

Solstice Messaging Management 1.0 Administrator's Guide



A Sun Microsystems, Inc. Business

2550 Garcia Avenue
Mountain View, CA 94043
U.S.A.

Part No.: 802-5048-10
Revision A, February 1996

© 1996 Sun Microsystems, Inc. 2550 Garcia Avenue, Mountain View, California 94043-1100 U.S.A.

All rights reserved. This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Portions of this product may be derived from the UNIX[®] system, licensed from UNIX System Laboratories, Inc., a wholly owned subsidiary of Novell, Inc., and from the Berkeley 4.3 BSD system, licensed from the University of California. Third-party software, including font technology in this product, is protected by copyright and licensed from Sun's suppliers.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19. The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

TRADEMARKS

Sun, Sun Microsystems, the Sun logo, Solaris, Solstice, SunLink, SunNet, and SunNet Manager are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and certain other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. OPEN LOOK is a registered trademark of Novell, Inc. PostScript and Display PostScript are trademarks of Adobe Systems, Inc.

All SPARC trademarks are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. SPARCcenter, SPARCcluster, SPARCcompiler, SPARCdesign, SPARC811, SPARCengine, SPARCprinter, SPARCserver, SPARCstation, SPARCstorage, SPARCworks, microSPARC, microSPARC-II, and UltraSPARC are licensed exclusively to Sun Microsystems, Inc. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK[®] and Sun[™] Graphical User Interfaces were developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

X Window System is a trademark of X Consortium, Inc.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.



Contents

1. Introduction to Solstice Messaging Management.....	1
Solstice Messaging Management Architecture.....	1
Solstice Messaging Manager.....	3
The Management Console	3
Messaging Manager Tools	5
The Messaging Manager Discover Tool.....	6
Statistics Tools.....	6
Predefined Graphs	6
Access to Configuration Tools	7
The SunNet Manager Management Database	8
Messaging Management Agents	9
Management Information Bases (MIBs)	10
MIBs Supported by the X.400 Server SNMP Agent ..	11
MIBs Supported by the X.400 XAPIA SNMP Agent .	13
How the Solstice Messaging Manager and the Agents Interact	14

The SNMP Protocol	14
The SNMP Relay	14
Example of Messaging Management Setup	15
Messaging Management Summary	16
2. Solstice Messaging Manager.	19
Starting the Solstice Messaging Manager	19
▼ How to Start Solstice Messaging Manager 1.0	20
Using the Messaging Manager Discover Tool	21
Creating a Messaging View for the First Time	21
▼ How to Run the Messaging Manager Discover Tool	21
Updating Messaging Views	25
Obtaining Messaging Statistics	25
Using the Statistics Tools	25
▼ How to Obtain Statistics on an MTA or a Gateway	26
▼ How to Obtain Statistics on a Message Store	29
▼ How to Update Statistics.	31
▼ How to Reset the Statistics for an MTA.	32
Using the Graphs Tool.	32
▼ How to Select and View a Predefined Graph	33
▼ How to Create your own Graph	34
▼ How to Change the Name in the Title Bar of a Graph.	35
▼ How to Merge Graphs.	36
Creating Event Requests	37

Example of Critical Load for an MTA	37
▼ How to Create an Event Request to Monitor the Load on an MTA	38
Examples of Useful Event Requests	41
Applying an Event Request to Several Messaging Applications	41
▼ How to Create a Predefined Event Request for a Messaging Application	42
Viewing Messaging Events, Traps, and Errors	42
▼ How to View Alarm Reports for all Applications Represented in the Messaging View	43
▼ How to View Alarm Reports from a Messaging Application Icon	44
▼ How to View Alarm Reports for a Messaging Application from the Host Icon	45
▼ How to Acknowledge an Alarm	46
▼ How to Check that the Process Responsible for Sending Traps to Messaging Icons is Running	46
Configuring the Display of Information	47
Color Conventions	47
Effects Produced by Events, Traps, and Errors	47
▼ How to configure the Effect of Traps, Events and Errors from the Props Menu	48
▼ How to Configure the Effect of an Event from an Event Icon	49

3. Solstice X.400 SNMP Agents	51
The Solstice X.400 Server Agent.....	51
Management Information Bases	52
Standard Management Information Bases	52
Extensions	52
Examples of Data Reports and Traps	54
▼ How to Obtain a Simple Data Report for an X.400 MTA or Message Store.....	54
Installing the Solstice X.400 Server SNMP Agent	59
▼ How to Install the Solstice X.400 Server SNMP Agent.....	59
SNMP Server Agent Configuration.....	60
Access Control	60
Trap Parameters	60
▼ How to Modify the X.400 Server SNMP Agent Configuration File	60
Configuration File for SNMP Relay.....	62
The Solstice X.400 XAPIA Agent	62
Management Information Bases	62
Standard Management Information Bases	62
Extensions	63
Examples of Data Reports and Traps	63
▼ How to Obtain a Simple Data Report for an X.400 XAPIA Client	63
Installing the Solstice X.400 XAPIA SNMP Agent.....	65

▼ How to Install the Solstice X.400 XAPIA SNMP Agent.....	65
X.400 XAPIA SNMP Agent Configuration.....	66
▼ How to Modify the X.400 XAPIA SNMP Agent Configuration File	66
Configuration File for SNMP Relay.....	67
A. SNMP Relay Configuration.....	69
Introducing the SNMP Relay Configuration	69
Modifying the SNMP Relay Configuration	71
▼ To Assign a Different Port Number to an Agent .	71
▼ To Add a Configuration File for an SNMP Agent Manually.....	72
▼ Stopping and Restarting the SNMP Relay	73

Figures

Figure 1-1	Solstice Messaging Management Architecture	2
Figure 1-2	Home view in the SunNet Manager Console	4
Figure 1-3	A Messaging View.	5
Figure 1-4	Part of the Global Information Model	11
Figure 1-5	Messaging Management with the Solstice Messaging Manager	15
Figure 2-1	The Messaging Manager Discover Tool Main Window	23
Figure 2-2	A Messaging Cloud.	24
Figure 2-3	Inside the Messaging Cloud.	24
Figure 2-4	Icon Menu of an MTA.	26
Figure 2-5	MTA or Gateway Statistics Main Window	27
Figure 2-6	Message Statistics for an MTA.	28
Figure 2-7	Message Store Statistics Main Window	30
Figure 2-8	Message Store Group Statistics	30
Figure 2-9	User Mailbox Statistics	31
Figure 2-10	The Messaging Manager Grapher Main Window	33
Figure 2-11	Graph Configuration Window	35

Figure 2-12	A Graph Properties Window	36
Figure 2-13	Request Builder Window	38
Figure 2-14	SunNet Manager Event Request Window	39
Figure 2-15	An Alarm Reports Summary	44
Figure 2-16	An Alarm Report for a Messaging Application	45
Figure 2-17	Properties Window	49
Figure 3-1	Trap Report Caused by a Change in Operating Status	54
Figure 3-2	Application Table Variables.	56
Figure 3-3	Association Table Variables.	57
Figure 3-4	Message Store User Group Table	57
Figure 3-5	Message Store User Table.	58
Figure 3-6	Application Table Variables.	64

Tables

Table 1-1	Messaging Management Summary	16
Table 2-1	Group Statistics	28

Preface

The *Solstice Messaging Management Administrator's Guide* describes the Solstice™ Messaging Management architecture which includes:

- The Solstice Messaging Manager 1.0 that runs over SunNet Manager™ 2.2.2 and later
- The Solstice X.400 Server SNMP Agent included with the Solstice X.400 Messaging Server 9.0 and the Solstice X.400 Internet Adaptor 9.0
- The Solstice X.400 XAPIA SNMP Agent included with the Solstice X.400 Client Toolkit 9.0

This manual explains how messaging management works and how to use the Solstice Messaging Manager to monitor your messaging system. It does not explain how to configure or maintain your messaging system.

This manual is intended for system administrators who are familiar with SunNet Manager.

Before You Read This Book

The Solstice Messaging Manager uses many features of SunNet Manager, therefore you need to be familiar with the following books:

- *SunNet Manager User's Guide*
- *SunNet Manager Reference Manual*

Before using the Solstice Messaging Manager, you need a view of your network in the SunNet Manager management console. Instructions on how to create a network view are provided in the *SunNet Manager 2.2.2 User's Guide*.

How This Book Is Organized

This book contains three chapters and one appendix:

Chapter 1, "Introduction to Solstice Messaging Management," provides an introduction to messaging management with the Solstice Messaging Manager and the Solstice management agents.

Chapter 2, "Solstice Messaging Manager," provides detailed instructions on how to use the Solstice Messaging Manager tools to monitor your messaging system. It also contains examples.

Chapter 3, "Solstice X.400 SNMP Agents," provides detailed information on how the Solstice X.400 SNMP Agents work, the standard Management Information Base (MIB) variables they support, extensions, traps, and configuration information.

Appendix A, "SNMP Relay Configuration," provides detailed configuration information on the SNMP Relay.

Troubleshooting information is provided in the *Important Product Information* booklet.

Related Books

If you need information on how to configure and maintain your messaging system, read the *Solstice Messaging Server Administrator's Guide* and the *Solstice X.400 Client Toolkit Administrator's Guide*.

Information on installing the Solstice Messaging Manager and the SNMP agents for the Solstice X.400 Messaging Server, Internet Adaptor and Client Toolkit is provided in the *Installing and Licensing Solstice X.400 Products* CD booklet.

Troubleshooting information is provided in the *Important Product Information* booklet.

Terminology

This section defines frequently used terms.

Trap

A *trap* is an unsolicited report sent by an SNMP agent to the manager application when certain conditions occur. The conditions that can generate traps are determined by the agent. For the Solstice X.400 Server Agent, these are listed in the manpage `snmpx400d(8)`, and for the Solstice X.400 XAPIA agent, in the manpage `snmpxapiad(8)`. In SunNet Manager, traps can also occur when you make changes to the database.

Event

An *event* occurs when a set of user-defined conditions have been met. It causes the SunNet Manager SNMP proxy agent (`na.snmp`, see *SunNet Manager User's Guide*) to send an event report to the management console.

Error

An *error* is a SunNet Manager error. It is not related to the network or applications monitored using SunNet Manager and the Messaging Manager.

Alarm

An *alarm* is used to refer collectively to traps, events and errors.

Key

An application's *key* is the value of the `applIndex` MIB variable given in the `applTable` MIB table. The keys for the Solstice X.400 messaging applications are:

Messaging Application	Key
Solstice X.400 MTA	1
Solstice X.400 Internet Adaptor	2
Solstice X.400 Message Store	3
Solstice X.400 Client Toolkit	4

Examples are provided in Chapter 3, "Solstice X.400 SNMP Agents".

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 <code>.login</code> file. Use <code>ls -a</code> to list all files. machine_name% You have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	<pre>machine_name% su Password:</pre>
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type <code>rm filename</code> .
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.

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	machine_name%
C shell superuser prompt	machine_name#
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#

Introduction to Solstice Messaging Management

1 

This chapter provides an introduction to messaging management with the Solstice Messaging Manager 1.0 and the Solstice management agents.

<i>Solstice Messaging Management Architecture</i>	<i>page 1</i>
<i>Solstice Messaging Manager</i>	<i>page 3</i>
<i>Messaging Management Agents</i>	<i>page 9</i>
<i>How the Solstice Messaging Manager and the Agents Interact</i>	<i>page 14</i>
<i>Messaging Management Summary</i>	<i>page 16</i>

Solstice Messaging Management Architecture

To manage and monitor messaging applications over a network using the Solstice messaging management architecture, you need the following components:

- Solstice Messaging Manager working with SunNet Manager 2.2.2 or later on the management workstation
- Solstice Simple Network Management Protocol (SNMP) agents for the messaging applications on the machines where the applications reside
- The Solstice SNMP Relay. This allows several SNMP agents to run on the same host machine

These components use SNMP to communicate, as illustrated in Figure 1-1 on page 2.

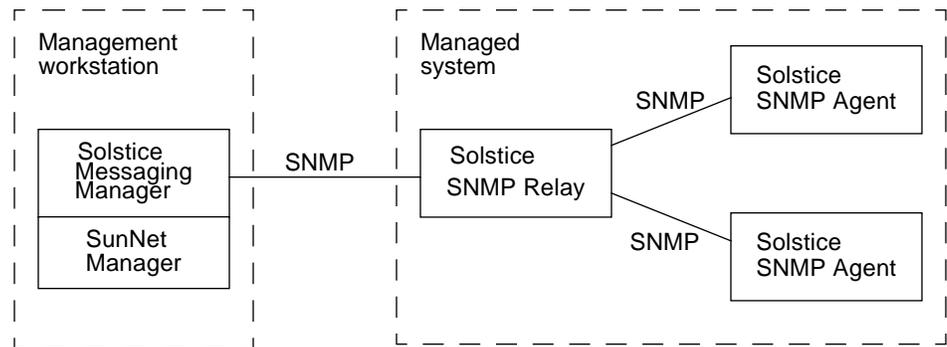


Figure 1-1 Solstice Messaging Management Architecture

The Solstice Messaging Manager is a set of management tools that enable you to monitor a network of messaging applications. You can use the Solstice Messaging Manager to:

- collect statistics about messaging traffic,
- help with load balancing,
- get early warning of potential problems,
- watch out for attempted security violations,
- perform troubleshooting,
- remotely configure a messaging application.

Each monitored messaging application is associated with an SNMP agent that handles requests for information and sends out alarms when necessary. You can use the Solstice Messaging Manager with the following Solstice SNMP agents:

- Solstice X.400 Server SNMP Agent, supplied with the Solstice X.400 Messaging Server 9.0
- Solstice X.400 XAPIA SNMP Agent, supplied with the Solstice X.400 Client Toolkit 9.0

The Solstice X.400 Server Agent can monitor the following Solstice X.400 processes:

- Solstice X.400 MTA (`osimta`)
- Solstice X.400 Message Store (`osix400ms`)
- Solstice X.400 Internet Adaptor (`osismtpx400`)

The Solstice X.400 XAPIA Agent monitors the following Solstice X.400 process:

- Solstice X.400 Client Toolkit (`osixapia`)

Solstice Messaging Manager

Solstice Messaging Manager works with SunNet Manager, a product that offers a set of tools for managing networks by monitoring system variables.

The tools supplied with Solstice Messaging Manager help you monitor and manage messaging applications on your network. These tools are integrated in the SunNet Manager Console window. Solstice Messaging Manager also uses the SunNet Manager management database.

This section provides an overview of:

- the management console
- the Messaging Manager tools
- the SunNet Manager management database

The Management Console

The SunNet Manager Console contains views of your network in your Home view. There are a variety of icons to represent servers, routers, workstations, printers and so on. Solstice Messaging Manager enables you to add messaging views onto the management console. A messaging view is represented by a cloud icon containing an envelope. Figure 1-2 on page 4 shows the Home view with a messaging icon next to the network icon.

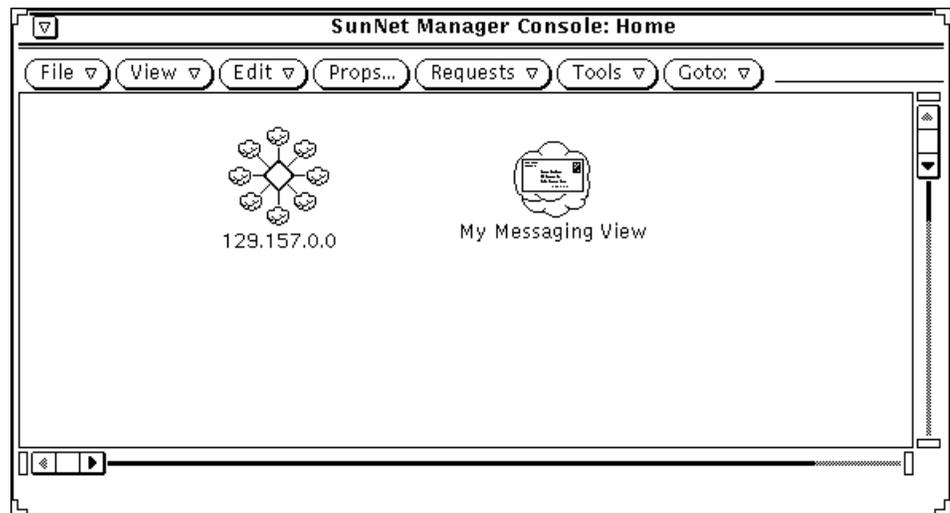


Figure 1-2 Home View in the SunNet Manager Console

By double-clicking on the cloud icon, you reveal the contents of the messaging view. See Figure 1-3 on page 5.

In a messaging view, each messaging application is represented by an icon with a name below of the form *hostname:application*, where *hostname* is the hostname of the machine the messaging application resides on, and *application* is the type of messaging application. Lines between icons represent potential connections.

Applications or processes that are not directly monitored by an SNMP agent are represented in the messaging view if they are associated with a monitored process. For example, in Figure 1-3 on page 5, the user agents *homere:x400-ua:tt* and *homere:x400-ua:gg* are represented because of their association with *homere:x400-mta*, the MTA on the host *homere*.

For a list of messaging icons and the applications they represent, refer to “Messaging Management Summary” on page 16.

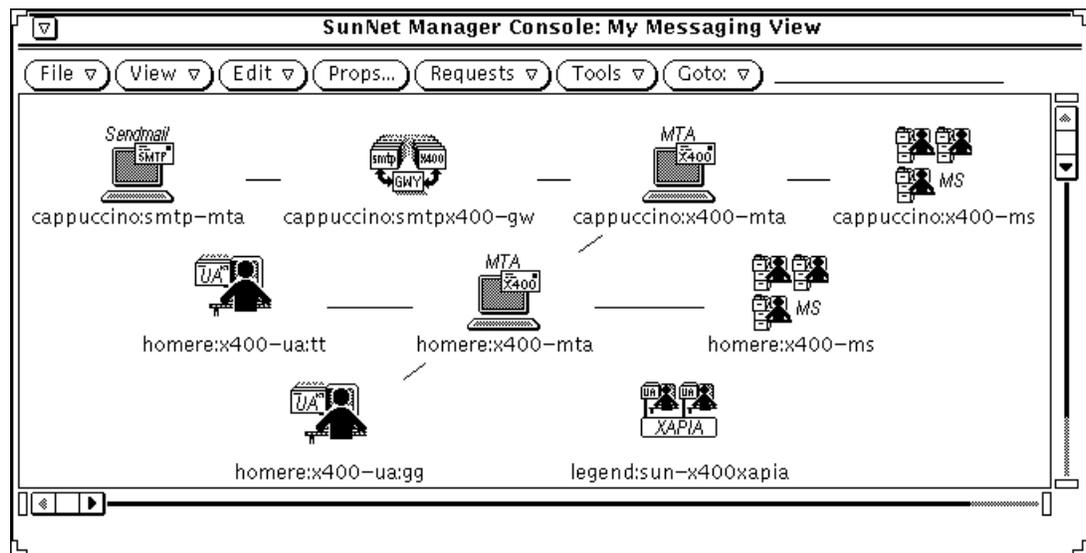


Figure 1-3 A Messaging View

Messaging Manager Tools

The Solstice Messaging Manager tools are additions to SunNet Manager. Solstice Messaging Manager tools include:

- A Messaging Manager Discover Tool that automatically builds a view of the messaging applications running on the machines in your network; see “Using the Messaging Manager Discover Tool” on page 21.
- Statistics tools, that hide the complexity of SunNet Manager requests by offering a set of requests and returning the information in a format that is easy to read; see “Using the Statistics Tools” on page 25.
- A choice of predefined graphs; see “Using the Graphs Tool” on page 32.
- Access to the configuration tools, `x400tool`, `ositool` and `xapiatool`; see “Access to Configuration Tools” on page 7.

The Messaging Manager Discover Tool

The Messaging Manager Discover tool automatically builds a view of the messaging processes that are running on machines on your network. The Discover Tool can contact all the hosts in the SunNet Manager management database to search for messaging processes. It builds a view of the “discovered” processes and of the associations between them. This messaging view, represented by a cloud icon, is added to the SunNet Manager management database. The messaging cloud contains a variety of icons, each representing a messaging process.

Using the Messaging Manager Discover tool, you can create different messaging views. If you have a large number of messaging applications on your network, you can, for example, break down the global messaging view into smaller, more manageable chunks. Also, if you manage a network that covers several sites, you may want to have one view per site.

The Messaging Manager Discover tool also offers an easy way of updating your messaging views. By running it regularly, you can detect changes that you may not have been aware of.

Read “Using the Messaging Manager Discover Tool” on page 21 for more information on how to create one or more messaging views.

Statistics Tools

Using the Statistics tools, you can obtain statistics for all monitored (or “discovered”) MTAs, gateways and message stores. The information is presented in a format that is easy to read. The Statistics tools offers two different sets of statistics: one set applies to Solstice X.400 MTAs and gateways, the other to Solstice X.400 message stores. Refer to “Using the Statistics Tools” on page 25 for instructions on how to obtain statistics and for examples of displays.

Predefined Graphs

When you start the Graphs tool, the Messaging Manager Grapher window is displayed. It offers a number of predefined graphs that you can select from a scrollable list. You can create your own messaging graphs and add them to the

list of predefined graphs by using the configuration options. You can also modify the predefined graphs. This is described in “Using the Graphs Tool” on page 32.

Access to Configuration Tools

The Messaging Manager offers access to the following configuration tools:

- `x400tool`
- `ositool`
- `xapiatool`

When you start a configuration tool for a messaging application from the management console, you perform a remote Xdisplay via remote login to the host where the messaging application is running. You are prompted for the root password of the remote host, unless the management station is declared in the `/etc/hosts.equiv` or the `.rhosts` file on the remote host.

Note – In a remote login operation, the root password for the remote host can be transmitted in the clear over the network.

`x400tool`

The `x400tool` configuration tool offers configuration facilities for the Solstice X.400 Messaging Server, which includes an MTA, a message store, and a Solstice X.400 Internet Adaptor. You can start `x400tool` from the menu associated with the server component’s icon in the management console.

Using `x400tool`, you can, for example, start or stop X.400 processes, configure the messaging server, add information about users, test associations between MTAs, test message routing, and save and restore message store user mailboxes. `x400tool` also allows you to perform tasks that you can carry out directly with the Messaging Manager, such as request status information, and monitor messaging traffic.

ositol

You can start `ositol`, the graphical user interface for the SunLink™ OSI communication platform (stack) from the menu associated with X.400 MTAs, gateways, and message stores.

Using `ositol`, you can set stack parameters, configure the type of network used (X.25, LAN, TCP-IP), configure channel resources, perform end system to intermediate system (ES-IS) protocol configuration, perform network addressing and configure routes to remote systems.

xapiatool

The `xapiatool` configuration tool offers configuration facilities for the Solstice X.400 Client Toolkit. You can start `xapiatool` from the menu associated with the XAPIA user agents' icon.

Using `xapiatool` you can maintain the XAPIA libraries for your applications and define the server (MTA or message store) that serves your applications.

For detailed information on the tasks you can perform with `x400tool`, `ositol`, and `xapiatool`, refer to:

Configuration Tool	Manual
<code>x400tool</code>	<i>Solstice X.400 Messaging Server Administrator's Guide</i>
<code>ositol</code>	<i>SunLink OSI Communication Platform Administrator's Guide</i>
<code>xapiatool</code>	<i>Solstice X.400 Client Toolkit Administrator's Guide</i>

The SunNet Manager Management Database

The SunNet Manager management database is a collection of files that contain definitions of:

- machine types (for example SPARCstation 10 or SunServer 2000),
- application types (for example MTA or message store),
- icons representing machine types and application types,

- specific machines and applications,
- SNMP agents and the type of information they monitor (described in the schema files *.schema).

As you work with SunNet Manager and Solstice Messaging Manager to create views of your network and of the messaging applications running on it, you create your own *runtime database*. This database reflects the state of your network. You can save and restore this database. This allows you to keep multiple views of your network through multiple saved databases. However, SunNet Manager will only allow you to display and use one database file at a time.

For more information on database files, refer to the *SunNet Manager User's Guide*.

Messaging Management Agents

The Solstice X.400 Messaging Server, Solstice X.400 Internet Adaptor, and Solstice X.400 Client Toolkit are supplied with SNMP agents. These agents make it possible to monitor and manage the applications from a central management station.

The Solstice X.400 Server Agent monitors:

- the Solstice X.400 Messaging Server 9.0 (includes an X.400 MTA and an X.400 message store)
- the Solstice X.400 Internet Adaptor 9.0 (an SMTP/X.400 gateway)

The Solstice X.400 XAPIA Agent monitors:

- Solstice X.400 Client Toolkit 9.0

Both these SNMP agents are compliant with the Management Information Bases (MIBs) defined in the MADMAN (Messaging And Directory MANagement) standard, in RFC 1565 and RFC 1566. These MIBs describe the type of information an SNMP agent can collect. Solstice SNMP Agents also support extensions that handle message store data and traps. Detailed information on the Solstice SNMP Agents is provided in “The Solstice X.400 Server Agent” on page 51 and “The Solstice X.400 XAPIA Agent” on page 62.

Management Information Bases (MIBs)

The Management Information Base defined by Internet standards groups is a global information model for network management. This model contains information objects that are organized in a tree structure to allow for future extensions. Figure 1-4 on page 11 illustrates part of the global information model.

Subtrees of the global MIB tree, which address a particular area of network management, are also called MIBs. For example, there is a Mail Monitoring MIB (RFC 1566) for message transfer agents such as the Solstice X.400 MTA (included in the Messaging Server product) and the Solstice X.400 Internet Adaptor.

Every object in the global MIB has a meaningful English-language object name and a unique object identifier (OID). The English-language object name reflects the semantic contents of the object, whereas the OID is a sequence of numbers that is obtained by combining the OIDs of all objects on the “path” between the root and a particular object. The OID indicates the exact location of the corresponding object in the global MIB. For example, the application table object has the object name `applTable` and the OID 1.3.6.1.2.1.27.1.

The standard information objects designed to manage and monitor systems and applications are included under the management subtree *mgmt(2)*. The *application(27)* subtree and the tables below, *applTable* and *assocTable*, are defined in the Network Services Monitoring MIB. The information objects, or variables, that are in these tables are not shown in Figure 1-4. Examples are provided in Chapter 3, “Solstice X.400 SNMP Agents”.

An SNMP agent can support an entire subtree of the global MIB, or specific tables or individual objects. When an SNMP agent receives a request from a management application, it will return the values of the MIB objects it supports.

For example, the Solstice Messaging Manager can query the X.400 Server SNMP Agent for information such as application status, number of associations between applications, and number and volume of messages transmitted or stored.

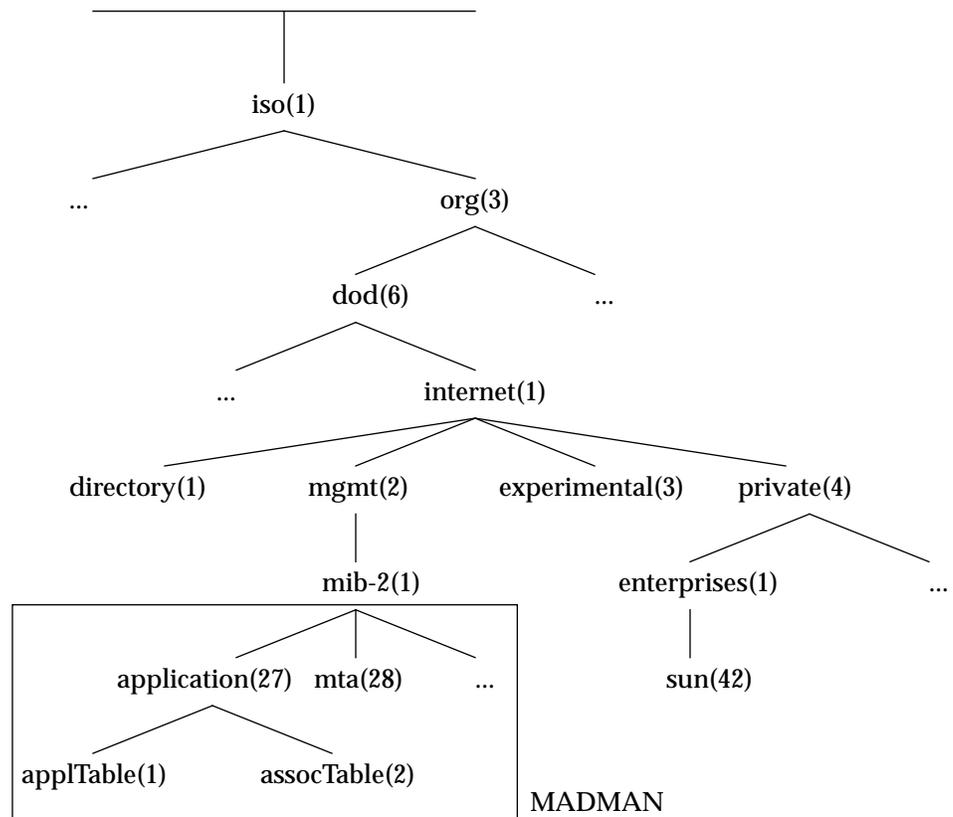


Figure 1-4 Part of the Global Information Model

MIBs Supported by the X.400 Server SNMP Agent

The X.400 Server SNMP Agent conforms to the following MIBs, which belong to the MADMAN standard:

- The Network Services Monitoring MIB (RFC 1565) that applies to all network applications.
- The Mail Monitoring MIB (RFC 1566) that applies to message transfer agents and messaging gateways.

Examples of the information objects contained in these MIBs are provided in Chapter 3, “Solstice X.400 SNMP Agents”.

The X.400 Server SNMP Agent also supports the following extensions to the standard:

- A MIB for message stores, enabling a management platform to obtain statistics for the entire message store, and for each individual user.
- Support for unsolicited event reports or SNMP *traps*. When the X.400 SNMP Agent detects an abnormal condition, it sends out an unsolicited event report (called an SNMP *trap*) without waiting to receive a specific request from the management station. SNMP traps can be divided into two categories:
 - changes in the operating status of monitored applications
 - alarms generated by monitored applications

The possible values for the operating status of the Solstice X.400 MTA are: *up, down, congested, restarting*.

The possible values for the operating status of the Solstice X.400 Message Store are: *up, down, restarting*.

The possible values for the operating status of the Solstice X.400 Internet Adaptor (SMTP/X.400 gateway) are: *up, down, restarting*.

The possible values for the operating status of the Solstice X.400 Client Toolkit are: *up, down, restarting*.

Alarms generated by monitored applications are diverse. Here are a few typical examples:

- Failure to connect to another MTA or gateway
- Failure to deliver or to redirect a message
- Message looping
- Failure in message handling

Traps caused by an alarm generated by a monitored application contain:

- the application name (`applName`)
- an alarm identification number (`alarmId`), which is always *-1*
- an alarm severity level (`alarmSeverity`), which can be *low, medium, or high*
- a description of the cause of the alarm (`alarmDescr`)

Examples of message store data reports and traps are provided in Chapter 3, “Solstice X.400 SNMP Agents”.

Note – These extensions provide additional management features without affecting compliance to existing RFCs.

MIBs Supported by the X.400 XAPIA SNMP Agent

The X.400 XAPIA SNMP Agent supports the following variables belonging to the application table (`applTable`) defined in the Network Services Monitoring MIB (RFC 1565):

- `applName`
- `applVersion`
- `applUpTime`
- `applOperStatus`

The X.400 XAPIA Agent also provides support for the following two categories of SNMP traps:

- changes in the operating status of the monitored application (possible values: *up*, *down*, *restarting*)
- alarms generated by the monitored application

Traps caused by an alarm generated by a monitored application contain:

- the application name (`applName`)
- an alarm identification number (`alarmId`), which is always *-1*
- an alarm severity level (`alarmSeverity`), which can be *low*, *medium*, or *high*
- a description of the cause of the alarm (`alarmDescr`)

Examples of data reports and traps are provided in Chapter 3, “Solstice X.400 SNMP Agents”.

Note – These extensions provide additional management features without affecting compliance to existing RFCs.

How the Solstice Messaging Manager and the Agents Interact

This section describes the SNMP version 1 protocol used for communications between the Messaging Manager and the SNMP agents. It also describes the SNMP Relay.

The SNMP Protocol

SNMP is a standard protocol designed to offer simple management services for TCP/IP networks. When an agent and a management application communicate using SNMP, they form an SNMP *community* identified by a *community name*.

The messages that the agent and the management application exchange always contain this community name as a simple authentication method, and an SNMP operation.

The SNMP operation can be one of the following: `get`, `get-next`, or `trap`.

- The management application uses the `get` and `get-next` operations to send a request to an SNMP agent (`get-request` or `get-next-request`).
- SNMP agents use the `get-response` operation to send a response to a request from the management application. SNMP agents also use the `trap` operation to send unsolicited event reports.

The SNMP Relay

The SNMP standard states that an SNMP agent must wait on UDP port 161 for incoming requests. This means that a host can normally have only one agent. To bypass this limitation, the SNMP Relay waits on UDP port 161 while the SNMP agents are set to wait on different UDP ports. The SNMP Relay dispatches incoming requests to the UDP ports where the agents actually reside, as shown in Figure 1-5 on page 15.

Example of Messaging Management Setup

Figure 1-5 shows an example of communication setup between Solstice X.400 SNMP Agents and the Solstice Messaging Manager.

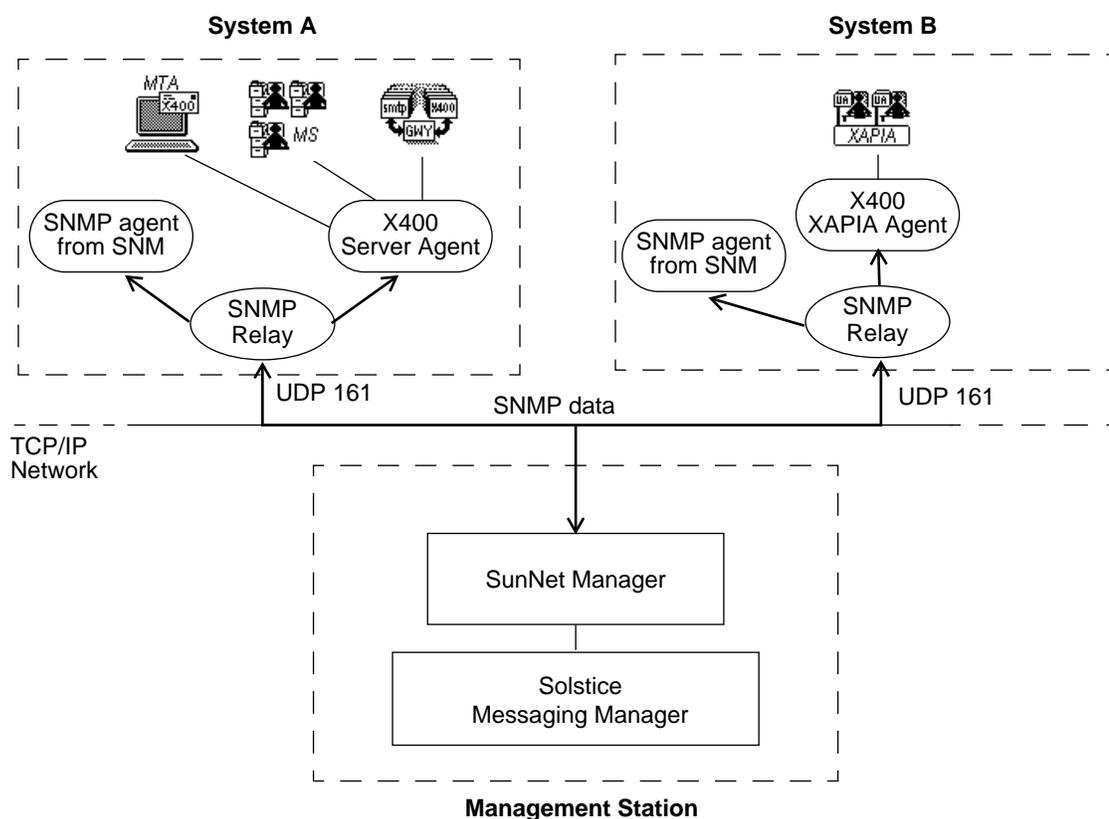


Figure 1-5 Messaging Management with the Solstice Messaging Manager

On System A, a single X.400 Server SNMP Agent monitors an X.400 MTA, an X.400 message store (both part of the Solstice X.400 Messaging Server 9.0 product) and an SMTP/X.400 gateway (the Solstice Internet Adapter). The SNMP agent supplied with SunNet Manager responds to requests concerning system variables (defined in `mib-2`). The SNMP Relay routes the information between the SNMP agents and the management station.

On System B, an X.400 SNMP XAPIA Agent monitors the XAPIA daemon. The SNMP agent provided with SunNet Manager monitors system variables.

The presence of the SNMP agent for SunNet Manager is not strictly required, but it is helpful because it provides useful system and network statistics.

In the case where there is only one SNMP agent on a host, the SNMP Relay is nonetheless required, for reasons of consistency in the messaging management architecture.

Messaging Management Summary

Table 1-1 provides a summary of the different messaging icons that you may see on the management console, the messaging components and processes they represent, and the SNMP agents used to manage them.

Table 1-1 Messaging Management Summary

Icon	Messaging component	Messaging process	Key	SNMP Agent	SNMP Agent process
	Solstice X.400 MTA	osimta	1	Solstice X.400 Server SNMP Agent	snmpx400d
	Solstice X.400 Message Store	osix400ms	2	Solstice X.400 Server SNMP Agent	snmpx400d
	Solstice X.400 Internet Adaptor	osismtpx400	3	Solstice X.400 Server SNMP Agent	snmpx400d

Table 1-1 Messaging Management Summary

Icon	Messaging component	Messaging process	Key	SNMP Agent	SNMP Agent process
	Sendmail SMTP MTA	sendmail	-		-
	Third-party P3 X.400 User Agent	-	-		-
	Solstice X.400 Client Toolkit	osixapia	4	Solstice X.400 XAPIA SNMP Agent	snmpxapiad

Third-party MTAs, message stores and gateways are represented by a plain square icon.

Solstice Messaging Manager



This chapter provides detailed instructions on how to start and use the Solstice Messaging Manager 1.0 to monitor your messaging system. It also contains examples.

<i>Starting the Solstice Messaging Manager</i>	<i>page 19</i>
<i>Using the Messaging Manager Discover Tool</i>	<i>page 21</i>
<i>Obtaining Messaging Statistics</i>	<i>page 25</i>
<i>Creating Event Requests</i>	<i>page 37</i>
<i>Viewing Messaging Events, Traps, and Errors</i>	<i>page 42</i>
<i>Configuring the Display of Information</i>	<i>page 47</i>

Starting the Solstice Messaging Manager

This section assumes that:

- SunNet Manager 2.2.2 or later is installed and running on the workstation you want to use as a management station. Refer to the *SunNet Manager Installation Guide*.
- Solstice Messaging Manager is installed on your management station. Refer to the *Installing and Licensing Solstice X.400 Products* CD booklet.

Before you can use Solstice Messaging Manager, you must reinitialize SunNet Manager to load the schema used by the Messaging Manager.

▼ **How to Start Solstice Messaging Manager 1.0**

1. Save your SunNet Manager runtime database. To do this:

- a. In the SunNet Manager Console window, pull down the File menu and, from the Save submenu, select Management Database.**

A popup window is displayed. If you started SunNet Manager from your home directory, this window shows the contents of your home directory.

- b. In the popup window, give a name to your runtime database and save it.**

This operation is important because when you reinitialize SunNet Manager, your runtime database will be erased.

2. Quit SunNet Manager.

3. Restart SunNet Manager by entering the following command:

```
prompt% snm -i &
```

This command reinitializes SunNet Manager. During this operation, the schemas used by the Messaging Manager are detected and loaded into SunNet Manager. This command also updates the SunNet Manager database (not the runtime database you saved to file).

4. In the SunNet Manager Quick Start window, select Basic Start.

This starts SunNet Manager with an empty runtime database.

5. Load the runtime database you saved in Step 1. To do this:

- a. In the SunNet Manager Console window, pull down the File menu and, from the Load submenu, select Management Database.**

A popup window is displayed. It usually shows the contents of your home directory.

- b. In your directory tree, select your database file and load it.**

The Solstice Messaging Manager tools are now present under the Tools menu in the SunNet Manager console.

Using the Messaging Manager Discover Tool

This section explains how to create a view of the messaging applications running on your network with the Messaging Manager Discover Tool. It also explains how you can use the Messaging Manager Discover Tool to monitor changes in your messaging system and update your messaging view.

This section assumes that:

- SunNet Manager 2.2.2 or later is installed and running on the workstation you want to use as a management station. Refer to the *SunNet Manager Installation Guide*.
- Solstice Messaging Manager is installed and running on your management station. Refer to “Starting the Solstice Messaging Manager”.
- you have a view of your network in the management console. If not, you can create one using the SunNet Manager Discover tool. Refer to the *SunNet Manager User’s Guide*.
- SNMP agents are installed on the same hosts as the messaging applications they monitor.

Creating a Messaging View for the First Time

The easiest way of creating a messaging view is to run the messaging Manager Discover tool.

This section explains how to run the Messaging Manager Discover tool.

▼ **How to Run the Messaging Manager Discover Tool**

- 1. Pull down the Tools menu in the SunNet Manager Console window and select Messaging Manager Discover.**

The Messaging Manager Discover Tool is displayed, as shown in Figure 2-1 on page 23.

- 2. All hosts managed by SunNet Manager are listed and selected in the Hosts scrolling list. You can either:**

- accept the default selection and run the Discover tool on all hosts;
- deselect the few hosts on which you do not want to run the Discover tool;

- deselect all hosts by pressing the MENU mouse button anywhere in the scrolling list and selecting Clear All Choices. Then select the host machines you want the Discover tool to contact.

3. Set the options you need to create your messaging view:

- a. Select the type of application you want to discover.**
the available options are: Sun X.400 MTAs, Sun X.400 message stores, Sun X.400 XAPIA Clients, third-party MTAs, and other third-party applications. By default, all options are selected.
- b. If required, change the default name of the view.**
- c. Select verbose mode if you want detailed feedback on the Discover process.**
- d. Choose to draw or hide connections between applications.**
When the “Draw Connections” option is enabled, the tool will draw lines between applications that *can* connect to each other even when there is no current connection.
- e. Accept the default setting (Yes) for Copy Icons Under Host View, if you want the messaging icons to be represented both in the messaging view and in the network view, under the corresponding host icons.**
- f. Accept the default settings for Allow to Remove Icons and Allow to Remove Connections (respectively Never and No).**
These options are used to update existing messaging views. For more details, refer to “Updating Messaging Views” on page 25.
- g. If necessary, change the default number of maximum simultaneous requests.**
This number is not related to the number of hosts selected for the Discover operation; it is used to limit the load on the network.

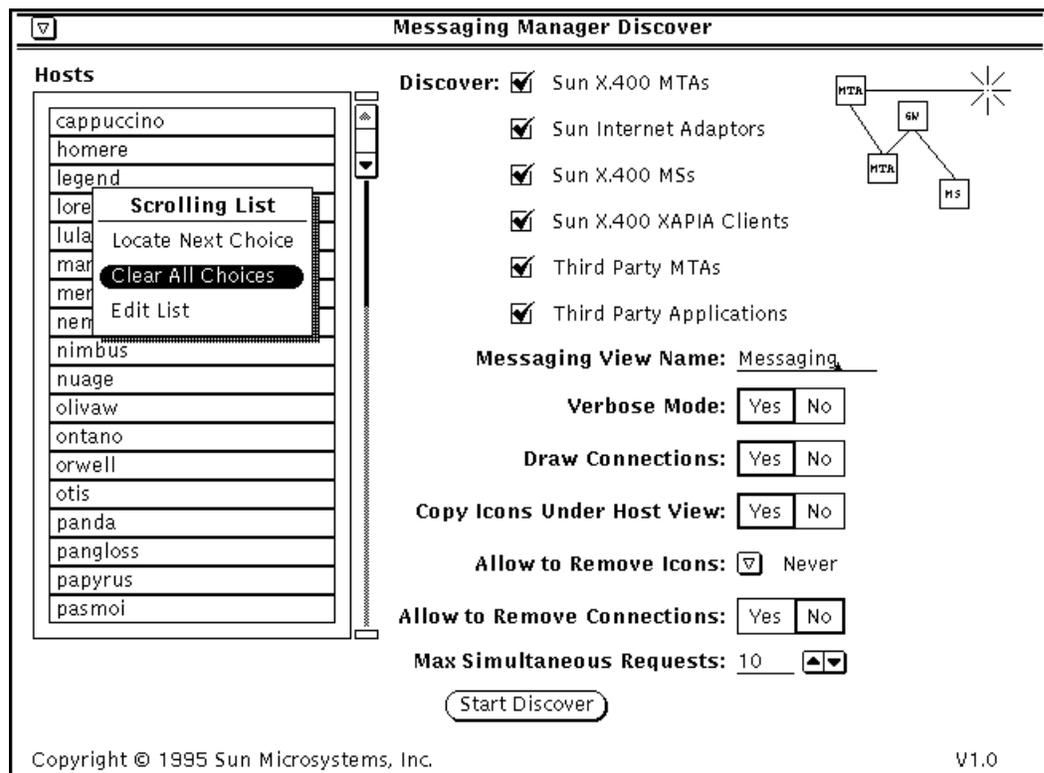


Figure 2-1 The Messaging Manager Discover Tool Main Window

4. Click on the Start Discover button.

A Messaging Discover Console window appears. Messages are displayed to report on the progress of the Discover process. A summary is displayed when the process is finished.

5. When the Discover process is finished, quit the Messaging Manager Discover window.

In the SunNet Manager console, there is now a messaging cloud next to the network cloud as shown in Figure 2-2. Double click on the messaging cloud icon to reveal the messaging applications that have been discovered. See Figure 2-3 on page 24.

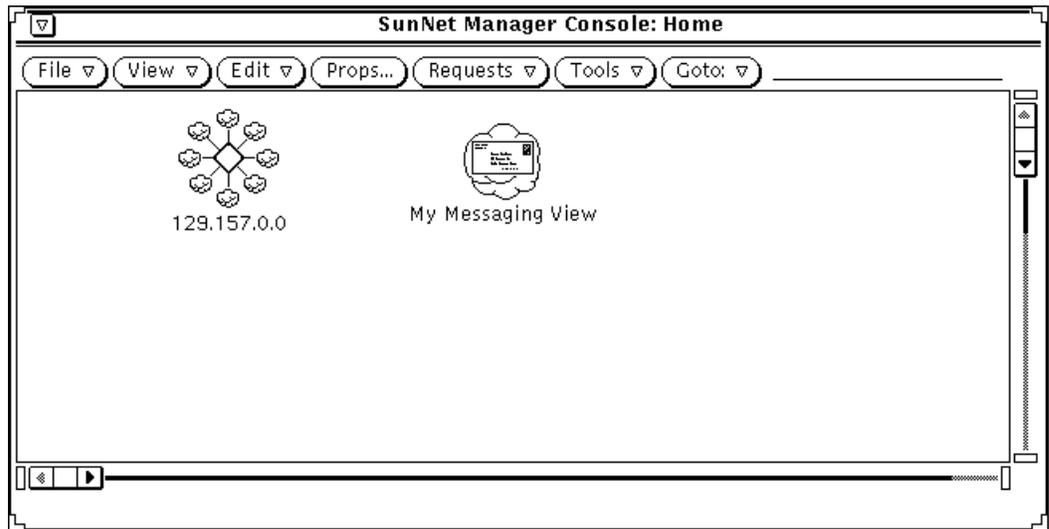


Figure 2-2 A Messaging Cloud

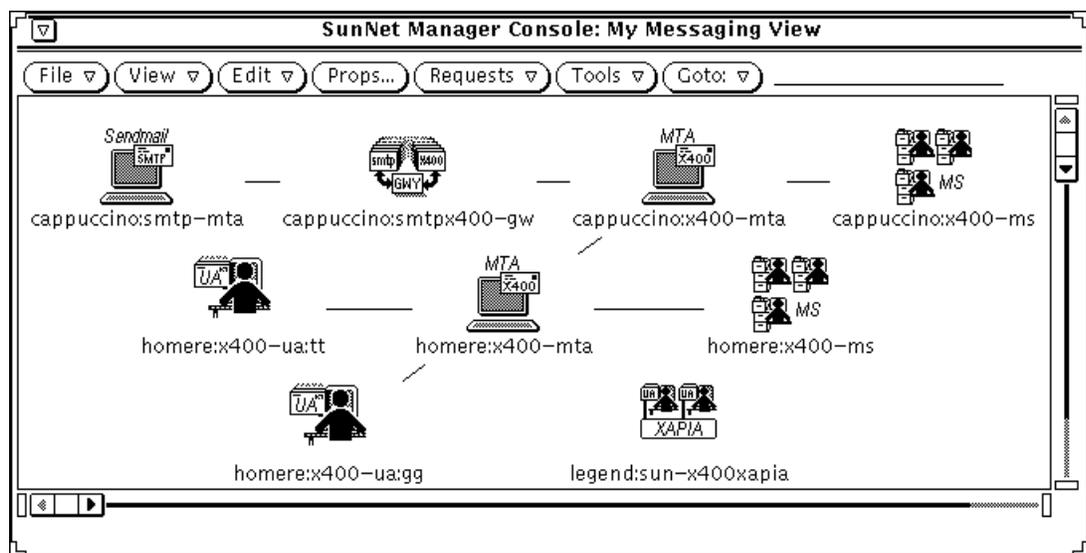


Figure 2-3 Inside the Messaging Cloud

Updating Messaging Views

Run the Messaging Manager Discover Tool regularly to update your messaging views. There are two reasons why you should do this:

- you may not be aware of newly installed messaging applications,
- if you have not set up specific event requests to poll all messaging applications, you may not be aware of recently removed messaging applications.

Two options in the Messaging Manager Discover Tool enable you to remove non-representative icons and connections from your messaging views during an update: “Allow to Remove Icons”, and “Allow to Remove Connections”.

To enable these options, set “Allow to Remove Icons” to “From all Views” or “From Messaging View”, and set “Allow to Remove Connections” to “Yes”.

If these options are disabled, that is, if “Allow to Remove Icons” is set to “Never” and “Allow to Remove Connections” is set to “No” (the default), icons and connections that are no longer representative will blink or are colored red (see “Configuring the Display of Information” on page 47). This allows you to determine whether it is normal for a particular application icon to be displayed in red or if it indicates a problem. It also makes any changes to the messaging system more obvious.

Obtaining Messaging Statistics

This section explains how to obtain messaging statistics for the Solstice X.400 MTA, Solstice X.400 Message Store, and Solstice X.400 Internet Adaptor using the Messaging Manager Statistics tools and Graphs tool.

Using the Statistics Tools

This section describes how to obtain and update messaging statistics with the Messaging Manager Statistics tools.

There are two statistics tools: one displays statistics on MTAs and gateways, the other displays statistics on message stores. When you select “Statistics tool” from a messaging application icon menu, you start the statistics tool that is relevant for that application.

This section explains how to:

- obtain statistics for an MTA or a gateway
- obtain statistics for a message store
- update statistics
- reset the statistics for an MTA

▼ How to Obtain Statistics on an MTA or a Gateway

1. Pull down the icon menu of the MTA or gateway application you want to query. In the Tools submenu, select Statistics.

This displays the MTA Statistics main window, as shown in Figure 2-4 and Figure 2-5 on page 27. The MTA Statistics main window contains the name of the application being queried, its version, and its operating status.

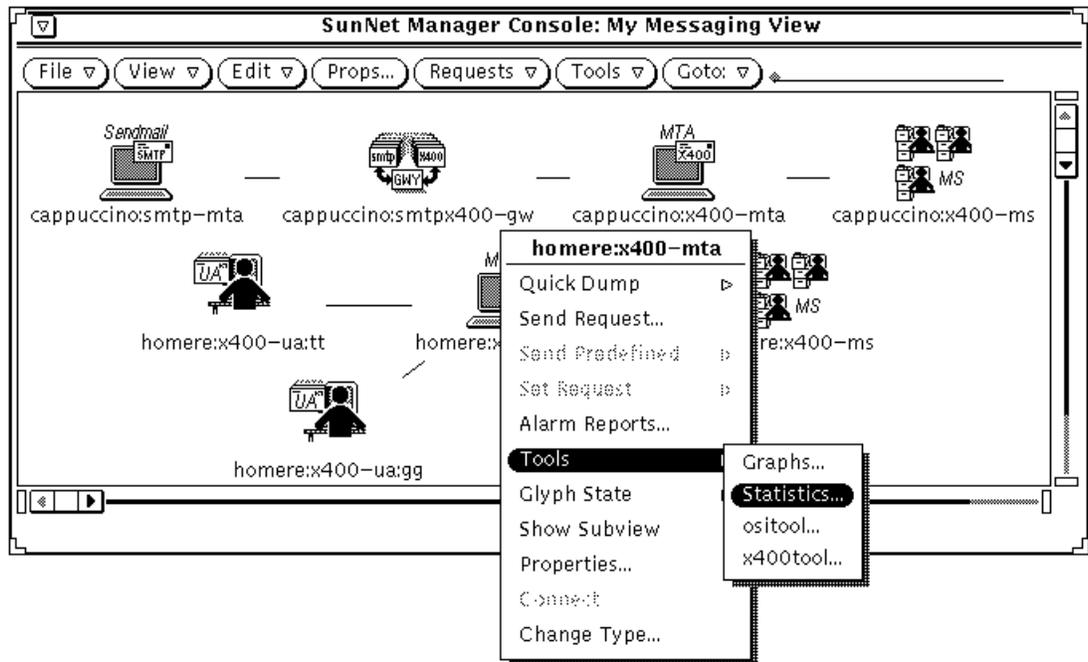


Figure 2-4 Icon Menu of an MTA

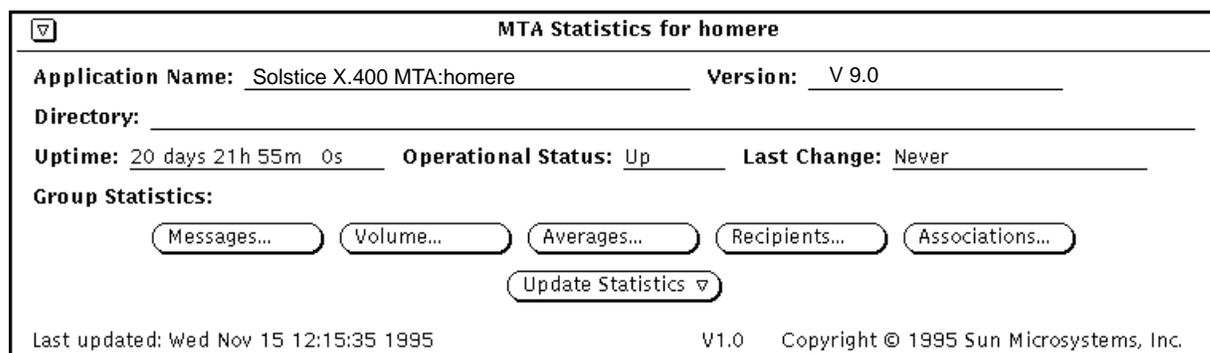


Figure 2-5 MTA or Gateway Statistics Main Window

2. Select one or several of the Group Statistics buttons.

For each type of group statistics you select, detailed statistics are displayed in a separate window. Table 2-1 on page 28 describes the statistics corresponding to each Group Statistics button. Figure 2-6 on page 28 shows the message statistics for an MTA. The Application field contains the name of the MTA. The MTA Group Name list contains the names of applications that have an association with the MTA. (In this context, an application that has an association with the queried application is considered to be an *MTA group*).

3. For the detailed list of associations between the queried application and an application listed in the MTA Group Name field:

a. Display the Associations group statistics by clicking on the Associations button in the MTA statistics main window

b. Highlight an item in the MTA Group Name List and click on the Association List button.

Detailed statistics for that MTA group are displayed including a list of current associations.

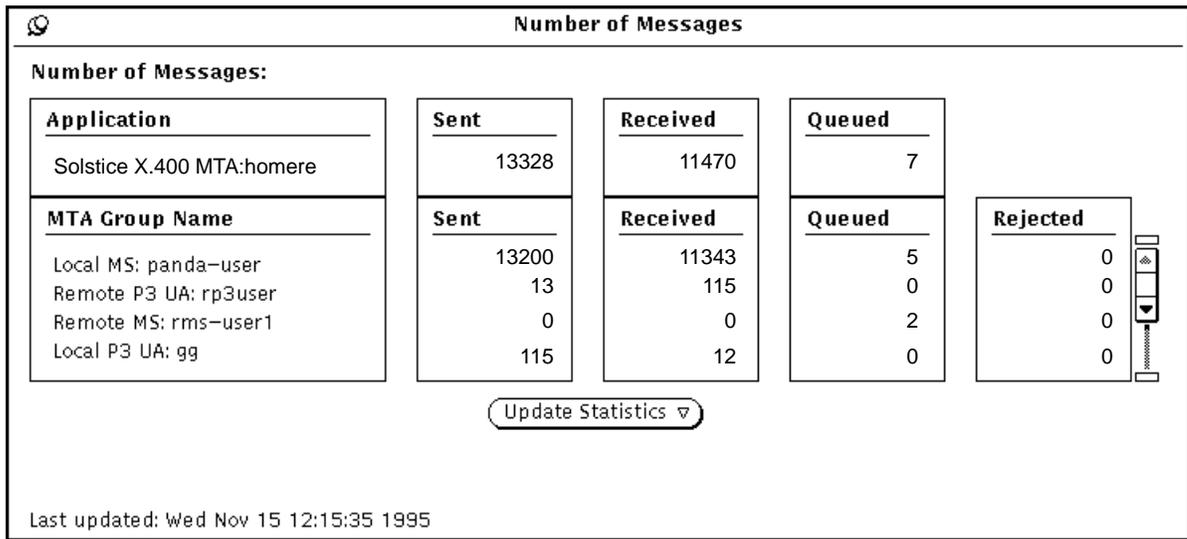


Figure 2-6 Message Statistics for an MTA

Table 2-1 Group Statistics

Group Statistics	Description
Messages	Gives the number of messages sent, received, queued, and rejected for each application associated with the queried MTA.
Volume	Gives the volume (in Kilobytes) of messages sent, received, and queued for each application associated with the queried MTA.
Averages	Gives the average message length (in Kilobytes) of messages sent, received, and queued for each application associated with the queried MTA.
Recipients	Gives the number of recipients specified in messages sent, received, and queued for each application associated with the queried MTA.
Associations	Gives the number of current inbound and outbound associations between the queried MTA and other messaging applications, the number of inbound and outbound associations since the MTA was started, and the number of rejected inbound and failed outbound associations.

▼ **How to Obtain Statistics on a Message Store**

- 1. Pull down the icon menu of the message store application you want to query and in the Tools submenu, select Statistics.**

This displays the Message Store Statistics main window, as shown in Figure 2-7 on page 30.

The upper part of the window contains the name of the application being queried, its revision level, and its operating status.

P3 connections are incoming connections from an MTA (mail arriving for a user) and outgoing connections to an MTA (a user connected to the message store is sending mail out via the MTA).

P7 connections are incoming connections from user agents (users reading their mail).

The lower part of the window displays statistics on user groups.

- 2. For detailed information on a particular group of users, highlight a group name in the list and click on the Show Group button.**

Another window is displayed, showing statistics per user, as shown in Figure 2-8 on page 30.

- 3. For detailed information on a particular user, highlight a user name in the list and click on the Show User button.**

The window that is displayed contains detailed statistics on that particular user's mailbox, as shown in Figure 2-9 on page 31.

- 4. For detailed information on current associations between a particular user mailbox and other messaging applications, click on the Current Associations List button.**

The window that is displayed contains detailed information about current associations.

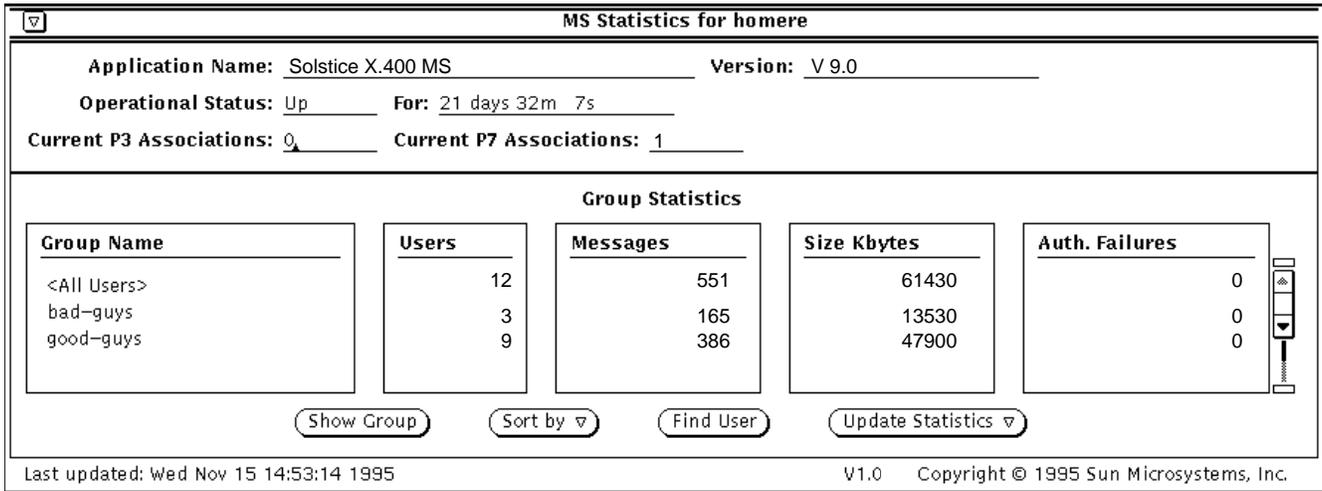


Figure 2-7 Message Store Statistics Main Window

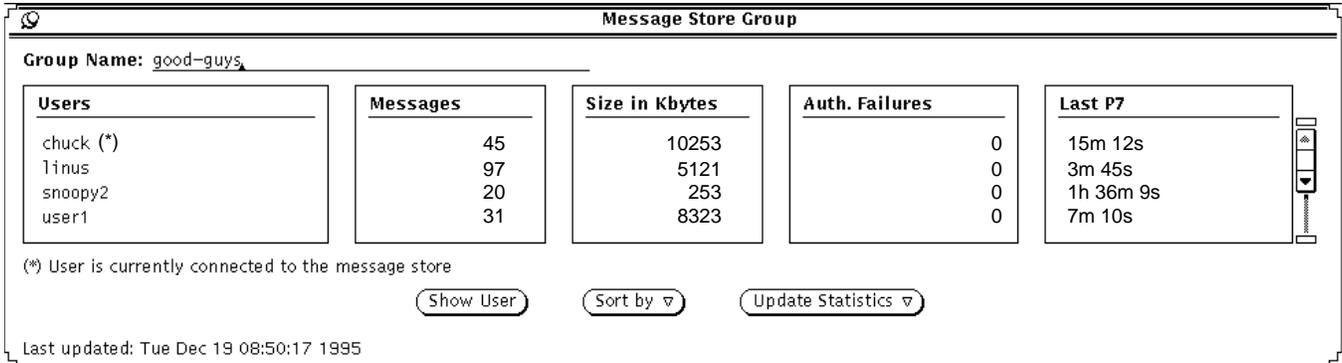


Figure 2-8 Message Store Group Statistics

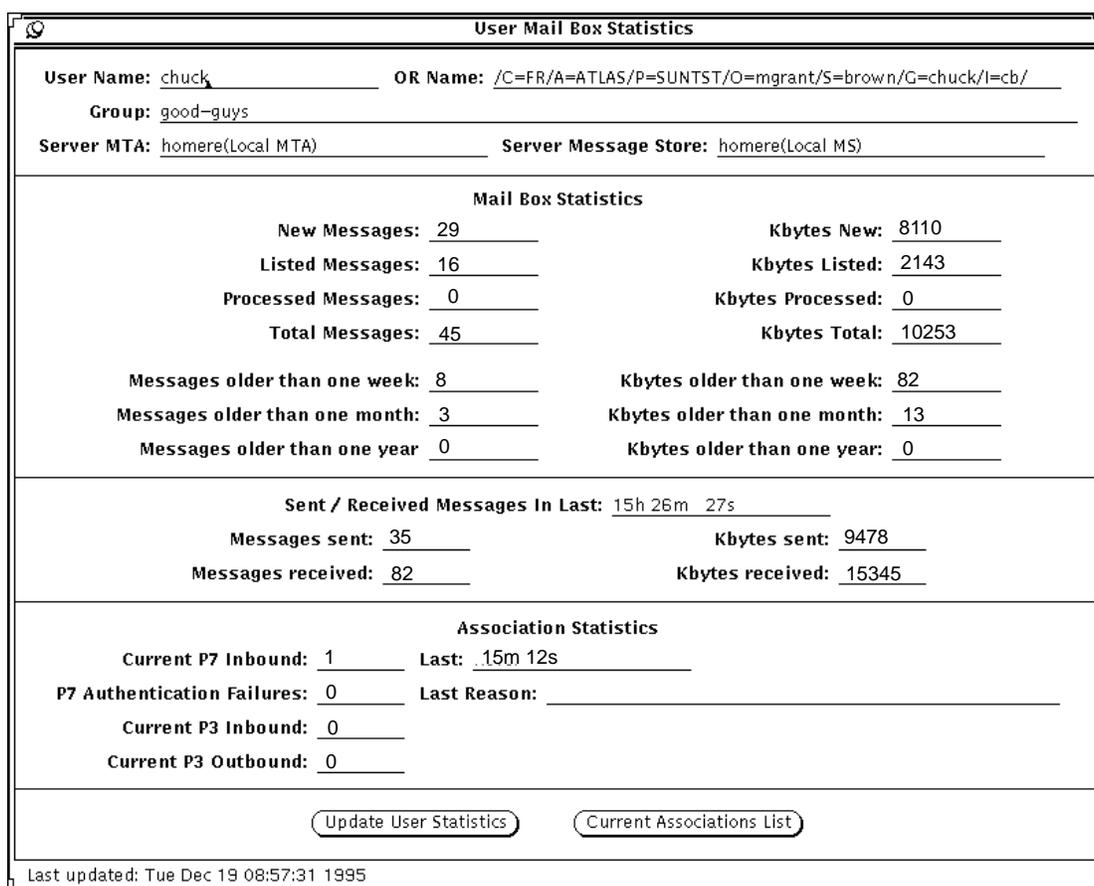


Figure 2-9 User Mailbox Statistics

▼ How to Update Statistics

An Update Statistics button is provided in all the statistics windows. This button offers two options:

- “Once”: updates the statistics for the application immediately.
- “Automatically”: displays a popup window that allows you to set the frequency of updates. This option also performs an update immediately.

▼ **How to Reset the Statistics for an MTA**

- 1. From the MTA icon menu in the Messaging Manager console, start `x400tool`.**
- 2. In the `x400tool` window, from the Manage submenu, select **Stop Collecting and Start Collecting consecutively**.
This resets the counters for the MTA statistics.**

Note – This operation will *not* reset the statistics for all the messaging applications represented in the `x400tool` window, but only for the local MTA.

Using the Graphs Tool

You can use the graph tool to select a predefined graph, or to create your own predefined graphs. The predefined graphs available let you monitor:

- current associations
- accumulated associations
- traffic, in number of messages, in volume (Kilobytes), and in number of recipients

Graphs displayed on your screen are updated continuously.

The Graphs tool enables you to merge several graphs into one. This feature offers a simple way of comparing variables (for instance traffic loads) for two messaging applications.

For more information on the Graphs tool features, refer to the *SunNet Manager User's Guide*.

This section explains how to:

- select and view a predefined graph
- create your own graph
- change the name in the title bar of a graph
- merge graphs

▼ How to Select and View a Predefined Graph

1. Pull down the icon menu of the messaging application you want to query and in the Tools submenu, select Graphs.

The Messaging Manager Grapher is displayed. It contains a scrolling list of predefined graphs, a Configure button and a Start Graph button. See Figure 2-10.

2. Select one or more of the graphs from the scrolling list, then click SELECT on the Start Graph button.

The Messaging Manager Grapher window closes and a graph is displayed for each graph name selected. These graphs are updated constantly.

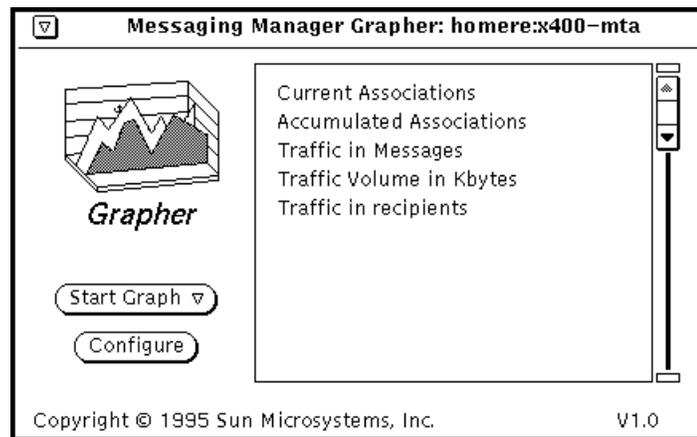


Figure 2-10 The Messaging Manager Grapher Main Window

Note – If you do not want the Grapher window to close, select “Start Graphs Without Exit” from the Start Graph button menu. This enables you to start another graph for the same application at a later time.

▼ **How to Create your own Graph**

- 1. Pull down the icon menu of the messaging application you want to query and in the Tools submenu, select Graphs.**

This displays the Messaging Management Grapher that contains a scrolling list of predefined graphs, a Configure button and a Start Graph button.

- 2. Click on the Configure button.**

The Grapher Configuration window is displayed, as shown in Figure 2-11 on page 35.

The Graphs scrolling list contains all existing predefined graphs, the Table scrolling list contains the names of MIB tables that you can plot, and the Attributes scrolling list contains the names of MIB variables that you can plot.

- 3. Click on the Insert button below the Graphs scrolling list.**

The default name *newgraph* appears at the end of the scrolling list and in the Name field.

- 4. Change the default name in the Name field to the name you want for your graph.**

- 5. In the Table scrolling list, select one MIB table.**

You can select one MIB table only because a graph can only plot variables belonging to the same MIB table. The table you select determines the contents of the Attributes scrolling list.

- 6. In the Attributes scrolling list, select the variables you want to plot.**

- 7. Click on Apply.**

Your new graph is added to the Graphs scrolling list in the Grapher Configuration window. It also appears in the scrolling list of graphs in the Messaging Management Grapher window.

- 8. Click on Done to exit from the Grapher Configuration window.**

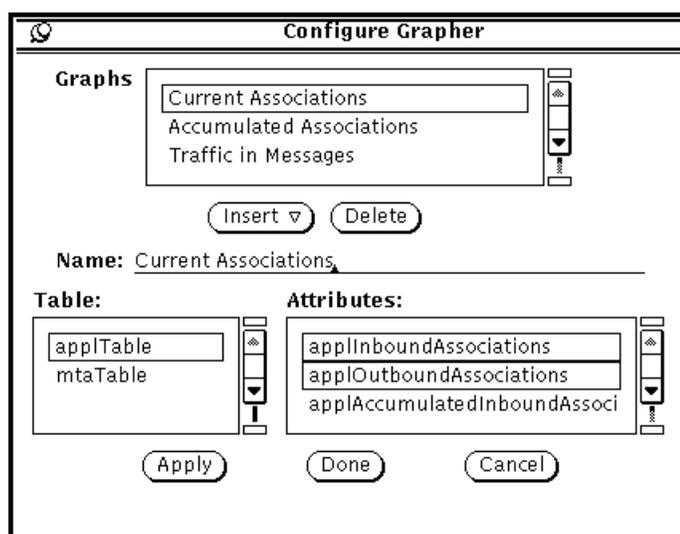


Figure 2-11 Graph Configuration Window

▼ How to Change the Name in the Title Bar of a Graph

- 1. Press the MENU mouse button in the background of a graph displayed on your screen, and select Properties.**

A Graph Properties window is displayed, as shown in Figure 2-12 on page 36.

- 2. In the Graph Properties window, change the graph name in the Name field to the name you want.**

The original name is simply an enumeration of the MIB variables used to plot the graph. It is useful to change it to a shorter name.

- 3. Click on Apply**

The new name is displayed in the title bar of the graph window and in the Results Grapher window.

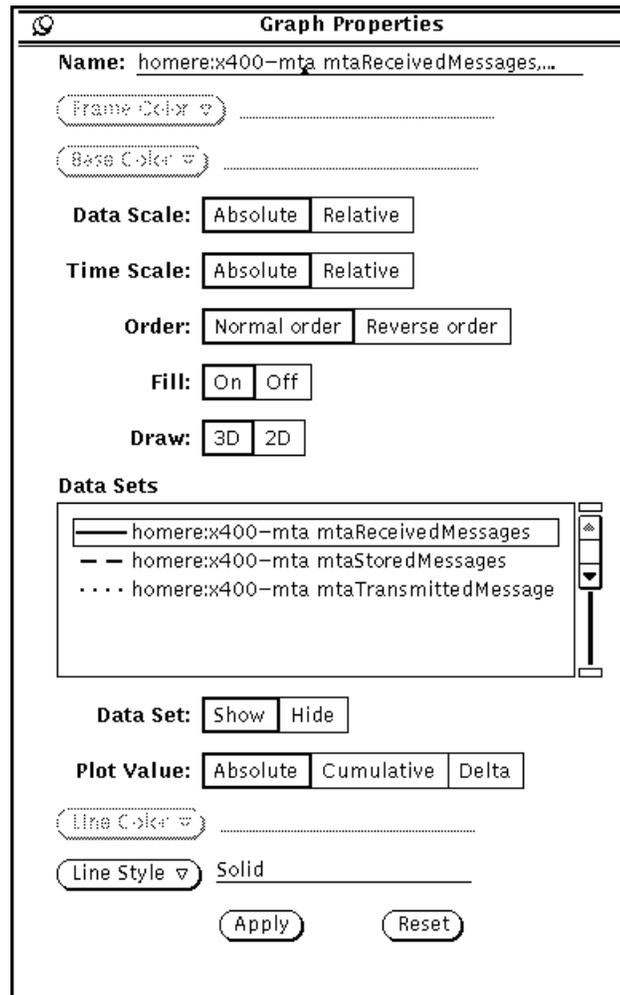


Figure 2-12 A Graph Properties Window

▼ **How to Merge Graphs**

- 1. Start the graphs you want to merge, as explained in “How to Select and View a Predefined Graph” on page 33.**

When these are displayed, their names appear in the scrolling list of the Results Grapher window.

2. Select the names of the graphs you want to merge in the scrolling list of the Results Grapher window.

3. Click on the Merge button in the Results Grapher window.

A new graph entitled Merged Graph is displayed. You may need to expand the Merged Graph window to see the keys for all plotted variables.

You may also want to change the name in the title bar of the graph. See the procedure on page 35.

Creating Event Requests

An event is a critical condition that needs to be reported whenever it occurs. Because every organization has its own definition of what is critical, the SunNet Manager Requests tool enables you to define event thresholds.

This section contains a detailed example of how to set up an event request to monitor for a critical load on an MTA. It also contains suggestions of potentially critical thresholds that could be monitored by creating specific event requests. It explains how to apply an existing event request to several messaging applications.

Note – When you set up an event request, the Messaging Manager continuously polls the target applications, thus using up CPU resources and creating an extra load on the network.

Example of Critical Load for an MTA

This example applies to a Solstice X.400 MTA which can, given the performance of the host, transmit approximately 15 messages per second. If the number of messages per second exceeds this limit, the messages are queued. If the queue grows, the MTA will go into congested state. Therefore, you may want to create an event request that will warn you whenever the message traffic through the MTA exceeds 10 messages per second.

▼ How to Create an Event Request to Monitor the Load on an MTA

1. Pull down the icon menu of a messaging application and select Send Request.

The SunNet Manager Request Builder window is displayed, as shown in Figure 2-13. The Agent Schema scrolling list contains the schema for the SNMP agent associated with the application concerned by the event request.

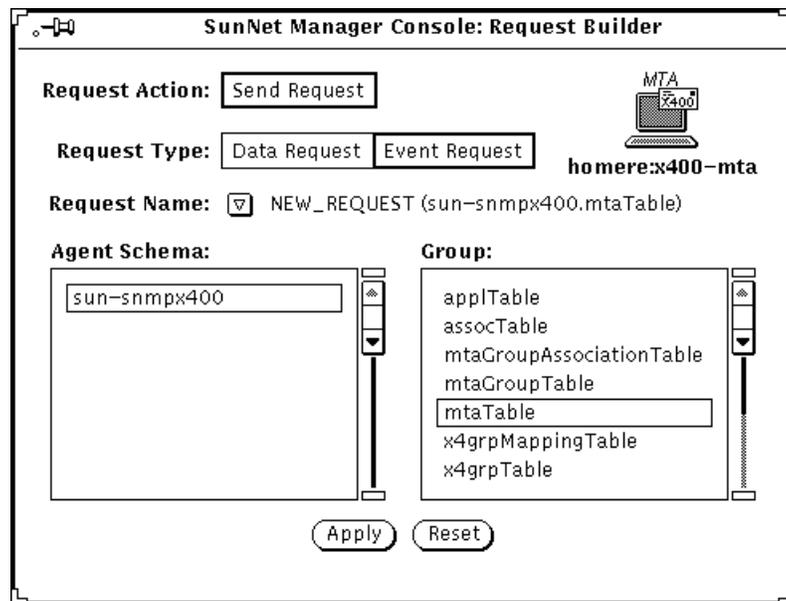


Figure 2-13 Request Builder Window

2. Select the Event Request option.

3. In the Group scrolling list, select mtaTable.

4. Click on Apply.

The SunNet Manager Event Request window is displayed as shown in Figure 2-14 on page 39. The title bar indicates the messaging application from which the request was started and the MIB table used.

The screenshot shows the SunNet Manager Console Event Request window for the request 'MTA transmitted messages'. The window is titled 'SunNet Manager Console: Event Request (homere:x400-mta.sun-snmpx400.mtaTable)'. It contains several fields and controls:

- Name:** MTA transmitted messages
- Proxy System:** localhost
- Interval:** 60 (with up/down arrows)
- Count:** 0 (with up/down arrows)
- Key:** 1
- Restart:**
- Send Once:**
- Defer Reports:**
- On Completion:** Delete Request
- Options:** _____
- Attributes:** (Empty list box)
- Attribute:** mtaTransmittedMessages
- Relation1:** Increased By More Than
- Threshold1:** 600
- Relation2:** Threshold Not Set
- Threshold2:** _____
- Priority:** Medium
- Glyph Effect:** Blink Glyph
- Audio Effect:** None
- Audio File:** _____
- Mail To:** _____
- To Program:** _____

At the bottom, there are buttons for 'Start', 'Hold', 'Reset', 'Apply', 'Reset', and 'Delete'. The status bar at the bottom left shows 'mtaTable' and the bottom right shows 'The number of messages transmitted since M'.

Figure 2-14 SunNet Manager Event Request Window

5. Fill in the Name field for your request, for example “MTA transmitted messages”.

Names are limited to 64 characters maximum.

6. Set a polling interval of 60 (seconds) for the agent in the Interval field so that the agent will poll the application every minute.

If this field contains a zero value, the agent’s default polling interval applies. Events may occur between polling intervals without causing the agent to send an event report.

7. Set the Count field to the number of reports you want to receive.

If this field is set to zero, the agent will send reports indefinitely, whenever the defined event conditions are fulfilled at the time of polling.

- 8. In the Key field, type in 1, which is the key for the Solstice X.400 MTA.**
To find the key for a particular application, look up the Properties for that application. A list of keys for Solstice X.400 applications is provided in “Messaging Management Summary” on page 16.
- 9. Enable the Restart option by checking the checkbox.**
This will restart the request automatically whenever the system reboots, the SunNet Manager console is restarted, or the SMNP agent itself is restarted.
- 10. In the Attribute submenu, select the variable `mtaTransmittedMessages`.**
Before you can add this variable to the Selected Attributes scrolling list, you must define the conditions you want to associate with it.
- 11. In the Relation1 submenu, select the option “Increased by More Than”.**
The relation you select needs to be associated with a threshold before you can apply your choice to the variable you selected in the previous step.
- 12. Type in the Threshold1 field the value you consider to be critical for the selected variable.**
In this example, you want to be warned whenever the number of transmitted messages exceeds 10 per second. Therefore, with a polling interval of 60 seconds, the critical threshold is reached when the number of transmitted messages has increased by more than 600.
- 13. You can change the default options for Priority, Glyph Effect and Audio Effect, specify an audio file to start, a recipient to send mail to, or a program to run when the defined condition occurs.**
- 14. Click on the Apply button.**
The variable name is added to the Attribute scrolling list in the window.
- 15. Click on the Start button to start the Request for the messaging application.**
If you then double-click on the messaging application icon, the request icon is displayed with all other request icons applying to the same application.

Examples of Useful Event Requests

You can apply the method described in “Example of Critical Load for an MTA” on page 37 for any conditions you consider to be critical for your messaging system. If you need information on some of the options or fields in the SunNet Manager Event Request window that are not described in the previous example, refer to the *SunNet Manager Reference Manual*.

Here is a short list of conditions that would, in most organizations, warrant an event report:

- repeated failure in attempting to connect to another messaging application,
- a messaging application is reaching the saturation threshold,
- volume of traffic in Kilobytes is reaching a critical threshold,
- number or volume of queued messages is becoming critical,
- a user’s mailbox is taking up more than a specified volume in Kilobytes,
- a user’s mailbox contains a high percentage of messages older than a specified period of time.

Applying an Event Request to Several Messaging Applications

There are two methods for applying an event request to several messaging applications:

- copying an existing request icon and pasting it over another messaging application
- creating a predefined event request

This section describes how to create a predefined event request. Once created, predefined event requests are available under the icon menu of every messaging application to which they can apply.

Note – Remember to check the Key field in the request when copying and pasting an existing request icon or using a predefined event request. The number in this field must match the key specified in the application’s Properties sheet. A list of keys for Solstice X.400 applications is provided in “Messaging Management Summary” on page 16.

▼ **How to Create a Predefined Event Request for a Messaging Application**

- 1. Make sure no icons are selected in the management console window, pull down the Requests menu, and select Create Predefined.**

The SunNet Manager Request Builder window is displayed. See Figure 2-13 on page 38.

- 2. Select the Request Type Event Request.**

- 3. In the Agent Schema scrolling list, select the appropriate schema. Select `sun-snmpx400` for a messaging application monitored by the Solstice X.400 Server SNMP Agent, or `sun-snmpxapia` for a Solstice Client Toolkit application.**

The Group scrolling list displays the corresponding list of MIB tables and variables.

- 4. Click on the Apply button.**

The SunNet Manager Predefined Event Request Builder window is displayed. This window is similar to the SunNet Manager Event Request window shown in Figure 2-14 on page 39.

- 5. Fill in the fields and select the options that you need to create your request.**

A summary of the most important fields is provided in the example “How to Create an Event Request to Monitor the Load on an MTA” on page 38. For full details, refer to the *SunNet Manager Reference Manual*.

- 6. Click on the Define button.**

Your event request is now available for all messaging applications monitored through the same agent schema. All relevant event requests for an application are accessible from the application’s icon menu, under “Send Predefined”.

Viewing Messaging Events, Traps, and Errors

SunNet Manager offers four different types of reports: alarm reports, event/trap reports, error reports, and an events summary. Alarm reports list incoming events, traps, and errors together. Event/trap reports specifically list events and traps, while error reports list errors alone. The Events Summary provides a list of events and traps by icon.

When an alarm occurs, you are notified by a visual or audible effect, even if the management console is iconified. Refer to “Configuring the Display of Information” on page 47 to find out how you can configure the signals that will advise you of incoming alarm reports.

Note – The management console receives alarms from monitored applications only. Make sure all your messaging applications are represented in the messaging view by running the Messaging Discover Tool regularly.

This section describes how to:

- view alarm reports for all applications represented in the messaging view
- view alarm reports from a messaging application icon
- view alarm reports for a messaging application from the host icon
- acknowledge an alarm
- check that the process responsible for sending traps is running

▼ **How to View Alarm Reports for all Applications Represented in the Messaging View**

- 1. In the messaging view, make sure that all icons are deselected.**
- 2. Pull down the View menu in the management console window and select Alarm Reports.**

An Alarm Reports Summary is displayed, as shown in Figure 2-15 on page 44.

- 3. To read the reports for a particular application, highlight its name in the Device Name list, and click on the Alarms Report button, or double click on the application name.**

Figure 2-16 on page 45 shows an example of an alarm report. The scrolling list at the top displays the list of events, traps and errors for the application. The scrolling pane at the bottom displays text describing the alarm condition.

- 4. Click on an item in the scrolling list and read the description of the alarm in the scrolling pane.**

For more information on the Show View and Find buttons in the Alarm Reports window, refer to the *SunNet Manager User's Guide*.

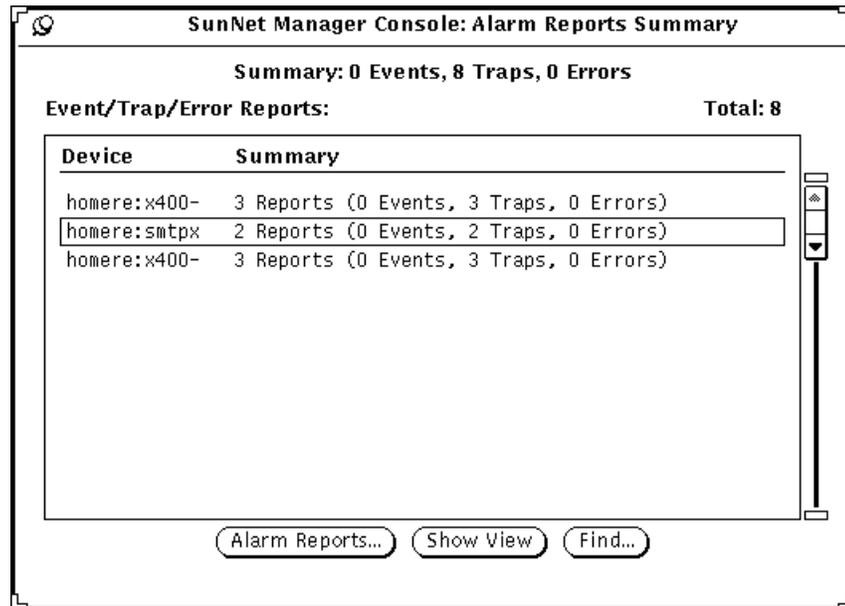


Figure 2-15 An Alarm Reports Summary

▼ **How to View Alarm Reports from a Messaging Application Icon**

1. Pull down the icon menu of a messaging application and select Alarm Reports.

Figure 2-16 on page 45 shows an example of report. The scrolling list at the top displays the list of events, traps and errors for the application. The scrolling pane at the bottom displays text describing the alarm condition.

2. Click on an item in the scrolling list and read the description of the alarm in the scrolling pane.

For more information on the Show View and Find buttons in the Alarm Reports Summary window, refer to the *SunNet Manager User's Guide*.

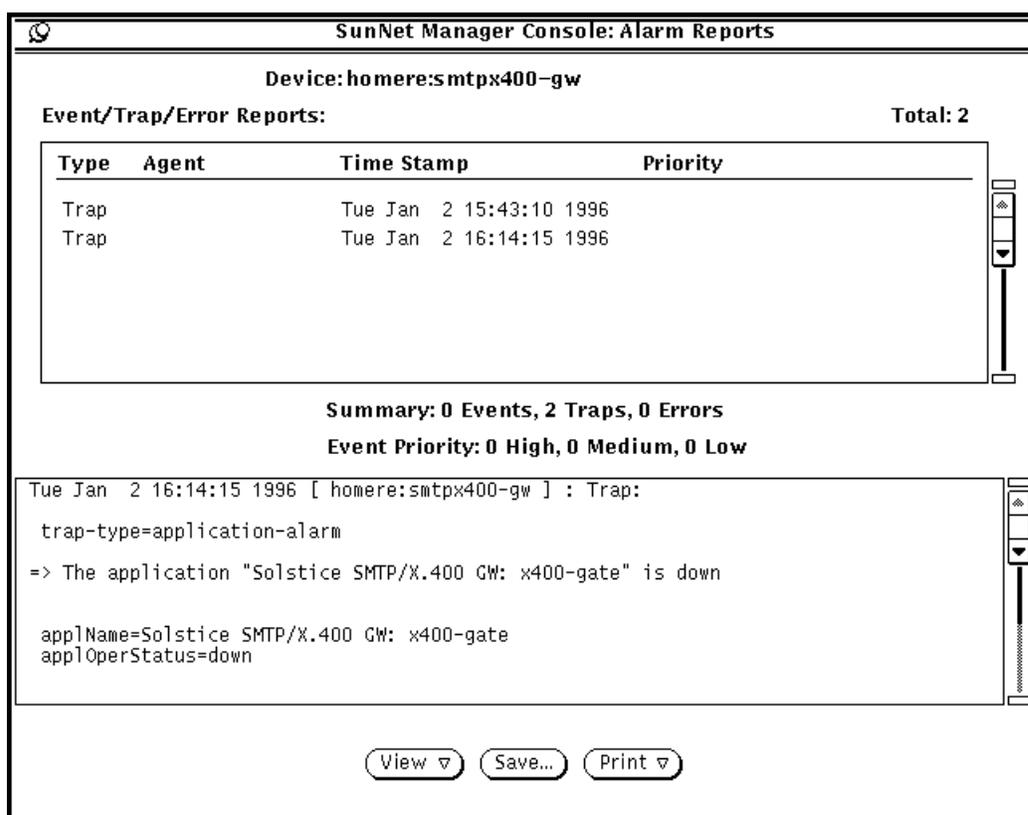


Figure 2-16 An Alarm Report for a Messaging Application

▼ How to View Alarm Reports for a Messaging Application from the Host Icon

You can view alarm reports for a messaging application from the host icon whether the messaging application is represented under the host icon or not.

1. Pull down the icon menu of a host that has monitored messaging applications running on it and select Alarm Reports.

An Alarm Reports Summary is displayed. It contains the list of alarm reports for that host and for all the messaging applications running on it.

2. **To read the reports for a particular application, highlight its name in the Device Name list, and click on the Alarms Report button, or double click on the application name.**

Figure 2-16 on page 45 shows an example of alarm report. The scrolling list at the top displays the list of events, traps and errors for the application. The scrolling pane at the bottom displays text describing the alarm condition.

3. **Click on an item in the scrolling list and read the description of the alarm in the scrolling pane.**

For more information on the Show, Save and Find buttons in the Alarm Reports window, refer to the *SunNet Manager User's Guide*.

▼ How to Acknowledge an Alarm

When you have noted that an alarm has occurred and no longer need to see it on the management console, you can cancel the effect it produced. This can be done in two ways:

- Pull down the icon menu of the application that is in alarm state, and in the Glyph State submenu select Normal. This cancels the visual effect that the alarm had on the application icon and also on the messaging cloud icon above it.
- Pull down the network icon menu, and in the Glyph State submenu, select Normal. This cancels the visual effect of a messaging trap on the network icon and on the application icon below it, if present. When using this method, make sure you are not discarding any alarms you are not aware of.

▼ How to Check that the Process Responsible for Sending Traps to Messaging Icons is Running

1. **In a shell tool, enter the following command:**

```
machine_name% ps -ef | grep msg_mgr_trapd
```

If this process is not running, messaging traps are logged under the host view only.

2. If necessary, restart `msg_mgr_trapd`. As root, enter the following command:

```
machine_name# /etc/init.d/mm_trapd start
```

Configuring the Display of Information

SunNet Manager enables you to apply the same visual and audio effects to messaging application icons as to host machine icons. This section describes the color conventions for messaging icons and the effects a trap or error can trigger.

Color Conventions

The following color conventions apply to messaging application icons:

Green:

The application is managed (it has an SNMP agent that monitors it), *and* you specifically requested it to be discovered when you created the messaging view.

Blue:

The application is not managed, *or* you did not specifically request it to be discovered when you created the messaging view. It is displayed as the neighbor of a managed application.

Effects Produced by Events, Traps, and Errors

You can configure the effect an event, trap or error will trigger from the Props menu in the SunNet Manager Console. In the case of an event, you can also configure the effect it will trigger from the event icon menu.

The effects an event, trap, or error can trigger are:

- blink icon
- dim icon
- color by priority
- ring bell
- play audio file
- send mail to specified recipients

- run a specified program

The color by priority option uses the following defaults:

low priority = yellow
 medium priority = orange
 high priority = red

All traps sent to host icons are displayed as high priority. If you have selected the color by priority option from the Props menu in the SunNet Manager console, the host icons will turn to red on receiving a trap.

Traps sent to messaging icons are classified according to severity and are displayed as follows:

Trap type	Trap Value	Trap Priority	Icon Color
Change in application operating status	up	low	yellow
	restarting	low	yellow
	congested	medium	orange
	down	high	red
Alarm received from monitored application		low, medium, or high	yellow, orange, or red

This section explains how to:

- configure the effect of traps, events and errors from the Props menu
- configure the effect of an event from an event icon

▼ **How to configure the Effect of Traps, Events and Errors from the Props Menu**

1. Select the Props menu in the management console.

This displays a Properties window, as shown in Figure 2-17 on page 49.

2. From the Category menu button, select the Errors category or the Events and Traps category.

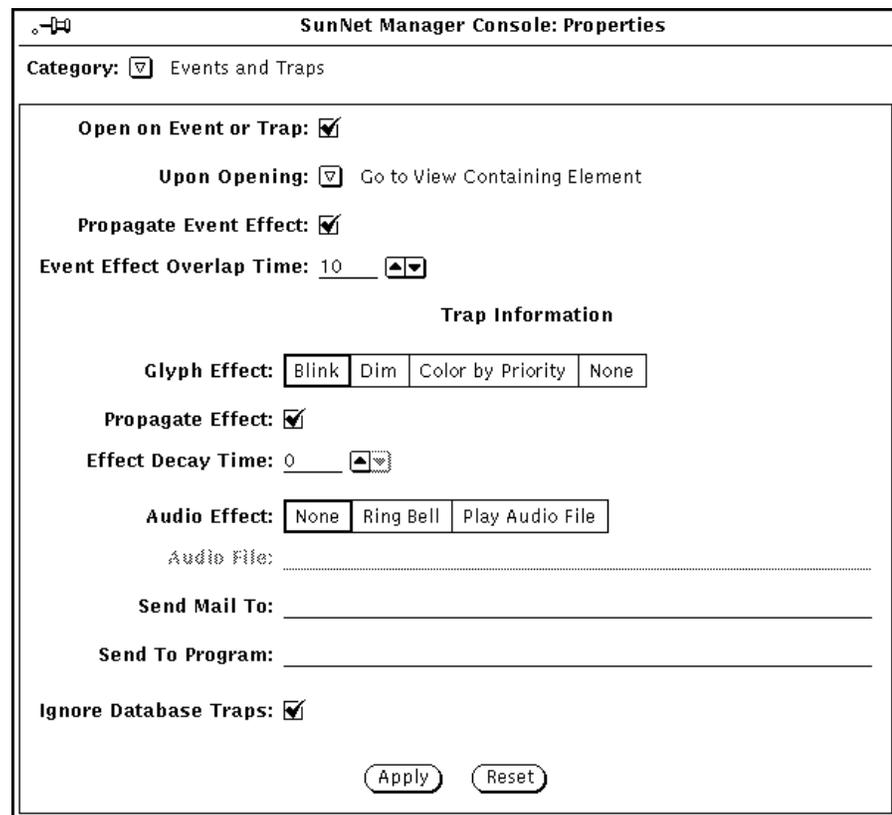
Because events and traps are in the same category, all types of traps and of events will be configured in the same way.

3. Fill in the fields in the Properties window.

For detailed information on the fields and options available, refer to the *SunNet Manager Reference Manual*.

4. Click on Apply.

Your configuration is taken into account and the Properties window is dismissed.



Screenshot of the SunNet Manager Console: Properties window. The window title is "SunNet Manager Console: Properties". It has a "Category:" dropdown set to "Events and Traps". The main area contains several settings:

- Open on Event or Trap:**
- Upon Opening:** Go to View Containing Element
- Propagate Event Effect:**
- Event Effect Overlap Time:** 10
- Trap Information**
- Glyph Effect:**
- Propagate Effect:**
- Effect Decay Time:** 0
- Audio Effect:**
- Audio File:**
- Send Mail To:** _____
- Send To Program:** _____
- Ignore Database Traps:**

At the bottom are and .

Figure 2-17 Properties Window

▼ How to Configure the Effect of an Event from an Event Icon

- 1. Double click on a messaging application icon to reveal the event requests that are running for that messaging application**

2. Pull down the icon menu of a request icon and select Properties.

This displays an event request window such as the one shown in Figure 2-14 on page 39.

3. Modify or fill in the fields that determine the effect produced when an event occurs.

For full details on the fields and options in this window, refer to the *SunNet Manager Reference Manual*.

4. Click on the Apply button to apply your changes.

5. Click on the Restart button to restart the event request.

Solstice X.400 SNMP Agents

3 

This chapter provides detailed information on how the Solstice X.400 SNMP Agents work, the standard MIB variables they support, extensions, traps, and configuration information.

<i>The Solstice X.400 Server Agent</i>	<i>page 51</i>
<i>The Solstice X.400 XAPIA Agent</i>	<i>page 62</i>

The Solstice X.400 Server Agent

This section introduces the Management Information Bases used by the X.400 Server SNMP Agent. This agent monitors the following processes:

Product Component	Process Name
Solstice X.400 MTA (included in Messaging Server product)	osimta
Solstice X.400 Message Store (included in Messaging Server product)	osix400ms
Solstice X.400 Internet Adaptor (an SMTP/X.400 gateway)	osismtpx400

This section also provides installation and configuration information for this agent and examples of data returned.

Management Information Bases

The X.400 Server SNMP Agent supports the messaging management MIBs that are part of the MADMAN standard. It also supports extensions that extend the management facilities the agent can offer.

Standard Management Information Bases

The X.400 Server SNMP Agent conforms to the following MIBs belonging to the MADMAN standard:

- The Network Services Monitoring MIB (RFC 1565) that applies to all messaging and directory applications.
- The Mail Monitoring MIB (RFC 1566) that applies to message transfer agents and gateways.

The Network Services Monitoring MIB is composed of two sets of related objects that are organized in tables: an application table (`applTable`) and an association table (`assocTable`).

The Mail Monitoring MIB is composed of three sets of related objects that are organized in tables: an MTA table (`mtaTable`), an MTA group table (`mtaGroupTable`) and an MTA group association table (`mtaGroupAssociationTable`).

The X.400 Server SNMP Agent returns the values of the objects (also called *variables*) defined in these MIBs upon request from a management station.

Extensions

The X.400 Server SNMP Agent supports the following extensions to the standard:

- A MIB for message stores, that enables a management platform to obtain statistics for the message store globally, and for each message store user.
- Support for unsolicited event reports or SNMP *traps*. When the X.400 SNMP Agent detects an abnormal condition, it sends out an unsolicited event report (called an SNMP *trap*) without waiting to receive a specific request from the management station. SNMP traps can be divided into two categories:
 - changes in the operating status of monitored applications.

- alarms generated by monitored applications

The possible values for the operating status of the Solstice X.400 MTA are: *up*, *down*, *congested*, *restarting*.

The possible values for the operating status of the Solstice X.400 Message Store are: *up*, *down*, *restarting*.

The possible values for the operating status of the Solstice X.400 Internet Adaptor (SMTP/X.400 gateway) are: *up*, *down*, *restarting*.

Alarms generated by monitored applications are diverse. Here are a few typical examples:

- Failure to connect to another MTA or gateway
- Failure to deliver or to redirect a message
- Message looping
- Failure in message handling

Traps caused by an alarm generated by a monitored application contain:

- the application name (`applName`)
- an alarm identification number (`alarmId`), which is always *-1*
- an alarm severity level (`alarmSeverity`), which can be *low*, *medium*, or *high*
- a description of the cause of the alarm (`alarmDescr`)

For an ASN.1 description of the message store and trap variables, refer to the following files:

```
/var/opt/SUNWconn/OSIROOT/mib/root.mib
```

This file gives the location of the variables in the global MIB tree.

```
/var/opt/SUNWconn/OSIROOT/mib/x4ms.mib
```

This file gives the ASN.1 definitions of the message store variables.

```
/var/opt/SUNWconn/OSIROOT/mib/x4grp.mib
```

This file gives the ASN.1 definitions of the message store user group variables

```
/var/opt/SUNWconn/OSIROOT/mib/alarm.mib
```

This file gives the ASN.1 definitions of the alarm variables.

Figure 3-1 shows an example of trap report caused by a change in the operating status of an SMTP/X.400 gateway.

```

Mon Nov 13 13:44:07 1995 [ homere ] : Trap:

sequence=29517
receive-time=Mon Nov 13 13:44:05 1995
version=0
community=SNMP-trap
enterprise=Sun
Microsystems.products.messaging.agents.snmpx400d.1
source-time=122:00:14.33
trap-type=application-alarm

KEY=2
applName=Solstice SMTP/X.400 GW: x400-gate
applOperStatus=down

```

Figure 3-1 Trap Report Caused by a Change in Operating Status

Examples of Data Reports and Traps

This section explains how to obtain simple data reports for X.400 MTAs and message stores and shows examples of these data reports.

▼ How to Obtain a Simple Data Report for an X.400 MTA or Message Store

- ◆ **Pull down the icon menu of the X.400 MTA or message store for which you want information, move the cursor over the Quick Dump submenu to highlight the sun-snmpx400 schema, and, in the sun-snmpx400 submenu, select the MIB table you want.**

For an X.400 MTA, you can select the following MIB tables:

- applTable
- assocTable
- mtaTable
- mtaGroupTable
- mtaGroupAssociationTable

See Figure 3-2 on page 56 for an example of the `applTable` MIB table and Figure 3-3 on page 57 for an example of the `assocTable` MIB table.

For an X.400 Message Store, you can select the following MIB tables:

- `x4grpTable`
- `x4grpMappingTable`
- `x4msMtaTable`
- `x4msUserTablePart1`
- `x4msUserTablePart2`
- `x4msUserAssociationTable`

See Figure 3-4 on page 57 for an example of the `x4grpTable` MIB table, and Figure 3-5 on page 58 for an example of the `x4msUserTablePart1` MIB table.

Figure 3-2 on page 56 shows the result of a request for the variables contained in the application table (`applTable`). This example is the result of a SunNet Manager “quick dump”.

```

KEY=1
applName=Solstice X.400 MTA: mta-cloud
applDirectoryName=
applVersion=V9.0
applUptime=71:02:58.46
applOperStatus=up
applLastChange=356:57:38.01
applInboundAssociations=0
applOutboundAssociations=0
applAccumulatedInboundAssociations=0
applAccumulatedOutboundAssociations=0
applLastInboundActivity=00:00:00.00
applLastOutboundActivity=00:00:00.00
applRejectedInboundAssociations=0
applFailedOutboundAssociations=0

KEY=2
applName=Solstice SMTP/X.400 GW: gw-cloud
applDirectoryName=
applVersion=(9.0)
applUptime=71:03:33.72
applOperStatus=up
applLastChange=71:03:36.72
applInboundAssociations=0
applOutboundAssociations=0
applAccumulatedInboundAssociations=0
applAccumulatedOutboundAssociations=1
applLastInboundActivity=00:00:00.00
applLastOutboundActivity=71:03:34.72
applRejectedInboundAssociations=0
applFailedOutboundAssociations=0

```

Figure 3-2 Application Table Variables

In the standard description of the application table `applTable`, each row corresponds to one application, identified by a key number, and each column corresponds to one of the variables listed in Figure 3-2 on page 56. In this figure, it is presented as a list so that it is readable.

Figure 3-3 shows the result of a request for the variables contained in the associations table (`assocTable`). This example is the result of a SunNet Manager “quick dump”.

```
KEY=1.1
assocRemoteApplication=Solstice X.400 Gateway
assocApplicationProtocol=2.6.0.1.6
assocApplicationType=peer-initiator
assocDuration=71:03:34.37

KEY=2.1
assocRemoteApplication=Solstice X.400 MTA
assocApplicationProtocol=2.6.0.1.6
assocApplicationType=peer-responder
assocDuration=71:03:34.37
```

Figure 3-3 Association Table Variables

In this example, Key 1.1 represents the first association on the application identified by Key=1 (the X.400 MTA, see Figure 3-2); Key 2.1 represents the first association, or connection, on the application identified by Key=2 (the X.400 gateway, see Figure 3-2).

For a full description of the contents of each table and of the meaning of each individual object, refer to the appropriate RFC (see “Standard Management Information Bases” on page 52).

Figure 3-4 shows the result of a request for the variables contained in the message store user group table (`x4grpTable`). This example is the result of a SunNet Manager “quick dump”.

```
KEY x4grpName

1 good-guys
2 bad-guys
3 remote-ms-group
4 remote-mta-grp
```

Figure 3-4 Message Store User Group Table

The message store user group table provides a list of the user groups of the message store.

Figure 3-5 on page 58 shows the result of a request for the variables contained in Part 1 of the Message Store User table (x4msUserTablePart1). This example is the result of a SunNet Manager “quick dump”.

```
KEY=1
x4msUserTotalMessages=0
x4msUserTotalVolume=0
x4msUserP3Associations=0
x4msUserP7Associations=0
x4msUserLastP7Association=0
x4msUserAuthenticationFailures=0
x4msUserAuthenticationFailureReason=
x4msUserName=chuck

KEY=2
x4msUserTotalMessages=0
x4msUserTotalVolume=0
x4msUserP3Associations=0
x4msUserP7Associations=0
x4msUserLastP7Association=0
x4msUserAuthenticationFailures=0
x4msUserAuthenticationFailureReason=
x4msUserName=linus

KEY=3
x4msUserTotalMessages=0
x4msUserTotalVolume=0
x4msUserP3Associations=0
x4msUserP7Associations=0
x4msUserLastP7Association=0
x4msUserAuthenticationFailures=0
x4msUserAuthenticationFailureReason=
x4msUserName=snoopy
```

Figure 3-5 Message Store User Table

The message store user table provides a list of all users of the message store.

Installing the Solstice X.400 Server SNMP Agent

You can install the Solstice X.400 Server SNMP Agent during the installation process for the X.400 Messaging Server. You can also install this agent at any time.

▼ How to Install the Solstice X.400 Server SNMP Agent

1. Log in as root or become superuser.

2. Enter the following commands:

```
# cd /opt/SUNWconn/sbin
# ./snmpx4_genconf install
```

These commands execute a script that installs and starts the X.400 Server SNMP Agent and the SNMP Relay. This script will find a free UDP port on which to start the X.400 Server SNMP Agent. It also creates the configuration files for the X.400 Server SNMP Agent and for the SNMP Relay.

In addition, these commands install `rc` scripts that will stop and start the SNMP Agent automatically when the system is rebooted.

3. To declare the management station that the X.400 Server SNMP Agent will report to, enter the following command:

```
# ./snmpx4_genconf configure
```

This command runs a script that updates the configuration file for the X.400 Server SNMP Agent, `snmpx400d.conf`. You will be prompted for the hostnames of the machines you will use as management stations for your messaging system.

Once you have completed the installation procedure the agent is ready to work using a standard configuration. You can customize this configuration to restrict access to certain users. This is done by manually modifying the agent's configuration file. Refer to "SNMP Server Agent Configuration" on page 60 for instructions.

SNMP Server Agent Configuration

The configuration file for the Solstice X.400 Server SNMP Agent, `snmpx400d.conf`, is divided into two sections under the following headings:

- access control
- trap parameters

This section describes the information under each heading and how you can modify it to suit the needs of your messaging system.

The default pathname for the X.400 Server SNMP Agent configuration file is `/var/opt/SUNWconn/OSIROOT/conf/snmpx400d.conf`.

Access Control

Access control information contains community names used to identify users who can have read or write access to the MIB variables supported by the Solstice X.400 Server SNMP Agent.

The default community name for read access is *public*. This provides no access control. If you wish to restrict the possibility to query the X.400 Server SNMP Agent to a small group of people, change the community name and communicate it to authorized users only. When initiating a query, these users must specify the community name in the SunNet Manager Properties window.

Trap Parameters

All alarms reported by the X.400 Server SNMP Agent contain the community name *SNMP-trap*. You can use this parameter to filter the incoming traps on the management station.

The trap parameters section also contains a list of *trap recipients*. This list contains the hostnames of machines you specified at installation time and to which traps will be sent.

▼ How to Modify the X.400 Server SNMP Agent Configuration File

Method 1:

- 1. Log in as root or become superuser.**

2. Enter the following command:

```
# /opt/SUNWconn/sbin/snmpx4_genconf configure
```

This command runs a script that updates the configuration file for the X.400 Server SNMP Agent, `snmpx400d.conf`. You will be prompted for hostnames of machines you will use as management stations for your messaging system. These machines will receive traps from the SNMP agent.

Method 2:**1. Log in as root or become superuser.****2. Open the file `snmpx400d.conf` using a text editor. For example:**

```
# vi /var/SUNWconn/OSIROOT/conf/snmpx400d.conf
```

You can then modify the configuration information to suit your particular needs.

3. Reload the SNMP Agent configuration. To do this:**a. Find out the process ID for the SNMP Agent daemon by using the following command:**

```
# ps -ef | grep snmpx400d
```

b. Enter the following command to reload the SNMP Agent configuration:

```
# kill -1 processId
```

Where *processId* is the ID of the `snmpx400d` process.

When the X.400 Server SNMP Agent configuration is reloaded, your changes are applied.

Configuration File for SNMP Relay

The SNMP Relay configuration file describing the X.400 Server SNMP Agent is the file `snmpx400d.snmprelay`. Its pathname is `/etc/SUNWconn/snmprelay/snmpx400d.snmprelay`. For more information, refer to Appendix A, “SNMP Relay Configuration”.

The Solstice X.400 XAPIA Agent

This section introduces the Management Information Bases used by the Solstice X.400 XAPIA SNMP Agent. This agent manages the Solstice X.400 Client Toolkit by monitoring the `osixapia` process. This process enables User Agents to make remote connections to message stores and MTAs.

This section also provides installation and configuration information for this agent and examples of data returned.

Management Information Bases

The X.400 XAPIA SNMP Agent supports a subset of the MADMAN variables. It also supports extensions that enable trap reporting.

Standard Management Information Bases

The X.400 XAPIA SNMP Agent supports the following variables belonging to the application table (`applTable`) defined in the Network Services Monitoring MIB (RFC 1565):

- `applName`
- `applVersion`
- `applUpTime`
- `applOperStatus`

All other standard objects in the application table return a zero value. Instructions on how to obtain information from supported variables are provided in “Examples of Data Reports and Traps” on page 54.

Extensions

The X.400 XAPIA Agent provides support for the following two categories of SNMP traps:

- changes in the operating status of the monitored application (possible values: *up*, *down*, *restarting*)
- alarms generated by the monitored application

Traps caused by an alarm generated by a monitored application contain:

- the application name (`applName`)
- an alarm identification number (`alarmId`), which is always *-1*
- an alarm severity level (`alarmSeverity`), which can be *low*, *medium*, or *high*
- a description of the cause of the alarm (`alarmDescr`)

Examples of Data Reports and Traps

This section explains how to obtain a simple data report for an X.400 XAPIA Client and provides an example of a data report.

▼ How to Obtain a Simple Data Report for an X.400 XAPIA Client

- ◆ **Pull down the icon menu of the X.400 XAPIA Client application for which you want information, move the cursor over the Quick Dump submenu to highlight the `sun-snmpxapia` MIB, and in the `sun-snmpxapia` submenu, select `applTable`.**

A list similar to the one shown in Figure 3-6 on page 64 is displayed.

Figure 3-6 shows the result of a request for the variables contained in the application table (`applTable`). Variables not supported by the X.400 XAPIA Agent are displayed with a zero value. This example is the result of a SunNet Manager “quick dump”.

```
Fri Nov 3 16:48:41 1995 [ legend:sun-x400xapia ] : Quick Dump:
sun-snmpxapia.applTable

KEY=4
applName=Solstice X.400 Client Toolkit
applDirectoryName=
applVersion=V8.1.15
applUptime=00:00:50.80
applOperStatus=up
applLastChange=00:00:00.00
applInboundAssociations=0
applOutboundAssociations=0
applAccumulatedInboundAssociations=0
applAccumulatedOutboundAssociations=0
applLastInboundActivity=00:00:00.00
applLastOutboundActivity=00:00:00.00
applRejectedInboundAssociations=0
applFailedOutboundAssociations=0
```

Figure 3-6 Application Table Variables

In the standard description of the application table `applTable`, each row corresponds to one application, identified by a key number, and each column corresponds to one of the variables listed above. In the example above, it is presented as a list so that it is readable.

Installing the Solstice X.400 XAPIA SNMP Agent

You can install the Solstice X.400 XAPIA SNMP Agent during the installation process for the X.400 Messaging Server. You can also install this agent at any time.

▼ How to Install the Solstice X.400 XAPIA SNMP Agent

1. Log in as root or become superuser.

2. Enter the following command:

```
# cd /opt/SUNWconn/sbin
# ./snmpxa_genconf install
```

This command executes a script that installs and starts the XAPIA SNMP Agent and the SNMP Relay. This script will find a free UDP port on which to start the X.400 XAPIA SNMP Agent. It also creates the configuration files for the X.400 XAPIA SNMP Agent and for the SNMP Relay.

In addition, these commands install `rc` scripts that will stop and start the SNMP Agent automatically when the system is rebooted.

3. To declare the management station that the XAPIA SNMP Agent will report to, enter the following command:

```
# ./snmpxa_genconf configure
```

This command runs a script that updates the configuration file for the XAPIA SNMP Agent, `snmpxapiad.conf`. You will be prompted for the hostnames of the machines you will use as management stations for your messaging system.

Once you have completed the installation procedure, the agent is ready to work using a standard configuration. You can customize this configuration to restrict access to certain users. This is done by manually modifying the agent's configuration file. Refer to "X.400 XAPIA SNMP Agent Configuration" on page 66 for instructions.

X.400 XAPIA SNMP Agent Configuration

The configuration file for the Solstice X.400 XAPIA SNMP Agent, `snmpxapiad.conf`, is divided into two sections with the same headings and information content as the Solstice X.400 Server SNMP Agent configuration file described on page 60.

The default pathname for the X.400 XAPIA SNMP Agent configuration file is `/var/SUNWconn/OSIROOT/conf/snmpxapiad.conf`.

▼ How to Modify the X.400 XAPIA SNMP Agent Configuration File

Method 1:

- 1. Log in as root or become superuser.**
- 2. Enter the following command:**

```
# /opt/SUNWconn/sbin/snmpxa_genconf configure
```

This command runs a script that updates the configuration file for the X.400 XAPIA SNMP Agent, `snmpxapiad.conf`. You will be prompted for hostnames of machines you will use as management stations for your messaging system. These machines will receive traps from the SNMP agent.

Method 2:

- 1. Log in as root or become superuser.**
- 2. Open the file `snmpxapiad.conf` using a text editor. For example:**

```
# vi /var/SUNWconn/OSIROOT/conf/snmpxapiad.conf
```

You can then modify the configuration information to suit your particular needs.

- 3. Reload the SNMP Agent configuration.**

- a. Find out the process ID for the SNMP Agent daemon using the following command:

```
# ps -ef | grep snmpxiad
```

- b. Enter the following command to reload the SNMP Agent configuration:

```
# kill -1 processId
```

Where *processId* is the ID of the `snmpxiad` process.

When the X.400 XAPIA SNMP Agent configuration is reloaded, your changes are applied.

Configuration File for SNMP Relay

The SNMP Relay configuration file describing the X.400 XAPIA SNMP Agent is the file `snmpxiad.snmprelay`. Its pathname is `/etc/SUNWconn/snmprelay/snmpxiad.snmprelay`. For more information, refer to Appendix A, “SNMP Relay Configuration”.

SNMP Relay Configuration



This Appendix introduces the SNMP Relay configuration directory, explains why you may need to modify it, and how to do so.

<i>Introducing the SNMP Relay Configuration</i>	<i>page 69</i>
<i>Modifying the SNMP Relay Configuration</i>	<i>page 71</i>

Introducing the SNMP Relay Configuration

The SNMP Relay gets its configuration information from a configuration directory (`/etc/SUNWconn/snmprelay`) that contains a configuration file for every SNMP agent installed on the same machine as the SNMP Relay.

All configuration files for the SNMP Relay are divided into two sections under the following headings:

- macros
- agents

This section describes the information content under each heading.

Note - The SNMP Relay configuration file describing an SNMP agent and the SNMP agent's own configuration file are two distinct files.

Macros

The SNMP agent needs the complete OIDs for the information objects it supports. The *macros* section lists the conventions used to name specific parts of the global MIB. This makes it easier to define a supported information object because instead of specifying the complete OID for an object, you can use one or more macros.

For example, in the SNMP Relay configuration file for the X.400 Server SNMP Agent, the macros section contains a definition for *application* and for *applTable*:

```
application = mib-2.27
applTable = application.1
```

The definition of `applTable` is based on the definition of `application`.

Note – The global information base model is introduced in “Management Information Bases (MIBs)” on page 10. It is fully defined in RFC 1155 *Structure and Identification of Management Information for TCP/IP Based Networks*, also known as *SMI*.

The macros section does not contain definitions of the MIB objects `mib-2`, `enterprise`, and `sun` because these are predefined in the code.

Agents

The *agent* section indicates:

- the name of the agent daemon (`snmpx400d` for the Solstice X.400 Server SNMP Agent, `snmpxapiad` for the Solstice X.400 XAPIA SNMP Agent);
- a list of supported subtrees, using the macro definitions given in the macros section;
- optionally, a list of MIB tables, based on the macro definitions given in the macros section;
- a time-out in micro-seconds;
- the UDP port number where the SNMP agent resides.

Modifying the SNMP Relay Configuration

There are three reasons for which you may want to modify the SNMP Relay's default configuration:

- To change an agent's UDP port number if, during the installation of the agent, you discover that another process already resides on the UDP port assigned by default to that agent. This involves modifying an existing configuration file.
- To add third-party agents compliant with SNMP. (The configuration files for Sun agents are automatically added to the Relay's configuration directory during the installation procedure). This involves creating a new configuration file.
- To change the default options for the SNMP Relay's configuration directory, log file, trace level, and port number. This involves stopping and restarting the SNMP Relay with the command-line options.

This section provides detailed instructions on how to:

- assign a different port number to an agent,
- add a configuration file for an SNMP agent manually,
- stop and restart the SNMP Relay.

▼ To Assign a Different Port Number to an Agent

1. As root, open the configuration file for that agent using a text editor:

```
# vi /etc/SUNWconn/snmprelay/snmpagent.snmprelay
```

where *snmpagent.snmprelay* is the name of the SNMP agent.

2. Change the UDP port number to any number except the reserved UDP port numbers and those already assigned.

UDP port numbers up to 1024 are reserved.

3. Save your changes.

4. Reload the SNMP Relay's configuration.

To do this:

- a. Find out the process ID for the SNMP Relay daemon using the following command:

```
# ps -ef | grep snmprelayd
```

- b. Enter the following command to reload the SNMP Relay configuration without restarting the SNMP Relay:

```
# kill -1 processId
```

Where *processId* is the ID of the `snmprelayd` process.

If you check the log file (`/var/SUNWconn/snmprelay/snmprelay.log`), you will see that the last logged message for the SNMP Relay is: "re-reading its configuration directory `<directory-name>` ... configuration re-read."

Note - Remember to modify the port number in the `rc` script that automatically stops and starts the agent when the machine is rebooted. The default location for this script is `/etc/init.d`.

▼ To Add a Configuration File for an SNMP Agent Manually

1. Create a new file in the directory `/etc/SUNWconn/snmprelay` with the `.snmprelay` extension:

```
# vi /etc/SUNWconn/snmprelay/snmpagent.snmprelay
```

Use the template `/etc/SUNWconn/snmprelay/snmprelayd.template` to define the new SNMP agent.

2. Save your changes.

3. Reload the SNMP Relay's configuration.

To do this:

- a. Find out the process ID for the SNMP Relay daemon using the following command:

```
# ps -ef | grep snmprelayd
```

- b. Enter the following command to reload the SNMP Relay configuration without restarting the SNMP Relay.

```
# kill -1 processId
```

Where *processId* is the ID of the `snmprelayd` process.

If you check the log file (`/var/SUNWconn/snmprelay/snmprelay.log`), you will see that the last logged message for the SNMP Relay is: "re-reading its configuration directory `<directory-name>` ... configuration re-read."

▼ Stopping and Restarting the SNMP Relay

1. To stop the SNMP Relay, as root, enter the following command:

```
# kill -2 processId
```

2. To restart the SNMP Relay, as root, use the following command syntax:

```
# /usr/sbin/snmprelayd [-p port] [-c config-directory] [-l log-file] [-T trace-level]
```

For a description of the options, type `/usr/sbin/snmprelayd -h` or refer to the SNMP Relay man page, `snmprelayd(8)`.

Entering the `snmprelayd` command with no options starts the SNMP Relay with the default settings.

≡ A

Index

A

- agents, 9
- alarms, xv, 12
 - acknowledging, 46
 - configuring effects, 48
 - definition, xv
 - effects, 47
 - viewing, 42
- application key, xvi, 16
- architecture, 1, 15

C

- color conventions, 47
- community name, 60
- configuration tools, 7
 - ositool, 8
 - x400tool, 7
 - xapiatool, 8
- configuring
 - SNMP Relay, 71
 - X.400 Server SNMP Agent, 60
 - X.400 XAPIA SNMP Agent, 66
- console, 3

D

- database

- management, 8
- runtime, 9
- Discover tool, 6, 21
 - running, 21
 - updating messaging views, 25

E

- errors, xv
 - configuring effects, 48
 - definition, xv
- event request, 37
 - copying, 38, 41
 - creating, 37
 - creating a predefined request, 42
 - example of monitoring MTA load, 38
- events, xv, 37
 - configuring effects, 48, 49
 - definition, xv
 - effects, 47
- extensions, 12, 13

G

- Graphs tool, 6, 32
 - changing graph name in title bar, 35
 - creating a graph, 34
 - merging graphs, 36
 - viewing a predefined graph, 33

I

- icons, 16
- installing
 - X.400 Server SNMP Agent, 59
 - X.400 XAPIA SNMP Agent, 65

K

- key, xvi, 16

M

- MADMAN standard, 9
- management console, 3
- management database, 8
- Management Information Base, *see* MIB
- messaging icons, 16
- messaging management
 - agents, 9
 - architecture, 1, 15
 - components, 1
- Messaging Manager, 3, 5
 - Discover tool, 6
 - Graphs tool, 6
 - starting, 19
 - Statistics tools, 6
- messaging view, 4
 - creating, 21
 - updating, 25
- MIB, 10
 - extensions, 12, 13
 - Mail Monitoring MIB, 11
 - message store, 53
 - Network Services Monitoring MIB, 11
 - variables, *see* variables

O

- object identifier (OID), 10
- OID, 10
- osimta, 51
- osismtpx400, 51
- ositool, 8

osix400ms, 51

R

- runtime database, 9
 - loading, 20
 - saving, 20

S

- SNMP agents, 9
- SNMP protocol, 14
- SNMP Relay, 14
 - adding a configuration file for an agent, 72
 - assigning a different UDP port, 71
 - configuration directory, 69
 - configuring, 71
 - stopping and restarting, 73
- SNMP traps, 12
 - categories, 13
 - structure, 12
- starting the Messaging Manager, 19
- Statistics tools, 6, 25
 - group statistics, 27
 - obtaining statistics on a gateway, 26
 - obtaining statistics on a message store, 29
 - obtaining statistics on an MTA, 26
 - resetting an MTA's statistics, 32
 - updating statistics, 31

T

- traps, xv, 12
 - configuring effects, 48
 - definition, xv
 - effects, 47

U

- UDP port, 14, 71

V

variables

- application table, 55, 63
- association table, 57
- message store user group table, 57
- message store user table, 58

viewing

- messaging events, traps, errors, 42

X

X.400 Server SNMP Agent, 51

- access control, 60
- configuring, 60
- data reports, 54
- installing, 59
- SNMP Relay configuration file, 62
- supported MIBs, 52

X.400 XAPIA SNMP Agent, 62

- configuring, 66
- data report, 63
- installing, 65
- SNMP Relay configuration file, 67
- supported MIBs, 62

x400tool, 7

xapiatool, 8

