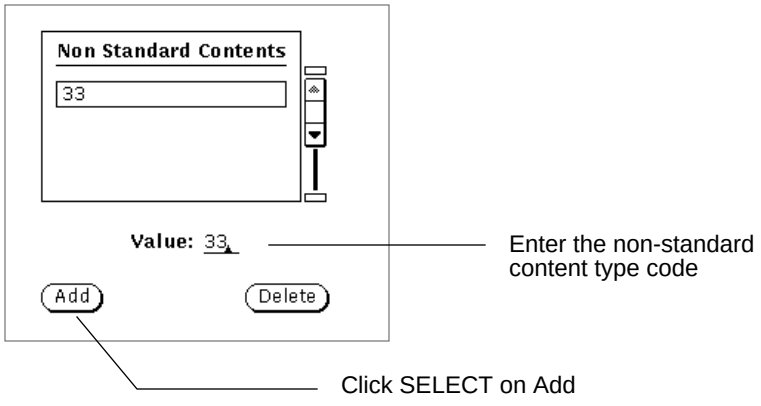


Figure 6-4 Specifying Non-Standard Content Types

Specifying User Agent Type

You can specify this user to be local or remote. A local user is one connected through the XAPIA MA interface directly to the local MTA. A remote user is connected through a subnetwork and uses P3 protocol. A message store user agent is a third party message store connected to the local MTA.

Note – SunLink X.400 does not currently provide either a remote P3 user agent or a message store user agent. However, you can obtain these from other suppliers.

---

1. **Double-click SELECT on the user agent icon to activate the User Agent Configuration window.**
2. **Click select on the Local or Remote button.**
   If you specify a remote user agent, then you must also declare its OSI address. When you choose Remote, the User Agent Address screen is displayed, as shown in Figure 6-5.

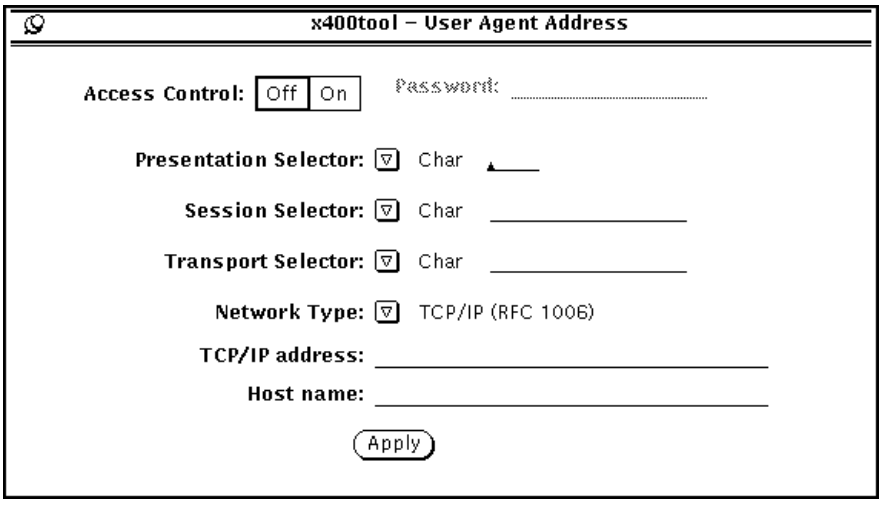


Figure 6-5 User Agent Address

Click SELECT to disable or enable access restriction, and enter a password (if required). This is the password that the local MTA expects to receive from the user agent before it will accept an association for an outgoing message.

Enter the OSI address for the remote user agent. The presentation, session and transport selectors should be the same as those defined in the remote stack configuration.

The type of subnetwork can be X.25, LAN, TCP/IP, or CONS (X.25 84). This will be defined in the remote agent's configuration. Depending on which subnetwork type you select, additional address information is required. For example, if you select X.25, you must enter the X.121 address, or if you select CONS X.25 1984, you need to enter the NSAP address. For a LAN, you can enter the NSAP in character or hexadecimal format.

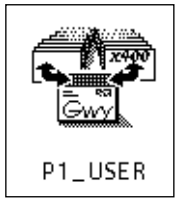
Once you have completed the basic configuration steps described in this section, apply your user agent configuration by clicking SELECT on the Apply button.

Configuring Routes to a User Agent

After you have added a new user agent to your message transfer system, you need to modify the routing table used by the local MTA to add at least one route for the user agent.

Refer to Chapter 7, "Routing Between Agents" for detailed instructions.

Adding and Configuring X.400 MT (P1) Users

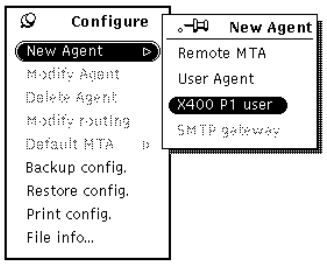


An X.400 MT (P1) user relies upon the X.400 message transfer (MT) service for the exchange of electronic messages between X.400-compatible systems. Message transfer agents (MTAs) and message gateways are typical examples of X.400 P1 users.

SunLink X.400 8.0.2 includes a native P1 user agent (the X.400/SMTP(MIME) gateway); however, you can also add third-party P1 user agents to your local MTA configuration. These should be developed using the XAPIA message transfer (MT) interface defined by X/Open. Refer to the *X/Open Electronic Messaging (X.400) API* for further details.

6

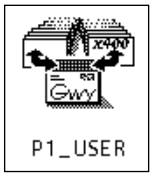
Configure ▽ *Adding a Third-Party P1 User*



You define a third-party P1 user by giving it a name and specifying its global domain identifier. By default, a new P1 user is assigned the same global domain identifier as the local MTA.

To add a third-party P1 user to your message transfer system:

1. **Press and drag MENU down and right to display the New Agent submenu.**
2. **Release MENU over the X.400 P1 User item to add a new (unconfigured) P1 user to your message transfer system.**



Specifying the P1 User Name

The P1 user name identifies the third-party P1 user within your message transfer system. It is not part of the X.400 address and is not used for routing messages; it is used as the client name in the `mt_open` function of the XAPIA message transfer (MT) interface.

To specify the P1 User name:

1. **Double-click SELECT on the P1 user icon to activate the MT User (Gateway) Configuration window.**
2. **Type the name assigned to this P1 user on the Name input line as shown in Figure 6-6.**
   An unassigned (blank) user name will generate an error when you try to apply your configuration. You cannot modify this name once it is applied.

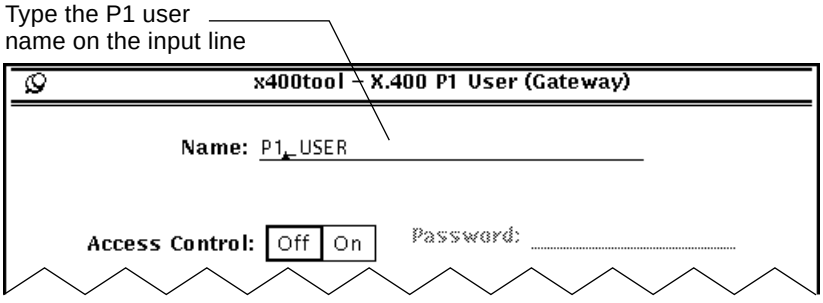
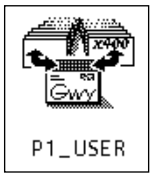


Figure 6-6 Specifying the P1 User Name



Enabling and Disabling Access Control

The access control mechanism is dependent upon the configuration of both the local MTA *and* the P1 user. Access control is enabled for each P1 user agent if:

- The P1 user configuration determines whether access control is enabled. If access control is enabled, then the local MTA will check the identity of the P1 user before it will accept an connection.
- The local MTA configuration determines what is transmitted when access control is enabled. Access control can be based on the name of the initiating agent only, or on the name *and* password of the initiating agent.
- Note that this algorithm can be further modified by setting the advanced security parameters for the local MTA as discussed in “Tuning the Security Options” on page 52.

To enable or disable access restrictions:

1. **Double-click SELECT on the P1 user icon to activate the MT User (Gateway) Configuration window.**
2. **Click SELECT to disable or enable access restriction, and enter a password (if required) as shown in Figure 6-7.**
   This is the password that the local MTA must receive from the P1 user before it will accept an association for an incoming message.

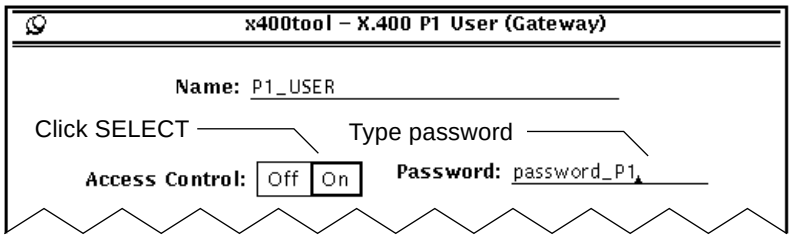


Figure 6-7 Enabling and Disabling Access Control for a P1 User

Specifying Type of P1 Access

You need to specify the type of access required for the P1 user. For XAPIA applications that use the P1 protocol to access the MTA specify XAPIA Message Transfer Interface.

For other applications which do not use XAPIA, you should use the message queue interface. This architecture reflects that of third party MTAs (non-XAPIA), which use message queues to interface between P1 applications and their MTAs.

To specify the type of access:

1. **Press MENU on Access and drag the pointer down to choose the XAPIA Message Transfer Interface or Message Queues item, as shown in Figure 6-8.**
2. **Release the MENU button on the appropriate access type.**
   For XAPIA P1 applications, choose the XAPIA Message Transfer Interface item, for access from other types of P1 applications, choose the Message Queues item. You can specify a maximum of 16 P1 user agents.

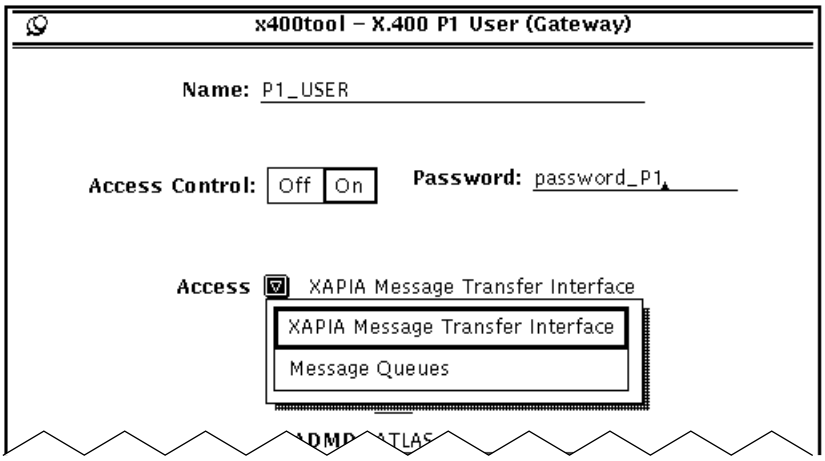
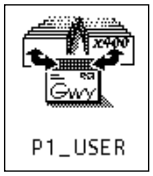


Figure 6-8 Specifying the Type of P1 Access

3. **Press Apply to save the changes and return to the P1 user (Gateway) configuration screen.**

Note – By default the incoming messages are queued in:
`/var/SUNWconn/OSIROOT/spool/<`*p1username*`>/in_queue`
and the outgoing messages are queued in:
`/var/SUNWconn/OSIROOT/spool/<`*p1username*`>/out_queue`
Sometimes these message queues can become large and may cause problems by being in this location. To avoid these problems, create a symbolic link between these directories and another location where file size is not so limited.



Specifying the Global Domain Identifier

The global domain identifier locates a P1 user within the global X.400 domain. It consists of a country code, an ADMD, and an optional PRMD. By default, a new P1 user is assigned the same global domain identifier as the local MTA.

To specify the global domain identifier:

1. **Double-click SELECT on the P1 User icon to activate the MT User (Gateway) Configuration window.**
2. **Enter the global domain identifier for the remote MTA as shown in Figure 6-9.**
   By default, the P1 user is assigned the same global domain identifier as your local MTA. If you need to modify the default global domain identifier:

- Type a country code and ADMD. If necessary use the domain help to locate this information. If your local MTA does not require an ADMD in its X.400 address, enter a space on the ADMD input line.
- Type your PRMD on the input line. If your local MTA is not part of a PRMD, you can leave a null PRMD entry. Do not insert a blank space.

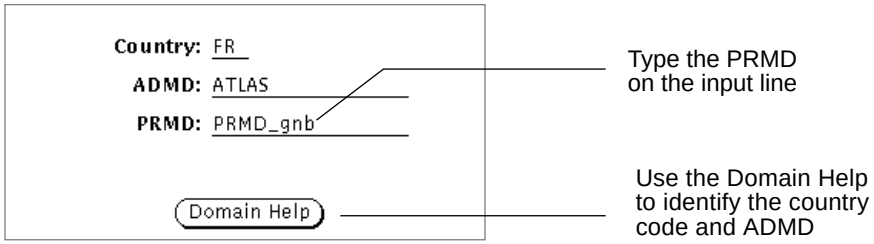


Figure 6-9 Specifying the Global Domain Identifier

Once you have completed the basic configuration steps described in this section, apply your P1 user configuration by clicking SELECT on the Apply button. This adds the P1 user to your message transfer system and adds a default route to the routing table used by the local MTA (provided an identical route does not exist).

Configuring Routes to a P1 User

When you add a new P1 user to your message transfer system, `x400tool` attempts to create a default entry in the local routing table. If `x400tool` cannot create a default route, you will have to modify the routing table manually.

For example:

If you already have a remote MTA defined with the same global domain identifier, the local MTA will not create a default route for the P1 user. You must create a new entry in the routing table and add some discriminating attribute (organization name, organizational unit name, etc.) to the route so that your local MTA can forward messages correctly to both systems.

Refer to Chapter 7, “Routing Between Agents” for detailed instructions on how to modify default routing entries.

Routing Between Agents 7

This chapter describes how to use `x400tool` to modify the routing table used by the local MTA. It also tells you how to use the test routing option to check the entries in the routing table.

Routing in the X.400 Domain

An MTA functions like a traditional postal service sorting office—sorting messages for delivery based on their addresses.

The MTA compares the component attributes of each O/R address against the entries in its local routing table. Each entry associates a given list of attributes with one of the recognized agents in the message transfer system. All messages with an O/R address (or part of an O/R address) that matches one of these lists of attributes will be forwarded to the same destination.

Figure 7-1 shows how messages are to be delivered to three remote MTAs in a typical message transfer system. Each entry in the local routing table is associated with a single remote MTA; however, each remote MTA can be associated with multiple routing entries.

In this example, the MTAs servicing the European headquarters for a company are all located within the same management domain and have the same global domain identifier `/P=EUROHQ/A=ATLAS/C=FR/`. Similarly, the MTAs servicing the United States headquarters are all located within the same management domain and have the same global domain identifier `/P=USHQ/A=MCI/C=US/`.

To differentiate between MTAs within the same global domain, the routing in this example is based on the organization to which the recipient belongs. Thus, messages for members of the sales and marketing groups are relayed through one MTA; messages for members of the product development or test groups are relayed through another. Messages to be delivered to the United States headquarters from outside are always relayed through the same MTA.

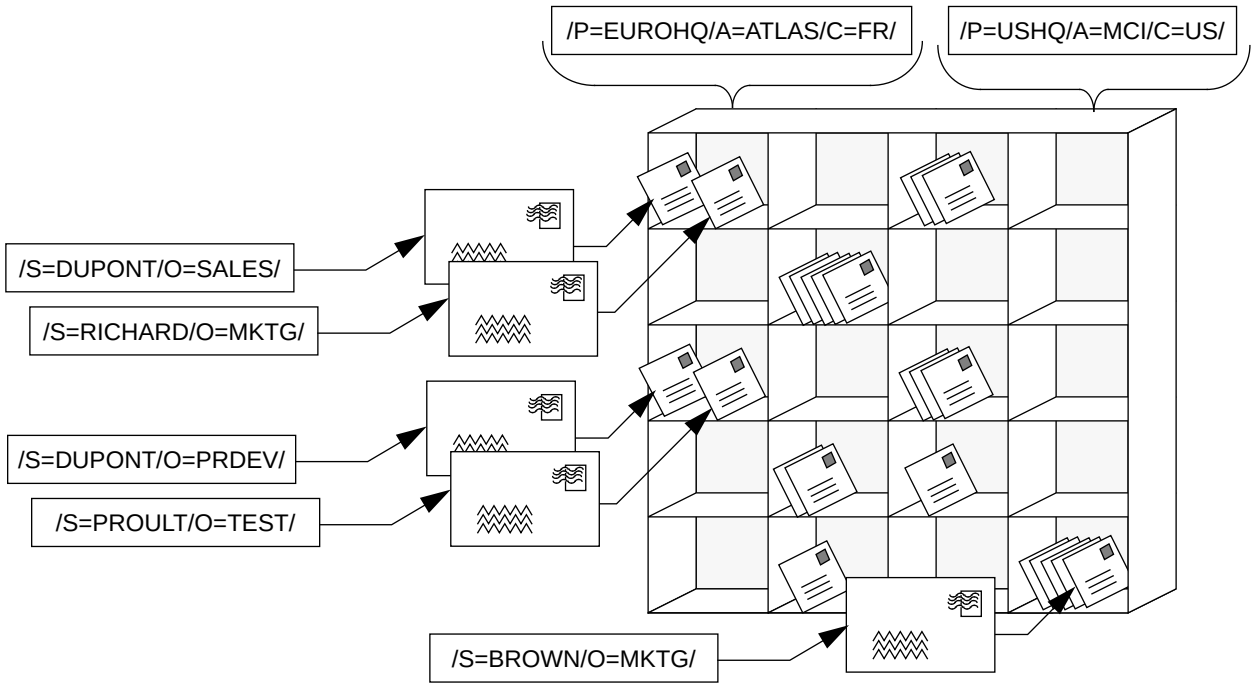


Figure 7-1 Example Routing Algorithm

The default routing entries for agents added to the message transfer system are always based on the global domain identifier; therefore, the routing table in this example will have to be modified to set up the routing algorithm illustrated in Figure 7-2.

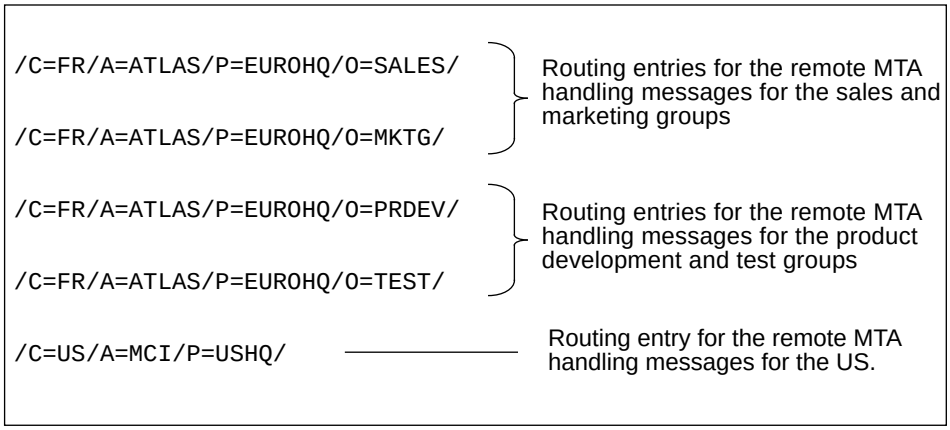


Figure 7-2 Example Routing Entries

Default Routing Entries

When you add a remote MTA or P1 user agent to your message transfer system, `x400tool` attempts to create a default entry in the local routing table. The default route is based upon the global domain identifier for the new agent and in many cases this information will be sufficient to allow your local MTA to route or relay messages to it.

A default routing entry is of the form:

/ C=<*country_code*> / A=<*admd*> / P=<*prmd*> /

Before creating the default entry, `x400tool` checks the local routing table for an identical entry. If a similar entry already exists, the default entry is not created and `x400tool` issues a warning that tells you to modify the default routing table. You will also need to modify the default routing entry if you want to improve the efficiency of the routing algorithm.

7

Modifying the Default Routing Table

The routing table for the local MTA is composed of groups of entries. Each group of entries is associated with one of the agents (remote MTA, X.400/SMTP(MIME) gateway, local user agents, and P1 users) in the local message transfer system.

Configure *Activating the Routing Window*

To activate the Routing window for one of the agents in your local message transfer system:

1. **Click SELECT on its icon to highlight it.**
2. **Press MENU on the Configure menu button and drag the pointer to the Modify Routing item. Release MENU to activate the Routing window for the currently selected agent.**

The Routing window has a scrolling-list that contains the current routing entries for the selected agent. You can add new routing entries to this list, or modify existing entries.

Add Route *Adding a New Routing Entry*

To add a new routing entry to the scrolling-list:

1. **Activate the Routing window for a selected agent in the local message transfer system.**
2. **Specify a global domain identifier of the agent (country, ADMD, and optionally, a PRMD) as the foundation for your routing entry.**
   You must specify a country code and an ADMD. Use the Domain Help to locate this information, if required. If the agent is not part of an established ADMD you must enter a blank space.
3. **Specify any other attributes that will be used to sort the messages sent to the selected agent.**
   Refer to the description of O/R addresses in “X.400 Addressing” on page 7 for description of the valid O/R address types.
4. **Click SELECT on Add Route to place the new routing entry in the scrolling-list.**

Change Route *Modifying an Existing Routing Entry*

To modify an existing routing entry:

1. **Activate the Routing window for one of the agents in the local message transfer system.**
2. **Click SELECT on one of the entries in the scrolling-list to highlight it and display its component attributes.**
3. **Specify a global domain identifier (country, ADMD, and optional PRMD) as the foundation for your routing entry.**
   You must specify a country code and an ADMD. Use the Domain Help to locate this information, if required. If the agent is not part of an established ADMD you must enter a blank space.
4. **Specify any other attributes that will be used to sort the messages sent to the selected agent.**
   Refer to the description of O/R addresses in "X.400 Addressing" on page 7 for description of the valid O/R address types.
5. **Click SELECT on Change Route to replace the selected entry in the scrolling-list.**

Delete Route *Deleting an Existing Routing Entry*

To delete an existing routing entry:

1. **Activate the Routing window for one of the agents in the local message transfer system.**
2. **Click SELECT on one of the entries in the scrolling-list to highlight it and display its component attributes.**
3. **Click SELECT on Delete Route to remove the selected entry from the scrolling-list.**

Defining the Alternate Recipient for a User Agent

Change Alternate

The alternate recipient address is used by the local MTA if it cannot route a message to the user agent defined by the O/R address contained in the message.

For example:

If the message contains a body part of a type that is not supported by the user agent specified by the O/R address in the message, the local MTA will forward the message to the alternate recipient address if one is defined.

You must choose the alternate recipient from the list of addresses you created when you configured the local MTA. Refer to "Specifying Alternate Recipients for User Agents" on page 57 for detailed instructions.

To define the alternate recipient for a user agent:

1. **Activate the Routing window for one of the third-party user agents in your local message transfer system.**
2. **Click SELECT on the Change Alternate button to display the list of alternate recipients that you created when you configured the local MTA.**
3. **Click SELECT to choose one of the addresses in this list.**
4. **Click SELECT on Apply to assign the highlighted address.**

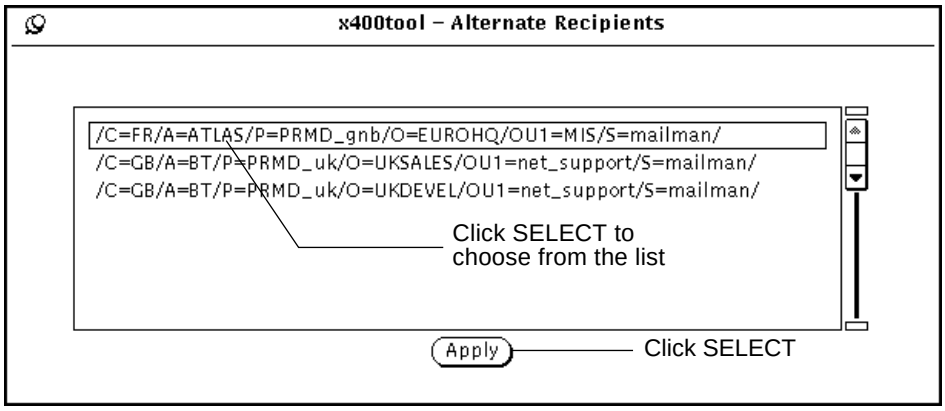


Figure 7-3 Choosing from the of Alternate Recipients

Testing the Routing Algorithm

You can use `x400tool` to test the routing algorithm defined by the entries in the local routing table. This feature does not send any messages; it tells you if the local MTA would be able to route a message based on a given O/R address.

To test the routing algorithm:

1. **Press MENU on the Test menu button and drag the pointer to the Test Routing item. Release MENU to activate the Test Routing window.**
2. **Type in the component attributes for the O/R address you want to test.** Refer to the description of O/R addresses in “X.400 Addressing” on page 7 for description of the valid O/R address types.

- Click SELECT to check the box for Use Default MTA if you want to allow the local MTA to use the default (“catch-all”) MTA to route messages that it cannot forward in any other way. See “Setting a Default MTA” on page 95 for more information.
- Click SELECT to check the box for Use Alternate Recipients if you want the local MTA to make use of any alternate recipients you may have defined for the third-party user agents in the message transfer system. See “Defining the Alternate Recipient for a User Agent” on page 116 for more information.

3. **Click SELECT on Test to see if the local MTA is able to route messages containing the specified O/R address.**

There are three possible results:

Routing Possible: If the local MTA is able to route the message it displays a status message in the bottom-left corner of the Test Routing window. This message includes the name of the agent that would have received the message, based on the current routing algorithm.

Routing Ambiguous: If the routing algorithm generates an ambiguous result—for example, if the local MTA is unable to distinguish between two possible destinations— or if the format of the O/R address is not compliant with the X.400 specification, `x400tool` generates an error message. This may occur if you have not specified enough details for the test route, for example, missing surname.

Routing Impossible: If the local MTA cannot route the message at all `x400tool` generates an error message.

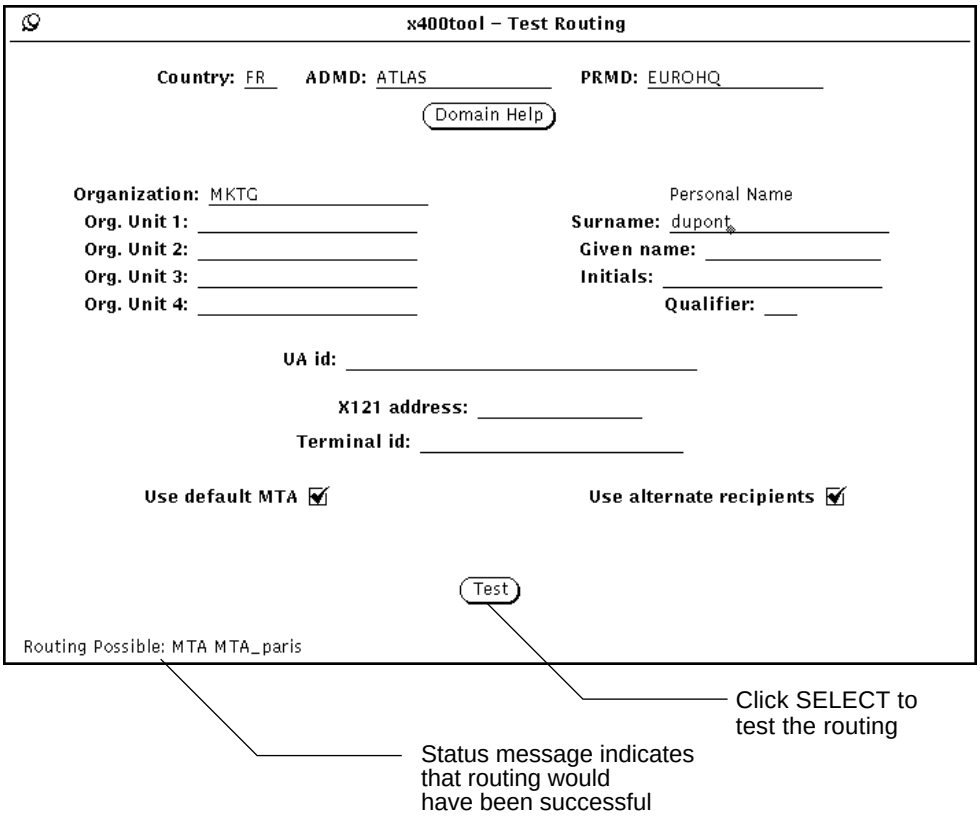


Figure 7-4 Testing the Routing Algorithm

Sending and Receiving UNIX Mail 8

This chapter describes how to use UNIX mail applications (such as `mailx` and `mailtool`) running in Solaris environments send and receive messages through the X.400/SMTP gateway. It assumes that you have already set up your message transfer system, including your local MTA and an X.400/SMTP gateway.

For detailed information on setting up a mail service entirely within the UNIX domain, see Chapter 8, “Understanding Mail Services”, in your Solaris *Setting Up User Accounts, Printers, and Mail* document for a detailed description of the components of a UNIX mail system.

Sending Messages using `mail` *or* `mailx`

The `mail(1)` and `mailx(1)` applications are interactive, command-line utilities for sending and receiving electronic mail messages. Although not identical, these utilities are very similar. (The `mailx` utility was introduced by UNIX System V, Release 2 and was patterned after the `mail` utility developed for Berkeley UNIX.)

They both rely on the `sendmail(8)` daemon to route messages between users. After the `sendmail` daemon has been reconfigured (by modifying `sendmail.cf`), you can use `mail` to exchange mail messages directly with the X.400 domain through the X.400/SMTP(MIME) gateway.

Addressing Messages to the Gateway

To address mail to a recipient through the X.400/SMTP(MIME) gateway, you need to specify the local address of the recipient and the domain address of the gateway.

The complete domain address for the X.400/SMTP(MIME) gateway is comprised of the pseudo host name (alias) assigned to the gateway, and the domain address of the UNIX mail domain in which the gateway is located. You can express the recipient's local address as a UNIX mail alias or as a full X.400-style address.

For example:

To use `mail` or `mailx` to send a message to a recipient Jane Bond whose local mail alias is `jbond` through an X.400/SMTP(MIME) gateway with a pseudo host name `x400-gate`, located in the domain `Division.Company.COM`:

```
host% mail jbond@x400-gate.Division.Company.COM
Subject:test
This is a test message.
.
EOT
host%
```

To use `mail` or `mailx` to send a message to the same recipient by specifying the full X.400 O/R address:

```
host% mail
/S=jbond/O=XYZ/A=BT/C=UK/@x400-gate.Division.Company.COM
Subject:test
This is a test message.
.
EOT
host%
```

When addressing messages to a gateway located within the same UNIX mail domain, you do not need to specify the full domain name for the X.400/SMTP(MIME) gateway.

To use `mail` or `mailx` to send a message to a recipient in the same UNIX mail domain:

```
host% mail /S=jbond/O=XYZ/A=BT/C=UK/@x400-gate
Subject:test
This is a test message.
.
EOT
host%
```

Sending Messages Using `mailtool`

The `mailtool(1)` application is an OpenWindows-based program for sending and receiving electronic mail messages. It provides a user-friendly interface for composing and manipulating messages through a system of menus and windows.

Addressing Messages to the Gateway

To address mail to a recipient through the X.400/SMTP(MIME) gateway, you need to specify the local address of the recipient and the domain address of the gateway.

The complete domain address for the X.400/SMTP(MIME) gateway is comprised of the pseudo host name (alias) assigned to the gateway, and the domain address of the UNIX mail domain in which the gateway is located. You can express the recipient's local address as a UNIX mail alias or as a full X.400-style address.

For example:

Figure 8-1 on page 122 shows how to use `mailtool` to send a message to a recipient Claire Bright whose local mail alias is `cbright` through an X.400/SMTP(MIME) gateway with a pseudo host name `x400-gate`, located in the domain `Division.Company.COM`.

Note that you can check the way that the gateway converts the UNIX address into an X.400 address using the Address Conversion feature. See “Testing the X.400/SMTP(MIME) Gateway” on page 69.

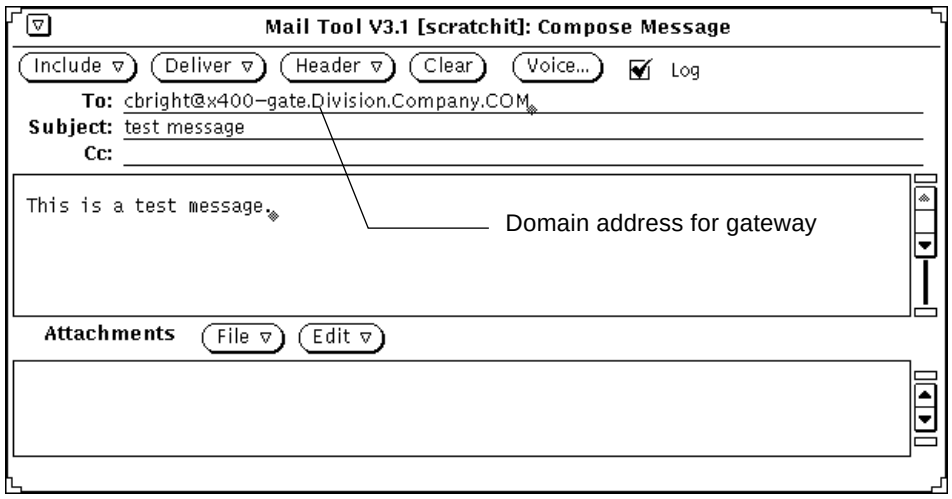


Figure 8-1 Sending Messages using an Alias

Figure 8-2 shows how to use `mailtool` to send a message to the same recipient by specifying the full X.400 O/R address:

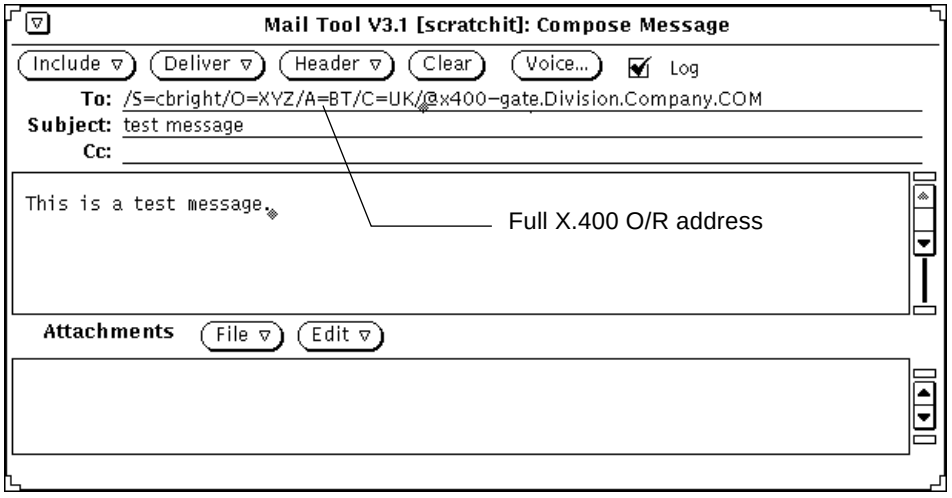


Figure 8-2 Sending Messages using an X.400 O/R Address

Using X.400 Mail Headers

X.400 mail headers are used to carry additional information and to modify the behavior of the mail delivery system on a per-message basis—for example, to mark the message for urgent delivery.

The X.400/SMTP(MIME) supports all the mail headers specified within RFC 822, and additional headers specified in RFC 987 and RFC 1327, as listed in Table 8-1. The most commonly used headers are shown in bold type.

Table 8-1 Supported Mail Headers

Header	**Usage**
Alternate-recipient-allowed	true/false
Bcc (blind carbon copy)	recipient address
Bilateral-info	string
Cc (carbon copy)	**recipient address**
Content-identifier	string
Conversion	true/false
Conversion-prohibited	true/false
Conversion-with-loss	true/false
Deferred-delivery	date
Delivery-Report	**always/never/audited/non-delivery**
Disclose-Recipient	true/false
Expiry-Date	RFC 822 format date
Importance	**low/high/routine**
In-reply-to	message id
Incomplete-copy	true/false
Language	one or more country codes (separated by ",")
Latest-delivery-time	date
Obsoletes	message-id
Originator-return-address	originator address
Prevent-non-delivery-notification	true/false

Table 8-1 Supported Mail Headers

Header	Usage
Priority	**low/urgent/normal**
Receipt-Notification	**always/non-receipt/never**
References	message id
Repertoire	ITA2/IA5
Reply-by	date
Reply-to	originator address
Request-delivery-notification	true/false
Sensitivity	personal/private/confidential/non-sensitive
Subject	string
To	recipient address

You set the X.400 headers from within `mailtool` by defining custom headers that you can add to the composition window.

To define a custom header:

1. **Press and drag MENU on the Edit pull-down menu.**
2. **Release MENU on the Properties... item to activate the Properties window.**
3. **Press and drag MENU on the Category pull-down menu. Release MENU on the Compose Window item.**
4. **Type in the name of the header on the Header Field input line.**
   Type in your preferred default value, if applicable. Refer to Table 8-1 on page 123 for details.
5. **Click SELECT on the Add button to place the custom header in the scrolling-list.**
6. **Click SELECT on the Apply button to apply your changes and add the custom headers to the compose window.**

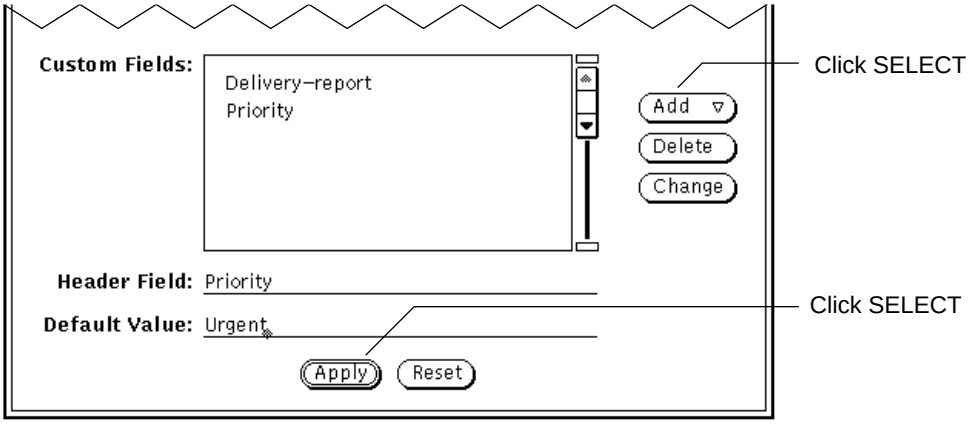


Figure 8-3 Defining a Custom Mail Header

To add a custom header to a message from within `mailtool`:

1. **Press and drag MENU on the Header pull-down menu.**
2. **Release MENU on the custom header that you want to add.**

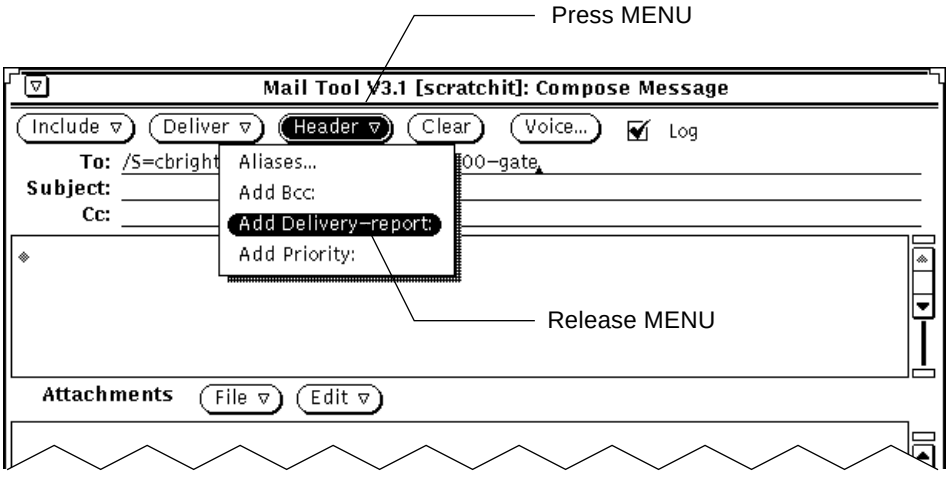


Figure 8-4 Adding a Custom Header

8

Sending Messages with International Character Sets

The X.400/SMTP(MIME) gateway supports the translation of the international character sets supported by the Sun UNIX mail applications.

When a message that includes international characters is set entirely within the UNIX mail domain, the service element `X-Sun-Charset` is set automatically to `ISO-8859-1`. Figure 8-5 on page 126 shows the full header of a message containing international characters and sent to a recipient in the UNIX mail domain.

When the message is received by the X.400/SMTP(MIME) gateway, the `X-Sun-Charset` service element is translated into the X.400 service element `Original-Encoded-Information-Types` and set to `ISO-6937-Text`. ISO-6937 provides full IA5 (ASCII), Teletext (T.61 a subset of ASCII), plus international (8 bit) characters. Figure 8-6 on page 127 shows the same message sent through the gateway.

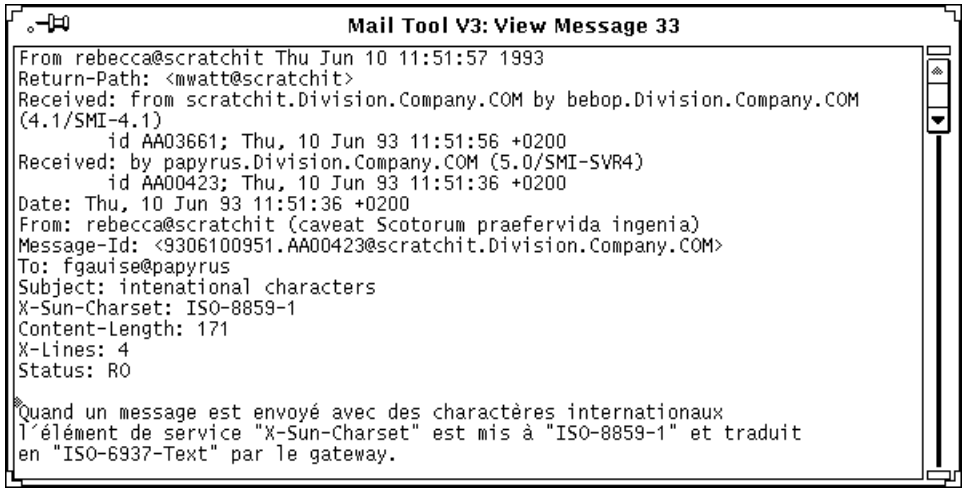


Figure 8-5 International Characters in the UNIX Mail Domain

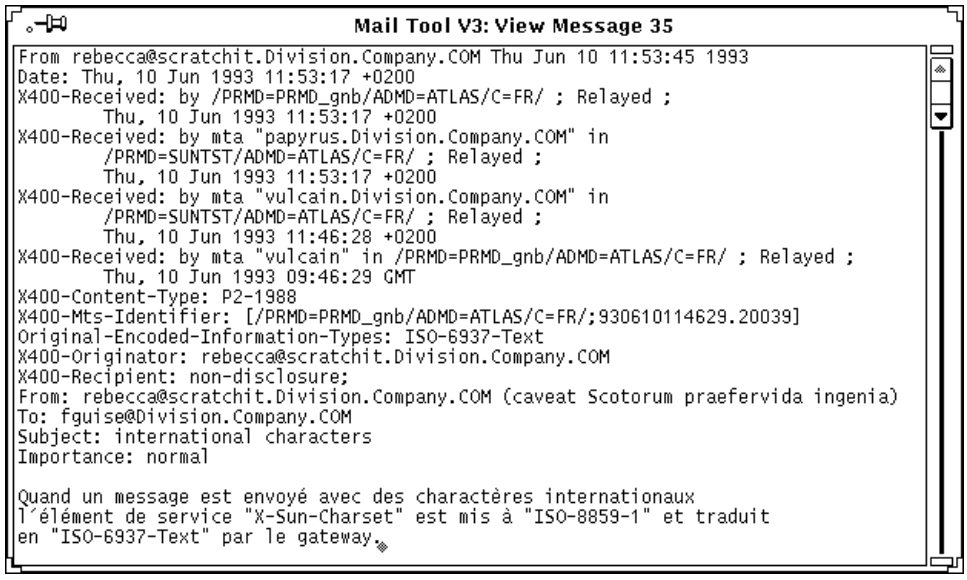


Figure 8-6 International Characters Through the Gateway

8

Mapping X.400 and UNIX Addresses

Some UNIX mail addresses contain ASCII characters that are not directly mapped to X.400 address elements. Abbreviations are used to represent characters such as “@”, “%”, and “!”, which appear commonly in UNIX mail addresses. Table 8-2 lists these special abbreviations:

Table 8-2 X.400 Abbreviations

X.400 Abbreviation	**ASCII Character**	
(a)	@	at character
(p)	%	percentage
(b)	!	exclamation (bang)
(q)	“	double-quotes
(u)	_	underscore
(l)	(	left parenthesis (bracket)
(r)	)	right parenthesis (bracket)

For example:

To map a UNIX mail address of the form:

```
blond!renzo@Division.Company.COM
```

The country, ADMD, and PRMD point to the X.400/SMTP(MIME) gateway that accesses the X.400 mail domain. The UNIX mail address can be specified by using the domain-defined identifier `DD.RFC-822`, as shown:

```
/C=US/A=MCI/P=XYZ/DD.RFC-822=blond(b)renzo(a)Division.Company.COM/
```

Managing Your Message Transfer System 9

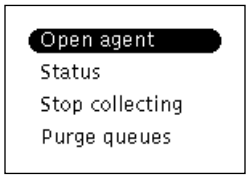
This chapter describes how to use `x400tool` to maintain your message handling system and to gather information about the current state of its component parts. It assumes that you have already set up your message transfer system, including your local MTA and an X.400/SMTP gateway.

Opening and Closing Agents

Closing an agent breaks its association with the local MTA, but does not remove it from the message transfer system. It will not be recognized by the local MTA or by any other agent. You cannot close your local MTA.

While an agent is closed, it will neither accept nor forward messages. Incoming message transfers in progress when an agent is closed are aborted and a non-delivery message is generated.

Manage ▽ *Opening a Closed Agent*



An agent can be closed either automatically or manually. To reopen an agent after it has been closed:

1. **Click SELECT on an agent that is showing "Closed" in its icon.**
2. **Press MENU on the Manage menu button and drag the pointer to the Open agent item. Release MENU to reopen the closed agent.**

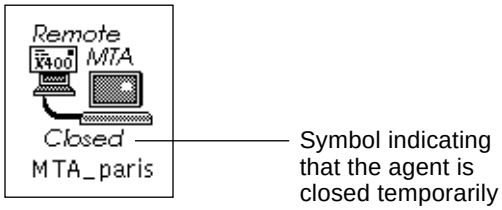
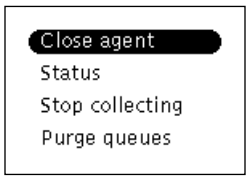


Figure 9-1 A Closed Message Transfer Agent

Manage ▽ *Closing an Open Agent*



An agent can be closed either automatically or manually. It might be closed automatically if it does not respond to the local MTA after a specified time, and there are no pending messages. To close an agent manually:

1. **Click SELECT on an open agent.**
2. **Press MENU on the Manage menu button and drag the pointer to the Close agent item. Release MENU to close the open agent.**

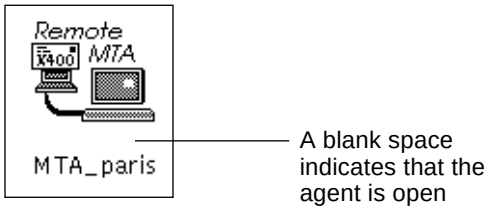
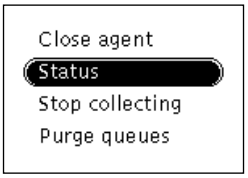


Figure 9-2 An Open Message Transfer Agent

Displaying Status Information

There is a status window associated with each element of your message transfer system. These windows display the status of the agent, current at the time that the window was last refreshed. Status windows can be refreshed automatically at specific intervals or refreshed manually. The behavior of the status windows is determined by setting the `x400tool` properties. Refer to “Changing the Tool Properties” on page 30” for detailed instructions.

Manage ▽ *Activating a Status Window*



To display the status window for one of the elements in your message transfer system:

1. **Click SELECT on its icon.**
2. **Press MENU on the Manage menu button and drag the pointer to the Status item. Release MENU to activate the associated status window.**

Refresh *Refreshing a Status Window Manually*

If you have selected manual refresh for the `x400tool` status windows (see “Changing the Tool Properties” on page 30) or if you want to see the most recent status for one of the agents, you can use the refresh button on each window to update the information displayed.

1. **Activate the Status window for one of the agents.**
2. **Click SELECT on the refresh button to update the information.**

Print *Printing the Current Status*

To print a summary of all the status information associated with a given element in the message transfer system:

1. **Activate the Status window for one of the agents.**
2. **Click SELECT on Print to activate the Print Selection subwindow.**
3. **Either choose the name of a printer from the pull-down menu, or specify the name of a file. Click SELECT on Print to print the status information.**

Displaying the Status of the Local MTA

The local MTA status window displays the information about the flow of messages throughout the message transfer system, as seen from the local MTA.

Use the local MTA status window to examine:

Queues

The current state of the queues for incoming messages (messages sent to the local MTA) and outgoing messages (messages sent by the local MTA) at the time the window was last refreshed. The information is displayed as the total number of messages of each type (urgent, normal, non-urgent, and notifications) and the volume of data (in bytes) held in each queue.

Traffic

A summary of the total traffic flow (messages sent and received) through the local MTA since it was last restarted, and the total number of associations open at the time the window was last refreshed.

Number of current associations: The total number of associations open between the local MTA and the other agents in the message transfer system at the time the window was last refreshed.

Total number of messages sent by local MTA: The total number of messages sent by the local MTA to other agents (MTAs, gateways, or user agents) in the message transfer system.

Total number of messages received by local MTA: The total number of messages received by the local MTA from other agents (MTAs, gateways, or user agents) in the message transfer system.

Failures

A summary of the total failed transfers and errors occurring since the local MTA was last restarted.

Authentication failures sent: The number of times that the local MTA has rejected an association indication from a remote MTA because the OSI address or password presented was incorrect.

Authentication failures received: The number of times that a remote MTA has rejected an association request from the local MTA because the OSI address or password presented was incorrect.

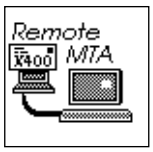
RTS busy indications sent: The number of RTS (reliable transfer system) busy indications sent by the local MTA to remote MTAs.

RTS busy indications received: The number of RTS (reliable transfer system) busy indications received by the local MTA from remote MTAs.

Abnormal transfers when sending: The number of abnormal transfers that occurred when the local MTA was sending outgoing messages.

Abnormal transfers when receiving: The number of abnormal transfers that occurred when the local MTA was receiving incoming messages.

Unacceptable dialog mode received: The number of times that a connection was refused with the reason "unacceptable dialog mode". For example, a two-way connection was attempted with a remote MTA that is configured for monologue only.



Displaying the Status of a Remote MTA

The remote MTA status window displays information about the performance of the association between the local MTA and a given remote MTA, as seen from the local MTA.

Use the remote MTA status window to examine:

Queues

The current state of the queues for outgoing messages—that is, messages sent from the local MTA to the remote MTA—at the time the window was last refreshed. The information is displayed as the total number of messages of each type (urgent, normal, non-urgent, and notifications) and the volume of data (in bytes) in each queue.

Traffic

A summary of the traffic flow (messages sent and received) between the local MTA and the remote MTA since the local MTA was last restarted, and the total number of associations open at the time the window was last refreshed.

Number of current associations: The total number of associations open between the local MTA and the remote MTA at the time the window was last refreshed.

Total number of messages sent by local MTA: The total number of messages sent by the local MTA to the remote MTA.

Total number of messages received by local MTA: The total number of messages received by the local MTA from the remote MTA.

Total number of bytes sent by local MTA: The total number of bytes sent by the local MTA to the remote MTA.

Total number of bytes received by the local MTA: The total number of bytes received by the local MTA from the remote MTA.

Connection

The current state of the remote MTA at the time the window was last refreshed, and a summary of the of the connection negotiation between the local MTA and the remote MTA since the time that the local MTA was last restarted.

Current state: The current state of the remote MTA (open or closed) and the current state of the association (if the remote MTA is open).

Connection requests sent: the number of times that the local MTA has issued a connection request to the remote MTA.

Connection responses received: the number of times the remote MTA has responded to a connection request from the local MTA.

Connection indications received: The number of times that the local MTA has received a connection indication from a remote MTA requesting an association.

Connection confirmation sent: The number of times that the local MTA has sent a connection confirmation in response to a connection request from the remote MTA.

Failures

A summary of the failed transfers and errors associated with the selected remote MTA since the local MTA was last restarted.

Authentication failures sent: The number of times that the local MTA has rejected an association indication from the selected remote MTA because the OSI address or password presented was incorrect.

Authentication failures received: The number of times that the selected remote MTA has rejected an association request from the local MTA because the OSI address or password presented was incorrect.

RTS busy indications sent: The number of RTS (reliable transfer system) busy indications sent by the local MTA to the selected remote MTA.

RTS busy indications received: The number of RTS (reliable transfer system) busy indications received by the local MTA from the selected remote MTA.

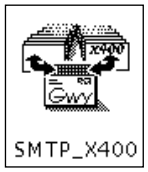
Abnormal transfers when sending: The number of abnormal transfers that occurred when the local MTA was sending outgoing messages to the selected remote MTA.

Abnormal transfers when receiving: The number of abnormal transfers that occurred when the local MTA was receiving incoming messages from the selected remote MTA.

Connection abort sent: The number of times that the local MTA has generated a connection abort to request the breaking of a connection.

Connection abort indication received: The number of times that the local MTA has received a connection abort request from the selected remote MTA.

Unacceptable dialog mode received: The number of times that a connection was refused with the reason "unacceptable dialog mode". For example, a two-way connection was attempted with a remote MTA that is configured for monologue only.



Displaying the Status of the X.400/SMTP(MIME) Gateway

The X.400/SMTP gateway status window displays information about the performance of the association between the local MTA and the X.400/SMTP(MIME) gateway (or other P1 user).

Use the X.400/SMTP gateway status window to examine:

Queues

The current state of the queues for outgoing messages—that is, messages sent from the local MTA to the gateway (or P1 user)—at the time the window was last refreshed. The information is displayed as the total number of messages of each type (urgent, normal, non-urgent, and notifications) and the volume of data (in bytes) in each queue.

Traffic

A summary of the traffic flow (messages sent and received) between the local MTA and the gateway since the local MTA was last restarted, and the total number of associations open at the time the window was last refreshed.

Number of current associations: The total number of associations open between the local MTA and the gateway (or P1 User) at the time the window was last refreshed.

Total number of messages sent by local MTA: The total number of messages sent by the local MTA to the gateway (or P1 User).

Total number of messages received by local MTA: The total number of messages received by the local MTA from the gateway (or P1 User).

Total number of bytes sent by the local MTA: The total number of bytes sent by the local MTA to the gateway.

Total number of bytes received by the local MTA: Total number of bytes received by the local MTA from the gateway.

Connection

The current state of the gateway (or P1 user) at the time the window was last refreshed, and a summary of the of the connection negotiation exchanged between the local MTA and the gateway since the time that the local MTA was last restarted or the statistics collection was started.

Current state: The current state of the gateway (open or closed) and the current state of the association (if the gateway is open).

Connection requests sent: the number of times that the local MTA has issued a connection request to the gateway.

Connection responses received: the number of times the gateway has responded to a connection request from the local MTA.

Connection indications received: The number of times that the local MTA has received a connection indication from a gateway requesting an association.

Connection confirmations sent: The number of times that the local MTA has sent a connection confirmation in response to a connection indication from the gateway.

Failures

A summary of the failed transfers and errors associated with the selected remote MTA since the local MTA was last restarted.

Authentication failures sent: The number of times that the local MTA has rejected an association indication from the gateway because the OSI address or password presented was incorrect.

Authentication failures received: The number of times that the gateway has rejected an association request from the local MTA because the OSI address or password presented was incorrect.

RTS busy indications sent: The number of RTS (reliable transfer system) busy indications sent by the local MTA to the gateway.

RTS busy indications received: The number of RTS (reliable transfer system) busy indications received by the local MTA from the gateway.

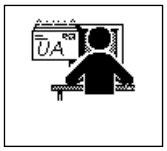
Abnormal transfers when sending: The number of abnormal transfers that occurred when the local MTA was sending outgoing messages to the gateway.

Abnormal transfers when receiving: The number of abnormal transfers that occurred when the local MTA was receiving incoming messages from the gateway.

Connection abort sent: The number of times that the local MTA has generated a connection abort to request the breaking of a connection with the gateway.

Connection abort indication received: The number of times that the local MTA has received a connection abort request from the gateway.

Unacceptable dialog mode received: The number of times that an error occurred when the local MTA was negotiating the handshaking applied to the exchange of messages with the gateway.



Displaying the Status of a User Agent

The user agent status window displays information about the performance of the connection between the local MTA and a User Agent.

Use the User Agent status window to examine:

Queue

The current state of the queues for outgoing messages—that is, messages sent from the local MTA to the user agent—at the time the window was last refreshed. The information is displayed as the total number of messages of each type (urgent, normal, non-urgent, and notifications) and the volume of data (in bytes) in each queue.

Traffic

A summary of the traffic flow (messages submitted and delivered) between the local MTA and the selected user agent since the local MTA was last restarted expressed in terms of the number of messages and the total number of bytes of data.

Messages Submitted: The number of messages sent from the user agent to the local MTA.

Messages Delivered: The number of messages sent from the local MTA to the user agent.

Bytes Submitted: The number of bytes sent from the user agent to the local MTA.

Bytes Delivered: The number of bytes sent from the local MTA to the user agent.

Connection

The current state of the user agent at the time the window was last refreshed, and a summary of the of the connection negotiation exchanged between the local MTA and the user agent since the time that the local MTA was last restarted.

Current state: The current state of the user agent (open or closed) and the current state of the association (if the user agent is open).

Connection requests sent: the number of times that the local MTA has issued a connection request to the user agent.

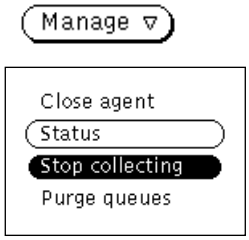
Connection responses received: the number of times the user agent has responded to a connection request from the local MTA.

Connection indication received: The number of times that the local MTA has received a connection indication from the user agent requesting a connection.

Connection confirmations sent: The number of times that the local MTA has sent a connection confirmation in response to a connection indication from the user agent.

Notification indications received: The number of times that the local MTA has received a notification indication from the user agent.

Stopping and Starting Statistics Collection



The information displayed in the `x400tool` status windows is based on data recovered from the message transfer system. You can improve the performance of your local MTA by switching this feature off.

You can only view status information if you have started statistics collection.

To stop collecting statistics from your message transfer system:

- Press MENU on the Manage menu button and drag the pointer to the Stop Collecting item. Release MENU to stop collecting statistics.

To restart collecting statistics from your message transfer system:

- Press MENU on the Manage menu button and drag the pointer to the Start Collecting item. Release MENU to start collecting statistics.

Journal Files

Journal files are automatically used to record messaging activity. These files are found in the directory `/var/SUNWconn/OSIROOT/spool`. There are two files, `journal1` and `journal2`. Each file holds up to 500 messages. Once one file is full SunLink X.400 switches to the other, alternating between the two every 500 messages. In this way a maximum of 1000 messages are recorded at any time.

An example journal file is shown below:

```
                **-----------------------------------**
94/08/12 13:29:02  ==>[0]  SunLink X.400 8.0.2 started
94/08/12 13:29:16  ==>[6]  Connection   indication from     MTA SMTP_X400.
94/08/12 13:29:16  ==>[7]  Connection   response   to       MTA SMTP_X400.
94/08/15 09:02:37  ==>[2]  Connection   request    to       MTA MTA_paris.
94/08/15 09:02:37  ==>[9]  Abort       indication from     MTA MTA_paris.
94/08/15 09:02:39  ==>[2]  Connection   request    to       MTA MTA_paris.
94/08/15 09:05:44  ==>[3]  Connection   confirm    from     MTA MTA_paris.
94/08/15 09:03:22  ==>[1]  SunLink X.400 8.0.2 stopped
```

Note – P1 users (SMTP_X400) are seen as MTAs in the journal file.

Purging the Mail Queues

When you purge the message queues, you remove either one or all the messages that are currently waiting to be delivered. This is a risky undertaking because there is no way to determine the content of the messages in the queue and there is the chance that you will destroy valuable correspondence. However, under exceptional circumstances, this feature can be used to unblock your message transfer system if there is a severe problem with one or more messages in the queue.

For example:

If your local MTA tries to send an unusually large message to a remote MTA that is unable to cope with it, the message may block the queue and trap a number of smaller messages behind it. In this case, you should purge the first message in the queue to resolve the problem. You will lose the contents of the first message, but the other messages will be delivered correctly.

Caution – Do not delete the files associated with the mail queues (or any other files associated with SunLink X.400 8.0.2). Always use the *purge* option if you need to clear the message queues.

Purging All Incoming Messages

Incoming messages are messages sent by the other agents in your message transfer system to the local MTA.

To purge all the queues containing incoming messages:

1. **Click SELECT on the icon for the local MTA.**
2. **Press MENU on the Manage menu button and drag the pointer to the Purge Queues item. Release MENU to activate the Purge Messages window for the local MTA.**
3. **Click SELECT on the check box for All Incoming Messages to specify the queues affected by the purge.**
4. **Click SELECT on the Purge button to remove all the messages waiting in incoming queues.**

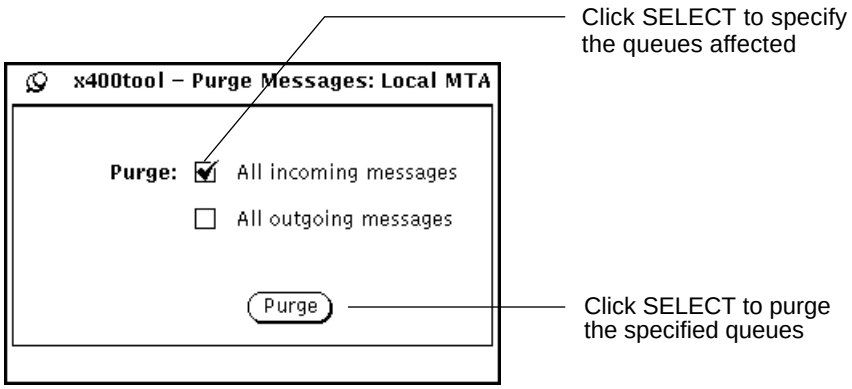


Figure 9-3 Purging Incoming Messages

Purging All Outgoing Messages

Outgoing messages are messages sent by the local MTA to the other agents in your message transfer system.

To purge all the queues containing outgoing messages:

1. **Click SELECT on the icon for the local MTA.**
2. **Press MENU on the Manage menu button and drag the pointer to the Purge Queues item. Release MENU to activate the Purge Messages window for the local MTA.**

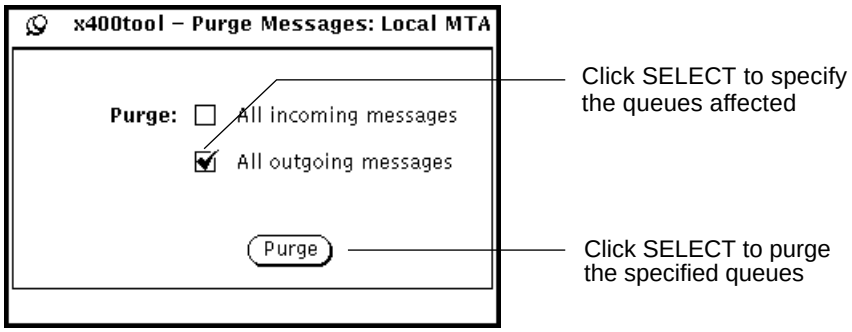


Figure 9-4 Purging Outgoing Messages

3. **Click SELECT on the check box for All Outgoing Messages to specify the queues affected by the purge.**
4. **Click SELECT on the Purge button to remove all the messages waiting in outgoing queues.**

Purging the First Message in the Queue

The local MTA holds the outgoing messages waiting to be sent to a given agent (remote MTA, X.400/SMTP(MIME) gateway, P1 user, or user agent) in a separate queue. You can purge the first message in the queue without affecting the other messages in it.

To purge the first message in the queue:

1. **Click SELECT on the icon for a remote MTA, X.400/SMTP(MIME) gateway, P1 user, or user agent.**
2. **Press MENU on the Manage menu button and drag the pointer to the Purge Queues item. Release MENU to activate the Purge Messages window for the local MTA.**
3. **Click SELECT on the First Message button to specify the first message only.**
4. **Click SELECT on the Purge button to remove all the messages waiting in outgoing queue for the selected agent.**

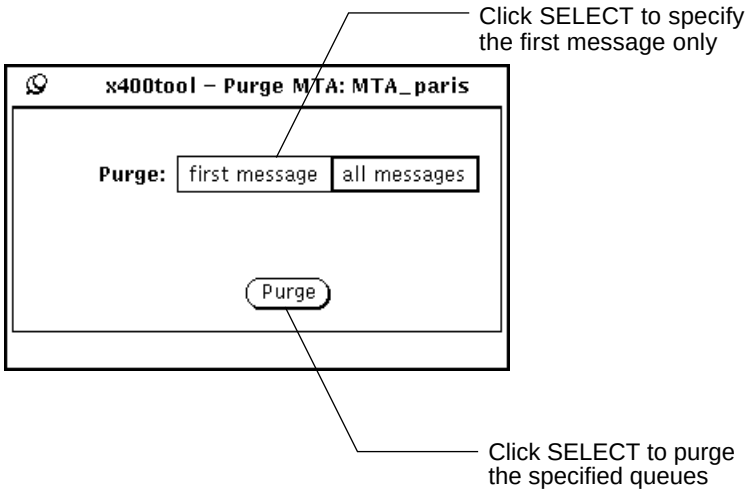


Figure 9-5 Purging the First Message in the Queue

Purging Messages for a Specific Agent

The local MTA holds the outgoing messages waiting to be sent to a given agent (remote MTA, X.400/SMTP(MIME) gateway, P1 user, or user agent) in a specific queue. You can purge the messages queued for one agent without affecting the queues for the other agents in the message transfer system.

To purge the queue containing outgoing messages for a specific agent:

1. **Click SELECT on the icon for a remote MTA, X.400/SMTP(MIME) gateway, P1 user, or user agent.**
2. **Press MENU on the Manage menu button and drag the pointer to the Purge Queues item. Release MENU to activate the Purge Messages window for the local MTA.**
3. **Click SELECT on the All Messages button to specify the queues affected by the purge.**
4. **Click SELECT on the Purge button to remove all the messages waiting in outgoing queue for the selected agent.**

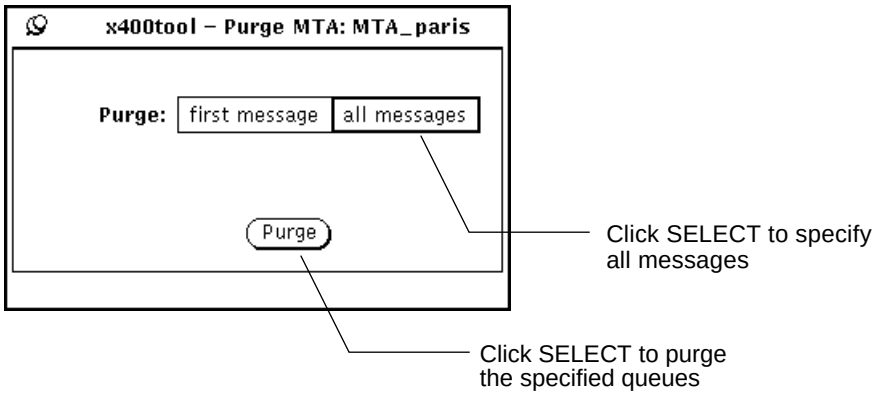


Figure 9-6 Purging Messages for a Specific Agent

9

Regenerating the Configuration from Text

The file <*prefix*>`.mhscf.text` is created when you backup your configuration and each time you change your current configuration. It is a textual representation of the current configuration and is used by the software to build the configuration for each component of X.400. You can use this file to transfer the configuration to another machine without copying all the related configuration files or to regenerate a lost configuration. To regenerate the configuration from the text file:

1. **Exit from** `x400tool`**, if necessary.**
   Press MENU in the title bar at the top of the tool and drag the pointer down and release it on Quit.

2. **Make sure that you are logged in as** `root`**, or** `superuser`**.**

3. **Stop the local MTA, X.400/SMTP(MIME) gateway, and the message queue access, if these processes are running**:

```
hostname# /opt/SUNWconn/bin/osistop osimta osix400mqa osismtpx400
```

4. **Change to the directory where the text file is located. By default, this is** `/var/SUNWconn/OSIROOT/mhs/conf`:

```
hostname# cd /var/SUNWconn/OSIROOT/mhs/conf
```

5. **Regenerate the configuration using** `x400_genconf`:

```
hostname# /opt/SUNWconn/bin/x400_genconf <prefix>.mhscf.text
```

   You might have to respond to some questions depending on your configuration, for example, to confirm that the configuration files can be overwritten.

6. **When the configuration has been re-generated, restart the local MTA and X.400/SMTP (MIME) gateway with**:

```
hostname# /opt/SUNWconn/bin/osistart osimta osix400mqa osismtpx400
```

You can now restart `x400tool` to configure and manage your X.400 network. If you copied this configuration from another system, you will have to update some of the addressing information.

Troubleshooting with `x400trace`

The SunLink X.400 8.0.2 tracing facility (`x400trace`) is used to return dynamic information recovered from the local MTA.

To start `x400trace`:

```
hostname# x400trace [-d] [-a] <filters>
```

The command-line options are:

-d: Used to recover a full trace of the internal reliable transfer service (RTS) and ACSE presentation.

-a: Used to recover a full trace of internal ASN.1 decoded information (raw state).

Valid filters are shown in Table 9-1

Table 9-1 `x400trace` Filters

Filters	Description
events	Returns status and error messages recovered from the local MTA and the X.400/SMTP(MIME) gateway.
pdu	Returns ASN.1 decoding of incoming and outgoing messages.
xom	Returns XOM objects sent and received by the X.400/SMTP(MIME) gateway.
rts	Returns a trace from the reliable transfer service (RTS).

Note – Since all requested trace information is saved to the log file `osilogd` in `/var/SUNWconn/osinet`, you should be aware that this file could quickly become very large.

9

Error Messages 10

This chapter provides a list common error messages. Each message is presented with a brief description of the possible cause and a suggested action, if applicable. All messages, errors, events and trace information is logged in `/var/SUNWconn/osinet/osilogd.log`.

Errors Returned by `x400tool`

`\` character forbidden in agent name
You must not use the backslash as part of an agent's name.

/ character forbidden in agent name
You must not use the forwards slash as part of an agent's name.

@ character forbidden in agent name
You must not use the "at" symbol as part of an agent's name.

 # character forbidden in agent name
You must not use the hash (pound) symbol as part of an agent's name.

Agent name can only contain printable characters
The name assigned to an agent must be printable (ASCII) characters.

Agent name must start with a letter
The name assigned to an agent can contain digits, provided the name starts with an alphabetic character.

Alternate Recipient already exists
You cannot assign two alternate recipients with the same O/R address.

An X.25/X.121 address must only contain digits
X.25/X.121 addresses must comprise numbers only; it must not contain non-numeric characters.

Another instance of the tool is already running
Because `x400tool` interacts directly with the local MTA running on the system, you cannot start two instances of `x400tool` on the same machine.

Backing up the configuration will overwrite the following file(s): <*list of files*>
If you specify the name of an existing file to which the configuration backup is to be saved, then that file will be overwritten.

calloc system call failure (<*errno*>**)**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Cannot close gateway while it is running
You must stop the X.400 SMTP gateway process before you can stop the gateway. Use `/usr/SUNWconn/bin/osistop osismtpx400` to stop the gateway process.

Cannot open SMTP/X.400 gateway
You must start the X.400 SMTP gateway process before you can start the gateway. Use `/opt/SUNWconn/bin/osistart osismtpx400` to start the gateway process.

Cannot close MTA <*name*>
The remote MTA cannot be closed. This might happen for example, if the remote MTA has been removed. Restart `x400tool`.

Cannot open MTA <*name*>
The remote MTA cannot be opened. This might happen for example, if the remote MTA has been removed. Restart `x400tool`.

Cannot close P1 user agent <*agent*>
You must stop the MT user application associated with the P1 user agent before it can be closed.

Cannot open P1 user agent <*agent*>
You must start the MT user application associated with the P1 user agent before it can be opened.

Cannot close user agent <*name*>
You must stop the MA user application associated with the specified user agent before it can be closed.

Cannot open user agent <*name*>
You must start the MA user application associated with the specified user agent before it can be opened.

Can't backup configuration
`x400tool` was unable to backup the existing configuration to the specified file. Your file system may be full or the permissions may not be set correctly.

Can't get MHS config file name
`x400tool` was unable to recover the <*prefix*> that defines the name of the current configuration file.

Can't open file: <*filename*>
The specified file does not have the correct access permissions or pathname to be opened.

Can't open new file: <*filename*>
The specified file cannot be created. You may have specified an illegal name or pathname.

Can't open/write file: <*filename*> **- errno** <*errno*>
The specified file does not have the correct access permissions or pathname for it to be opened or written to.

Can't update init file
Indicates a severe internal error that occurred when updating the `osimta.init` file. If this error is returned regularly, please report the occurrence to your authorized service provider.

Can't update `xmh.ini` **file**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Can't update `xom.ini` file
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Country & ADMD must be present
The global domain identifier must have at least a country code and an ADMD defined. If the agent is not part of a recognized ADMD, you can enter a blank space character as the ADMD; however, you must not leave a null entry.

Default route already exists (not created)
When you add an agent to the message transfer system, `x400tool` attempts to create a default entry in the local routing table. The default entry is always based on the global domain identifier assigned to the agent. If an identical entry already exists, `x400tool` generates this warning to inform you that you must modify the routing table manually to add a route for the new agent. See "Modifying the Default Routing Table" on page 114 for detailed instructions.

Deleting incoming queue: failed
There was an error while deleting the incoming message queue. Try again.

Deleting outgoing queue: failed
There was an error while deleting the outgoing message queue. Try again.

Duplicate O/R name *or* Duplicate name
You have created a routing table entry that matches an existing entry, or you have defined an agent with an O/R address that matches that of an existing agent.

Error: name is mandatory
You must define a name for each agent in your message transfer system. Agent names must not include space or tab characters.

Error: no body types supported
A user agent has been defined without specifying any supported body types. This will prevent the local MTA from forwarding any mail to it. Enable at least one body type for the user agent. See "Enabling and Disabling Access Control" on page 99 for more information.

Error: no content type supported
A user agent has been defined without specifying any supported content types. This will prevent the local MTA from forwarding any mail to it. Enable at least one content type for the user agent. See “Enabling and Disabling Access Control” on page 99 for more information.

Error: non-numeric content type
The value assigned to the non-standard content type defined for a user agent must be numeric.

Error: standard content type
The value assigned to the non-standard content type defined for a user agent must not match one of the standard content types. Standard content types are: 0, 1, 2, 22, 35.

Error: too many non std content types
You have defined more than the maximum number of non-standard content types allowed.

Error when creating <*directory*>
mkdir: <*message*>
See <*message*>. The pathname or access permissions might be incorrect.

Error when opening <*directory*>
opendir: <*message*>
See <*message*>. The pathname or access permissions might be incorrect.

Error while removing message
An error occurred when purging the message queues. If this error is returned regularly, please report the occurrence to your authorized service provider.

File error on <*filename*> **(**<*action*> **:** <*errno*>**)**
There was an error acting on the specified file. See <*action*> message for the type of error. For example, if <*action*> is `chmod`, then the access permissions are set incorrectly.

Host name and address do not correspond
You can enter a TCP/IP (RFC 1006) address as a numeric IP address (dot notation) or as a host name. If you enter a host name, `x400tool` retrieves the corresponding IP address by doing a `gethostbyname`. If you enter both a numeric IP address and a host name, the two addresses must be equivalent.

Host name or address must be present
You can assign TCP/IP (RFC1006) addresses for remote MTAs as numeric addresses or host names. You must enter at least one.

Incompatible addressing data
The X.400 address contains elements that do not combine to make a valid address. For example, a combination of a numeric-user-identifier (UA-ID) and a personal-name (PN). See "X.400 Addressing" on page 7 for a description of valid X.400 address types.

Initialization failed
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (calloc for remote mta)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (calloc for UA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (can't get msg number)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (can't get msg size)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid bmr header)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid bmr header)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid bmr header)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid code)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid state for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid state for UA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (invalid tlv suite: rem. mta)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Abnormal Transfer receiving)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Abnormal Transfer sending)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing APDUs received)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing APDUs sent)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing associations number)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Authentication Failures Issued)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Authentication Failures Received)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing Conf Spec cmd)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connect Abort Indication)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connect Abort RQ)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connection Indications)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connection Responses)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connect Confirmations)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Connect Requests)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Disconnect Indications)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Disconnect Requests)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing FILE ID in brm)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing non-urgent APDUs number)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing normal APDUs number)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Notification Indications)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Number of Delivered Messages)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Number of Octets Received)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Number of Octets Sent)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Number of Submitted Messages)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing OK cmd)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing RTS Busy Refused Confirm Received)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing RTS Busy Refused Response Issued)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal error (missing Unacceptable Dialogue Mode received)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (missing urgent APDUs number)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (mta cmd not OK)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (`MTS SHOW MSGSIZE`**: missing** `CMDOK`**)**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (`MTS SHOW MSGSIZE`**: missing header** <*hdr*>**)**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no add. usage for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no applic. ctx for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no country for local MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no country for remote MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no domain for local MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no domain for remote mta)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no encoded info. types)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no local MTA max contents)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no mta cmd ok)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no mta cmd OK. DSKDSP_HEA **brm missing)**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no mta cmd OK. VRSDSP_HEA **brm missing)**
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no name for local MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no name for remote mta)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no name for UA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no net. type for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no open order for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no path for MTA's current database)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no PRMD for remote MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no remote mta type)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no UA identifier)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no UA max contents)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no UA type)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no valid. for remote mta)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no valid. for UA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (no X.400 version for rem. MTA)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (show cmd inv. code)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error (show cmd not ok)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error: invalid network type
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Internal Error: Status: unknown obj type *<string>*
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Invalid ADMD code
The ADMD code that you have entered was not found in the list of standard ADMD codes. You can choose to correct the code or to force `x400tool` to accept it.

Invalid country code
The country code that you have entered was not found in the list of standard country codes. You can choose to correct the code or to force `x400tool` to accept it.

Invalid hexadecimal number
Use a number that only includes hexadecimal digits—0 through 9 and A through F.

Invalid host name: <*errno*>
You can enter a TCP/IP (RFC 1006) address as a numeric IP address (dot notation) or as a host name. If you enter a host name, `x400tool` retrieves the corresponding IP address by doing a `gethostbyname`. Host names must correspond to a valid IP address.

Invalid IP address (must be a.b.c.d)
Numeric IP addresses must be entered in Internet (dot) format.

Invalid MTA response
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Invalid User Id: must be an int (0,32767)
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

malloc system call failure (<*errno*>**)**
There was an error while allocating space. Check that there is enough disk space available.

Message queues are currently not empty
Please confirm <*name*> **deletion**
There are still some messages in the queue that you want to delete. Confirm that you still want to delete the message queue.

MTA or gateway not found
A configured local MTA or gateway were not found as required in the backup configuration. Either try the restore again or backup a different configuration.

MTA process is not running properly
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

MTA <*name*> **being closed**
The specified MTA is closing, as requested.

Network address must be present
You must specify an OSI network address when defining a remote MTA.

NSAP must be an hexadecimal number
X.25 and LAN addresses must be entered as hexadecimal numbers.

OSI Communication Platform not running
You cannot start `x400tool` unless the SunLink OSI Communication Platform (stack) is configured and running on your machine.

Process <*name*> **is not running**
The specified process needs to be started. Use the command `/opt/SUNWconn/bin/osistart` <*process*> to start it.

P1 user agent being closed
The specified P1 user agent is closing, as requested.

Restart the MTA. Use `osistart osimta`
You need to start the local MTA before you can complete the current operation. Type the command shown.

Routing ambiguous
The routing is ambiguous or the format of the O/R address is not compliant with the X.400 specification. For example, the local MTA might not be able to distinguish between two possible destinations. Verify the routing defined and ensure that there is enough information to distinguish a unique route.

Routing impossible
The local MTA cannot route the message. Verify the routing and ensure that the route has a unique definition.

Select an MTA icon as default
You need to select one of the remote MTAs in your message transfer system when defining a default ("catch-all") MTA. See "Setting a Default MTA" on page 95 for more information.

SMTP gateway already exists: <*string*>
You cannot add more than one X.400/SMTP(MIME) gateway to the message transfer system.

SMTP gateway being closed
The X.400 SMTP / MIME gateway is closing, as requested.

Statistics: unknown obj type <*name*>
Indicates a severe internal error. If this error is returned regularly, please report the occurrence to your authorized service provider.

Surname is mandatory when adding other personal name attributes
Personal names consist of four attributes: surname (S), given-name (G), initials (I), and generation-qualifier (GQ), of which only surname is mandatory.

Software has not been installed correctly: check the file `/etc/SUNWconn/OSIROOT` **or you have the variable** `$OSIROOT` **wrongly defined in your environment**
`x400tool` was unable to locate the expected files in the default directory. Either the files have been incorrectly installed, or the file `/etc/SUNWconn/OSIROOT` is pointing to the wrong location. Alternatively, if you defined an environment variable $OSIROOT, check that it is pointing to the true location of the SunLink X.400 8.0.2 configuration files.

Too many message queue P1 users
Limit is 16
You can have a maximum of 16 P1 user agents defined as message queues.

Unable to locate `OSIROOT` **directory**
`x400tool` was unable to locate the expected files in the directory defined by the file `/etc/SUNWconn/OSIROOT`.

User agent <*name*> **being closed**
The specified user agent is closing, as requested.

X.25 address can only contain decimal digits
Enter a numerical X.25 address.

10

Alarms Returned by the MTS

The following error messages are returned by the local MTA in the log file `/var/SUNWconn/osinet/osilogd.log`. Most of these error messages indicate a system error. If these errors are returned regularly, report the occurrence to your authorized service provider.

ALARM ! File Error <*oper*> <*filename*>	
Description:	Indicates a file error detected by the local MTA. If the error is due to a message file, processing is abandoned for this file in order to protect the rest of the message transfer system.
Action:	You may need to purge the message queues in order to clear a blocked message. See "Purging the Mail Queues" on page 139. Report the occurrence to your authorized service provider if this error is returned regularly.

<*oper*>	Type of operation in progress when the error occurred:
	`closing creating deleting linking`
	`opening reading seeking writing`

<*filename*>	Name of file causing error.
Example:	`ALARM ! File error opening` <*filename*>

ALARM ! Possible duplication to MTA <*mta_id*> **MPDU Id:** <*mpdu_id*>	
Description:	Indicates that the sent MPDU may be duplicated after an error which occurred during a critical phase in the transfer.
<*mta_id*>	Remote MTA identifier.
<*mpdu_id*>	MPDU identifier.
Action:	Warn the recipient system administrator, who can delete the duplicate message.
Example:	`ALARM ! Possible duplication to MTA 9 MPDU Id: </FR/ATLAS/XYZCORP/10/04/93>`

ALARM ! Database Error on <*filename*>

Description:	The message transfer system was unable to handle the specified file.
Action:	Check the file and restart the local MTA using `osistop/osistart`. Report the occurrence to your authorized service provider if this error is returned regularly.
<*filename*>	Name of file causing error.

ALARM ! Database Error on <*oper*> <*msg_id*> <*ln1*> <*msg*> <*dest*> <*file*> <*ln2*>

Description:	The message transfer system detected an error when trying to create, replace, or delete a message descriptor.
Action:	Report the occurrence to your authorized service provider if this error is returned regularly.
<*oper*>	Type of operation in progress when the error occurred: `creating replacing deleting`
<*msg_id*>	Message identifier.
<*ln1*>	Length of entire message.

<*msg*>	Message type:
	`non deferred list deferred list`
	`urgent message to normal message to`
	`notification to non urgent message to`
	`incoming APDU queue`

<*dest*>	Destination (outgoing messages only): remote MTA: `MTA` <*mta_id*> user agent: `LUAG` <*luag_id*>
<*file*>	File name or file names (if any).
<*ln2*>	Length of file (specified by <*file*>).

`Example:`	`ALARM ! Database error creating`
	`</FR/ATLAS/XYZCORP/20/03/93/>`
	`length= 750 urgent message to MTA 2`
	`file p000003 length=250`
	`file p000004 length=500`

ALARM ! OSIAM Internal Error CTX=-1

Description:	The local MTA was unable to open the association because there were no contexts available.
Action:	Report the occurrence to your authorized service provider if this error is returned regularly.
Example:	`ALARM ! OSIAM Internal Error CTX-1`

ALARM ! OSIAM Internal Error SAP=<*sap*> **MTA=**<*mta_id*>

Description:	Indicates that the specified SAP could not be accessed because it was invalid or closed.
<*sap*>	SAP (service access point) number.
<*mta_id*>	Remote MTA identifier.
Action:	Report the occurrence to your authorized service provider if this error is returned regularly.
Example:	`ALARM ! OSIAM Internal Error SAP=2 MTA=3`

ALARM ! Unacceptable Dialogue Mode ! MTA <*mta_id*>

Description:	The remote MTA refused an association because of an error during the negotiation phase. For example, the local MTA requested a two-way association from an MTA that only supports monologue connections. Messages to be delivered are kept in the relevant queue and the local MTA will continue to accept messages for this destination.
<*mta_id*>	Remote MTA identifier.
Action:	Redefine the association parameters for the remote MTA. See “Tuning the Remote MTA Associations Options” on page 90.
Example:	`ALARM ! Unacceptable Dialogue Mode ! MTA=3`

ALARM ! Maximum Number of Retries Reached, closing of MTA *<mta_id>*

Description:	The local MTA has exceeded the maximum number of unsuccessful association establishment retries. The remote MTA is closed. All pending messages are rerouted and no new messages will be forwarded.
<mta_id>	Remote MTA identifier.
Action:	Check the configuration and reopen specified remote MTA. See "Opening and Closing Agents" on page 129.
Example:	`ALARM ! Maximum number of retries reached, closing of MTA 4`

ALARM ! Loopback detected

Description:	A loopback condition is detected—that is, the message is routed back to an MTA that has already passed on the message. The local MTA already appears in the trace information for the message.

Action:	Check the routing table. See "Modifying the Default Routing Table" on page 114.
	You can suppress the loopback detection by appending `/var/SUNWconn/OSIROOT/conf/osimta.init` with the following line:
	`vary entity 67 flag 0 8 off`
	after the last occurrence of:
	`; END OF AUTOMATICALLY GENERATED PART`
	This, however, is not a recommended practice.

ALARM ! Originator Control Failure MTA <*mta_id*> **MD** <*domain_id*>	
Description:	An incoming message was deleted because the originating domain identifier is not associated with the specified remote MTA. The message is discarded and a non-delivery report is generated.
<*mta_id*>	Remote MTA identifier.
<*domain_id*>	Global domain identifier for the originating MTA.
Action:	Check the configuration for the specified remote MTA. See "Specifying the Global Domain Identifier" on page 83.
Example:	`ALARM ! Originator Control Failure MTA 2 MD /FR/ATLAS/XYZCORP/`

ALARM ! Congestion critical state	
Description:	The local MTA has been placed in a critical state because the space remaining in the spool file system has dropped below the predefined threshold. The local MTA will not accept any more message transfers; message transfers in progress will be completed.
Action:	Reduce the number of messages stored in the spool file system if possible. See "Purging the Mail Queues" on page 139. If this error occurs regularly, it indicates that your spool file system is too small for the traffic supported by the local MTA. Increase the size of your spool file system or decrease the congestion thresholds. See "Tuning the Other Options" on page 54.

ALARM ! Invalid sequence of Trace Information	
Description:	The timestamp sequence is incorrect. For example, incorrect time zone. By default the time tolerance is set to 255. This alarm may result from the existence of more than one MTA of the same name in the same management domain.
Action:	Modify the time tolerance using the Time Tolerance options on the Tuning (Other) pop-up menu from the Local MTA Configuration window in `x400tool`. If this does not solve the problem, check that there are no MTAs with the same name in the management domain.

10

Abnormal Events Returned by the MTS

The following messages are returned by the message transfer system in the log file `/var/SUNWconn/osinet/osilogd.log` when an abnormal event occurs.

These messages always indicate a fatal system error and you should report the occurrence to your authorized service provider.

Abnormal remote MTA state [MTA <*mta_id*>**]**

Abort Confirm from MTA <*mta_id*> **Reason code=**<*code*>

Abort indication from MTA <*mta_id*> **Reason code=**<*code*>

APDU Descriptor error

ASM Unknown Event EVT=<*code*>

Body type error: body type <*description*>

Connection is aborted by the provider

Connection is aborted by the remote user

Decoding error: -Status <*asn1_status*> **Index** <*asn1_index*>

Decoding error: [ASN1 status=<*errno*>**] Index** <*asn1_index*>

Error - Unknown: <*description*>

Illegal application protocol MTA <*mta_id*>

Inhibition flag set MTA <*mta_id*>

Interaction file error: FIERR=<*status*>

Invalid original MPDU error

Local User Error EVNT=<*event*> **RTS=(**<*ctx*>**,**<*st*>**)**

No free association MTA <*mta_id*>

Prot Error Num=<num> RTS=(<*ctx*>**,**<*st*>**)**

Protocol error STATE=<*current_state***> [MTA=**<*mta_id*>**]**

Protocol error: state=<*current_state*>

Provider Abort NUM=<*num*> **RTS=(**<*ctx*>**,**<*st*>**)**

Refuse confirm from MTA <*mta_id*> **Reason code=**<*code*>

Refuse response issued

Remote RTS User Abort RTS=(<*ctx*>**,**<*st*>**)**

Some recipients in the MPDU are unreachable: <*description*>

Still associations for MTA <*mts_id*>

Time-out RTS=(<*ctx*>**,**<*st*>**)**

Timer Block Id error - N_CNF

Transfer Resumption Reject (illegal seci)

Transfer Resumption Reject (illegal aci)

Unable to identify remote MTA

Unknown database: LUAG <*ident*>

Unknown Event Code EVT=<*code*>

Unknown refuse reason code MTA <*mta_id*> **Reason code=**<*code*>

Unsupported Body Type

User Error: <*description*>

Usrdata decoding failure

Warning! the following MTA is closed MTA <*mta_id*>

10

Technical Specification and Conformance Information A

This appendix contains a detailed technical specification for SunLink X.400 8.0.2 including a brief description of the CCITT X.400 recommendations to which it conforms and a list of the implemented features.

The following abbreviations are used in the tables throughout this chapter:

n/a — not applicable

S — feature supported

N — feature not-supported

A

CCITT MHS Recommendations Overview

X.400 MHS System Service and Overview: Describes in general terms how an originator interacts with a UA to prepare and receive messages, how a UA interacts with an MTA, and naming and addressing conventions.
(ISO 10021-1)

X.402 MHS Overall Architecture: Describes the overall system architecture of the X.400 MHS including suggested configurations, naming, and addressing information.
(ISO 10021-2)

X.403 MHS Conformance Testing: Provides guidelines and rules for conformance testing of MHS implementations.

X.407 MHS Abstract Service Definition: Specifies conventions used in distributed information processing.
(ISO 10021-3)

X.408 MHS Encoded Information Type Conversion Rules: Provides guidelines for code and format conversion algorithms used in the MHS.

X.411 MHS MTS Abstract Service Definition and Procedures: Describes how the user can exchange messages with the MTS based on abstract service definitions and syntaxes.
(ISO 10021-4)

X.413 MHS Abstract Service Definition: Describes how to implement a message store as an intermediary between the MTS and a UA.
(ISO 10021-5)

X.419 MHS Protocol Specifications: Describes the procedures used to exchange messages between the components of the MHS. Defines three protocols P1, P3, and P7.
(ISO 10021-6)

X.420 MHS Interpersonal Messaging System: Describes the procedures and syntax used for the exchange of interpersonal messages (electronic mail).
(ISO 10021-7)

SunLink X.400 8.0.2 Feature List

The following features from the 1988 revision of the CCITT X.400 recommendations are implemented by the various components of SunLink X.400 8.0.2.

MT Service Elements (P1)

Table A-1 Basic Message Transfer Service Support

Message Transfer Basic Service Elements	Out MTA	Out Gway	In MTA	In Gway
Access management	S	S	S	S
Content type indication	n/a	n/a	S	S[1]
Converted indication	n/a	n/a	S	S[2]
Delivery time stamp indication	n/a	n/a	n/a	n/a
Message identification	S	S[3]	S	S[3]
Non-delivery notification	S	S	S	N[4]
Original encoded information types indication	S	S[5]	S	S[5]
Submission time stamp indication	S	S	S	S
User/UA capabilities registration	n/a	n/a	S	S

1. New RFC Header “Content-Type”
2. New RFC Header “X.400-Received”
3. New RFC Header “X.400-MTS-Identifier”
4. If sendmail fails to deliver the message, a negative delivery is returned as an IPM Message
5. New RFC Header “Original-Encoded-Information-Type”

A

Table A-2 Optional Message Transfer Service support

Message Transfer Optional Service Elements	Out MTA	Out Gway	In MTA	In Gway
Alternate recipient allowed	S	N	S	N
Alternate recipient assignment	S	N	S	N
Content confidentiality		N		N
Content integrity		N		N
Conversion prohibition	S	N	S	S
Conversion prohibition due to loss of information	S	N	S	S
Deferred delivery	S	S[1]	S	S[1]
Deferred delivery cancelation	S	N	S	N
Delivery notification	S	S	S	S[2]
Designation of recipient by directory name	S	N	n/a	n/a
Disclosure of other recipients	S	S[3]	S	S[4]
Directory List expansion history indication	n/a	n/a		S
Directory List expansion prohibited	S	N	n/a	n/a
Explicit conversion		N	n/a	n/a
Grade of delivery selection	S	S	S	S
Hold for delivery	n/a	n/a		N
Implicit conversion		n/a		n/a
Latest delivery designation	S	S[5]	S	N
Message flow confidentiality		N		N
Message origin authentication		N		N
Message security labeling		N		N
Message sequence integrity		N		N
Multi-destination delivery	S	S	S	S
Non-repudiation of delivery		N		N
Non-repudiation of origin		N		N
Non-repudiation of submission		N		N
Originator requested alternate recipient	S	N	S	N[6]
Prevention of non-delivery notification	S	S[7]	S	N[8]
Probe	S	n/a	S	S

Table A-2 Optional Message Transfer Service support

Message Transfer Optional Service Elements	Out MTA	Out Gway	In MTA	In Gway
Probe origin authentication		n / a		N
Proof of delivery		N		N
Proof of submission		N		N
Redirection disallowed by originator	S	N	S	N
Redirection of incoming messages				
Report origin authentication		N		N
Requested delivery method		S		N
Restricted delivery	N	N	N	N
Return of content	S	S[9]	S	S[10]
Secure access management		n / a		n / a

1. New RFC Header “Deferred-Delivery”. Managed by MTA but never by gateway.
2. Indicates message received by sendmail but not necessarily delivered to recipient. A negative delivery report may still be returned after a positive delivery notification.
3. Always requested for outgoing messages.
4. New RFC Header “X.400-Recipients”.
5. New RFC Header “Latest-Delivery-Time”.
6. Not supported, but placed as a comment in the address field “X.400-Recipients”.
7. New RFC Header “Delivery-Report”, only on per message basis.
8. Sendmail interrogates the gateway to see if it can route the message. Since the local routing may not be the final one, this report has no real meaning.
9. A gateway parameter determines whether “return of content” is requested in the message or managed locally.
10. Return of content will be performed by the IPM message carrying the negative delivery report.

IPM Service Elements

Table A-3 Basic Inter-Personal Message Service Support

Message IPM Service Elements	Out MTA	Out Gwy	In MTA	In Gwy
IP-message identification	S	S	S	S

Table A-4 Optional Inter-Personal Message Service Support

Message IPM Service Elements	Out MTA	Out Gwy	In MTA	In Gwy
Additional physical rendition		N		n/a
Authorizing users indication	S	S	S	S
Auto-forwarded indication	n/a	n/a	S	S
Basic physical rendition		n/a		n/a
Blind copy recipient indication	S	S	S	S
Body part encryption indication	S	S[1]	S	S[1]
Counter collection		n/a		N
Counter collection with advice		n/a		N
Cross-referencing indication	S	S	S	S
Delivery via Bureaufax service		N		n/a
Express Mail Service (EMS)		N		n/a
Expiry date indication	S	S[2]	S	S[2]
Forwarded IP message indication	n/a	n/a	S	S[12]
Importance indication	S	S[3]	S	S[4]
Incomplete copy indication	S	S[4]	S	S[5]
Language indication	S	S[5]	S	S[6]
Message flow confidentiality		N		N
Multi-part body	S	S[6]	S	S[7]
Non-receipt notification request indication	S	N[7]	S	N[8]
Obsoleting indication	S	S[8]	S	S[9]
Ordinary mail		N		n/a
Originator indication	S	S	S	S
Physical delivery notification by MHS		N		n/a
Physical delivery indication by PDS		N		n/a
Physical forwarding allowed	S	S[9]	S	S[10]
Physical forwarding prohibited	S	S[10]	S	S[10]
Primary and copy recipients indication	S	S	S	S
Receipt notification request indication	S	N[8]	S	N[8]
Registered mail		N		n/a

Table A-4 Optional Inter-Personal Message Service Support

Message IPM Service Elements	Out MTA	Out Gwy	In MTA	In Gwy
Registered mail to addressee in person		N		n/a
Reply request indication	S	S[10]	S	S[11]
Reply IP message indication	S	S	S	S
Request for forwarding address		N		n/a
Sensitivity indication	S	S[11]	S	S[12]
Special delivery		N		n/a
Stored message deletion	n/a	n/a	n/a	n/a
Stored message fetching	n/a	n/a	n/a	n/a
Stored message listing	n/a	n/a	n/a	n/a
Stored message summary	n/a	n/a	n/a	n/a
Stored message alert	n/a	n/a	n/a	n/a
Stored message auto-forward	n/a	n/a	n/a	n/a
Subject indication	S	S	S	S
Undeliverable mail with return of physical message		n/a		n/a

1. New RFC header “Original-Encoded-Information-Types:”
2. New RFC header “Expiry-Date:”. No automatic action performed when date has expired.
3. New RFC header “Importance:”
4. New RFC header “Incomplete-Copy:”
5. New RFC header “Language:”
6. Generated and interpreted in SUN’s mailtool format.
7. May be implemented in next version.
8. New RFC header “Obsoletes”
9. Comment in the “X400-recipients:” header
10. Comment in address.
11. New RFC header “Sensitivity:”
12. IPM expanded in the RFC822 body, can only be interpreted visually.

A

Customizing `sendmail` *for SunLink X.400 8.0.2*

B

This appendix describes the changes that must be made to the `sendmail` configuration file (`/etc/mail/sendmail.cf`) so that the `sendmail` daemon recognizes the X.400/SMTP(MIME) gateway. For more general and detailed information on how to customize `sendmail.cf`, see your Solaris *Setting Up User Accounts, Printers, and Mail* document.

The sendmail.cf File

The `sendmail` configuration file (`/etc/mail/sendmail`.cf) has three parts:

1. **Definition of symbols, options, and parameters**
2. **Definition of mailers and mail delivery programs**
3. **Rule sets that determine how addresses are translated**

The `sendmail` configuration file is read each time the `sendmail` daemon is started. You can modify `sendmail.cf` to tailor the behavior of the `sendmail` daemon to suit your local environment and to add definitions for your local mailers and delivery programs.

B

Sample Script

The following code sample shows the script used to modify the `sendmail` configuration file (`/etc/mail/sendmail.cf`) when SunLink X.400 8.0.2 is installed.

Code Example B-1 Script for Modifying `sendmail.cf` (part 1)

```
#!/bin/sh
#
#ident "@(#)update_sendmail.cf 1.8 - 94/08/10 SMI"
#
# Copyright 1994 Sun Microsystems, Inc. All Rights Reserved
#
#   Modify sendmail.cf file in order to add
#   x400 Gateway
#
#   Parameters:
#
#   PSEUDOHOSTX400 Gateway pseudo host name
#   S2XMAIL full path of mailer
#   BSNM_S2XMAIL    basename of S2XMAIL
#   VALID_UPDTMark to add to the end if
#           everything goes right
#
#    Notice : if the format of sendmail.cf cannot be
#             updated, a warning is issued and the original
#             file is left untouched.
#
```

The following parameters are set as default in the (`SUNWmhs1a`) package:

- `PSEUDOHOST` **(default pseudo host name)**: `x400-gate`
- `S2XMAIL` **(full path to mailer)**: `/opt/SUNWconn/bin/osix400mail`
- `BSNM_S2XMAIL` **(basename for** `S2XMAIL`**)**:

Code Example B-2 Script for Modifying `sendmail.cf` (part 2)

```
BEGIN {

    for (i=0; i < 4; i++) PART[i]=0;

    }

#
#   Insert FIRST part *after*  the line that matches
#

/^CR/{

    PART[0]++
#       Print out the line which matches
    print
#       Add Gateway PART1
    print "#X400_GWY#UPDT1_START  ----------Do not remove this
line"
    print "#"
    print "#  This part has been automatically inserted "
    print "#  by the package: " PKG
    print "#"
    print "#  Do not edit or add anything to it. It will be removed "
    print "#  automatically when the package is deinstalled"
    print "#"
    print "# local MHS pseudo-hosts: must include the MHS”
     print "# encoded_orname_pseudo_host (typically x400-gate) and"
    print "# may include the 822 host addresses of local"
    print "# X.400 systems"
    printf("CX%s\n",PSEUDOHOST)
    print "#X400_GWY#UPDT1_END   ----------Do not remove this line"
    next
    }
```

The first part of the script (Code Example B-1) is concerned with adding the default pseudo host name for the X.400/SMTP(MIME) gateway—usually set to `x400-gate`. This is the entry that must be modified if you assign a different pseudo host name when you configure the gateway. Refer to “Configuring the X.400/SMTP(MIME) Gateway” on page 62 for more information.

Code Example B-3 Script for Modifying `sendmail.cf` (part 3)

```
#
#   Insert SECOND part *before* the line that matches
#
#   WARNING: I'm looking for a COMMENT LINE
#
/^S0/   {

    PART[1]++
    print "#X400_GWY#UPDT2_START  -----Do not remove this line ---"
    print "#"
    print "#  This part has been automatically inserted "
    print "#  by the package: " PKG
    print "#"
    print "#  Do not edit or add anything to it. It will be removed "
    print "#  automatically when the package is deinstalled"
    print "#"
    print "########################################################"
    print "#"
    print "#       MHS (X.400) Mailer specification"
    print "#"
    printf("Mmhs,   P=%s, F=mDFMuCnS, S=12, R=14,\n",S2XMAIL)
    printf("        A=%s $u\n",BSNM_S2XMAIL)
    print " "
    print "S12"
    print "R$*<@$%y>$*$@$1<@$2.LOCAL>$3user@etherhost"
    print "R$*<@$+.uucp>$@$2!$1<@$w.LOCAL>path@host.uucp"
    print "R$*<@$+>$*$@$1<@$2>$3already ok"
    print "R$+ $@$1<@$j>  tack on our hostname"
    print ""
    print "S14"
    print "R$*<@$%y>$*$@$1<@$2.LOCAL>$3user@etherhost"
    print "R$*<@$+.uucp>$@$2!$1<@$w.LOCAL>path@host.uucp"
    print "R$*<@$+>$*$@$1<@$2>$3already ok"
    print "R$+ $@$1<@$j>  tack on our hostname"
    print "#X400_GWY#UPDT2_END   ----Do not remove this line ---"
```

Code Example B-4 Script for Modifying `sendmail.cf` (part 4)

```
    PART[2]++
#       Copy all the lines till the matching one
    while ( $0 !~ /^R@/ ) {
        print
        getline
    }
#       Print the matching line
    print
    getline
#       Copy all the comments which follow the matching line
    while ( $0 ~ /^#/) {
        print
        getline
    }
#       Add my stuff
    print "#X400_GWY#UPDT3_START  ------Do not remove this line ----"
    print "#"
    print "#  This part has been automatically inserted "
    print "#  by the package: " PKG
    print "#"
    print "#  Do not edit or add anything to it. It will be removed "
    print "#  automatically when the package is deinstalled"
    print "#"
    print "# tag local MHS pseudo-hosts"
    print "R$*<@$*$=X.LOCAL>$*$1<@$2X400>$4user@mhs-host.LOCAL"
    print "R$*<@$+.$=X.$+>$*$1<@$2.$4.X400>$5user@mhs-host"
    print "R$*<@$=X.$+>$*$1<@$3.X400>$4user@mhs-host"
    print "R$*<@$+.$=X>$*$1<@$2.X400>$4user@mhs-host"
    print "R$*<@$=X>$*$1<@X400>$3user@mhs-host"
    print "#X400_GWY#UPDT3_END   ------Do not remove this line -----"
#       Copy the original line after the comments
    print
    next
    }
```

Code Example B-5 Script for Modifying `sendmail.cf` (part 5)

```
#
#   Insert the FOURTH part
#
#   WARNING: I'm looking for a COMMENT

/For numeric spec/ {

    PART[3]++
#       Add my stuff BEFORE the matching line
    print "#X400_GWY#UPDT4_START  ----------Do not remove this line
-------"
    print "#"
    print "#  This part has been automatically inserted "
    print "#  by the package: " PKG
    print "#"
    print "#  Do not edit or add anything to it. It will be removed "
    print "#  automatically when the package is deinstalled"
    print "#"
    print "# send mail addressed to local MHS pseudo-hosts to MHS"
    print "# gateway"
    print "R$+<@$*.X400>$#mhs $@X400 $:$1<@$2>user@mhs-host"
    print "R$+<@X400>$#mhs $@X400 $:$1<@$m>user@mhs-host"
    print ""
    print "# send mail addressed to external X.400 pseudo-domains"
    print "# to the MHS gateway (none in basic configuration)"
    print ""
    print "#X400_GWY#UPDT4_END    -----Do not remove this line --
--"
#       Copy the original matching line
    print
    next
    }
#
```

Code Example B-6 Script for Modifying `sendmail.cf` (part 6)

```
#
#   Print all the other lines
#
    {   print  }

END  {

    ERROR=0
    for (i=0; i< 4; i++){
        if ( PART[i] != 1 )
            ERROR=1
    }

    if ( ERROR == 0 )
        printf("%s\n",VALID_UPDT)

     }
```

The script ends by ensuring that all the other lines of `sendmail.cf` are left untouched by the modifications.

Mailing X.400 Recipients using UNIX-Style Addresses

Under most circumstances, you need to modify `sendmail.cf` in order to send mail to X.400 recipients using UNIX-style addresses of the form:

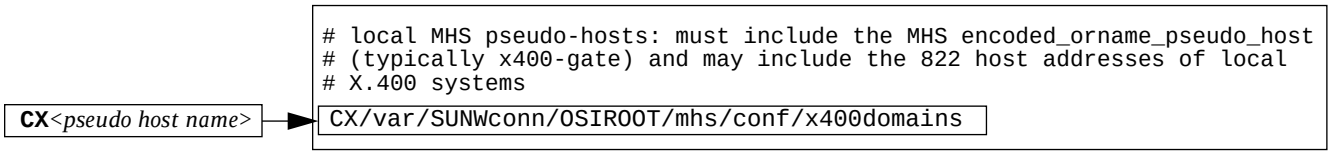
```
<recipient_name>@<domain_name>
```

On the machine on which the X.400/SMTP(MIME) gateway is running:

1. **Create the file** `/var/SUNWconn/OSIROOT/mhs/conf/x400domains` **with the following entries:**

```
<pseudo_hostname>
<domain_name>
```

2. **In** `sendmail.cf`**, replace the entry** `CX`*<pseudo_hostname>* **with the name of this file:**



On your mail host (provided this is not the machine on which the gateway is running):

1. **Create the file** `/etc/mail/x400domains` **with the following entries:**

```
<pseudo_hostname>
<domain_name>
```

2. **Edit** `sendmail.cf` **to add the following entries:**

```
FX/etc/mail/x400domains
DY<pseudo_hostname>
```

3. **Edit** `sendmail.cf` **to add the following lines after the start rule** `S0`**:**

```
R$*<@$*$=X.LOCAL>$*          $#$M $@$Y $:$1<@$2.$3>$4user@mhs-host.LOCAL
R$*<@$+.$=X.$+>$*            $#$M $@$Y $:$1<@$2.$3.$4>$5user@mhs-host
R$*<@$=X.$+>$*               $#$M $@$Y $:$1<@$2.$3>$4user@mhs-host
R$*<@$+.$=X>$*               $#$M $@$Y $:$1<@$2.$3>$4user@mhs-host
R$*<@$=X>$*                  $#$M $@$Y $:$1<@$2>$3user@mhs-host
```

4. **Edit the mapping tables used by the X.400/SMTP(MIME) gateway to map X.400 and UNIX mail addresses. See "Modifying the Mapping Tables" on page 73 for detailed instructions.**

- In the mapping table `rfc11848-mapping1`, add an entry to map from the UNIX domain to the X.400 domain.

```
<domain_name>    <x400_address>
```

- In the mapping table `rfc11848-mapping2`, add an entry to map from the X.400 domain to the UNIX domain.

```
<x400_address>      <domain_name>
```

B

Index

D

E

F

G

S

Y