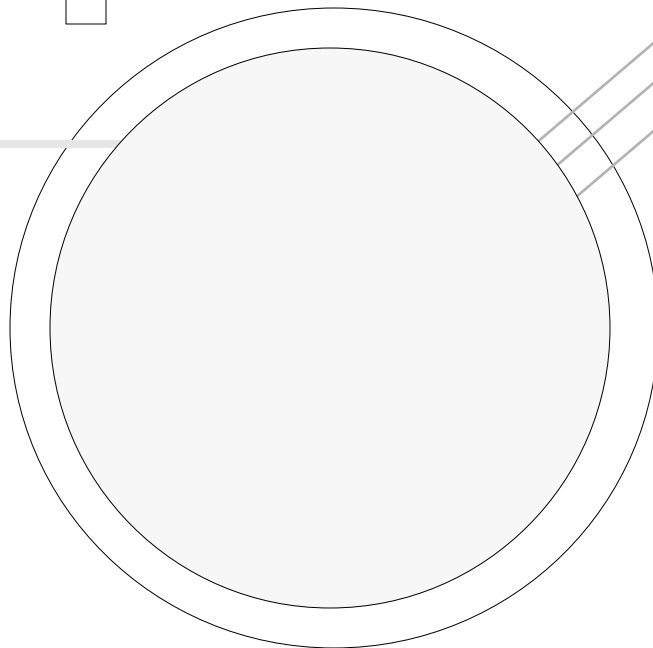


SunNet Manager™ 2.2.3

User's Guide



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

Part No: 802-4521-10
Revision A of October 1995



A Sun Microsystems, Inc. Business

© 1995 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 Systems 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, and Solaris, SunSoft, the SunSoft logo, SunOS, OpenWindows, DeskSet, ONC, SNM, and NFS are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and 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 GUI's 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 EXPRESS 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 PROGRAMS(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.



Contents

Preface	xix
1. Overview and Concepts.	1-1
1.1 Management Applications and Agents	1-1
1.2 SunNet Manager Console	1-4
1.3 Management Database.	1-5
1.4 Configuration	1-7
2. Network Management with SunNet Manager	2-1
2.1 Planning for Network Management	2-1
2.2 Using the Console	2-12
2.2.1 Using Event Requests to Monitor Critical Nodes	2-12
2.2.2 Using Data Requests to Monitor Performance	2-22
2.2.3 Monitoring Network Traffic Load.	2-34
2.3 Using Monitor to Update the Management Database	2-36
3. Creating and Modifying the Management Database	3-1
3.1 Adding SunNet Manager to the Your PATH Variable	3-2

3.2	Starting the Console.....	3-3
3.2.1	Startup Commands.....	3-3
3.2.2	Quick Start Window.....	3-6
3.2.3	Notes on the Console Window.....	3-8
3.3	Letting the Discover Tool Build Your Database.....	3-9
3.3.1	Notes.....	3-12
3.4	Traversing the View Hierarchy.....	3-14
3.4.1	Notes.....	3-15
3.5	Creating Elements.....	3-15
3.5.1	Notes.....	3-21
3.6	Creating Aliases.....	3-22
3.7	Finding Elements.....	3-25
3.7.1	Notes.....	3-26
3.8	Modifying Element Properties.....	3-26
3.9	Changing Element Types.....	3-28
3.9.1	Notes.....	3-30
3.10	Moving Elements.....	3-30
3.10.1	Moving Elements within a View.....	3-30
3.11	Moving Elements from One View to Another.....	3-31
3.11.1	Notes.....	3-31
3.12	Connecting Elements.....	3-32
3.12.1	Notes.....	3-33
3.13	Copying Elements.....	3-34
3.13.1	Notes.....	3-35

3.14	Deleting Elements	3-35
3.14.1	Notes.....	3-36
3.15	Saving the Management Database.....	3-36
3.15.1	Notes.....	3-37
3.16	Quitting the Console	3-38
3.16.1	Notes.....	3-38
4.	Requesting Data from Agents	4-1
4.1	Making a One-Time Request for Data.....	4-2
4.1.1	Quick Dump via the Console Requests Menu.....	4-2
4.1.2	Quick Dump via the Glyph Menu	4-4
4.1.3	Notes.....	4-6
4.2	Requesting Periodic Data	4-6
4.2.1	Sending a Data Request via the Console Requests Menu	4-7
4.2.2	Sending a Data Request via the Glyph Menu	4-10
4.2.3	Sending a Predefined Data Request via the Glyph Menu.....	4-10
4.2.4	Notes.....	4-12
4.3	Copying Requests.....	4-13
4.3.1	Notes.....	4-13
4.4	Viewing Incoming Data.....	4-14
4.4.1	Viewing Incoming Data for All Systems: Data Reports Window	4-14
4.4.2	Notes.....	4-17
4.4.3	Viewing Incoming Data: Grapher.....	4-17

4.4.4	Notes.....	4-18
4.4.5	Viewing Incoming Data: Strip Charts and Indicators 4-19	
4.4.6	Notes.....	4-21
4.5	Analyzing Stored Data.....	4-22
4.5.1	Analyzing Stored Data: Results Browser.....	4-22
4.5.2	Analyzing Stored Data: Results Grapher.....	4-30
4.6	Modifying the Display of a Graph.....	4-31
4.7	Printing a Graph.....	4-33
4.7.1	Notes.....	4-34
5.	Specifying Events.....	5-1
5.1	Specifying an Event.....	5-2
5.1.1	Sending an Event Request via the Console Requests Menu.....	5-2
5.1.2	Sending an Event Request via the Glyph Menu...	5-6
5.1.3	Sending a Predefined Event Request via the Glyph Menu.....	5-6
5.1.4	Notes.....	5-8
5.2	Detecting the Presence of an Event.....	5-9
5.3	Checking the Cause of an Event.....	5-10
5.3.1	Notes.....	5-12
5.4	Changing the State of a Glyph.....	5-12
5.4.1	Notes.....	5-13
5.5	Changing the Propagation of Glyph State Changes.....	5-14
6.	Viewing and Managing Requests.....	6-1

6.1	Viewing the Status of Requests	6-1
6.1.1	Notes	6-3
6.2	Viewing and Modifying Properties of a Request	6-3
6.2.1	Notes	6-5
6.3	Stopping or Killing Requests	6-6
7.	Viewing Reports	7-1
7.1	Viewing Alarm Reports	7-1
7.1.1	Finding a Device	7-3
7.1.2	Switching Views	7-4
7.1.3	Obtaining Device-specific Alarm Reports	7-5
7.1.4	Features of Device-specific Alarm Reports Window	7-7
7.2	Viewing Error Messages and Error Reports	7-7
7.2.1	Notes	7-10
7.3	Viewing Traps	7-10
7.3.1	Notes	7-12
8.	Managing Printers	8-1
9.	Managing SNMP Devices	9-1
9.1	Adding SNMP Devices	9-2
9.1.1	Notes	9-3
9.2	Creating an SNMP Element in the Database	9-5
9.2.1	Notes	9-9
9.3	Setting Up SNM to Receive Traps from a Device	9-10
9.3.1	Notes	9-11
9.4	Using the Set Tool to Retrieve SNMP Attribute Values	9-12

9.4.1	Notes.....	9-15
9.5	Using the Set Tool to Change SNMP Attribute Values .	9-17
9.5.1	Notes.....	9-18
10.	How to Create and Manage a Link.....	10-1
10.1	Using the Console's Edit Function.....	10-1
10.2	Using Discover to Create Manageable Links	10-10
11.	Customizing SunNet Manager.....	11-1
11.1	Adding Background Image to Current View.....	11-1
11.1.1	Notes.....	11-6
11.2	Creating Types of Elements	11-7
11.2.1	Notes.....	11-9
11.3	Creating a New Glyph for an Element Type	11-10
11.3.1	Notes.....	11-11
11.4	Modifying the Console Tools Menu	11-11
11.5	Modifying the Tools Menu for an Element Type	11-12
11.6	Adding Agents and Glyphs	11-13
11.7	Forwarding Novell's NMS Alarms to SunNet Manager .	11-14
11.7.1	Software Requirements	11-14
11.7.2	Configuration Changes Needed to SNM and NMS	11-14
11.7.3	Example Forwarded Trap	11-17
12.	If You Encounter Problems.....	12-1
12.1	Starting the Console.....	12-1
12.2	Letting the Discover Tool Build Your Database	12-3
12.3	Viewing, Creating, and Modifying Elements	12-4

12.3.1	Traversing the View Hierarchy	12-4
12.3.2	Creating Elements	12-5
12.3.3	Modifying Element Properties	12-6
12.3.4	Changing Element Types	12-6
12.3.5	Moving Elements from One View to Another	12-6
12.3.6	Deleting Elements	12-7
12.3.7	Saving the Management Database	12-7
12.4	Requesting Data from Agents	12-8
12.4.1	Making a One-Time Request for Data	12-8
12.4.2	Requesting Periodic Data	12-8
12.4.3	Copying Requests	12-9
12.4.4	Viewing Incoming Data	12-10
12.5	Viewing Data	12-10
12.5.1	Viewing Incoming Data with the Grapher	12-10
12.5.2	Viewing Incoming Data with Strip Charts and Indicators	12-11
12.5.3	Analyzing Stored Data with the Grapher	12-11
12.5.4	Printing a Graph	12-12
12.6	Specifying Events	12-12
12.6.1	Sending an Event Request	12-12
12.6.2	Viewing the Status of Requests	12-14
12.6.3	Viewing and Modifying the Properties of a Request	12-14
12.7	Creating an SNMP Element in the Database	12-14
12.8	Setting Up SNM to Receive Traps from a Device	12-15

12.9	Using the Set Tool.....	12-16
12.9.1	Using the Set Tool to Retrieve SNMP Attribute Values	12-16
12.9.2	Using the Set Tool to Change SNMP Attribute Values	12-17
12.10	Loading Background Images	12-18
12.11	Creating Types of Elements.....	12-20
12.12	Creating a New Glyph for an Element Type.....	12-20
	Index	Index-1

Figures

Figure 1-1	Agent and Proxy Communications Protocol.....	1-2
Figure 1-2	Using Proxy Agents across Networks	1-3
Figure 1-3	Using the Console to Initiate Management Tasks and Display Data.....	1-4
Figure 2-1	Example of a LAN Configuration.....	2-3
Figure 2-2	Critical Nodes in Home View	2-4
Figure 2-3	SunNet Manager Console Views.....	2-5
Figure 2-4	Elements within Console Views	2-6
Figure 2-5	Using Proxy Agents across Networks	2-11
Figure 2-6	Sending Predefined Event Request.....	2-13
Figure 2-7	Accessing a Predefined Event Request Properties Sheet.....	2-15
Figure 2-8	Example: Event Request Properties Sheet.....	2-16
Figure 2-9	Accessing snmp system Group for Event Request.....	2-17
Figure 2-10	sysUpTime Event Request	2-18
Figure 2-11	Accessing snmp ifStatus Group for Event Request	2-19

Figure 2-12	Event Request Properties Sheet for <code>ifOperStatus</code> Request	2-20
Figure 2-13	Requesting a Quick Dump to Check Router Interface Status.....	2-21
Figure 2-14	Quick Dump of Router Interface Status.....	2-22
Figure 2-15	Predefined Data Request Using <code>hostperf</code> Agent	2-24
Figure 2-16	Properties Sheet for Predefined Data Request	2-25
Figure 2-17	Graph from Predefined Request	2-26
Figure 2-18	Building Data Request with <code>hostperf</code> Agent.....	2-27
Figure 2-19	Data Request Properties Sheet with Log File Specified.....	2-28
Figure 2-20	Copying a Request from an Element's Subview.....	2-29
Figure 2-21	Data Report Files in Browser	2-30
Figure 2-22	Sending Data to Grapher	2-32
Figure 2-23	Merged Graphs	2-33
Figure 2-24	Event Request with <code>traffic</code> Agent	2-34
Figure 2-25	Example of <code>traffic</code> Event Request	2-35
Figure 2-26	Example of Monitor Configuration	2-37
Figure 3-1	Console Window.....	3-6
Figure 3-2	Quick Start Window	3-7
Figure 3-3	Discover Tool Window.....	3-11
Figure 3-4	Default Discover Properties.....	3-13
Figure 3-5	Selecting a View Name in the Goto Menu.....	3-14
Figure 3-6	Create Object Window	3-16
Figure 3-7	Object Properties Window (Component)	3-17
Figure 3-8	Top Portions of Object Properties Windows.....	3-19
Figure 3-9	Alias Window	3-23

Figure 3-10	Properties Window for Router	3-24
Figure 3-11	Selecting the View—Find Menu Item.	3-25
Figure 3-12	View—Find Window	3-25
Figure 3-13	Selecting the Glyph—Properties Menu Item.	3-27
Figure 3-14	Change Type Window	3-29
Figure 3-15	Moving a Glyph to a New Location	3-31
Figure 3-16	Glyph—Connect Example	3-33
Figure 3-17	Selecting the Edit—Copy Menu Item.	3-34
Figure 3-18	Selecting the Edit—Delete Menu Item	3-36
Figure 3-19	Selecting the File—Save—Management Database Menu Item.	3-37
Figure 3-20	Console—Quit Window	3-38
Figure 4-1	Requests Menu—Quick Dump Request	4-3
Figure 4-2	Glyph Menu—Quick Dump Request	4-5
Figure 4-3	Quick Dump Report Window	4-6
Figure 4-4	Sample Request Builder Window.	4-7
Figure 4-5	Request Name Menu.	4-8
Figure 4-6	Sample Data Request	4-9
Figure 4-7	Predefined Data Request	4-11
Figure 4-8	View—Data Reports Option	4-15
Figure 4-9	Sample Data Reports Window	4-16
Figure 4-10	Graph Tool Menu	4-18
Figure 4-11	Strip Chart and Indicator Samples	4-19
Figure 4-12	Data Request Properties Template	4-20
Figure 4-13	Strip Chart Menu.	4-21
Figure 4-14	Tools Menu.	4-23

Figure 4-15	Results Browser Window	4-24
Figure 4-16	File Menu for Results Browser	4-25
Figure 4-17	Results Browser with Reports Loaded	4-26
Figure 4-18	Browser Edit Menu	4-28
Figure 4-19	Browser Tool Edit Menu	4-29
Figure 4-20	Browser Properties Window	4-30
Figure 4-21	Results Grapher Window	4-32
Figure 4-22	Tools—Snapshot Window	4-33
Figure 5-1	Sample Request Builder Window	5-3
Figure 5-2	Request Name Menu	5-4
Figure 5-3	Sample Event Request	5-5
Figure 5-4	Predefined Event Request	5-7
Figure 5-5	View—Event/Traps Window	5-11
Figure 5-6	Glyph—Glyph State Menu	5-13
Figure 5-7	Properties Window for a View	5-15
Figure 5-8	Console—Properties—Category Menu	5-16
Figure 5-9	Properties—Event/Trap Window	5-17
Figure 6-1	Sample Requests—Summary Window	6-2
Figure 6-2	Requests—Summary Window	6-4
Figure 6-3	Request Glyph Menu	6-5
Figure 7-1	Alarm Reports Summary Window	7-2
Figure 7-2	Alarm Reports Find Window	7-3
Figure 7-3	Alarm Reports: Show View Window	7-4
Figure 7-4	Device-specific Alarm Reports Window	7-6
Figure 7-5	Console Window Footer Display	7-7

Figure 7-6	Console Pop-up or Tool Window Footer Display	7-8
Figure 7-7	Sample Error Reports Window	7-9
Figure 7-8	View—Event/Trap Reports Window	7-11
Figure 8-1	Creating a Printer	8-2
Figure 8-2	Properties for New Printer.	8-3
Figure 8-3	Sending Predefined Request to Printer	8-4
Figure 9-1	Edit—Create Window.	9-6
Figure 9-2	Properties Window for a New Component.	9-8
Figure 9-3	Glyph—Set Request Menus.	9-13
Figure 9-4	Set Tool Window	9-14
Figure 9-5	Set Tool—Agent Menu	9-16
Figure 9-6	Set Tool—Group Menu.	9-17
Figure 10-1	Creating a Connection Object	10-2
Figure 10-2	Properties for New Connection.	10-3
Figure 10-3	New Link in Console.	10-4
Figure 10-4	Link in View with Connected Objects	10-5
Figure 10-5	Invoking Send Request	10-7
Figure 10-6	Request Builder Window	10-8
Figure 10-7	Event Request Properties	10-9
Figure 10-8	Discover Configuration Window	10-11
Figure 10-9	Network Icon for View “Routers”	10-12
Figure 10-10	View Created by Discover	10-13
Figure 10-11	Link Name as Created by Discover	10-14
Figure 10-12	Properties of Discovered Link	10-15
Figure 11-1	Console’s Add Background Option	11-2

Figure 11-2	Add Background File Menu.	11-3
Figure 11-3	Console with New Background	11-4
Figure 11-4	Selecting the File—Save—Management Database Menu Item.	11-5
Figure 11-5	File—Save—Management Database Window	11-6
Figure 11-6	Selecting the File—Load—Management Database Menu Item.	11-8
Figure 11-7	File—Load—Management Database Window	11-9
Figure 11-8	Tools—Customize Window.	11-11
Figure 11-9	Properties/Locations Window	11-13

Tables

Table 2-1	Summary of SNM 2.2.3 Agents and Proxies	2-8
Table 2-2	Predefined Event Requests Supplied with SNM	2-12
Table 2-3	SNM Supplied Predefined Data Requests	2-23
Table 3-1	Glyphs Used for Multiple Element Types	3-21

Preface

The *SunNet Manager 2.2.3 User's Guide* provides information on how to use SunNet Manager™. The document focuses on helping users perform basic management tasks with SunNet Manager. This book is task-oriented; the *SunNet Manager 2.2.3 Reference Manual* provides more depth of detail on the topics covered in this guide.

Like other OpenWindows applications, the SunNet Manager Console uses the OPEN LOOK™ graphical user interface. The OPEN LOOK interface allows you to perform a variety of operations through direct manipulation of windows, icons, glyphs and menus on your workstation screen. This guide assumes that you are already familiar with the use of OPEN LOOK screen objects, such as buttons, scroll bars, and the like. If you are new to the OpenWindows user interface, you might consult the following SunSoft Press books:

- *Solaris OpenWindows User's Guide*
- John A. Pew, *Guide to Solaris*

At the end of this chapter there is an explanation of the conventions followed in this guide when describing use of the mouse.

How to Use this Book

Chapters 3 through 11 of the *SunNet Manager 2.2.3 User's Guide* each describe a series of steps for common tasks you will perform with SunNet Manager. Use the Table of Contents or the Index to locate the task you want more information about.

Help

On-line help is available.

On-line help is available for most SunNet Manager windows. On-line help provides brief descriptions of window menus, buttons, and fields. Because this manual does not include detailed descriptions of every field in the many windows that make up the SunNet Manager user interface, you should use on-line help or the *SunNet Manager 2.2.3 Reference Manual* to choose menu options or to fill in field values. To get on-line help, press the Help key on your keyboard. (See Chapter 3 of the *SunNet Manager 2.2.3 Installation Guide* for instructions on setting up access to on-line help.)

How This Book Is Organized

Below is a summary of the chapters in this book. If you are unfamiliar with SunNet Manager, you should read the chapters and use the procedures in consecutive order.

Chapter 1, “Overview and Concepts,” introduces basic SunNet Manager concepts, such as Console, agents, and management database, that you will encounter throughout this guide.

Chapter 2, “Network Management with SunNet Manager,” provides some guidance on how to use SunNet Manager to accomplish network management objectives.

Chapter 3, “Creating and Modifying the Management Database,” contains step-by-step tutorials that show you the tasks involved in creating a management database.

Chapter 4, “Requesting Data from Agents,” contains tutorials showing how to retrieve data from agents.

Chapter 5, “Specifying Events,” contains steps for setting up and modifying event notification.

Chapter 6, “Viewing and Managing Requests,” contains tutorials showing how to use the Request Viewer.

Chapter 7, “Viewing Reports,” shows how to obtain error and trap reports for your network.

Chapter 8, “Managing Printers,” provides steps to follow to implement management of printers.

Chapter 9, “Managing SNMP Devices,” introduces SNMP concepts and contains tutorials for managing machines running the SNMP proxy agent.

Chapter 10, “How to Create and Manage a Link,” provides examples of the use of link management, using both the Console’s graphical editor function and the Discover Tool.

Chapter 11, “Customizing SunNet Manager,” contains tutorials for customizing the Console environment, such as creating new glyphs and modifying the Tools menus.

Chapter 12, “If You Encounter Problems...,” provides some guidance for situations where you encounter problems using SunNet Manager.

Compatibility

For definitive compatibility information, see the *SunNet Manager 2.2.3 Important Product Information* document that accompanies this product.

SunNet Manager Electronic Mail Distribution Service

SunSoft has available a service on a mail server that contains information and software from various sources that are relevant to SunNet Manager.

Note – SunSoft provides this material as a service to the SNM community—without charge, without warranty, and without support of any kind whatsoever.

For information on accessing the service, send a mail message to `snm-server@sun.com`, with “help” as the body of the message. The server sends back a help file describing how to access the service through electronic mail.

If you wish to submit any nonproprietary applications, agents, MIBs, application notes, or other data to the server, contact `snm-server-manager@sun.com`.

Note – The server does not process messages from users named `root`, `operator`, `system`, `daemon`, or `mailer-daemon`.

Command Line Examples

All command line examples in this guide use the C-shell environment. If you use either the Bourne or Korn shells, refer to `sh(1)` and `ksh(1)` man pages for command equivalents to the C-shell.

What Typographic Changes and Symbols Mean

The following table describes the type changes and symbols 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. system% You have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	system% su Password:
<AaBbCc123>	Command-line placeholder: replace with a real name or value	To delete a file, type <code>rm <filename></code> .
<i>AaBbCc123</i>	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.
Code samples are included in boxes and may display the following:		

Table P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
%	UNIX C shell prompt	system%
\$	UNIX Bourne and Korn shell prompt	system\$
#	Superuser prompt, all shells	system#

Mouse Conventions

This book assumes that you are using a Standard Sun workstation three-button mouse. The mouse buttons are called SELECT (left), ADJUST (middle), and MENU (right).

Click means to press and quickly release a mouse button.

Press indicates you should hold the button down until an action is completed, such as a menu appearing.

Overview and Concepts



<i>Management Applications and Agents</i>	<i>page 1-1</i>
<i>SunNet Manager Console</i>	<i>page 1-4</i>
<i>Management Database</i>	<i>page 1-5</i>
<i>Configuration</i>	<i>page 1-7</i>

SunNet Manager is a comprehensive set of tools and services that you can use to perform fundamental tasks in managing your network. SunNet Manager is also an extensible platform that allows you to develop your own network management applications. This chapter introduces basic concepts underlying the use of SunNet Manager to manage your network.

1.1 Management Applications and Agents

The SunNet Manager package provides both management applications and agent software. You install the SunNet Manager software on the system from which you will manage the network—this system is known as the *management station*. *Management applications* are the processes that allow you to initiate management tasks and collect management information. *Agents* are processes that access the device or element being managed at the request of a management application.

Most agents that are provided with SunNet Manager return information about entities on the Sun workstation on which the agent software is installed. A second type of agent, a *proxy agent*, provides information about entities on *other* systems or other vendors' devices. Each agent returns a certain set of information or *attributes* to the management application. For example, the *hostmem* agent returns information about memory usage on the system on which the agent is installed. The Simple Network Management Protocol (SNMP) proxy agent returns information about SNMP objects on any device that supports the SNMP standard.

Proxy agents provide two main advantages:

- They allow the management application to manage objects using virtually any protocol. SunNet Manager agents and proxy agents communicate with the management applications through the Remote Procedure Call (RPC) protocol. Proxy agents translate the RPC protocol into the protocol that the managed objects understand. This is illustrated in Figure 1-1.

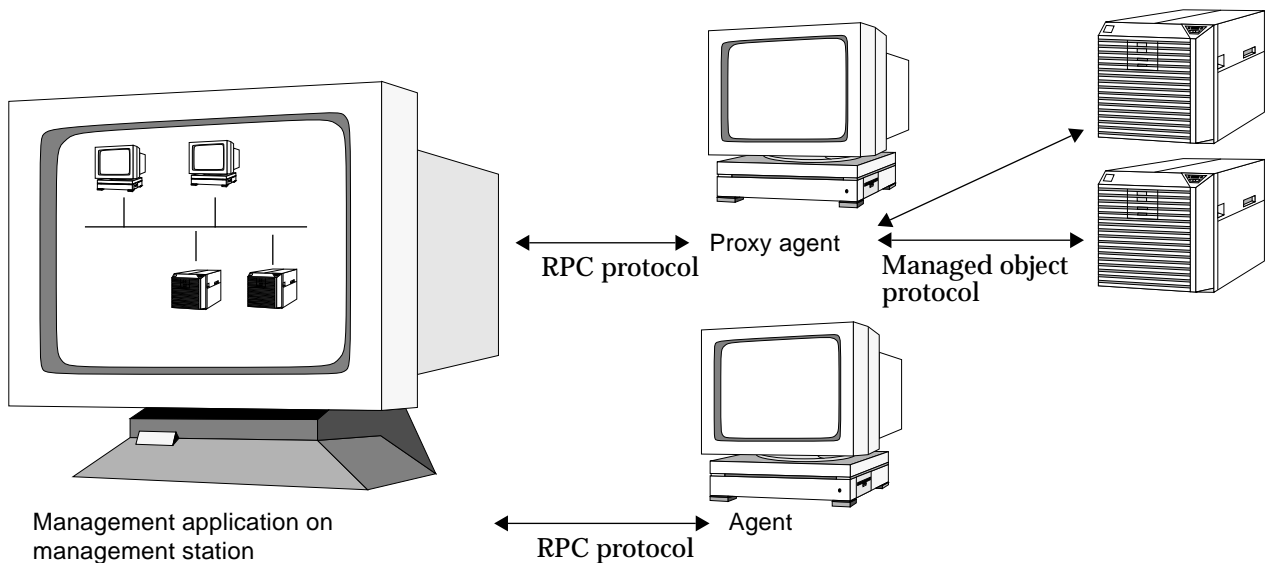


Figure 1-1 Agent and Proxy Communications Protocol

- A single proxy agent can provide management access to multiple devices. The management application only needs to communicate with one proxy agent to manage many devices. The real advantage of this becomes apparent

when the proxy agent is installed in a different subnet or domain from the management application. The proxy agent handles the low-level gathering of data from the managed objects. Only minimal network traffic containing the relevant management information passes between the proxy agent and the management application. This is illustrated in Figure 1-2.

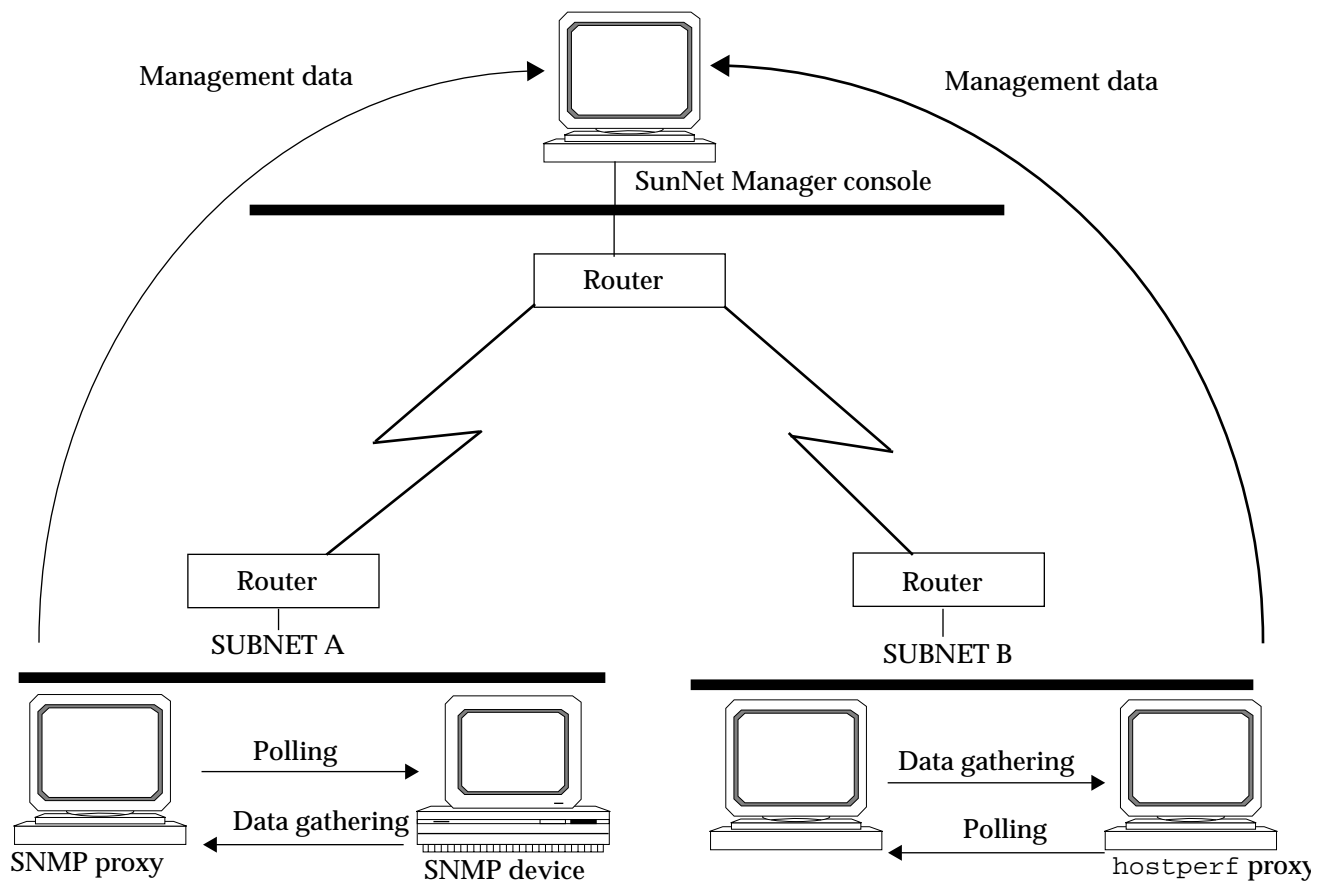


Figure 1-2 Using Proxy Agents across Networks

The SunNet Manager package includes a collection of agents and proxy agents. For a list of SunNet Manager agents and brief descriptions of the data they return, see Appendix B of the *SunNet Manager 2.2.3 Reference Manual*.

1.2 SunNet Manager Console

The SunNet Manager Console is the central management application in the SunNet Manager package. The Console is a graphically-oriented interface that allows you to create a representation of your network. You can use the Console to initiate management tasks and display management information. Figure 1-3 shows some examples of Console functions.

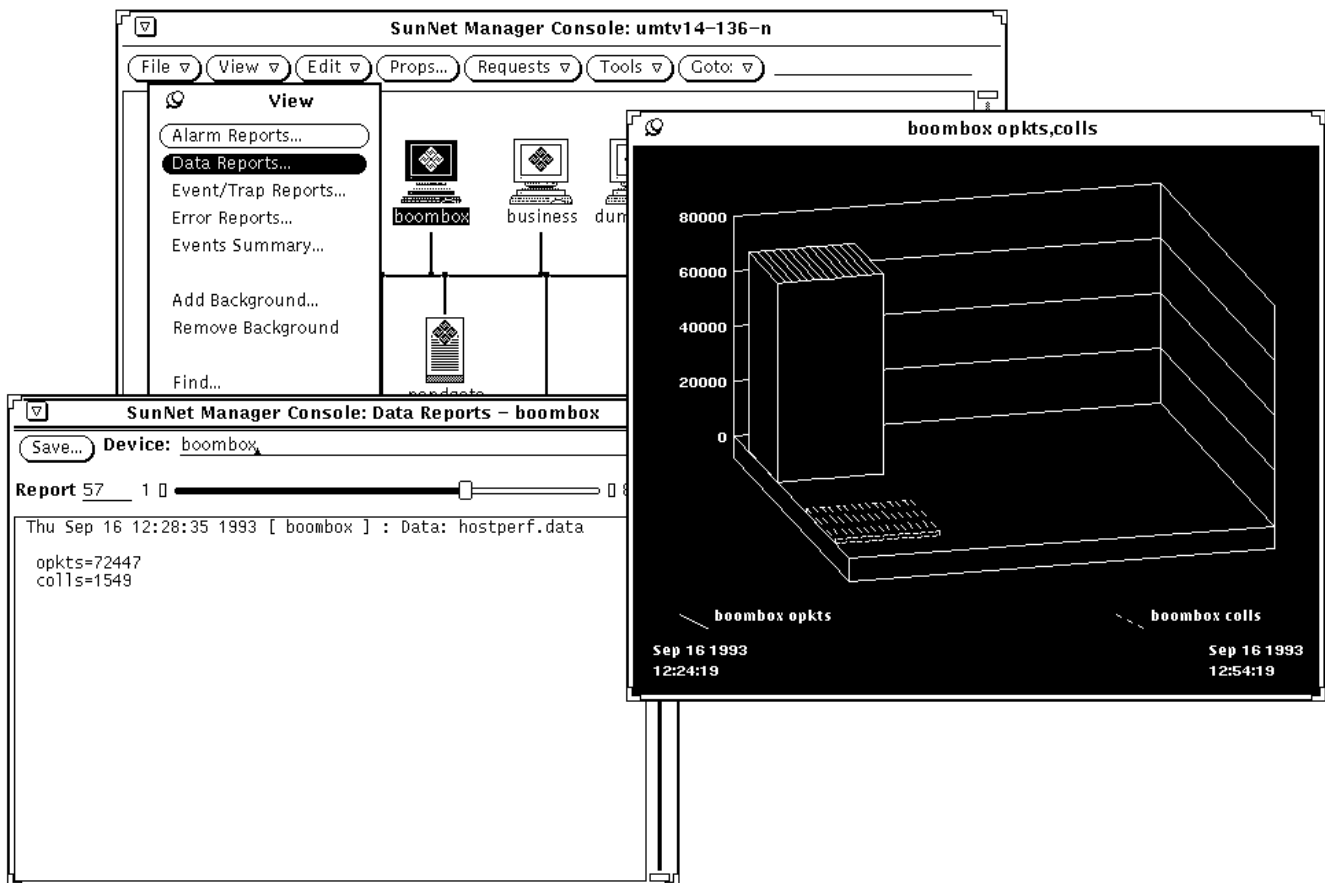


Figure 1-3 Using the Console to Initiate Management Tasks and Display Data

The Console provides mechanisms to initiate requests to agents for *data reporting* and for specifying *events*.



Data reporting allows you to direct agents to send reports of management data on a periodic basis. For example, you can direct the `hostperf` agent to return at one-hour intervals the percentage of CPU being used on a particular system. You can choose to have the reported data displayed in a log, in a chart or graph, or stored in a disk file.

SunNet Manager provides additional tools for viewing and analyzing the returned data: the Results Browser allows you to analyze data that has been stored to a disk file, while the Results Grapher allows you to see a graphical representation of either incoming data or stored data.



Event reporting allows you to direct agents to send reports of management data when an event takes place in the network. An event is an occurrence of certain user-defined conditions. For example, you can direct the `hostperf` agent to send a report whenever the CPU percentage on a system exceeds a set number. You can choose to have the Console reflect the report of an event by visual or audible indicators, or have the report of an event automatically launch a predefined program.

1.3 Management Database

The Console and other management applications rely on a *management database* (MDB) that contains definitions of the elements being managed, the agents that are available, and the requests that have been made to agents. The management database contains:



- **Definitions of each *type* of element that can be represented in the SNM Console.** This element type definition specifies the name of the element type (for example, `ss10` for a SPARCstation 10) and the glyph (or icon) associated with it. The `elements.schema` file provided with SunNet Manager defines many general element types.

The `elements.schema` file is located in the `struct` directory. (The default path for this directory is `/usr/snm/struct` for the Solaris 1.1.1 version of SNM, or `/opt/SUNWconn/snm/struct` for the Solaris 2.3 version.) In addition, you can create your own element schema file that defines one or more element types.



- **Definitions of *instances* of element types.** The element instance definition represents a particular element in your network—usually the name of a device. An element instance also defines those agents that can be used to manage the element. In the Console, glyphs represent the instance definition

of each element. Element instance definitions can be created automatically by a management application such as the Discover Tool, or created “manually” using the Console’s Edit►Create function.

- **Definitions of the agents that the management application can use to manage elements.** Each agent can return different sets of information or *attributes*. The set of attributes that can be returned by each agent is defined in an agent *schema* file. At least one agent schema file should be installed on the management station for each agent that a management application will direct. (The SNMP proxy agent can be used with many agent schema files for different SNMP devices. Three SNMP schema files are included with SNM: `snmp.schema`, `snmp-mibII.schema`, and `sun-snm.schema`.)

Note that while technically all agents and schema files are available for any element instance, some agents are more appropriate for certain element types than others. A set of agent schema files are provided with SunNet Manager. The default location for these agent schema files is:

- `/usr/snm/agents`, if you’ve installed the Solaris 1.1.1 version of SNM
- `/opt/SUNWconn/snm/agents`, if you’ve installed the Solaris 2.3 version of SNM

The contents of the agent schema files are described in the man page for each agent.

- **Definitions of predefined requests that you can invoke for a managed object in the Console.** SNM has a set of predefined requests that cover a wide range of your information-gathering needs. These save you the trouble of building requests for individual elements. These requests are stored in `$HOME/.SNMpredefined`.

The management database present while you are running the Console—referred to as the *runtime database*—can be saved to an ASCII file and later reloaded into the Console. This feature allows you to save or backup your database—with any customizations you might have made—across system reboots. It also allows you the advantage of a portable database file. For example, you can manage multiple databases from the same Console or, within the same network, manage the elements in the same database from different machines.

1.4 Configuration

The two basic types of SunNet Manager configuration are:

- **Configuration of the operation of the Console and SunNet Manager tools.** You change values associated with these programs through the Props (Properties) button in the Console window. An example of this type of configuration is changing the way a glyph responds to an event from blinking (the default) to changing color. See Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for a description of configurable properties.
- **Configuration of certain operating characteristics of SunNet Manager agents and daemons on the system on which the agents and daemons are installed.** Most network administrators do not need to perform this type of configuration.

Depending on your network management needs, you might not need to do much in the way of configuration of SNM to make the product very useful. The default values for Console- and agent-related parameters are designed to be appropriate for most network administrators' needs.

The characteristics of SNM agents and daemons are defined in the `snm.conf` file. For example, you can specify the locations of the log files generated by the SunNet Manager daemons. (The `snm.conf` file is located in the `/etc` directory if you've installed SNM 2.2.3 on a SunOS 4.x machine; if you've installed the Solaris 2.3 version of SNM 2.2.3, this file is located in `/etc/opt/SUNWconn/snm`.)

Additionally, you can specify information relevant to the operation of the SNMP proxy agent, such as the location of SNMP schema files and the maximum number of requests that an SNMP proxy agent subprocess will handle. You can also specify security access for agents on the system where the `snm.conf` file resides. See the `snm.conf (5)` man page and the man pages for individual agents for more information. There is list of all the agents shipped with SNM 2.2.3 in Table 2-1 in the next chapter.

Network Management with SunNet Manager



<i>Planning for Network Management</i>	<i>page 2-1</i>
<i>Using the Console</i>	<i>page 2-12</i>
<i>Using Monitor to Update the Management Database</i>	<i>page 2-36</i>

This chapter is intended to provide you with some ideas on how to set up and use SunNet Manager to meet network management goals. The methods described here are not the *only* way these goals could be met. The approach that is best suited for a given situation will depend upon the particular network configuration, network management priorities, and the network management applications available.

2.1 Planning for Network Management

Before installing the agent software and starting up the management Console, a typical first stage is to devote some thought to planning your network management installation. How are you going to use SunNet Manager to manage your network? The following steps indicate the types of specific questions you will need to answer:

1. What are your critical nodes?

You need to identify those devices that have impact on the greatest number of users on the network — such as gateways, hubs, print servers, and software servers. If you are only interested in monitoring these devices, you can reduce the number of elements to create and monitor on the SNM Console.

2. What views do you want to have of your network?

On a small network, you may choose to place all the critical nodes into a single view. For example, Figure 2-1 shows a network consisting of two subnets, A and B, which are connected by a gateway.

SPARCstations and diskless workstations mount their software from the servers. One of the software servers in each subnet doubles as a print server. An IP/X.25 router provides a connection to a public switching network.

Taking the servers and gateways as the critical nodes, these could be placed into a single view. You could create these elements one-at-a-time, using the Console's Edit►Create function, as described in Section 3.5, "Creating Elements." With only one view required, the elements could be simply placed in the Home view, as shown in Figure 2-2.

For most situations, however, you will want to have multiple views to represent functional groupings of network devices and to represent the network topology — the various networks and subnetworks, and the types of connections used and locations of the routers and gateways. For example, you might want views to depict devices in particular buildings, or a view that consists of only routers.

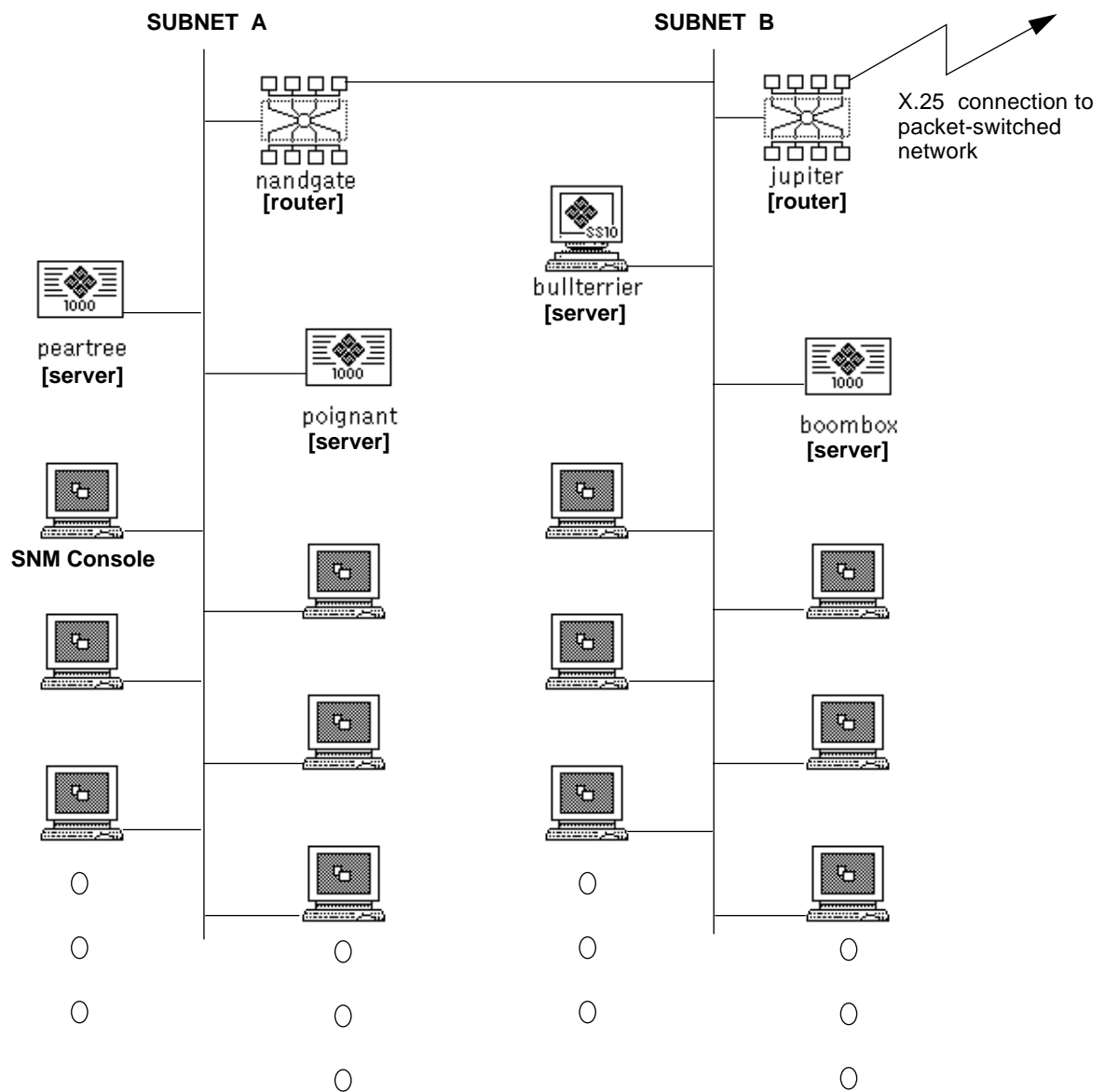


Figure 2-1 Example of a LAN Configuration

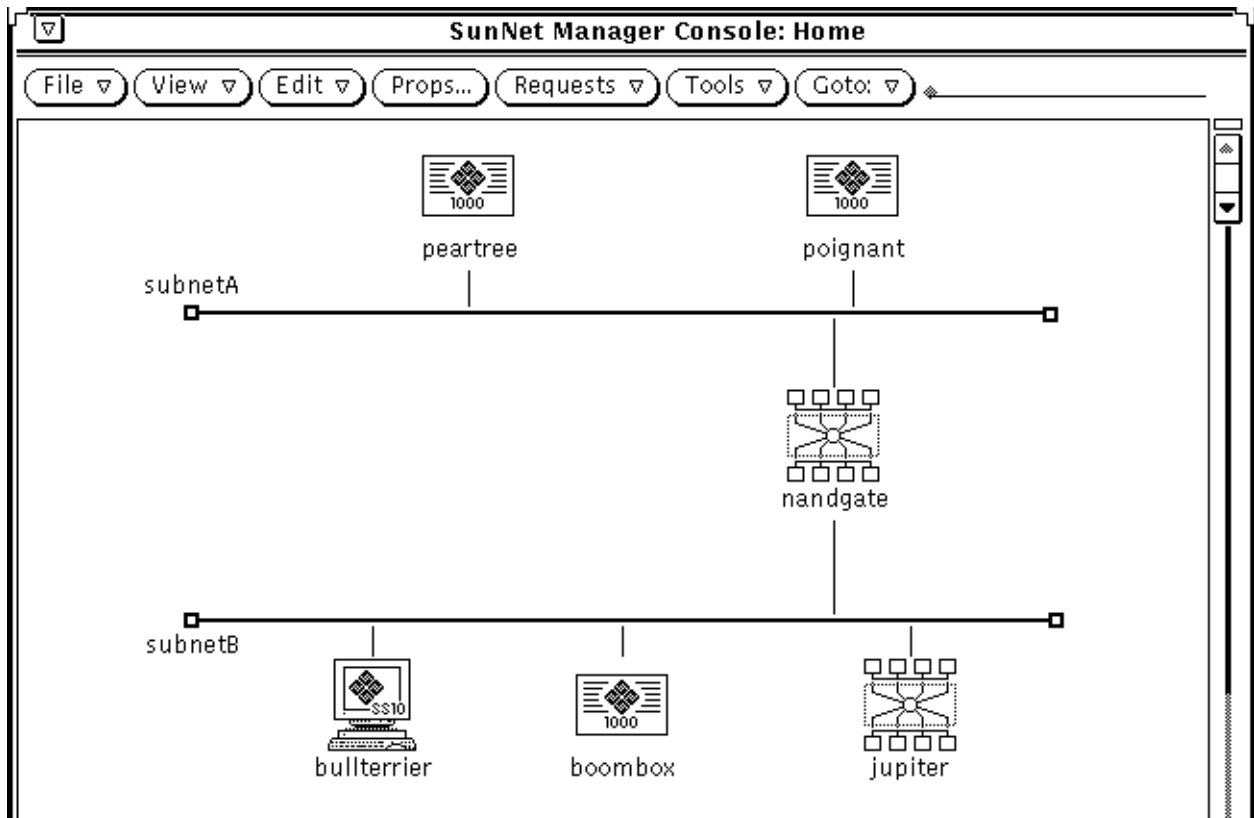


Figure 2-2 Critical Nodes in Home View

Taking our sample network in Figure 2-1, we might want to create a separate view for each subnet as well as separate views by type of device — routers, software servers, and print servers. You could create these views one-at-a-time using the Console Edit>Create function, as described in Section 3.5, “Creating Elements.” For most purposes, though, it is more convenient to let the Discover Tool build a hierarchy of views to represent your network topology, as described in Chapter 5 of the *SunNet Manager 2.2.3 Reference Manual*. For our sample network of Figure 2-1, views

grouping elements by function (software servers, routers, etc.) and subnetwork could be created in the Home view, as shown in Figure 2-3.

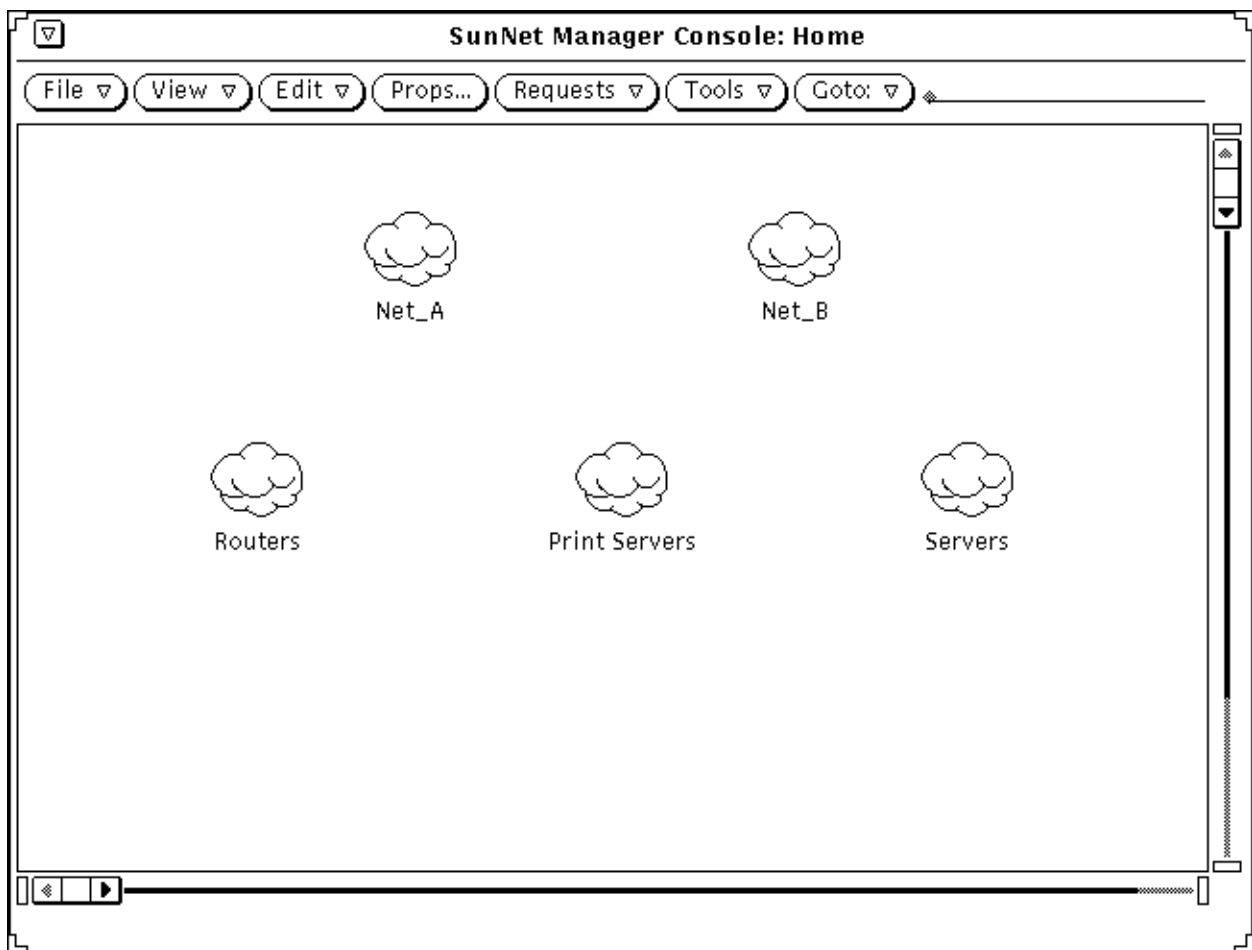


Figure 2-3 SunNet Manager Console Views

The cloud glyphs in Figure 2-3 represent the separate views into the LAN and its subnetworks. Figure 2-4 shows the elements within these clouds. The same element may occur within multiple views. A software server, such as poignant, can occur both in the Servers view as well as in the Net_B view, which shows all nodes in a subnetwork.

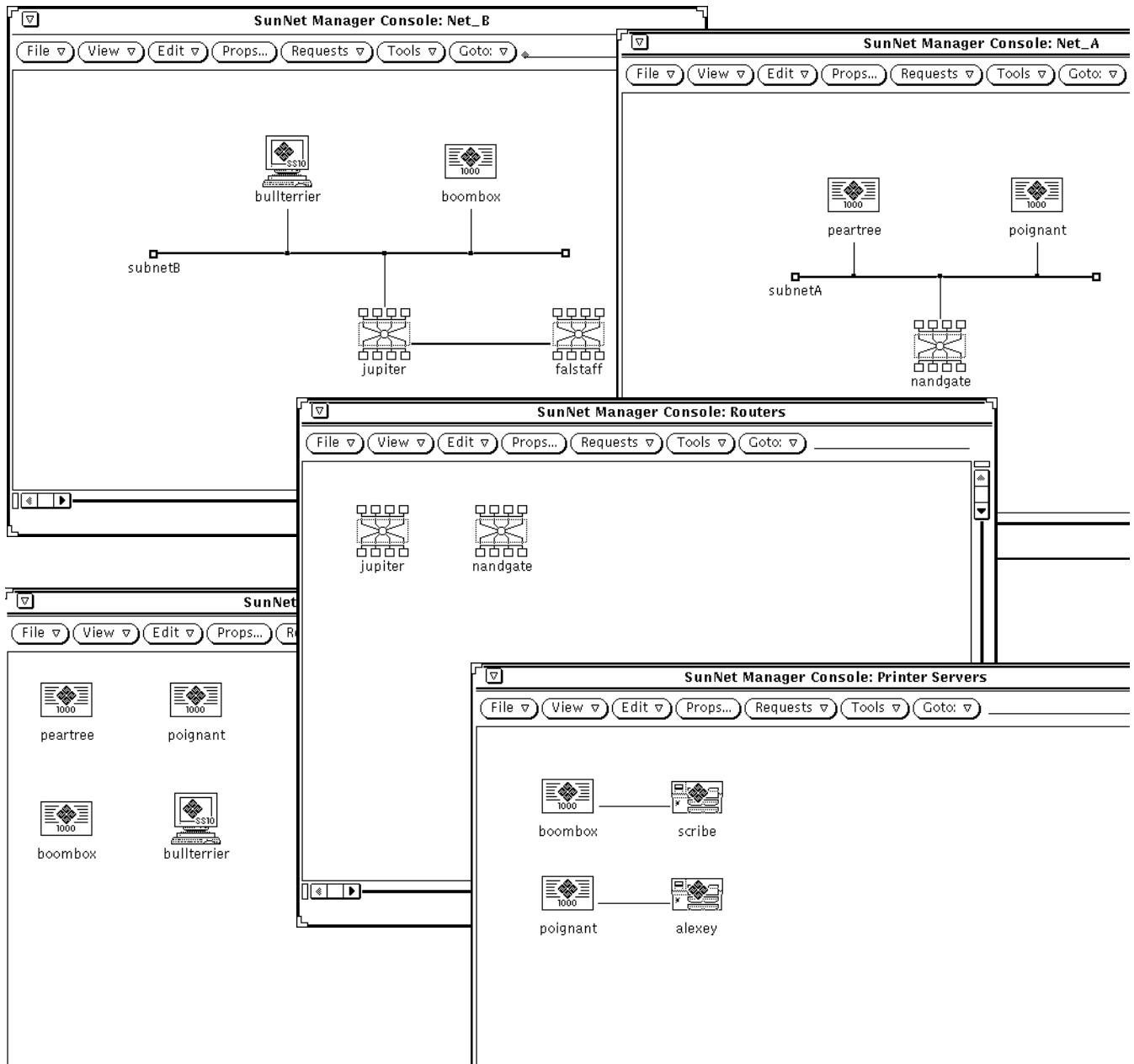


Figure 2-4 Elements within Console Views

3. What type of information do you need to manage the network?

There are three different types of information that SNM can provide you:

a. Event notification

You will want to be notified of critical events. SNM's event request mechanism allows you to define the conditions that will generate an event notification. Once the event request is specified, it is sent to the agent. The agent generates an event if the specified condition becomes true. You will need to select agents that support the particular conditions you want to test for.

If one of your critical nodes becomes inoperative or unavailable to users, you will want to know this *immediately*. This means that you will want to specify a fairly frequent interval of polling in the appropriate event requests (for example, every five minutes).

If you want to know of certain key devices, such as routers, not only whether they are currently down, but whether they have been down at any time since you last cleared an event, you will want to choose Color By Priority as the method for notifying you of a critical event on the Console. You can then take advantage of the "decay-to-blue" feature. When the specified event occurs for the target device, its glyph will turn red and then will change to blue if the condition (e.g., unavailability) is no longer true.

In addition to events generated by agents in response to SNM event requests, there are also unsolicited events — called "traps" — generated by Simple Network Management Protocol (SNMP) devices, such as routers. For information on how to set up SNM to receive traps, refer to Section 9.3, "Setting Up SNM to Receive Traps from a Device."

b. Data reporting

You will want statistical information to compare the performance of your critical nodes, such as servers and gateways, over a period of time. Data reporting can also provide you with statistics on network traffic levels at various times. Collecting data on resource utilization rates can help you determine whether particular network resources are being overburdened.

In most cases, you will probably not want continual polling for data as this can itself add an additional burden to the network. If you activate data-gathering periodically, you can develop an historical record that can help you spot trends and determine "normal" load levels.

c. Topology information

You will also want information on changes to the network's topology, such as the addition of new devices and connections. Discover Tool's Monitor function can be used to update the management database. Configuration of a typical network is likely to change slowly. Rather than burden the network with frequent Discover searches, weekly searches may be sufficient.

4. What agents will provide you with the type of information you want?

Once you know what type of event or data reports you will need to manage your network, you will be able to determine which agents are required to provide the type of information you want.

Table 2-1 provides a summary of the agents shipped with SNM 2.2.3. In some cases agents return information similar to that provided by certain UNIX commands, and this is indicated in the table.

Table 2-1 Summary of SNM 2.2.3 Agents and Proxies

Name	Description	Related UNIX Command	Type
diskinfo	Reports disk usage information	df	Agent
etherif	Ethernet interface statistics for SunOS 4.x clients	—	SunOS 4.x agent
etherif2	Ethernet interface statistics for Solaris 2.x clients	—	Solaris 2.x agent
hostif	Monitors interfaces that send IP packets	netstat -i	Agent (see note)
hostmem	Memory utilization information for SunOS 4.x clients	netstat -m	SunOS 4.x agent
hostmem2	Memory utilization information for Solaris 2.x clients	netstat -m	Solaris 2.x agent
hostperf	Reports host system performance data	rup and perfmeter	Proxy agent
iostat	Reports input/output statistics for SunOS 4.x clients	iostat	SunOS 4.x agent
iostat2	Reports input/output statistics for Solaris 2.x clients	iostat	Solaris 2.x agent
ippath	Reports IP packet trace information	—	Proxy agent
iproutes	Reports IP route table and statistics	netstat -r	Agent
layers	Protocol layer statistics for SunOS 4.x clients	netstat -rs netstat -s	SunOS 4.x agent
layers2	Protocol layer statistics for Solaris 2.x clients	netstat -rs, netstat -s	Solaris 2.x agent

Table 2-1 Summary of SNM 2.2.3 Agents and Proxies

Name	Description	Related UNIX Command	Type
lpstat	Reports printer status	lpq and lpstat	Proxy agent
ping	IP connectivity information	ping	Proxy agent
rpcnfs	Remote Procedure Call and Network File System statistics	nfsstat	Agent
snmp	Returns information from MIB I-compliant SNMP devices.	—	Proxy agent
snmpv2	For managing SNMP Version 1 and Version 2 devices	—	Proxy agent
snmp-mibII	Returns information from MIB II-compliant SNMP devices.	—	Proxy agent
sun-snmp	Returns MIB I-compliant and Sun-specific information from Sun workstations.	—	Proxy agent
sync	Monitors synchronous serial lines	syncstat	Agent
traffic	Ethernet traffic analyzer	—	Proxy Agent

If you've installed SNM, you can get specific information about each agent by consulting the man page for `na.<agent-name>`. For example:

```
hostname% man na.ping
```

To have access to the man pages, make sure that you have set your MANPATH environment variable, as described in Chapter 3 of the *SunNet Manager 2.2.3 Installation Guide*.

In the case of the `na.snmp` proxy agent, there are three schema files shipped with SNM that can be used with it (`snmp`, `snmp-mibII`, and `sun-snmp`). You can get information on the `snmp` and `snmp-mibII` schema files in the man pages for `<agent-name>.schema`. For example:

```
hostname% man snmp-mibII.schema
```

The `sun-smnp.schema` file supports the features of the Sun enterprise-specific SNMP agent, `snmpd`, for Sun workstations and servers. To access information on this agent, enter the following command:

```
hostname% man snmpd
```

Proxy agents *can* be mounted solely on the management machine. However, as the proxy agent polls remote devices, and these devices respond, this adds to the network traffic load. A more efficient arrangement is to distribute proxy agents to collect information within separate domains or subnetworks, as depicted in Figure 2-5. This reduces the network traffic between the management station and managed devices.

For example, if the management station wants to know if any router in a remote subnet is down, it can send a single event request to a `ping` proxy agent in that domain and the proxy agent only responds when it detects that a router is not available. The regular polling of the routers is limited to the subnet where the proxy system is located.

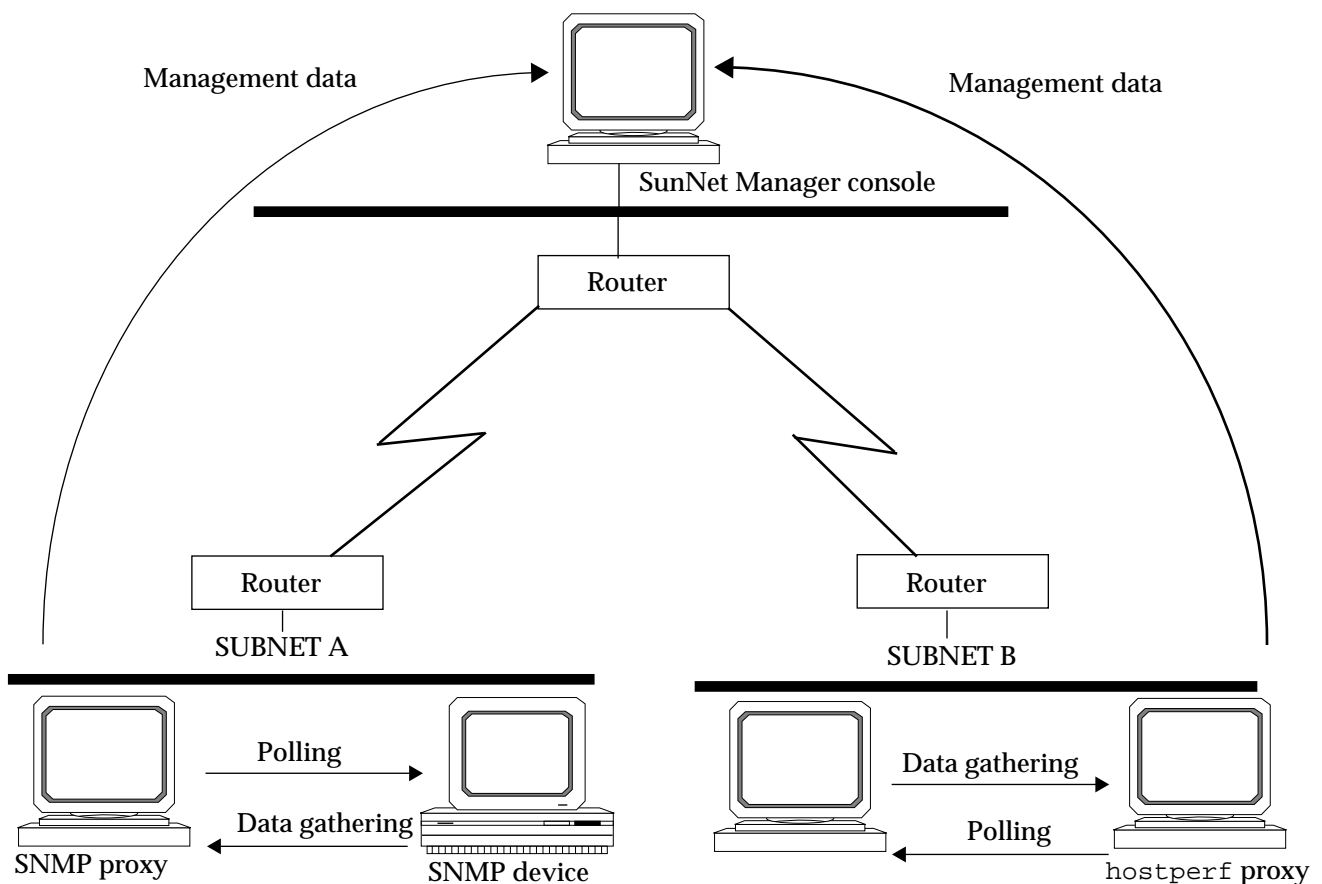


Figure 2-5 Using Proxy Agents across Networks

For information on installing the SNM agents, refer to Chapter 4 of the *SunNet Manager 2.2.3 Installation Guide*. Note that certain of the agents listed in Table 2-1 are to be installed only on SunOS 4.x machines. For each of these agents there is a corresponding agent (those with a name ending in "2") intended specifically for use on Solaris 2.x machines.

2.2 Using the Console

The SNM Console provides you with three methods for gathering information from agents:

- *Quick Dumps* are one-time data reports of values for all attributes in an agent attribute group or table. You can find detailed instructions for using Quick Dumps in Section 4.1, “Making a One-Time Request for Data.”
- *Data* reports gather values for selected attributes over time. They are useful for comparative analysis and observing trends. You can find detailed instructions for creating data requests in Section 4.2, “Requesting Periodic Data.”
- *Event* reports notify you of changes in the values of attributes, based upon predefined conditions. They are useful for reporting abnormal conditions. You can find detailed instructions for creating event requests in Section 5.1, “Specifying an Event.”

What follows are some examples of how these functions can be used to accomplish network management goals.

2.2.1 Using Event Requests to Monitor Critical Nodes

You can specify the conditions that define an event, and the type of notification you want to receive, using the Event Request properties window. You can compose your own event request or, more conveniently, you can use one of SNM’s predefined requests. The predefined requests included with SNM 2.2.3 are summarized in Table 2-2.

Table 2-2 Predefined Event Requests Supplied with SNM

Request Name	Agent Name	Group Name	Attributes Supported	Event to be Reported
when Disk is Full	diskinfo	diskSpace	capacity	disk file system is full
If System Reboot	hostperf	data	uptime	if system reboots
when Printer Error	lpstat	status	statusCode	line printer error
when System is not Reachable	ping	reach	reachable	system not reachable

The use of event requests is illustrated in the examples that follow. Detailed step-by-step instructions on how to define and launch event requests can be found in Chapter 5, “Specifying Events.”

2.2.1.1 Example: Using `ping` to Monitor Availability of Critical Nodes

To be informed immediately if any of your critical nodes goes down, you can use an event request with the `ping` agent. The most convenient method to set up such a request is to use the predefined event request “when System is not Reachable.”

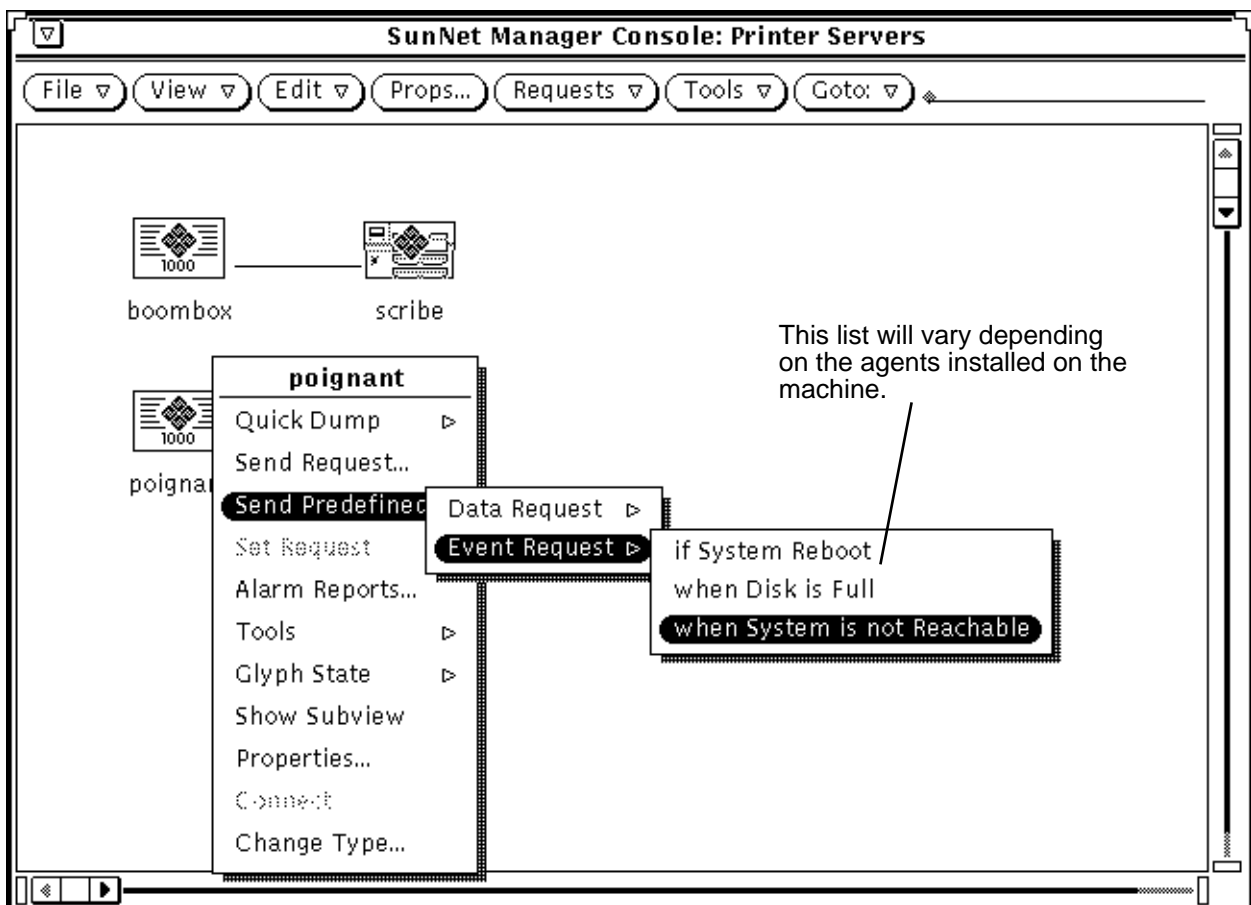


Figure 2-6 Sending Predefined Event Request

If you press the MENU button over the glyph representing the target device, this displays the glyph menu. You can select the predefined event request from this menu as shown in Figure 2-6.

However, the “when System is not Reachable” predefined request does not take advantage of the “decay-to-blue” feature because its effect on the glyph, when an event occurs, is to blink the glyph (as indicated on the properties sheet for this request in Figure 2-8).

If you want to know if certain critical devices, such as routers, have been unreachable at any time since you last cleared an event for them, even if they are reachable now, the decay-to-blue feature will turn the glyph blue to indicate this. You can define a new event request for your routers, to take advantage of this feature, by using the “when System is not Reachable” predefined request as a starting point. To do this, you first select the target router and then access the Request Builder window by pulling down the Console Requests menu, as shown in Figure 2-7.

In the example in Figure 2-7, you select the agent (`ping`), attribute group (`reach`), request type (Event Request), and then “when System is not Reachable” — the name of the predefined event request that you can use as a starting point for specifying the new event request. Once these are selected, then click SELECT on the Apply button and the properties sheet will be displayed, as shown in Figure 2-8.

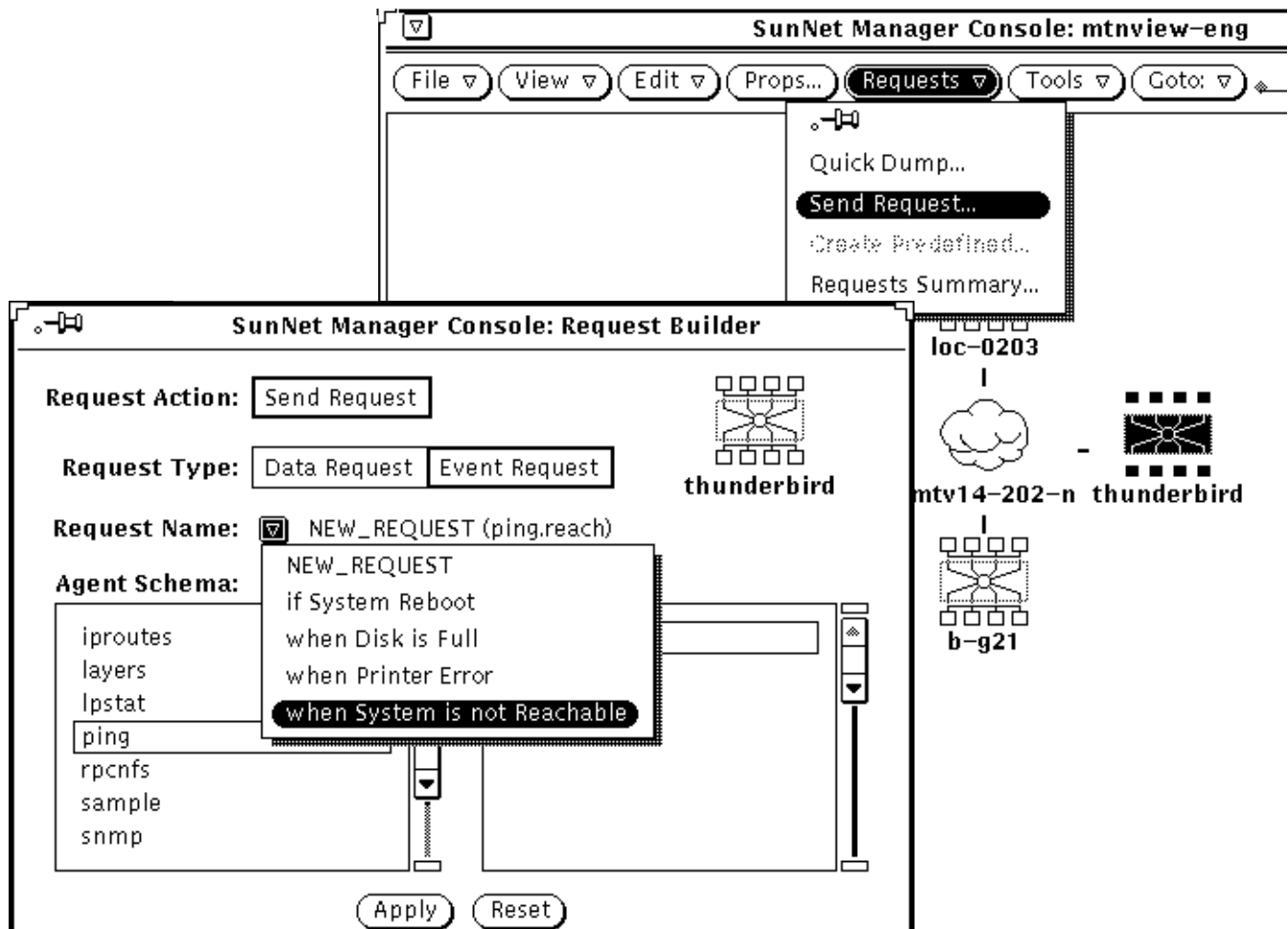


Figure 2-7 Accessing a Predefined Event Request Properties Sheet

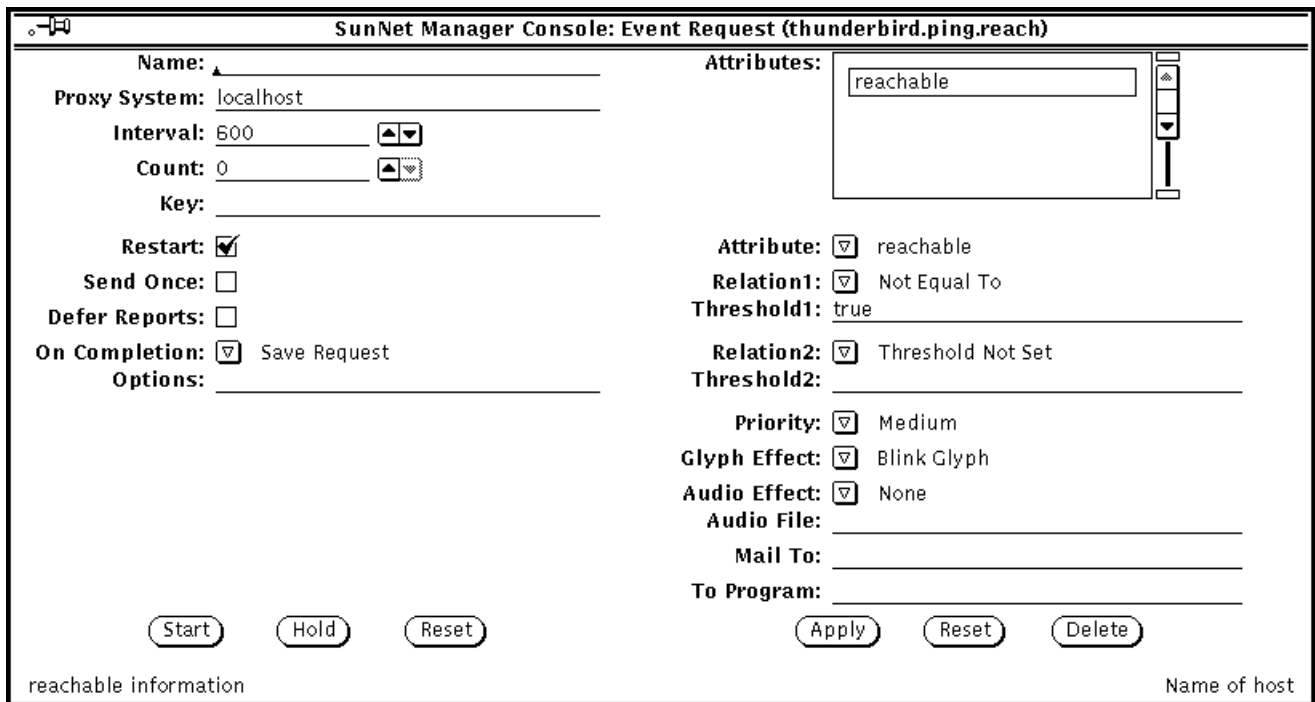


Figure 2-8 Example: Event Request Properties Sheet

Once you have accessed the properties sheet for the event request, you can create a new event request to take advantage of the decay-to-blue feature by changing the Glyph Effect field to Color By Priority.

If an event causes the glyph state to change color, the new glyph state is propagated through the view hierarchy. If the glyph state is propagated to the Home view and the Console is closed to an icon, the SNM icon changes to indicate that an event has occurred that changed the glyph state. You can thus be notified of this event even if the Console is displaying a different view or the Console is closed to an icon.

The Polling Interval value is stated in terms of seconds. In this case, the proxy agent polls every 600 seconds (ten minutes). A Count field value of 0 means that polling will continue indefinitely.

2.2.1.2 Example: Using `sysUpTime` to Monitor SNMP Devices

A limitation of the `ping` agent is that it can only determine if a device is available on the occasions that it polls the device. But you may want to be notified if routers have gone down momentarily and then become available again between polls. You can use the SNMP `sysUpTime` attribute to check for this on devices that support Simple Network Management Protocol (SNMP).

To build an event request, press MENU over the target element and select Send Request to invoke the Request Builder window.

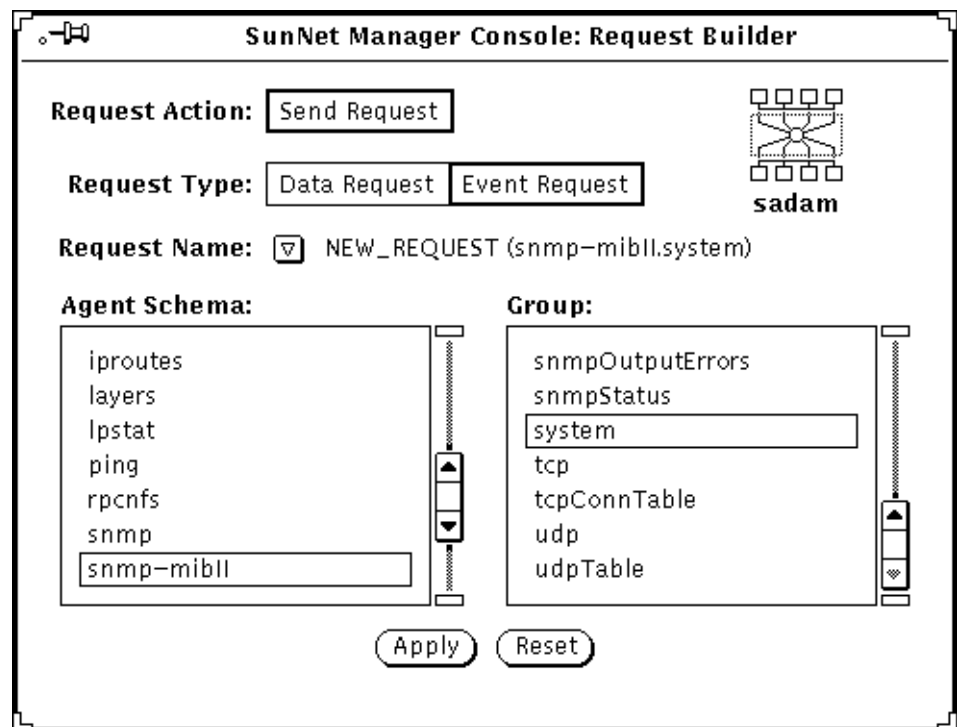


Figure 2-9 Accessing `snmp` `system` Group for Event Request

As shown in Figure 2-9, select Event Request, the `snmp-mibII` agent, and the `system` group. Click SELECT on the Apply button to access the event request properties sheet, as shown in Figure 2-10.

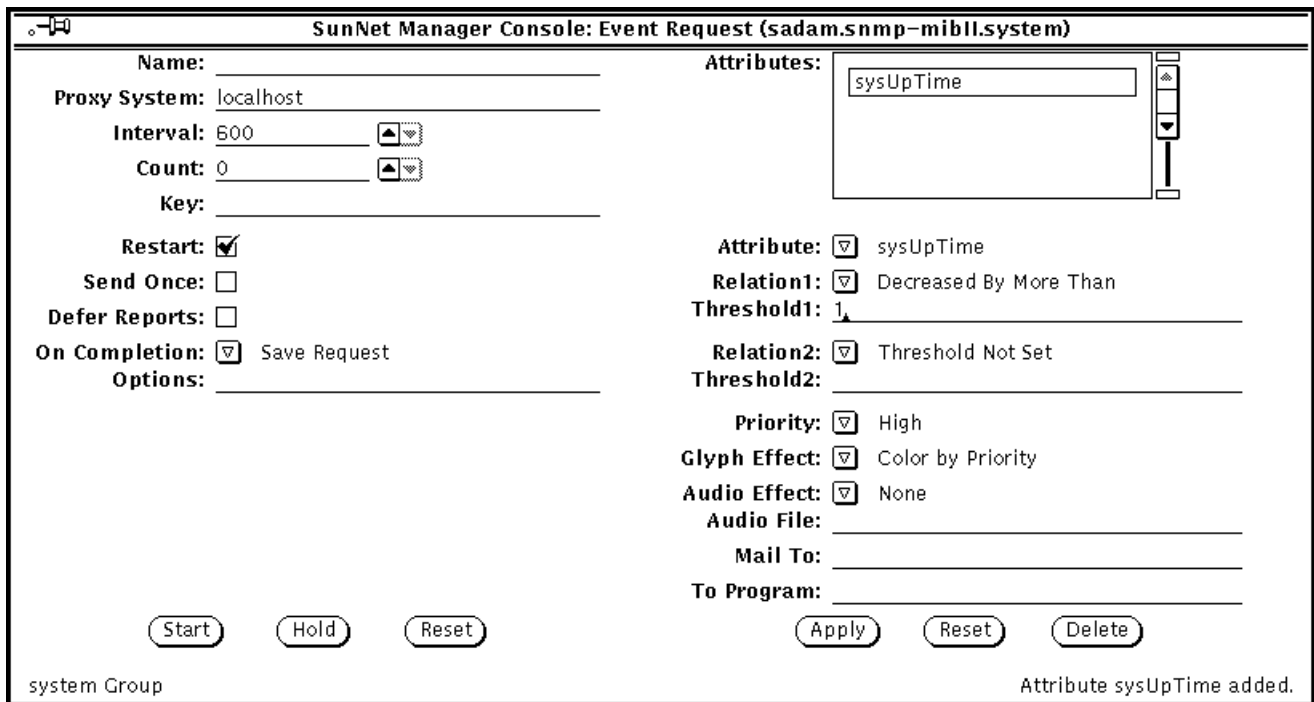


Figure 2-10 sysUpTime Event Request

In Figure 2-10 the following values have been entered in the event request fields:

- **Attribute:** sysUpTime is selected.
- **Relation:** Decreased by More Than is selected.
- **Threshold1:** Enter 1.

The condition that generates an event is the value of sysUpTime decreasing by more than .001 seconds. In other words, if the length of time the system is up is less than on the previous poll, we know that the system went down between polls. sysUpTime measures the time, in hundredths of a second, since the last system restart.

- **Interval:** The polling interval is set to 600 seconds (ten minutes).
- **Count:** Set to 0 to continue indefinitely.
- **On Completion:** By setting this field to Save Request, the request is not deleted if you stop it.

- **Priority:** High is selected.
- **Glyph Effect:** Because we have selected High Priority, Color by Priority will turn the glyph red if an event occurs. To make these selections take effect, click SELECT on the Apply button. The attribute name will then appear in the window at the upper right. Click SELECT on the Start button to launch the request.

2.2.1.3 Example: Using `ifOperStatus` to Monitor Router Interfaces

You can also use the SNMP `ifOperStatus` attribute to monitor the availability of router interfaces. Once you have selected the target router, access the Request Builder, by selecting Send Request from the glyph popup menu or the Console Requests pulldown menu.

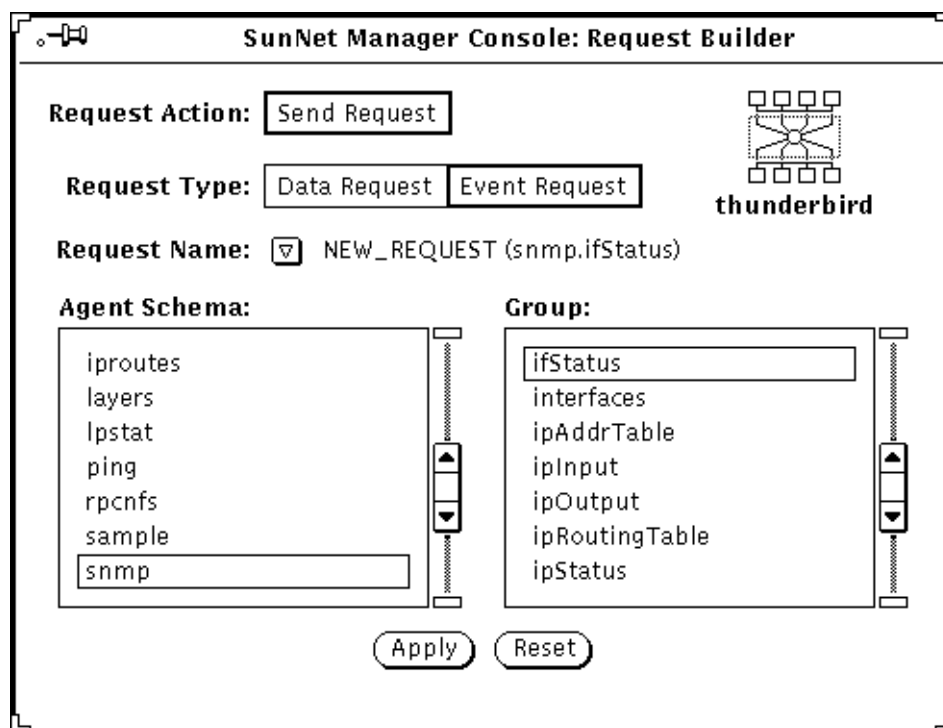


Figure 2-11 Accessing `snmp ifStatus` Group for Event Request

As shown in Figure 2-11, select Event Request, the snmp agent, and the ifStatus group. Click SELECT on the Apply button to access the event request properties sheet, as shown in Figure 2-12.

SunNet Manager Console: Event Request (thunderbird.snmp.ifStatus)

Name: _____

Proxy System: localhost

Interval: 600 ▲▼

Count: 0 ▲▼

Key: _____

Restart:

Send Once:

Defer Reports:

On Completion: Save Request

Options: _____

Attributes: ifOperStatus

Attribute: ifOperStatus

Relation1: Not Equal To

Threshold1: 1

Relation2: Threshold Not Set

Threshold2: _____

Priority: High

Glyph Effect: Color by Priority

Audio Effect: None

Audio File: _____

Mail To: _____

To Program: _____

Start Hold Reset Apply Reset Delete

key: ifIndex Attribute ifOperStatus added.

Figure 2-12 Event Request Properties Sheet for ifOperStatus Request

In Figure 2-12 the following values have been entered in the event request fields:

- **Attribute:** ifOperStatus is selected.
- **Relation:** Not Equal To is selected.
- **Threshold1:** Enter 1.
The condition that defines a critical event is the interface not being up. The interface is not up if ifOperStatus has a value other than 1.
- **Key:** If this field is left blank, an event is generated if *any* of the router's interfaces are not up. If you only want to test for a particular interface, then enter the ifIndex number for that router in the Key field.

If you want to generate a one-time report to check the status of all interfaces on a router, you can use the glyph popup menu to send a Quick Dump to a target router using the `snmp ifStatus` group, as shown in Figure 2-13.

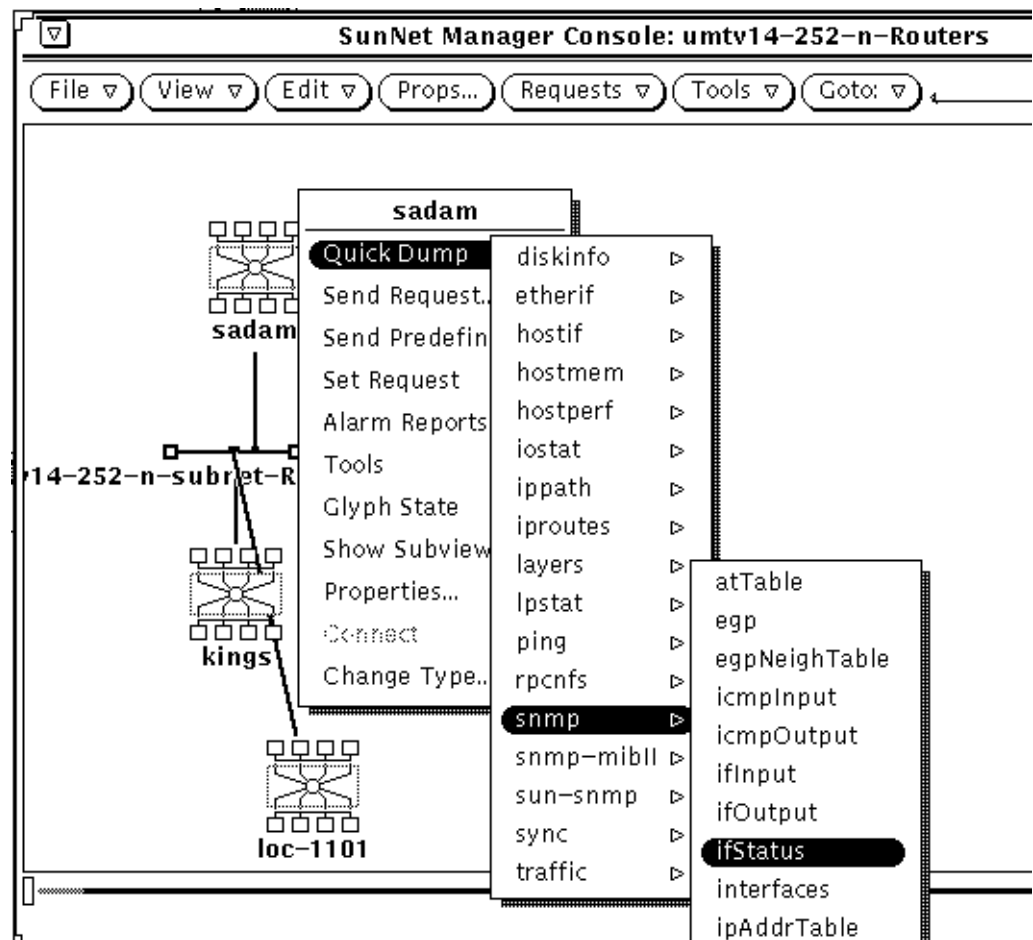


Figure 2-13 Requesting a Quick Dump to Check Router Interface Status

This Quick Dump returns the status of all interfaces, as shown in Figure 2-14.

KEY	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange
1	1	bf0	1	4352	9600		1	1	00:00:00.00
2	2	lo0	24	1536	10000000		1	1	00:00:00.00
3	3	le0	6	1500	10000000	08:00:20:12:E7:21	1	1	00:00:00.00

Figure 2-14 Quick Dump of Router Interface Status

2.2.2 Using Data Requests to Monitor Performance

Data requests can be used to gather comparative data in such areas as network traffic levels or the performance of critical nodes, such as servers and routers. A data request causes an agent to report the values of specified attributes for a target device. You can request a one-time report of current data (a Quick Dump), or reporting of data at periodic intervals. Data reports can be viewed in a real-time graph or logged to a file for later viewing.

Continual data polling can generate a lot of additional network traffic. You will probably want to collect data only at periodic intervals, to establish an historical record, to help you gauge trends and determine normal levels of activity.

You can define your own data requests using the Data Requests properties window (shown below in Figure 2-19), or, more conveniently, you can use one of SNM's predefined data requests. Table 2-3 lists the predefined data requests shipped with SNM 2.2.3.

Table 2-3 SNM Supplied Predefined Data Requests

Request Name	Agent Name	Group Name	Attributes Supported	Function
Graph Host Performance	hostperf	data	cpu% intr disk ipkts opkts	CPU utilization # of device interrupts # of disk transfers # of if input pkts # of if output pkts
Record Disk Space	diskinfo	diskSpace	all	disk space information
Record Host Performance	hostperf	data	all	Statistics of Host
Show Host Interfaces	hostif	if	all	host interface statistics
Show NFS Statistics	rpcnfs	client	all	RPC and NFS statistics
Show Path to Host	ippath	path	all	trace IP packet's path between proxy and target system
Show Routing Statistics	iproutes	routes	all	Routing statistics
Show snmp System Info	snmp	system	all	System information
Show snmp-mibII System Info	snmp-mibII	system	all	System information
Show sun-snmp System Info	sun-snmp	system	all	System information

To view a system's performance in a real-time graph, you can select the predefined data request "Graph Host Performance." As shown in Figure 2-15, you can launch this data request from the target host's glyph popup menu.

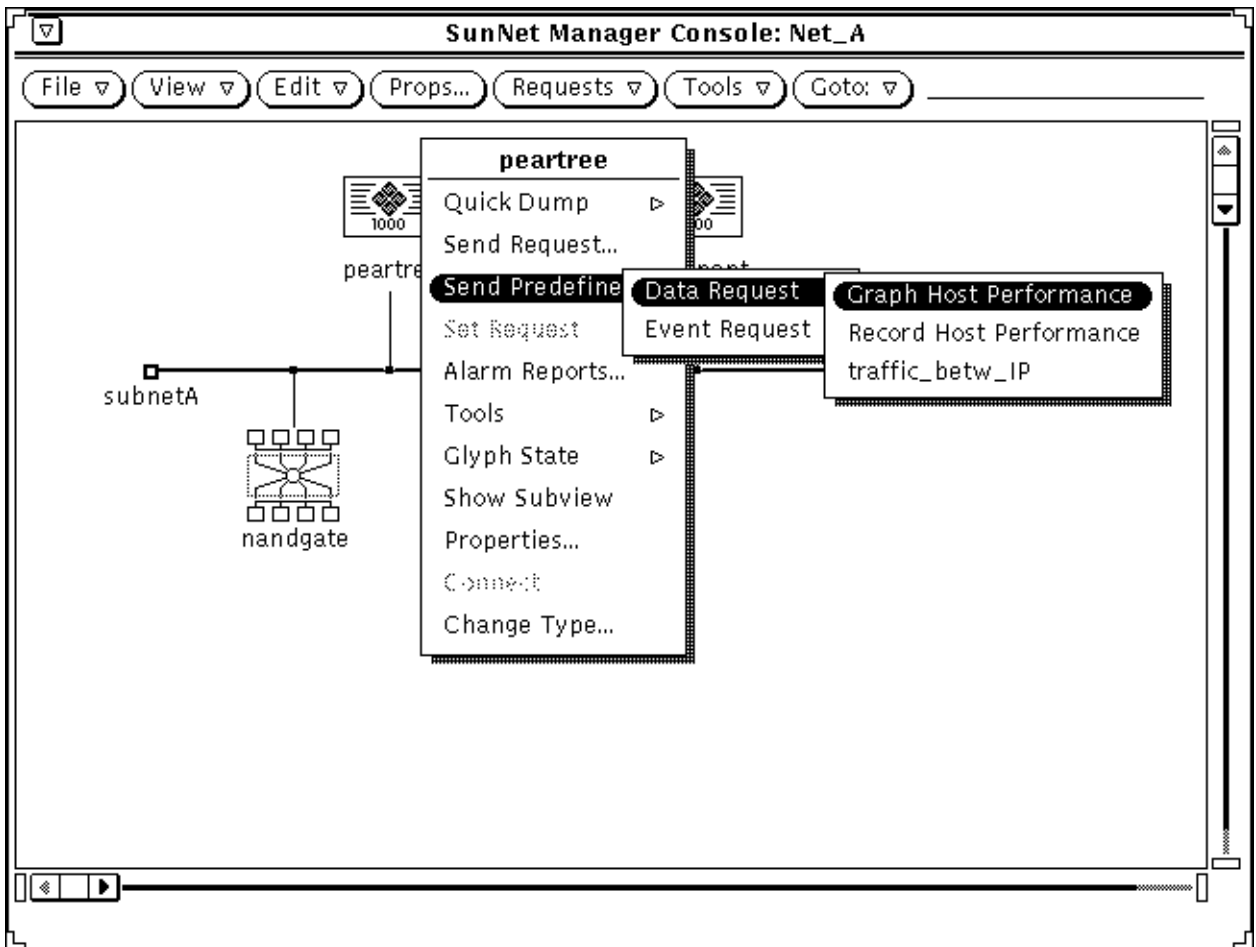


Figure 2-15 Predefined Data Request Using hostperf Agent

The Data Report Properties sheet reflecting the values of the predefined request is shown in Figure 2-16.

SunNet Manager Console: Data Request (peartree.hostperf.data)

Name: Graph Host Performance.4	Attributes:
Proxy System: localhost	cpu%
Interval: 30	intr
Count: 0	disk
Key:	ipkts
Restart: <input checked="" type="checkbox"/>	Attribute: <input type="checkbox"/> cpu%
Defer Reports: <input type="checkbox"/>	Data Log: <input type="checkbox"/> False
On Completion: <input type="checkbox"/> Save Request	Indicator: <input type="checkbox"/>
Options:	Strip Chart: <input type="checkbox"/> None
Log to File:	Graph Tool: <input type="checkbox"/> Absolute Values
To Program:	

Restart Stop Reset Apply Reset Delete

Host performance data CPU utilization

Figure 2-16 Properties Sheet for Predefined Data Request

You can launch this request at each of your critical nodes. For each such request, you will receive a graph such as the one shown in Figure 2-17.

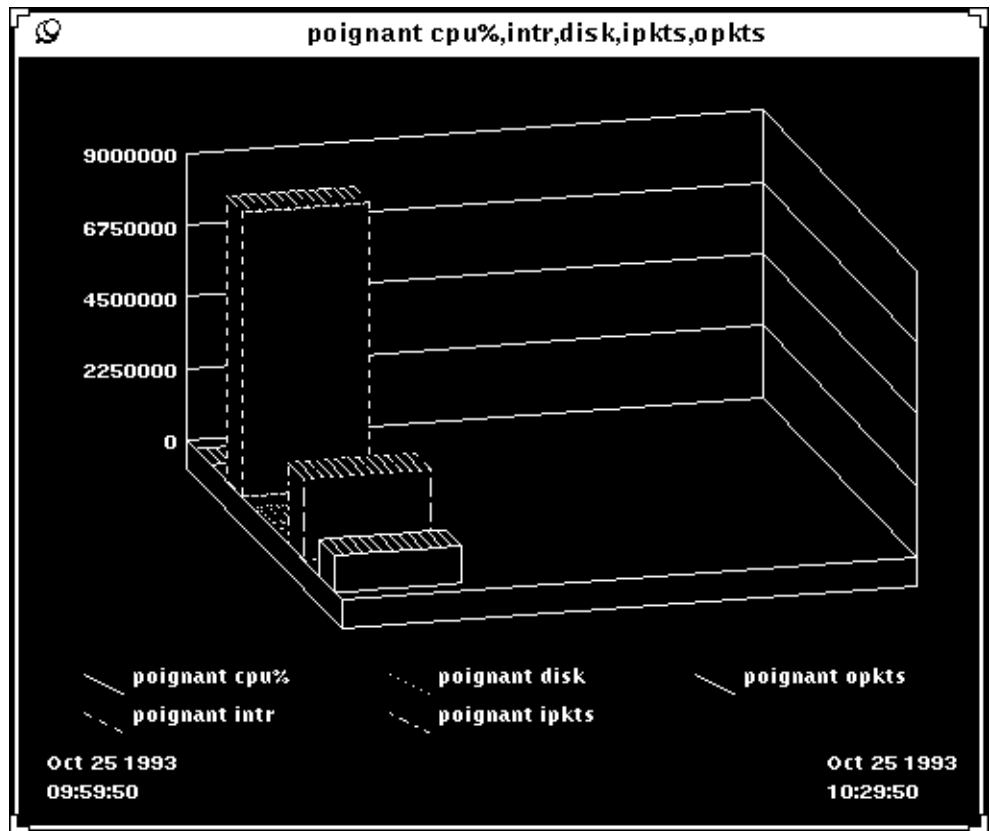


Figure 2-17 Graph from Predefined Request

The `hostperf` agent can also be used for data reports, where the data is logged to a file. To build such a request for a target device, you first select the device and then invoke the Request Builder window via the Console's Requests►Send Request option, as shown in Figure 2-18.

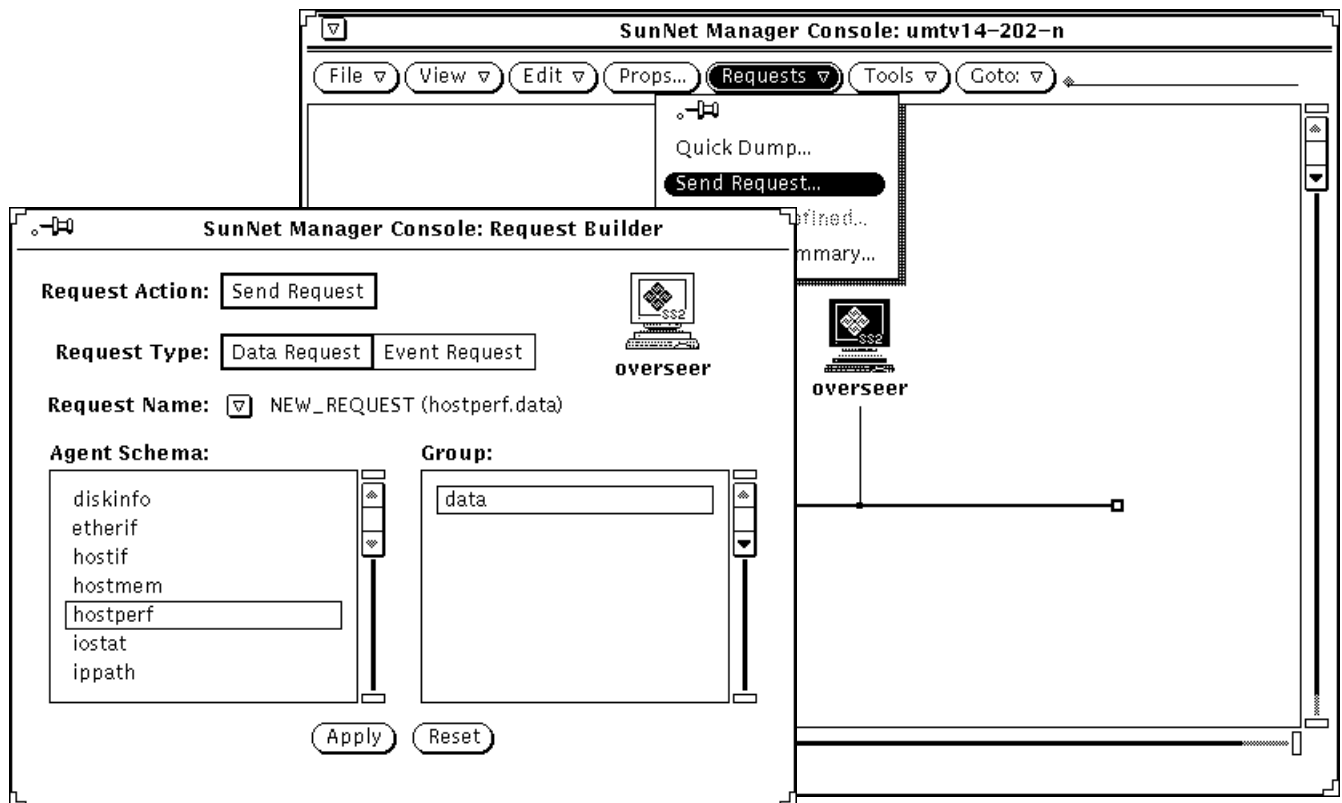


Figure 2-18 Building Data Request with hostperf Agent

After selecting Data Request type and the `hostperf` agent, you click on the Apply button to invoke the Data Request properties sheet, shown in Figure 2-19.

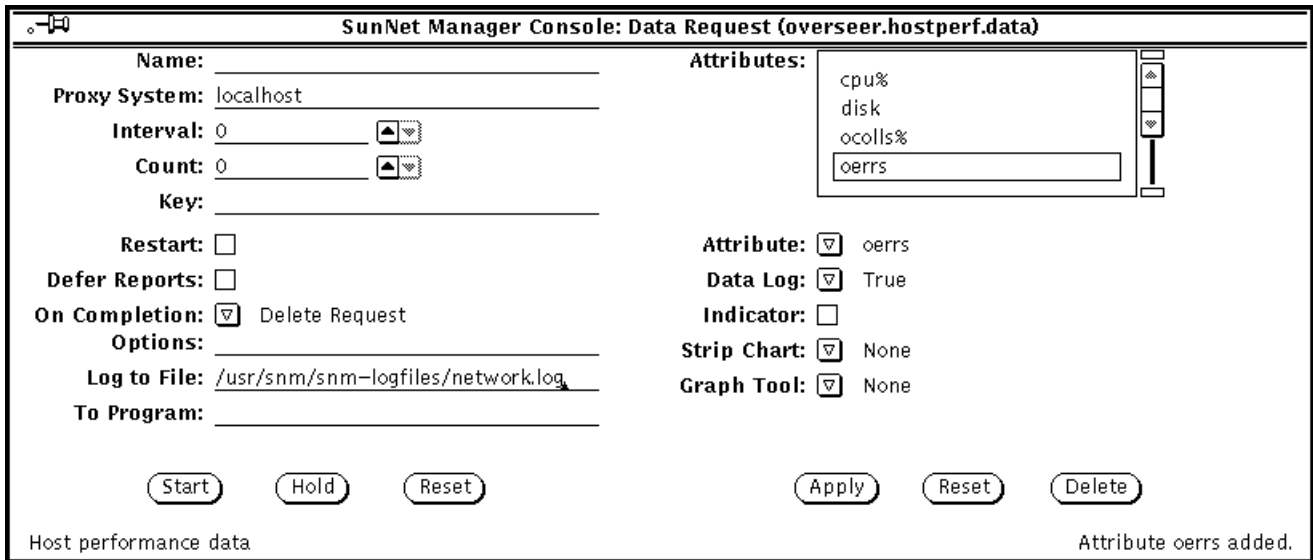


Figure 2-19 Data Request Properties Sheet with Log File Specified

The fields are filled in as follows:

- **Log to File:** Here we have entered `/usr/snm/snm-logfiles/network.log` as the file where the reports are stored.
- **Attribute:** We have selected the `cpu%`, `disk`, `ocolls%`, and `oerrs` attributes. After selecting each attribute we then added it to the Attributes window by clicking on the Apply button.
- **Data Log:** This is set to true (the default) to log data to the file indicated in the Log to File field.

Clicking SELECT on the Start button launches the request.

The subview for each device will show you all the active requests targeted at that device. To access the subview for a device, double-click SELECT on the glyph for that device. The active requests targeted at that device will be represented by glyphs, as shown in Figure 2-20.

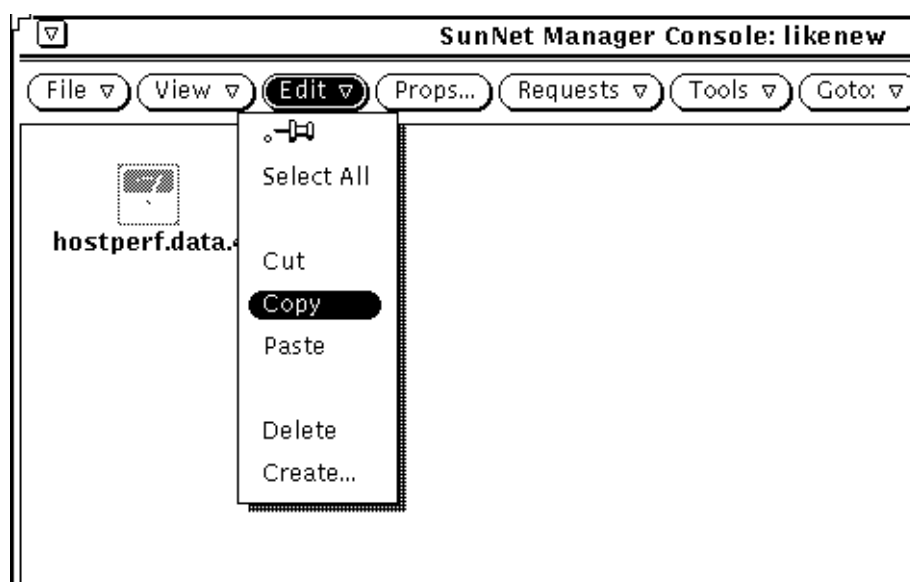


Figure 2-20 Copying a Request from an Element's Subview

Once a request is launched for one device, you can copy and paste this same request from the subview of the initial device to the subview of each additional device you want to track. As shown above, you can use the Console Edit►Copy function to copy requests from the subview of one element to the clipboard. You can then paste this request into the subview of each of multiple elements. This launches a clone of the initial data request for each additional device where you paste the request.

The data reports received from these requests can be viewed using the Results Browser. The Results Browser is invoked from the Console Tools menu. The log file where the data is stored can be loaded into the Results Browser via the Browser's File►Load option. Figure 2-21 shows the Results Browser loaded with the log file specified in the Log to File field in Figure 2-19 above.

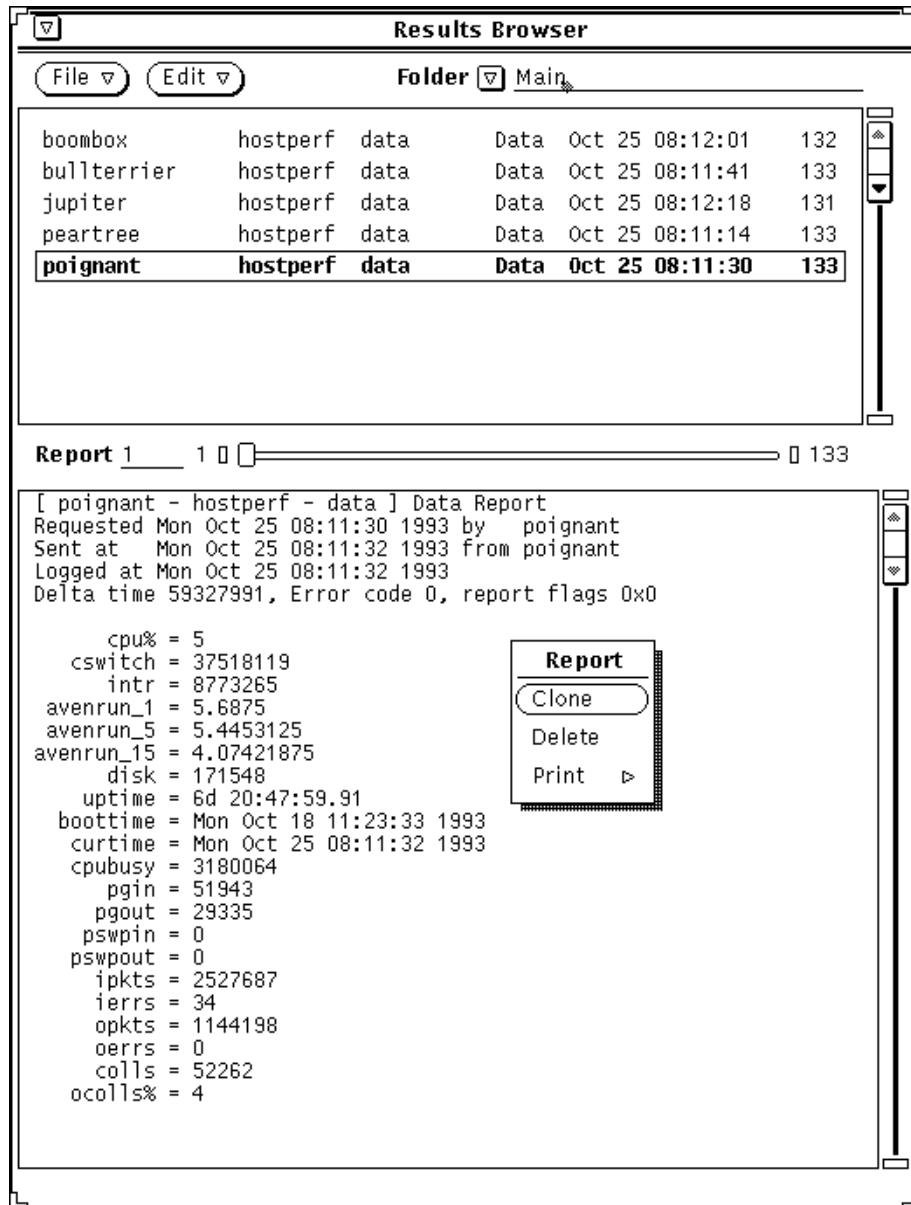


Figure 2-21 Data Report Files in Browser

The report streams from each request can be selected in the top window of the Browser, and various operations can be performed on streams. Within each stream, you can view individual reports, and print, clone, or delete reports. Using the Results Browser is discussed in Section 4.5.1, “Analyzing Stored Data: Results Browser,” and in Chapter 6 of the *SunNet Manager 2.2.3 Reference Manual*.

If you want to compare the data from the different streams over a particular attribute, such as `cpu%`, you can do this by merging the data from the various files into a single graph. To accomplish this, the Grapher tool can be invoked from the Browser as shown in Figure 2-22.

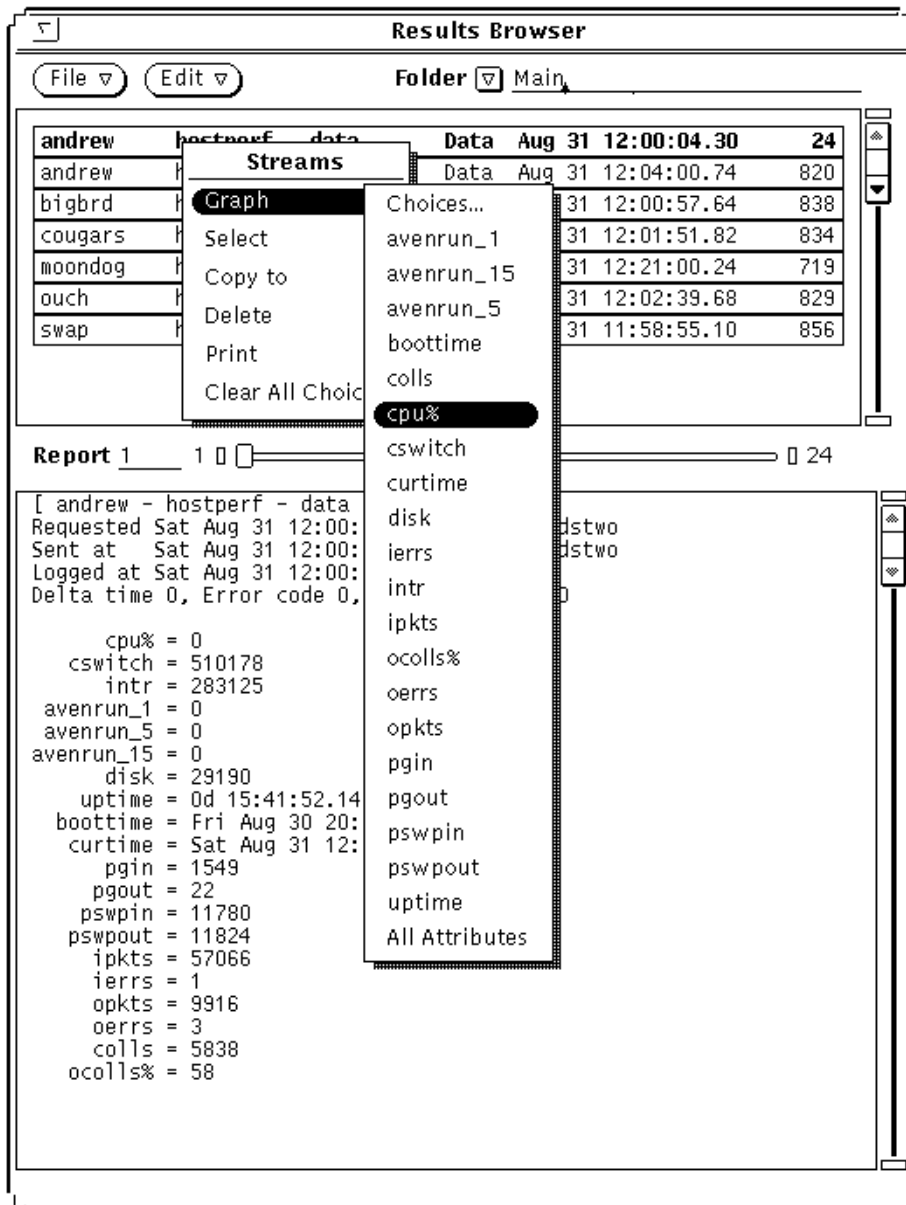


Figure 2-22 Sending Data to Grapher

After invoking the Grapher from the Browser, as shown above, you receive the window shown in Figure 2-23. The merged graph allows you to quickly compare the CPU utilization of multiple nodes.

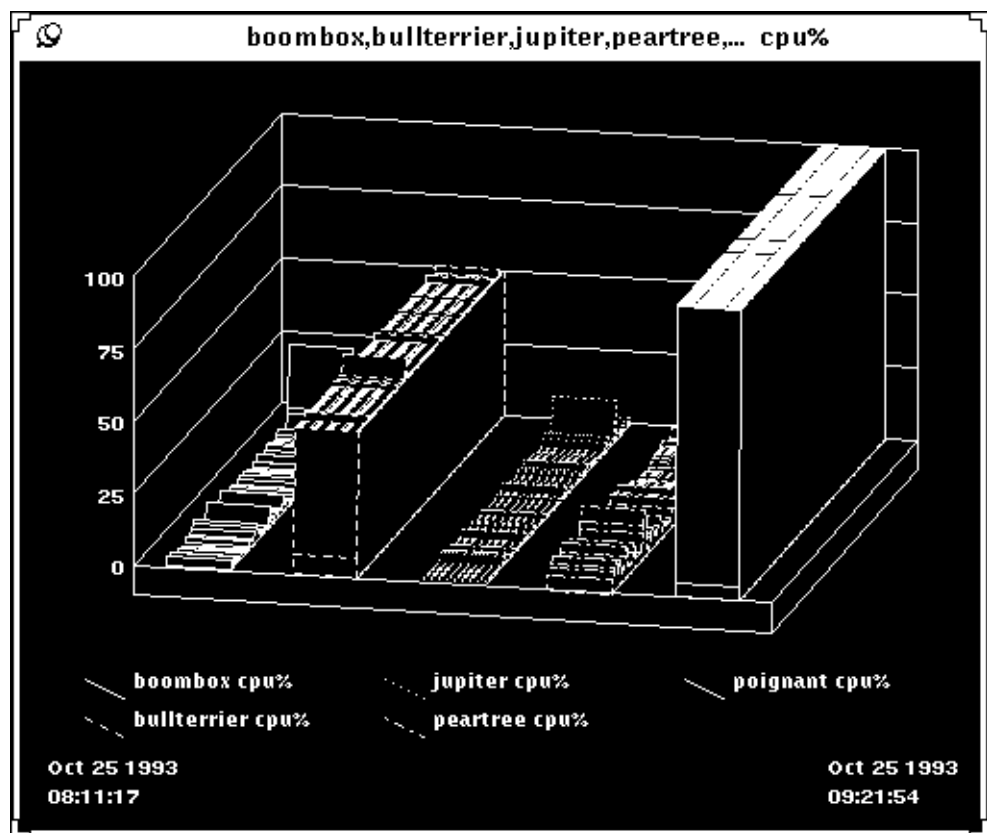


Figure 2-23 Merged Graphs

Graphing the various attributes available from the Streams>Graph menu shown in Figure 2-22 allows you to quickly assess the individual performance characteristics of each critical node, as well as determine potential problem areas for overall operation of the network. Grapher features such as “zooming” and merging can help you to refine comparisons of the data you have logged. A detailed discussion of the Grapher’s features can be found in Chapter 7 of the *SunNet Manager 2.2.3 Reference Manual*.

2.2.3 Monitoring Network Traffic Load

The use of periodic data reporting may help you to determine thresholds in capacity utilization rates or traffic levels where problems begin to occur. You can then use these known threshold levels to define event requests, so that you are notified when these conditions occur. In the example below the `traffic` agent is used to generate an event report when there is an unusually high level of activity between any two nodes on the network. In this case the particular threshold may have been determined by previous sampling of traffic levels on this network.

This event request is targeted at the Ethernet bus in each of the network's subnets. To generate this event request, you select the Ethernet bus glyph in a subnet view, and then invoke the Request Builder by selecting the Console's Requests►Send Request option. As shown in Figure 2-24, you select Event Request type, the `traffic` agent, and the `BetweenIP` group.

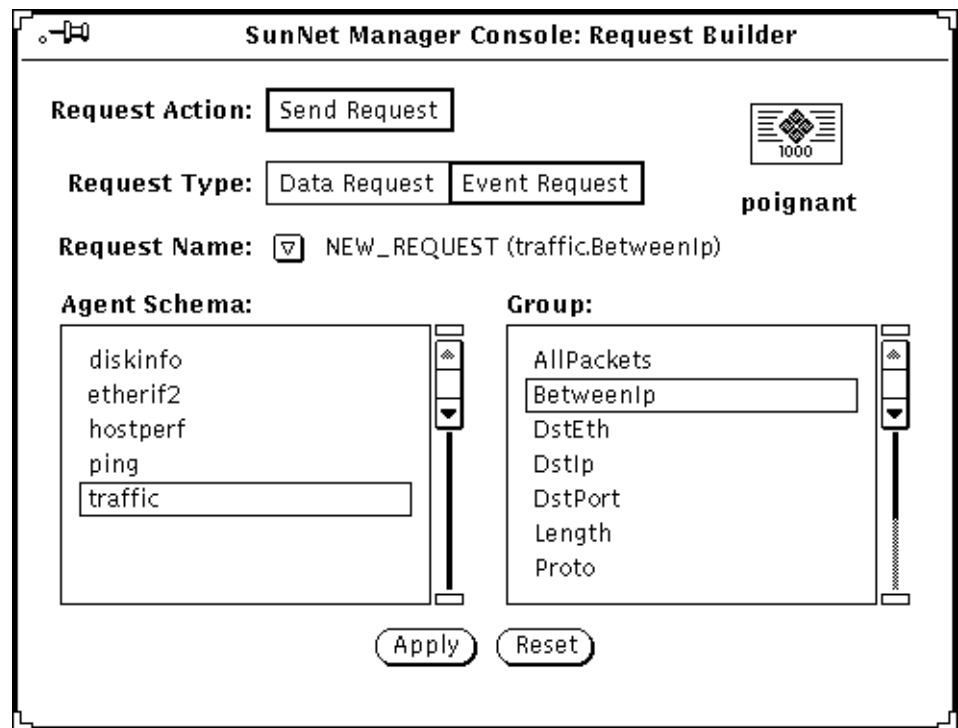
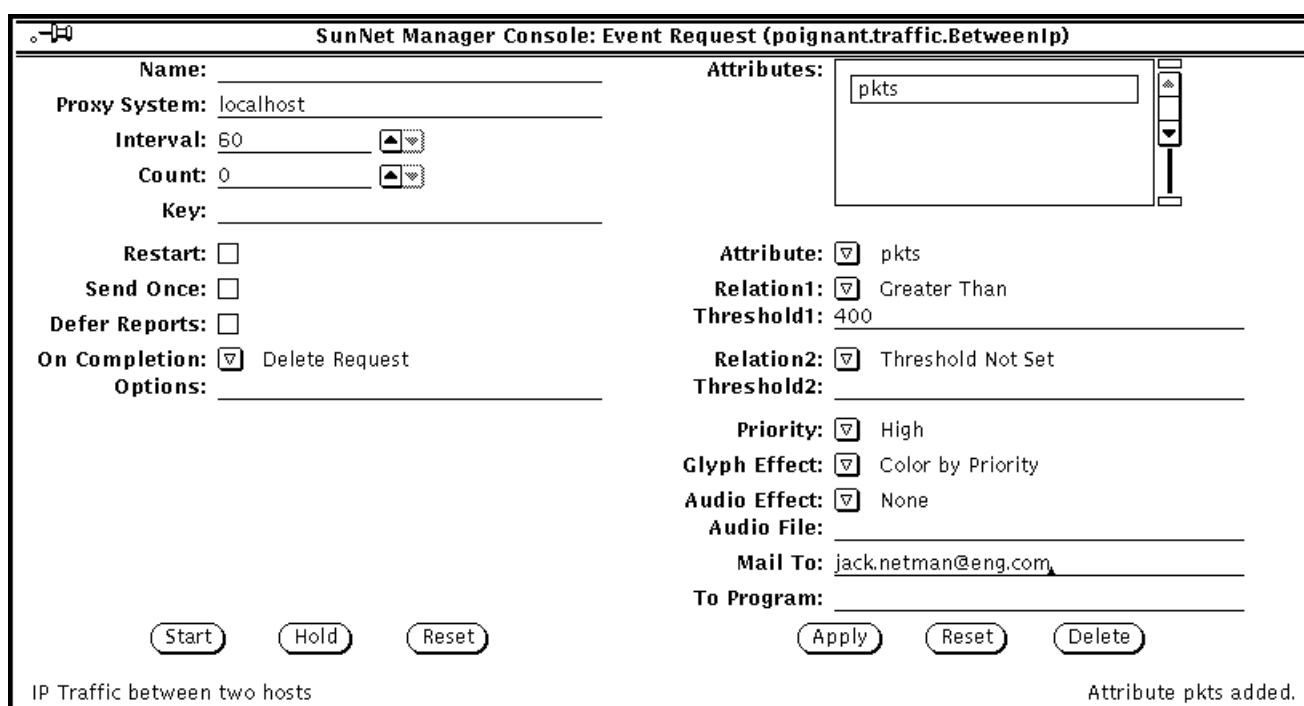


Figure 2-24 Event Request with `traffic` Agent

You click SELECT on the Apply button to invoke the Event Request Properties window, as shown in Figure 2-25.



SunNet Manager Console: Event Request (poignant.traffic.BetweenIp)

Name: _____

Proxy System: localhost

Interval: 60

Count: 0

Key: _____

Restart:

Send Once:

Defer Reports:

On Completion: Delete Request

Options: _____

Attributes: [pkts]

Attribute: pkts

Relation1: Greater Than

Threshold1: 400

Relation2: Threshold Not Set

Threshold2: _____

Priority: High

Glyph Effect: Color by Priority

Audio Effect: None

Audio File: _____

Mail To: jack.netman@eng.com

To Program: _____

IP Traffic between two hosts Attribute pkts added.

Figure 2-25 Example of traffic Event Request

In this case the fields have been filled out as follows:

- **Attribute:** Set to “pkts”.
- **Relation1:** Set to Greater Than.
- **Threshold1:** Set to 400.

From past observation of the network you may have determined that if more than 400 packets are being sent between any two nodes, this is an abnormally high rate of network activity. “Greater Than 400” thus defines the condition for an event notification being generated.

- **Glyph Effect:** Set to Color by Priority. This allows you to take advantage of the decay-to-blue feature, to indicate that this condition has occurred at some time since you last cleared an event.

- **Mail To:** You can specify your e-mail address in this field. Any e-mail message generated by this event would contain the IP addresses of the two nodes whose packet activity exceeded 400.
- **Interval:** This value is set to 60 so that the agent polls every minute to compare the result with the specified threshold value.
- **Count:** This value is left at 0 (the default) so that the event request will continue indefinitely.

When you click SELECT on the Start button you launch this request. Once you have launched this event request for the gateway node in one subnet, you can copy this request (see Figure 2-20 on page 2-29) from the subview of that node and paste it into the subview of a gateway node on each additional Ethernet subnet you want to monitor. Copying the request to the subview of an element launches a clone of that event request targeted at the node where the request has been copied.

2.3 Using Monitor to Update the Management Database

The Discover Tool provides you with a mechanism to build a hierarchy of views that represent the topology of your network. Discover's *monitor* function allows you to schedule periodic searches for new additions to the network, or nodes not uncovered previously.

Rather than burden the network with frequent Discover searches, Monitor might be scheduled to run once every week. To access the Monitor Configuration window (shown in Figure 2-26), do the following:

1. **Press MENU on the Tools button on the Console control panel to pull down the Tools menu. Select Discover.**
2. **When the Discover window appears, click SELECT on the Configuration Options button.**
3. **Press MENU on the Configuration Category button and select Monitor.**

A window like that in Figure 2-26 will appear.

Monitor Configuration

Category:

Holding Area Viewname: **Verbose Mode:** Yes No

Non-response Timeout: min **Start Time:**

Time Between Cycles: min **Stop Time:**

ICMP Timeout: sec **Start Date:**

Log History: Yes No **Stop Date:**

Log Filename: **Run Weekly:** Yes No

Mail Logfile To: **Day of Week:** Saturday

Ignore-host Filename:

Figure 2-26 Example of Monitor Configuration

When Monitor discovers new devices, it adds them to a holding area view. In Figure 2-26 this view is named “New_Devices.” In this example Monitor is configured to run weekly. You can select the day of the week Monitor will run, and define the time period for it to run on those days.

Refer to Chapter 5 of the *SunNet Manager 2.2.3 Reference Manual* for information on configuring Monitor.

Creating and Modifying the Management Database



<i>Starting the Console</i>	<i>page 3-3</i>
<i>Letting the Discover Tool Build Your Database</i>	<i>page 3-9</i>
<i>Traversing the View Hierarchy</i>	<i>page 3-14</i>
<i>Creating Elements</i>	<i>page 3-15</i>
<i>Finding Elements</i>	<i>page 3-25</i>
<i>Modifying Element Properties</i>	<i>page 3-26</i>
<i>Changing Element Types</i>	<i>page 3-28</i>
<i>Moving Elements</i>	<i>page 3-30</i>
<i>Moving Elements from One View to Another</i>	<i>page 3-31</i>
<i>Connecting Elements</i>	<i>page 3-32</i>
<i>Copying Elements</i>	<i>page 3-34</i>
<i>Deleting Elements</i>	<i>page 3-35</i>
<i>Saving the Management Database</i>	<i>page 3-36</i>
<i>Quitting the Console</i>	<i>page 3-38</i>

The SunNet Manager (SNM) Console allows you to depict the network elements that you manage in a hierarchy of glyphs (pictorial representations of network elements). This graphic representation of your management domain is reflected in the *runtime management database*, which is your entire collection of network elements, possible element types, and predefined requests, as that collection is stored on your machine.

This chapter addresses the critical tasks of how to start and quit the Console and how to create the initial runtime database. This chapter also describes the tasks of modifying the database as network elements and agents are added, deleted, or modified.

Note – All command line examples in this guide use the C-shell environment. If you use the Bourne or Korn shells, refer to the `sh(1)` or `ksh(1)` man pages, respectively, for compatibility information.

The Discover Tool is a utility that automatically finds (discovers) *physical* elements in your network and places them in the runtime database. The alternative to running Discover is to create elements one-at-a-time, using the Console's Edit►Create function.

The Discover Tool allows you to conduct “customized” searches for network elements, so that you can, for example, find all of your routers or all of the machines running SNM agents. You can also target your search to a specific subnetwork or limit your search to the set of subnetworks within a specified number of hops of your subnetwork. Discover Tool is discussed briefly in this chapter and in more detail in Chapter 5 of the *SunNet Manager 2.2.3 Reference Manual*.

3.1 Adding SunNet Manager to the Your PATH Variable

You start the SNM Console from the command line. To do this, you could type the full path name. For example, if SNM was installed on a Solaris 2.3 machine in the default location, you could enter:

```
host% /opt/SUNWconn/bin/snm &
```

However, to save yourself the trouble of typing the complete path each time you start up the SNM Console, you should set the PATH environment variable in your `.cshrc` file (or `.profile` file if a Bourne or Korn shell is used) to point to the location of the SNM executable files (the SNM Console, and tools such as Discover).

For a C-shell, enter the following in your `.cshrc` file:

For Solaris 1.x:

```
setenv PATH ${PATH}:/usr/snm/bin
```

For Solaris 2.x:

```
setenv PATH ${PATH}:/opt/SUNWconn/bin
```

If you're using a Bourne or Korn shell, consult the examples in Chapter 3 of the *SunNet Manager 2.2.3 Installation Guide*. The examples in the rest of this chapter assume that you've set the `PATH` environment variable to point to the appropriate location.

Note – If you installed SunNet Manager in a location other than the default (`/usr/snm` on Solaris 1.x machines, `/opt/SUNWconn/snm` on Solaris 2.x), you must set the environment variable `SNMHOME` to the installation directory before invoking the command to start SunNet Manager. See Chapter 3 of *SunNet Manager 2.2.3 Installation Guide* for instructions for setting this variable.

3.2 Starting the Console

You can use the `-q` option to suppress the Quick Start window. See the following subsection for details.

If no management database exists when you start the SNM Console — which is the case for first-time users—you receive a Quick Start window, shown in Figure 3-2 on page 3-7. If a database exists, you go directly to the SNM Console window (shown in Figure 3-1), skipping the Quick Start window.

3.2.1 Startup Commands

Append an ampersand (&) to your `snm` command line to put your command in the background.

To start the Console when there is no database or to restart the Console with the runtime management database from the last Console session (assuming no intervening reboot), enter

```
host% snm &
```

If there is no database present you receive the Quick Start window, described in the following subsection.

To start the Console and initialize (in effect clearing) the runtime database, enter:

```
host% snm -i &
```

After invoking this command, you receive the Quick Start window, described in the following subsection.



Caution - Use the `-i` option with care. If you have created a runtime management database in a prior Console session, the `-i` option deletes this database.

You can use the `-i` option in conjunction with the file name of an ASCII database file. For example:

```
host% snm -i /home/alex/snm/osaka.dbase &
```

The effect of a command such as the preceding is to delete a runtime database, if one exists, and to load the specified ASCII database file into the runtime database. The Quick Start window will not appear. Section 3.15, “Saving the Management Database,” on page 3-36 tells you how to save your runtime database to an ASCII file.

A variation of the preceding command example is to invoke `snm`, specifying an ASCII database, but not specifying the `-i` option. For example:

```
host% snm /home/alex/snm/osaka.dbase &
```

The effect of a command such as the preceding is to merge the specified ASCII database file into the runtime database, if one exists.

Note – If a database specified on an `snm` command line has any elements in common with an already-present runtime database, `snm` generates an error and does not load the specified database. In the Console, invoke **View**►**Error Reports** to obtain a message telling you why the load was unsuccessful.

The `snm` command has two additional command-line options, `v1` and `v2`. Use the `v1` option if you are loading database files used with SNM 1.x. Use the `v2` option only if you are loading multiple database files, one or more, but not all, of which are for SNM version 1.x. The `v2` option allows you to distinguish those files that are not from version 1.x. For example:

```
host% snm -v1 /home/alex/snm/west.dbase -v2 /home/alex/snm/osaka.dbase
```

If you enter an invalid option, `snm` displays a usage message and exits. If you enter an invalid file argument (either the file is not found or has an invalid format), you receive the SNM Console display, with a message indicating that the specified file could not be loaded.

After invoking a valid `snm` command, if you do not receive the Quick Start window, you receive the Console window such as the one shown in Figure 3-1.

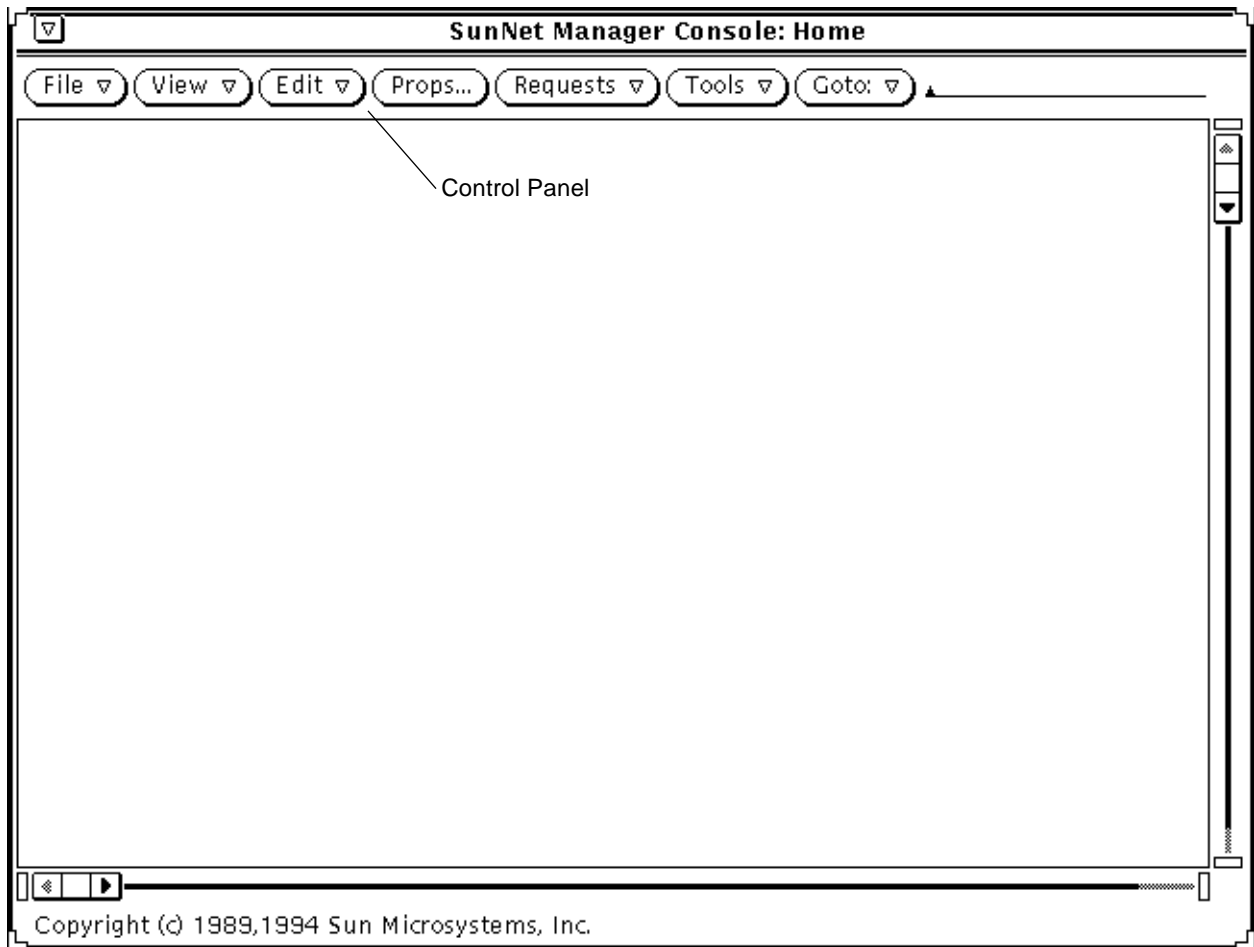


Figure 3-1 Console Window

3.2.2 Quick Start Window

After invoking SunNet Manager with the `-i` option or with no command-line arguments when there is no database present, you receive the Quick Start window shown in Figure 3-2.

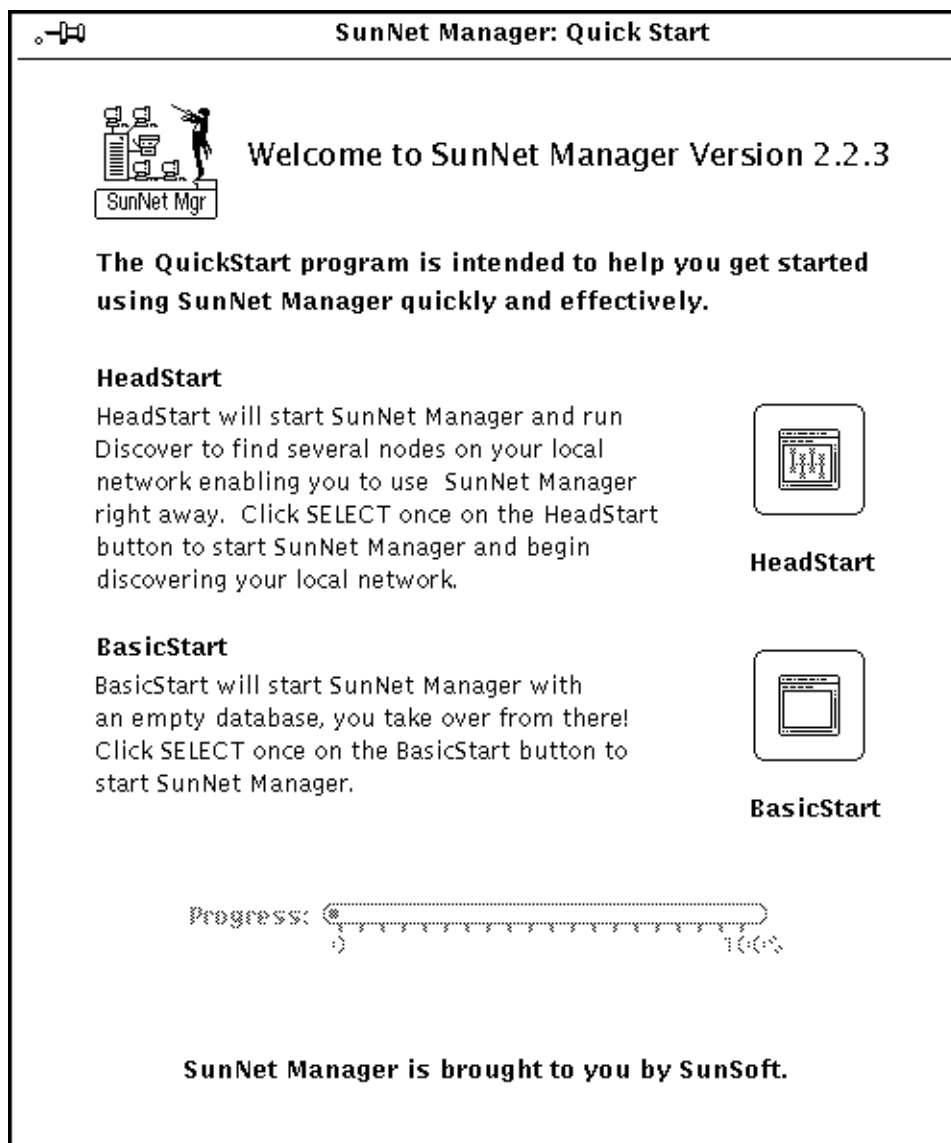


Figure 3-2 Quick Start Window

Note – You can suppress the Quick Start window by using the `-q` option. This option works when you invoke `snm` with no other options or with the `-i` option.

In the Quick Start window, you have two large buttons—HeadStart and BasicStart—to choose from. When the window first comes up, the Progress bar is dimmed. Clicking SELECT on these buttons has the following effects:

- The HeadStart button launches the SNM Console and discovers a few nodes (up to a maximum of ten) on the local subnetwork, so that you can begin using SunNet Manager immediately.
- The BasicStart button skips the discovery of local nodes, and directly invokes the SNM Console window, as shown in Figure 3-1.

The HeadStart button is the recommended choice for first-time users.

When you select either HeadStart or BasicStart, SunNet Manager loads the `snm.glue` file (a file used by SunNet Manager that you should never edit), plus the various schema files for the agents and element definitions shipped with the product. Watch the progress bar in the Quick Start window to view the progress of the files being loaded. When all of these files are in place, the Console window is displayed.

3.2.3 Notes on the Console Window

There are a number of characteristics of the Console window that you can configure. For example, you can change the text that appears in the title bar of the Console window. This and other settings are specified in the Windows category of the Console Properties window. See Chapter 9 in the *SunNet Manager 2.2.3 Reference Manual* for more information.

You initiate most SNM activities through pull-down menus accessed in the abbreviated menu buttons in the Console's control area. (See Figure 3-1 on page 3-6.) The effect of a menu selection differs depending on whether or not a glyph is selected (highlighted) in the Console window. In general, if a glyph is selected, your menu choice affects only the highlighted element. If no glyph is selected, your menu choice either affects all elements or has no consequences for any single element.

3.3 Letting the Discover Tool Build Your Database

In this section, we discuss only the discover function of the Discover Tool. This is the only function you are likely to need when you first bring up the Console. See Chapter 5 in the *SunNet Manager 2.2.3 Reference Manual* for detailed instructions on all features of the Discover Tool.

The Discover Tool, invoked from the Tools menu in the Console window or from a command line, finds subnetworks, routers, and hosts. By default, Discover limits its search to the local subnetwork to which your SunNet Manager machine (the machine on which the Console is running) is attached. Discover can be configured to extend its search beyond the local subnetwork by invoking the Discover “properties sheet,” available through the ConfigurationOptions button (see Figure 3-3). Discover Tool provides a convenient means to introduce and add elements to your database.

The Discover Tool has two functions:

- A discover function, which, from the machine on which the SNM Console is running, finds hosts, routers, networks, and Simple Network Management Protocol (SNMP) devices reachable from the Console machine. On finding a network element, Discover stores a record for that element in the runtime database.
- A monitor function, which compares the elements stored in the runtime database with the elements it finds at a specified interval or specified time. If new elements are detected, the monitor function stores elements in a holding area view (which you can name) and records these elements in a log file.

Both the discover and monitor functions have configuration windows, available through the Configuration Options button, that allow you to fine-tune the depth and breadth of the activities of the discover and monitor functions.

In general, you should have a minimum of 10-15 Mbytes of disk space available in the directory where the runtime database is stored. You can check the available disk space with the following command:

- `df -a` (if you’re running Solaris 1.x)
- `df -k` (if you’re running Solaris 2.x)

You specify the database location during installation of the SNM software or by using the environment variable `SNMDBDIR`. If you have not specified `SNMDBDIR`, then the following directory is assumed:

- `/var/adm/snm` for Solaris 1.1.1
- `/var/opt/SUNWconn/snm` for Solaris 2.3.

The disk space required may vary according to the size of the network that is being discovered. As an example, a database that contains 647 components, 9 buses, and 11 views takes approximately 3.2 Mbytes of disk space. If your runtime database grows very large, you can run out of space in your file system. This can be a problem if the `/var` directory is in the root partition, which generally does not have a large amount of free disk space. In this case, you can change the directory specified by the `SNMDBDIR` environment variable to point to another partition with more free disk space.

The new directory should be created with mode 777 so that the database files can be written to the directory. When you run the Discover Tool, both you (as user) and root must be able to write to this directory—therefore, you should locate the database on a local file system rather than an NFS-mounted file system. (NFS servers usually do not allow root users on remote machines to have write permission.)

To invoke Discover, press `MENU` on the Tools button in the Console window and release `MENU` over Discover. You see the window shown in Figure 3-3.

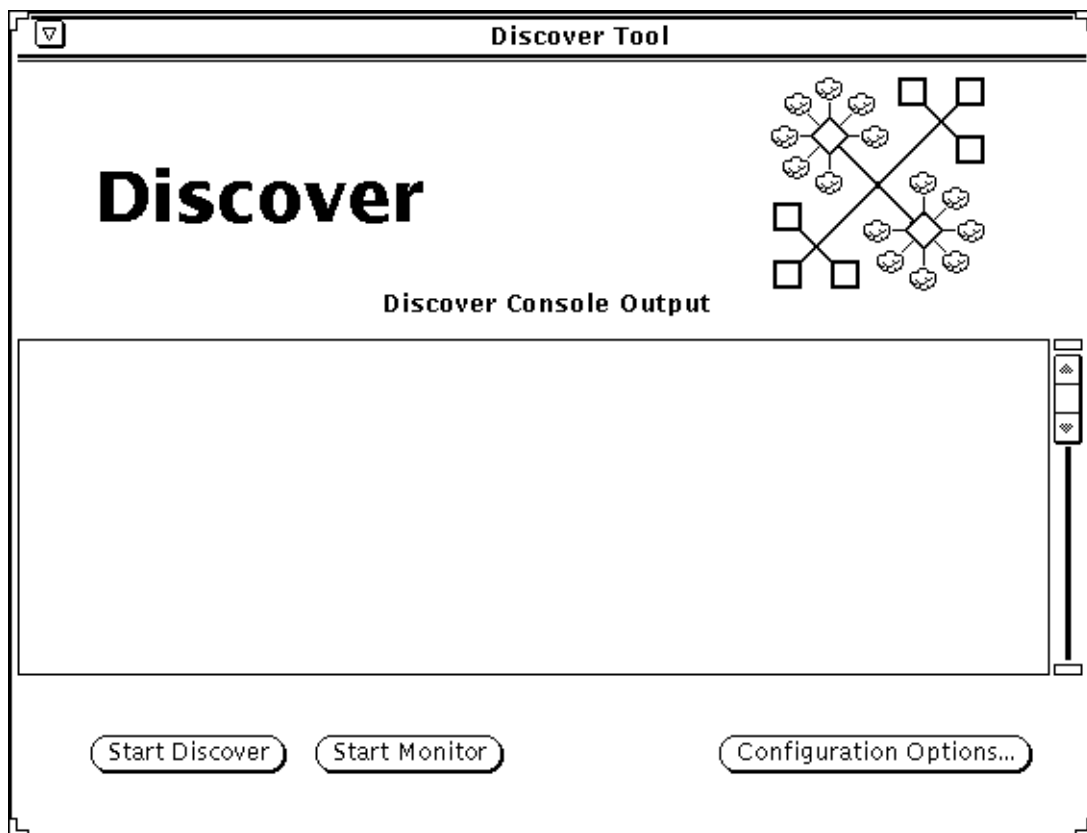


Figure 3-3 Discover Tool Window

Click **SELECT** on **Start Discover** to start the discover function. When you do, the **Start Discover** button changes to **Stop Discover**. The discover function continues to run, within the boundaries of your local subnetwork (the extent of the search is configurable), till it has found all elements within the subnetwork or till you click **SELECT** on **Stop Discover**.

As the discover function works, it reports its progress in the **Discover Console Output** window and adds elements to the current view in the **SNM Console** window. Simultaneously, it is adding these elements to the runtime database.

3.3.1 Notes

The Home view is the top level in the hierarchy of your management domain views.

As a default for the discover function, the Discover Tool finds network elements in the subnetwork to which the Console system is attached. If you enable the Discover Tool to reach beyond your local subnetwork, as it finds network elements, it constructs a hierarchy of views. You can double-click the SELECT button on each network glyph to display the elements, usually hosts and routers, contained in each of these views.

The console output section of the Discover window displays information about the program's progress.

You may want the management database to reflect logical groupings of elements. For example, you may want to have a view that only contains the routers in your management domain, or all the SNMP devices in a particular subnet. The Discover Tool has options that allow you to perform such specific groupings without difficulty. You customize Discover Tool searches by modifying the fields in the tool's "properties sheet," which is displayed when you click SELECT on the Configuration Options button. Figure 3-4 shows the Discover Tool properties sheet with the default values. Among the fields in this window we see the following:

- **Maximum Hops.** This determines how far Discover extends its search from the starting point. (By default, the starting point of the search is the subnetwork where the Console machine is located.) Number of hops is the number of routers that a message traverses to get to a given device. The default value of 0 limits the search to the local subnetwork.
- **Objects to Discover.** The options here allow you to search for all nodes, or only routers or only SNMP devices. To search for SNMP devices, make sure the correct SNMP read community string is used in order to gain access to information on SNMP devices. This is specified in the SNMP Community field.
- **Add to All Views.** This field is important if you want to partition your management database by function — for example, if you want a separate hierarchy of views for only routers or only SNMP devices. In that case, if you are doing searches to populate these views that have only certain types of devices, you will want to select "No" for this field. If you enter "No" here, then you will need to specify the name of the device-specific view in the Viewname field (for example, you might have a view named "Routers" that contains only routers).

For more details on configuring Discover, see Chapter 5 in the *SunNet Manager 2.2.3 Reference Manual*.

The screenshot shows a window titled "Discover Configuration" with a "Category" dropdown set to "Discover". The configuration is organized into two columns. The left column contains fields for "Net Name/Number" (umtv14-202-n), "Netmask" (0xfffff00), "Maximum Hops" (0), "ICMP Retries" (2), "ICMP Timeout" (1), "SNMP Retries" (3), "SNMP Community" (public), "SNMP Timeout" (2), and "Verbose Mode" (Yes/No). The right column contains "Viewname" (Home), "Add To All Views" (Yes/No), "Add Object Connections" (Yes/No), "Add Object Coordinates" (Yes/No), "Default Proxy" (localhost), and a list of "Objects To Discover" with checkboxes for "All Objects" (checked), "snm hosts", "SNMP devices", "Routers", and "Networks/Subnets". At the bottom are "Apply" and "Reset" buttons.

Field	Value
Category	Discover
Net Name/Number	umtv14-202-n
Viewname	Home
Netmask	0xfffff00
Add To All Views	Yes No
Maximum Hops	0
Add Object Connections	Yes No
ICMP Retries	2
Add Object Coordinates	Yes No
ICMP Timeout	1
Default Proxy	localhost
SNMP Retries	3
Objects To Discover	<input checked="" type="checkbox"/> All Objects <input type="checkbox"/> snm hosts <input type="checkbox"/> SNMP devices <input type="checkbox"/> Routers <input type="checkbox"/> Networks/Subnets
SNMP Community	public
SNMP Timeout	2
Verbose Mode	Yes No
Buttons	Apply Reset

Figure 3-4 Default Discover Properties

3.4 Traversing the View Hierarchy

Whenever you start the Console, the Home view is displayed. Elements that are views can contain other elements, including other views. Other types of elements, such as components, can also contain other elements. The Console keeps track of up to 16 different views or elements as they are displayed. You can traverse through the Console view hierarchy in several ways.

- If the element is a view, double-click SELECT over the glyph that represents the element to display the elements contained in the view.
- To return to any of the views that have already been displayed, press MENU on the Goto button and release MENU over the name of the view you want to display.

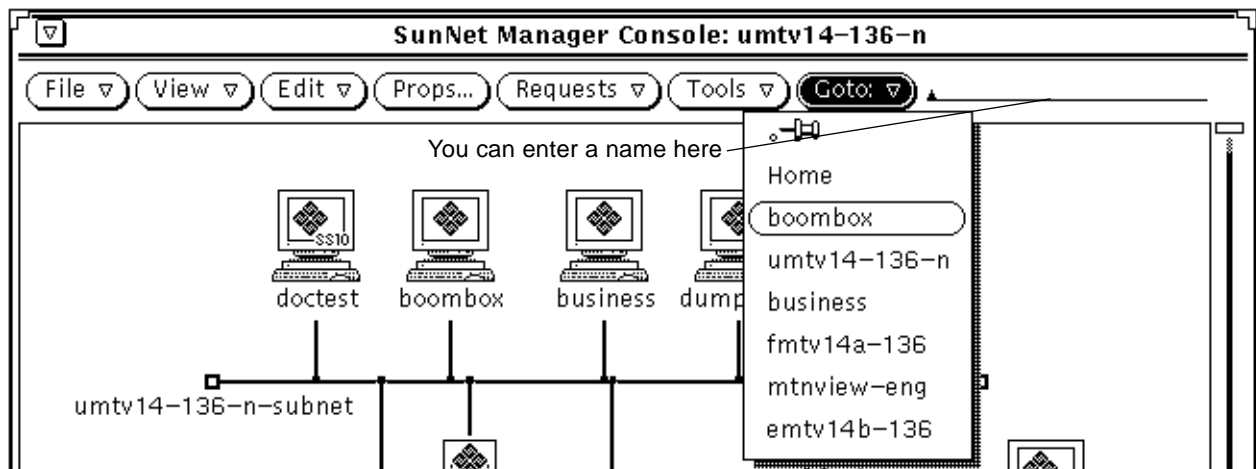


Figure 3-5 Selecting a View Name in the Goto Menu

- To return to the last view that was displayed, click SELECT on the Goto button.
- If you know the name of an element in a view, you can use the Find option in the View menu to display the view(s) that contain the particular element. See Section 3.7, "Finding Elements," on page 3-25.

- If you know the name of the view you want to see, type in the view name on the line next to the Goto button and press Return. If the view name you specify is not part of the runtime database, the Console displays a message “View name <view_name> does not exist” in the Console window footer area and leaves you in the current view.

3.4.1 Notes

To return to the Home view from any view, press MENU on the Goto button and choose the Home option. Or, you can type “Home” in the Goto line and click SELECT on the Goto button. If you often find it necessary to return to the Home view, you could have the Home view displayed whenever you click SELECT on the Goto button. This change is made in the Console Properties window Miscellaneous category. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

3.5 Creating Elements

This section describes the Console’s graphical editor function, accessible through the Edit►Create button. This function limits you to creating elements one-at-a-time. For most purposes — particularly for large networks, the Discover Tool, described in Section 3.3, “Letting the Discover Tool Build Your Database,” on page 3-9, and in Chapter 5 of *SunNet Manager 2.2.3 Reference Manual*, is a more convenient way to create elements.

You can create new elements of different types to represent particular views, networks, devices, and other components in your network. Elements are represented by glyphs, a type of icon, which appear in one or more views.

In the Console’s control area, press MENU on the Edit button to open the Edit menu. Release MENU over the Create item. (Alternatively, you can press MENU over an empty space in the view to obtain a floating popup menu. Release MENU over the Create item.) You receive the window shown in Figure 3-6.

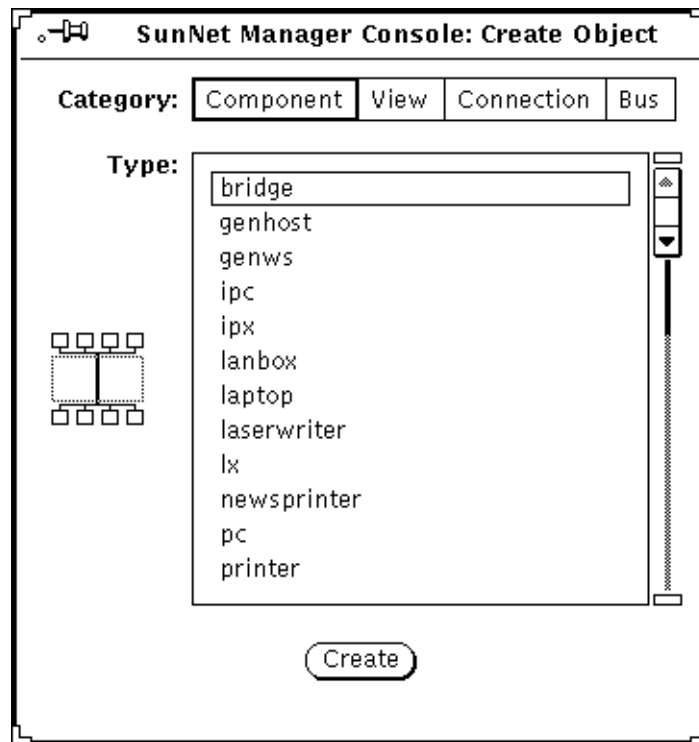


Figure 3-6 Create Object Window

Click SELECT on your choices for Category and Type, then click SELECT on Create. If you select a Component as a category, you receive the window shown in Figure 3-7.

SunNet Manager Console: New component.bridge

Name: _____

Net Address1: _____

Net Address2: _____

Contact: _____

Location: _____

Description: _____

SNMP RdCommunity: _____

<input type="checkbox"/>	diskinfo	disk space information
<input type="checkbox"/>	etherif	ethernet interface statistics
<input type="checkbox"/>	etherif2	ethernet interface statistics (Solaris
<input type="checkbox"/>	hostif	interface statistics
<input type="checkbox"/>	hostmem	memory utilization
<input type="checkbox"/>	hostmem2	memory utilization (Solaris 2.x)
<input type="checkbox"/>	hostperf	Host performance data
<input type="checkbox"/>	iostat	I/O statistics (SunOS 4.x)
<input type="checkbox"/>	iostat2	I/O statistics (Solaris 2.x)
<input type="checkbox"/>	ippath	IP path information

Red: 0 _____

Green: 0 _____

Blue: 0 _____

Apply Reset Alias... Create

This portion varies among different categories of elements

This portion is the same for all categories of elements

Alias button is greyed-out at time of creation

Figure 3-7 Object Properties Window (Component)

Help

On-line help is available for this window.

The top portion of the window in Figure 3-7 is the element data. You *must* fill in the Name field. Other fields are optional; you can use them to record information about the element for your reference. For the Name field, you can enter a valid IP address or name. If you enter a name, that name should be in a local operating-system configuration file (such as `/etc/hosts`) or in a directory service map or table. SNM does not check for the correctness of an IP

address or a name you enter until you send a request to that element after you have created it. (If the address or name is incorrect, obviously the request will be unsuccessful.)

Figure 3-7 shows the top, or data, portion of the object properties window for a component at creation time. Figure 3-8 shows the data portions of the object properties windows for the remaining element categories: view, connection, and bus.

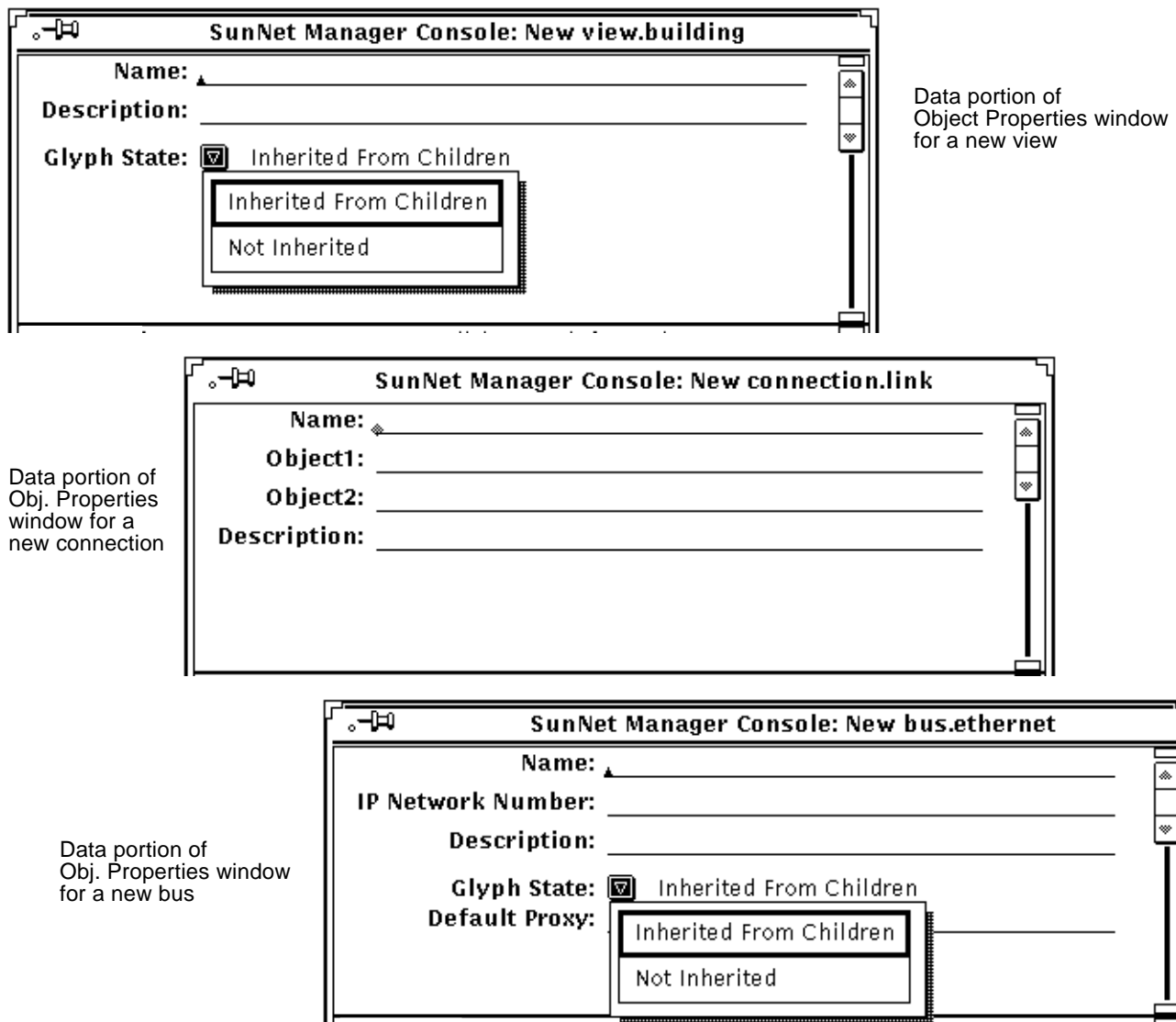


Figure 3-8 Top Portions of Object Properties Windows

The middle portion of the new-element window is the list of agent schema files that the Console knows about. This and the bottom portion are the same for all categories of elements and is shown in Figure 3-7.

In the middle portion, click SELECT on the box to the left of a listed schema to toggle a check mark—this specifies that the element can be managed with this schema. Check all schemas that apply to the element. The line to the right of some schema names indicates that a proxy system may be defined. If you do not define a proxy system, the default proxy system will be the system on which you are running the Console.






Note – Merely checking a schema does not make the element manageable from the Console; the appropriate agent software must be installed and running on the target system. See Chapter 4 of the *SunNet Manager 2.2.3 Installation Guide* for instructions on running the `getagents` script to install agents. The exceptions to this are the `hostperf` and `ping` proxy agents. On most Sun and many other vendors' machines on a TCP/IP network, you can check off the `hostperf` and `ping` agents and use the Console machine (`localhost`) as the proxy.

The bottom portion of the Properties window allows you to specify a color for the glyph associated with the element.

When you finish entering data and making selections in the new-element window, click SELECT on Apply. A glyph for the element you just defined appears in the current view with the name you specified.

Note – The glyphs in Table 3-1 are used for more than one type of element.

Table 3-1 Glyphs Used for Multiple Element Types

Glyph	Element Category	Element Type
	Component	ss330 ss370 sun-deskside
	Component	sun-server sun470
	Connection	link rs232

3.5.1 Notes

The IP address field in the Properties window for the element is not used to manage the device—it is for your information only.

The blank line next to some agent schema names allows you to specify the name of the system on which the proxy agent resides. This system name is for a default proxy system. You can specify a different proxy system name for data reports and when specifying events. If you do not specify a proxy system in the Properties window or in the report request, the system on which the Console is running is assumed to be where the proxy agent resides.

You can create an element that will logically contain other elements. For example, if managing all the file servers in your management domain is important, you may want to create a view called File Servers. To do so, perform the following steps:

1. Create an element of category **View**, as described previously.
2. Double-click **SELECT** on the new glyph.

- 3. In the empty view, create the element instance for each device. If the element instance definition already exists, copy the glyph into the view. (See Section 3.13, “Copying Elements,” on page 3-34.)**

You can change the font used for the labels under element glyphs. This is done in the Console Properties window. (If you change the font, you must restart the Console for the change to take effect.) See the description of the Icon Font setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

3.6 *Creating Aliases*

SunNet Manager has an alias feature that allows you assign multiple names to an element. This feature is useful with machines that have multiple network interfaces (usually routers). You can use an alias in the same way that you use element names. That is, you can search on an alias or send requests that specify an alias.

Note – If you use unique names for each interface, the Discover Tool fills in aliases automatically when it creates a router. The discover function part of that tool fills in the first name it finds as the name of the element and the names of subsequently-found network interfaces as aliases.

To add one or more aliases for an element, do the following:

- 1. Press MENU over the glyph to which you want to add aliases.**

You can also click SELECT on the glyph to highlight it, then press MENU over the glyph.

You receive the properties window for that element, such as the one shown in Figure 3-7 on page 3-17.

- 2. In the properties window, click SELECT on the Alias button.**

You receive the window shown in Figure 3-9.

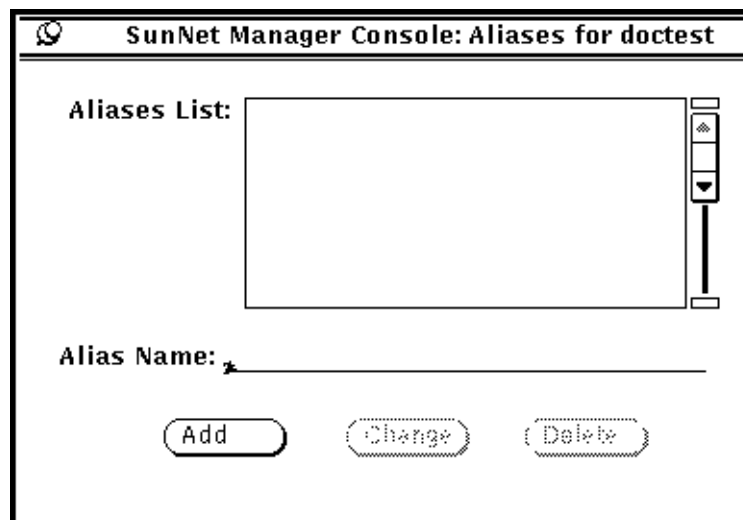


Figure 3-9 Alias Window

3. Enter a name and click SELECT on Add.

The name you entered appears in the Aliases List.

To change or delete an alias, click SELECT on the alias in the Aliases List, then click SELECT on Change or Delete.

The same rules apply to aliases as to element names, as specified in Section 3.5, "Creating Elements": you can use an IP address or a name.

The properties window for a router has two IP address fields. For example:

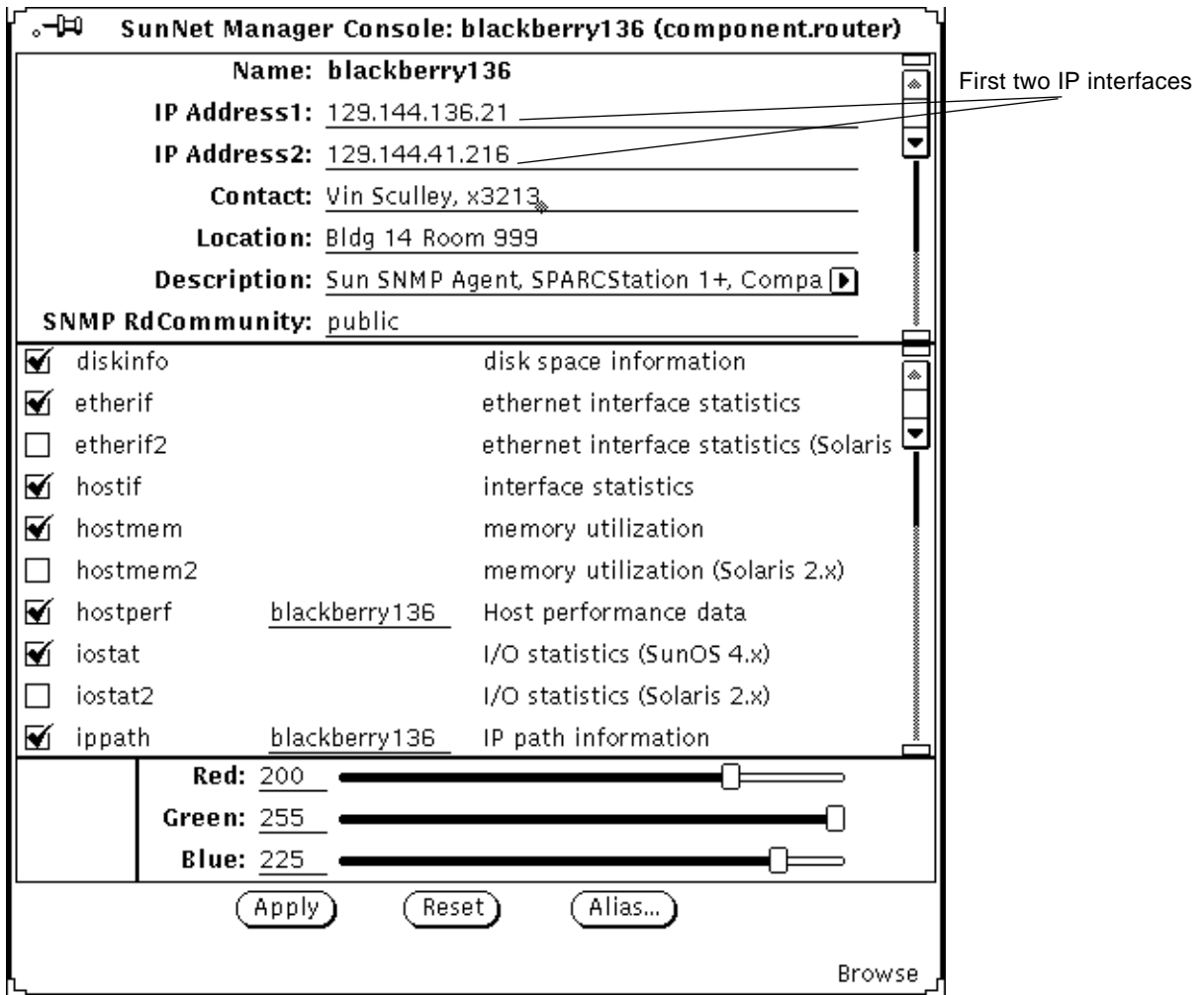


Figure 3-10 Properties Window for Router

You are not, however, limited to managing the two interfaces identified in the IP Address fields. The alias feature allows you to add a name for each interface on a machine. As noted above, the Discover Tool does this automatically.

3.7 Finding Elements

The Find option of the View menu displays the view(s) in which a specified element is located.

1. In the Console window, invoke **View**►**Find**.

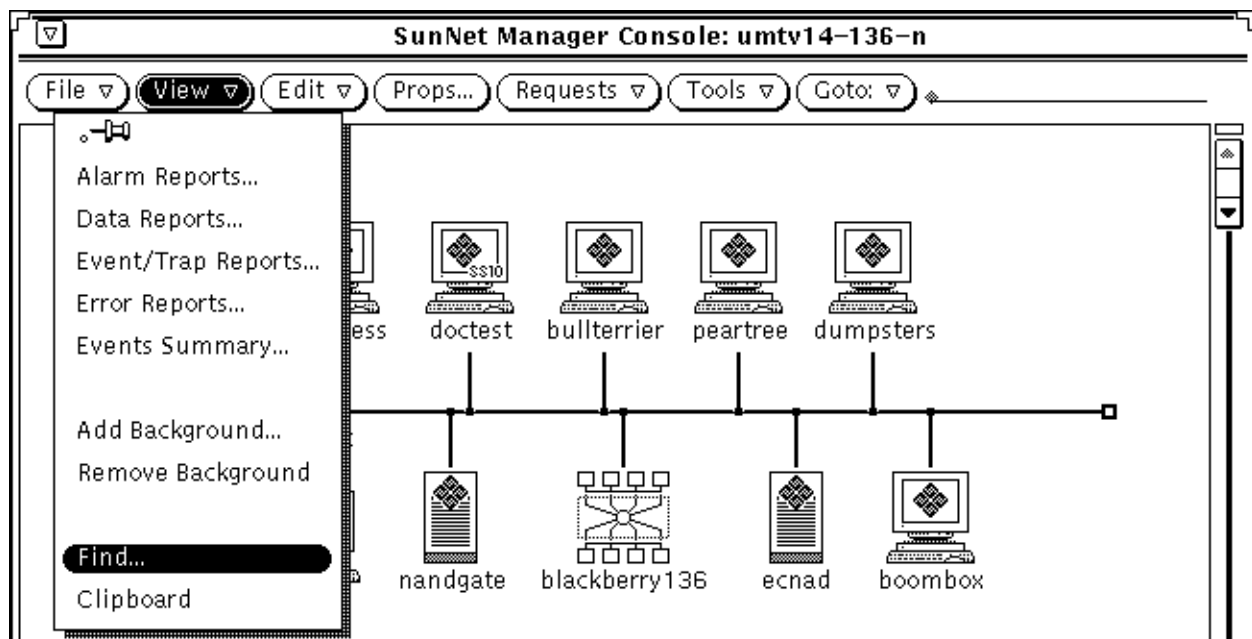


Figure 3-11 Selecting the View—Find Menu Item

2. In the Find window, enter the name of the element you want to find.

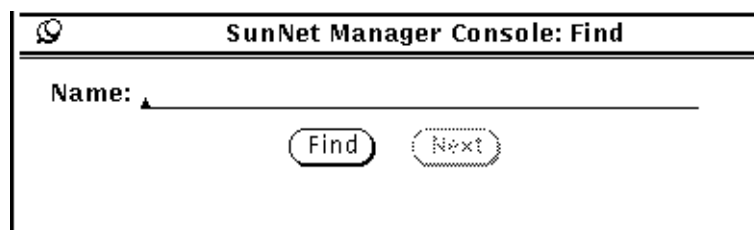


Figure 3-12 View—Find Window

3. Click **SELECT** on the Find button in the window or press **Return**.

3.7.1 Notes

If an element is found, the Console displays the view in which the element is located and the element is highlighted. If the element appears in more than one view, the Next button displays normally (not greyed-out). Click SELECT on the Next button to see the next view in which the element is located.

You can also use the Find function key on the left side of your keyboard to display the Find window.

SNM has an alias feature that allows an element to have multiple names. You can use the Find feature to search on any of the names associated with an element.

3.8 Modifying Element Properties

The properties of an element instance that can be modified in the element's properties sheet are the agent schemas that apply to the element, the color of the element, and the information in the optional fields. Chapter 2 of the *SunNet Manager 2.2.3 Reference Manual* describes the fields in the Properties window. Note that you cannot modify the name of an element instance once it has been created. To rename an element instance, you must delete and re-create it with the new name.

- 1. Over the glyph that represents the element that you want to modify, press MENU to open the Glyph menu.**
Alternatively, click SELECT on the glyph and press the Props button on the left side of your keyboard.
- 2. Release MENU over Properties to open the Properties window for the element.**

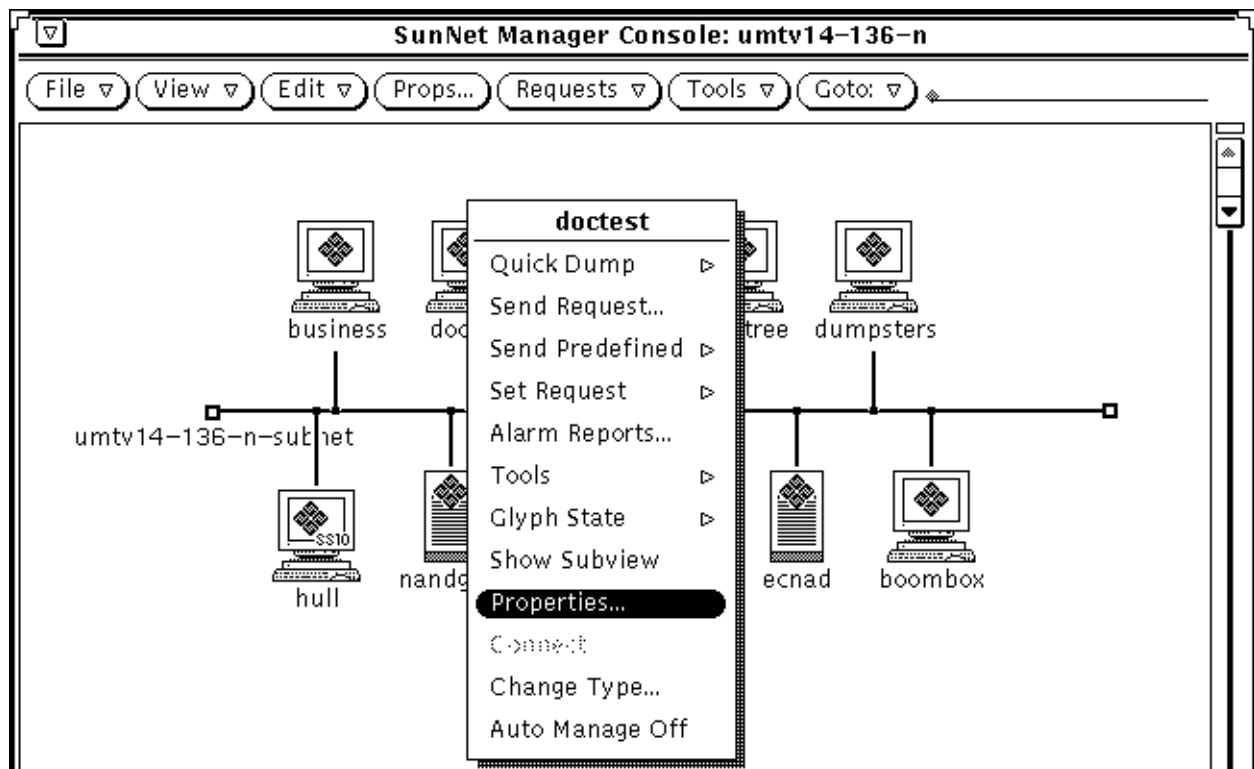


Figure 3-13 Selecting the Glyph—Properties Menu Item

3. Modify the fields within the Properties window for the element, as you want.

See Figure 3-7 on page 3-17 and Figure 3-8 on page 3-19 for examples of Properties windows.

4. Click SELECT on the Apply button to incorporate the changes to the element.

3.9 *Changing Element Types*

SNM has four categories of elements: component, view, bus, and connection. See Figure 3-6 on page 3-16. Of these categories, only an element in the component category allows for a change of type. A partial list of the types is visible in Figure 3-6. You might find it useful to change the type of a component. To do so, perform the following steps:

- 1. Over the glyph that represents the element that you want to modify. Press MENU to open the Glyph menu.**
- 2. Release MENU over Change Type. You receive the following Change Type window shown in Figure 3-14.**

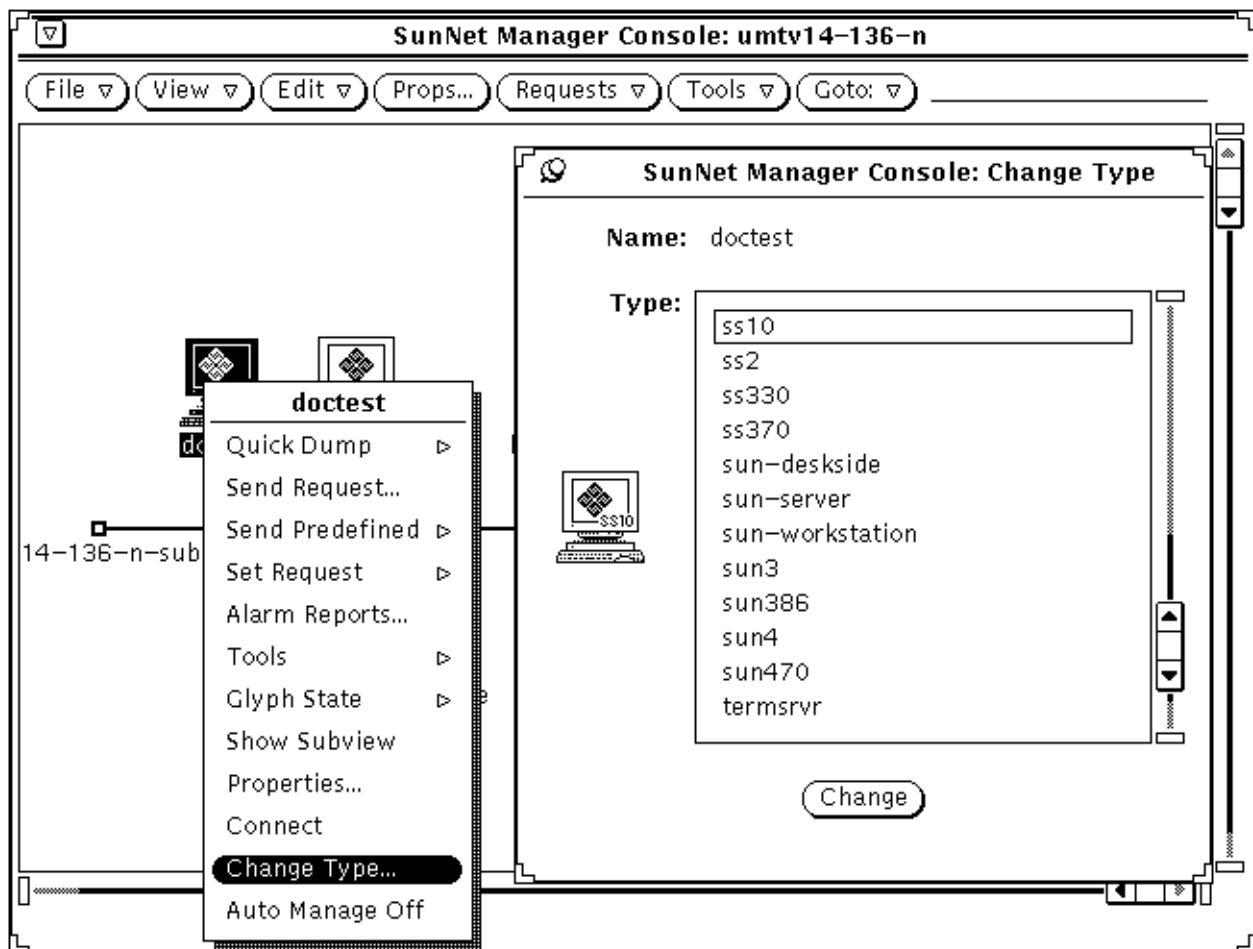


Figure 3-14 Change Type Window

3. Click **SELECT** on the new element type and click **SELECT** on **Change**. At this point, the Change Type window disappears and the changed element appears in the Console window represented by its new glyph.

3.9.1 Notes

You can change element types only for components, such as workstations, servers, printers. These types are displayed in the Type menu in the Change Type window, such as the one shown in Figure 3-14. You cannot change elements of category view, bus, or connection.

As the Discover Tool finds network elements, it distinguishes among machines running SNM agents, SNMP devices, routers, and networks and subnetworks. (You can, in fact, restrict the Discover Tool's search to one or any combination of these types of objects.) The first three object types are in the component category of SNM elements. The last, networks and subnetworks, are in the view category and cannot be changed.

3.10 Moving Elements

You can move an element within a view or from one view to another.

3.10.1 Moving Elements within a View

- 1. Over the glyph that represents the element to be moved, press SELECT to highlight the glyph.**
If you wish to move multiple elements at the same time, click ADJUST on subsequent glyphs.
- 2. Drag the mouse pointer to the desired new location and release.**

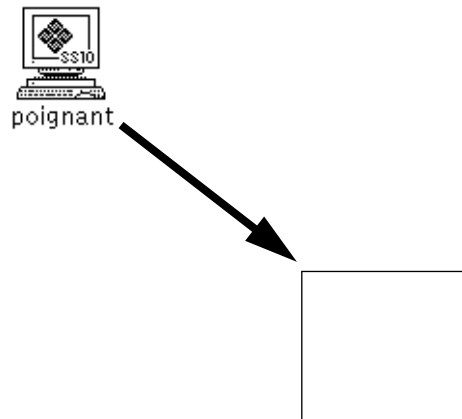


Figure 3-15 Moving a Glyph to a New Location

3.11 Moving Elements from One View to Another

1. **Over the glyph that represents the element to be moved, click SELECT to highlight that glyph.**

To move multiple elements at the same time, click ADJUST on subsequent glyphs.

2. **In the control area of the Console window, invoke Edit►Cut.**

Or, press MENU over an empty space in the view to open the Edit menu as a floating popup menu. Release MENU over Cut.

3. **Use the Goto button in the Console's control area to switch to the view where the glyph(s) will be moved.**

See Section 3.4, "Traversing the View Hierarchy," on page 3-14.

4. **In the Console's control area, invoke Edit►Paste.**

When you cut or copy an element or set of elements, the element(s) are stored in the clipboard, a staging area for subsequent paste operations. To view the contents of the clipboard, in the Console window, press MENU on View►Clipboard and release MENU.

3.11.1 Notes

You can also use the Cut and Paste function keys on the left side of your keyboard instead of Edit menu functions.

You cannot cut an element with an associated request, nor delete an element that contains another element in its subview.

3.12 *Connecting Elements*

You can draw a connection from a selected (highlighted) element to the element glyph where the mouse pointer is located.

1. Click **SELECT** over one of the elements to highlight it.
2. Over the other element (the element to be connected to), press **MENU** to open that element's **Glyph Menu**.
3. Release **MENU** over **Connect**.

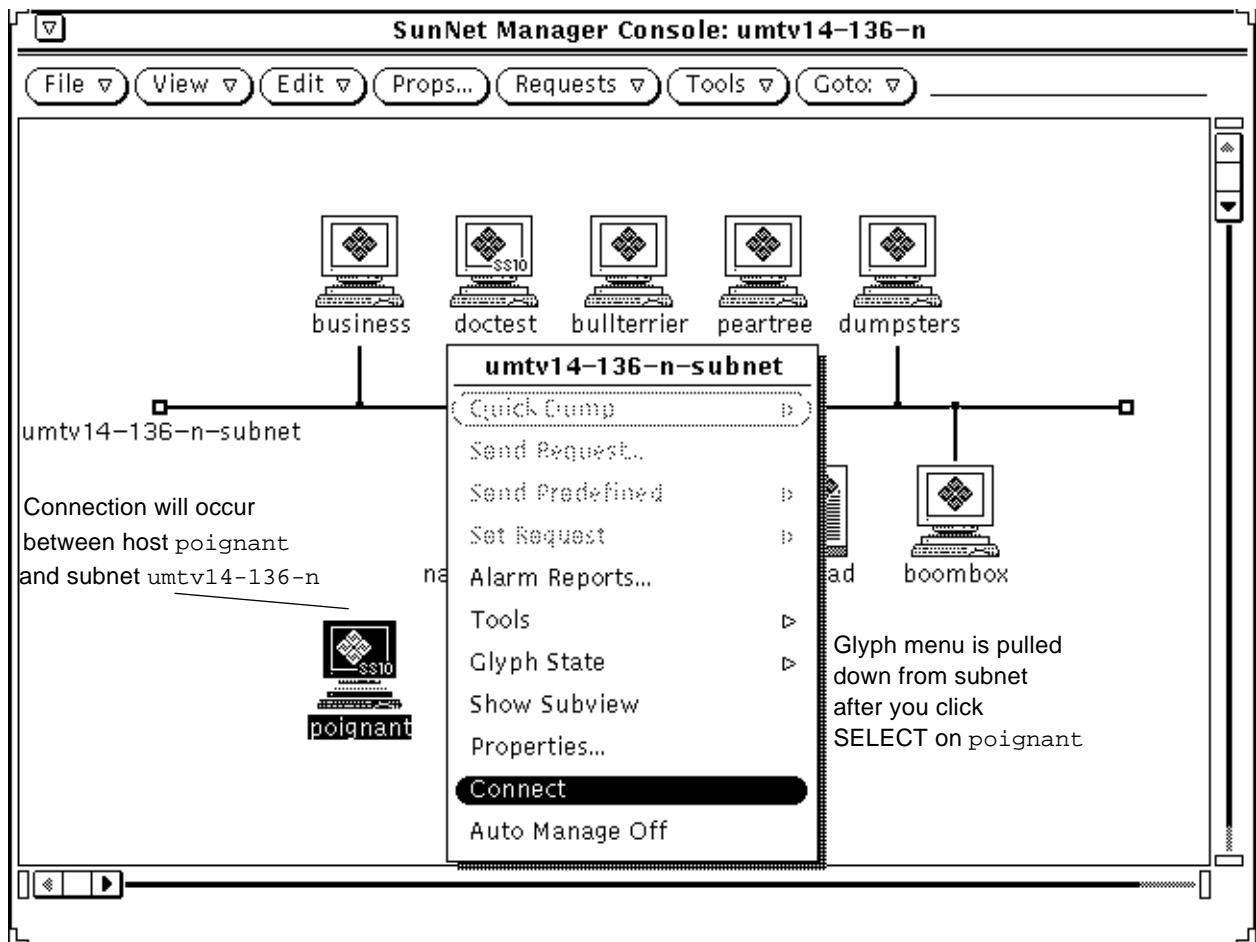


Figure 3-16 Glyph—Connect Example

3.12.1 Notes

These connections should not be confused with the Connections element type category, which includes RS-232 connections and other links. The connections described in this task are also known as “simple” connections. They are *not* elements and cannot be managed. Simple connections are useful only in graphically representing connectivity between elements.

When either of the connected elements is moved, the connection moves also.

The color of the connection is based on the color of the second, “connected to” element. Whenever you select (highlight) this element, the connection is also highlighted.

3.13 Copying Elements

Once you have created an element, you can create many instances of that element in various views in your database. To do this, you copy the element from one view to another.

When you cut or copy an element or set of elements, the element(s) are stored in the clipboard, a staging area for subsequent paste operations. To view the contents of the clipboard, in the Console window, press MENU on View▶Clipboard and release MENU.

1. **Click SELECT on the glyph that represents the element to be copied to highlight it.**
If you wish to copy multiple elements in a view at the same time, click ADJUST on subsequent glyphs.
2. **In the control area of the Console window, invoke Edit▶Copy.**
Alternatively, you can press MENU over an empty space in the view to open the Edit menu as a floating popup menu.

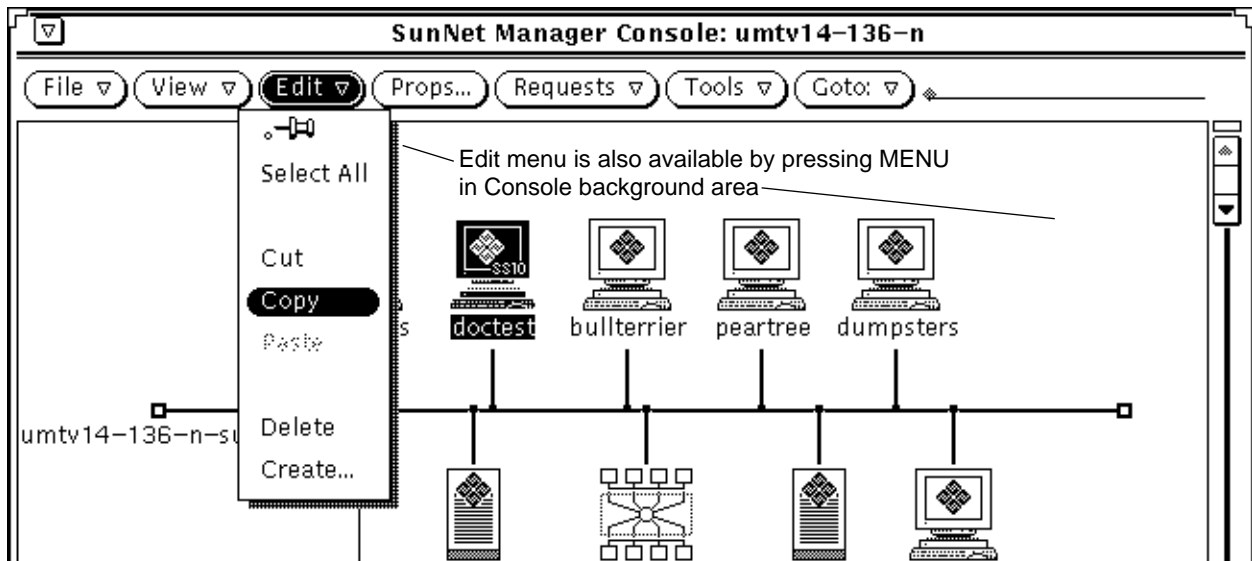


Figure 3-17 Selecting the Edit—Copy Menu Item

3. Use the Goto menu to move to the view to which the element will be copied.
4. Invoke Edit►Paste (from the Edit button or from a floating popup menu in an empty space in the new view).

3.13.1 Notes

You can use the Copy and Paste function keys on the left side of your keyboard instead of the Edit menu functions.

The Copy function copies the element into the Console clipboard. Once an element has been copied into the clipboard, it can be pasted into as many views as needed.

If an element and the view into which it will be copied are both displayed in the same view, you can use the Console's "drag and drop" function:

1. Press SELECT over the glyph that represents the element to be copied to highlight it.
2. While still pressing the SELECT mouse button, drag the mouse pointer to the glyph that represents the view to which the element will be copied. Then, release the mouse button.

3.14 Deleting Elements

You can delete an element instance from a view.

When you cut or copy an element or set of elements, the element(s) are stored in the clipboard, a staging area for subsequent paste operations. To view the contents of the clipboard, in the Console window, press MENU on View►Clipboard and release MENU.

1. Click SELECT over the glyph to be deleted to highlight it.
If you wish to delete multiple elements at the same time, click ADJUST on subsequent glyphs.
2. In the Console's control area, invoke Edit►Delete.
Alternatively, you can press MENU over an empty space in the view to open the Edit MENU as a floating popup menu.

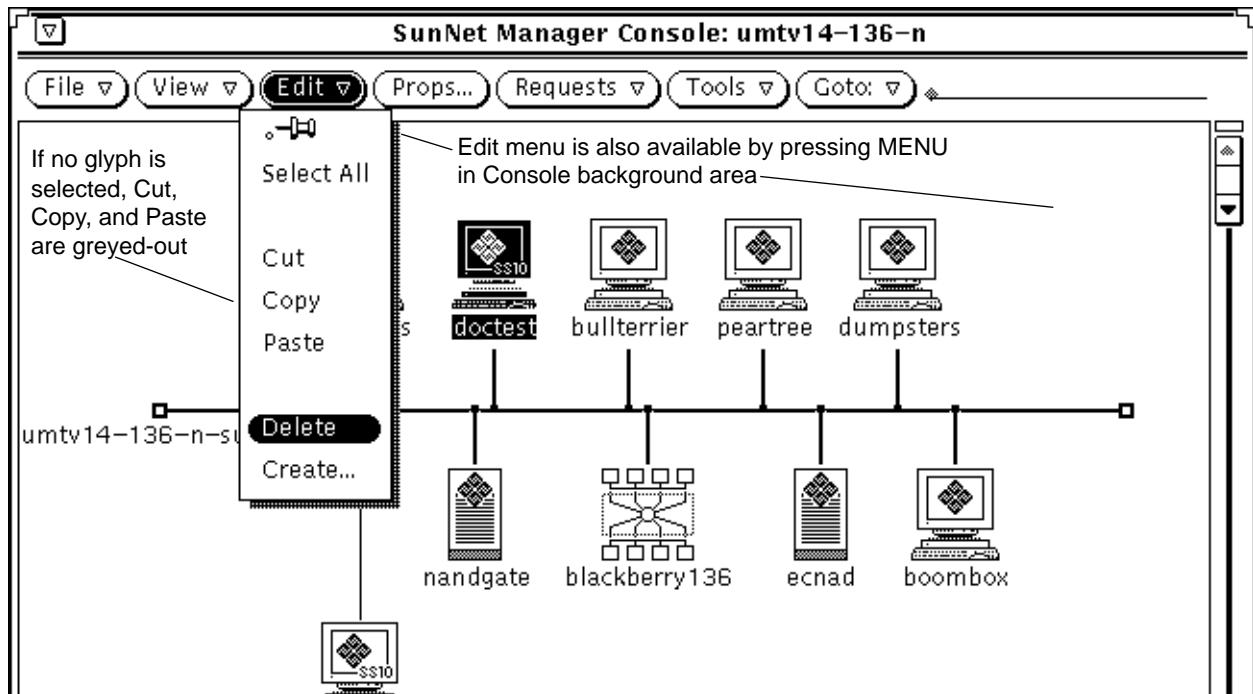


Figure 3-18 Selecting the Edit—Delete Menu Item

3.14.1 Notes

You cannot delete an element that has a request associated with it. You also cannot delete an element that contains another element in its subview.

The Cut option of the Edit menu removes an element from a view and places it in a clipboard, but the Delete option removes the element from the view but also from the database. The Delete option does not place an element in the clipboard so you cannot paste a deleted element.

3.15 Saving the Management Database

The runtime database contains element and request instances that you have created. This runtime database can be saved to an ASCII file, allowing you to reinvoke the SNM Console with the same database.

1. In the Console window, press MENU on File►Save►Management Database and release MENU.

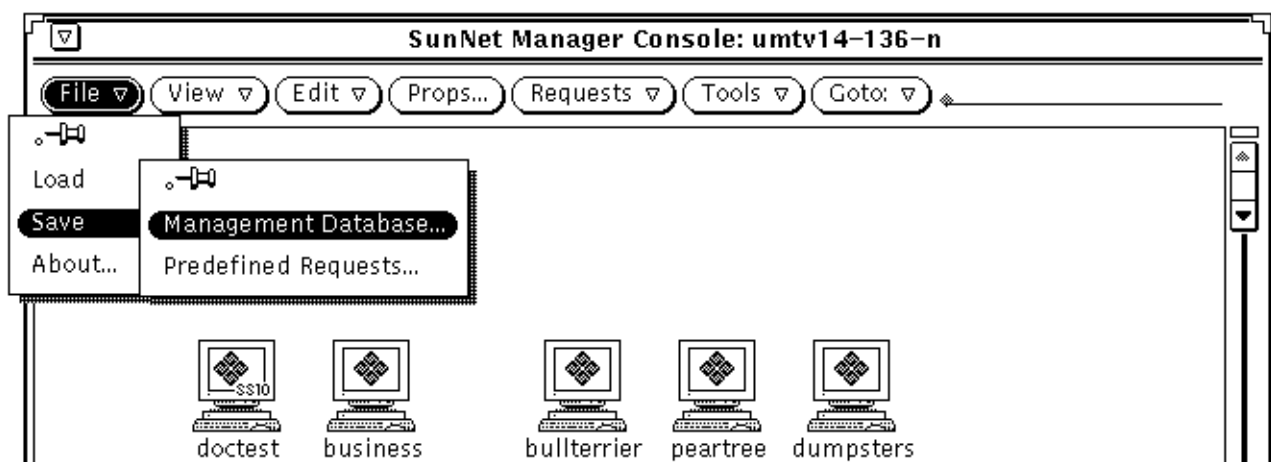


Figure 3-19 Selecting the File—Save—Management Database Menu Item

Help

On-line help is available for this window.

2. In the Save popup window, enter the directory and file name in which you want the management database stored.
3. Click SELECT on the Save button to store the database to the file.

3.15.1 Notes

When you invoke File►Save►Management Database, SNM takes a snapshot of the current database and stores it in a single, ASCII file. Note that the structure of this stored database—a single file—is entirely different from the structure of the runtime database. The runtime database consists of a set of special database files under a directory name having the following form:

- `/var/adm/snm (or $SNM_HOME)/db.<login> (or db.<$SNM_NAME>)` for Solaris 1.1.1
- `/var/opt/SUNWconn/snm (or $$SNM_HOME)/db.<login> (or db.<$SNM_NAME>)` for Solaris 2.3

Assuming `/var` is for files that grow and because a saved ASCII database is static and possibly large, it is recommended you not store the ASCII files under `/var`.

When restarting the Console, you may specify whether to continue to use the runtime database from the previous run of the Console, or to reinitialize the database from ASCII structure and instance files. See the section Section 3.2, “Starting the Console,” on page 3-3 in this chapter for instructions for reinitializing the database.

3.16 Quitting the Console

You quit a Console session by using the Quit option of the Console’s window menu.

1. In the title bar of the Console window, press **MENU** and release **MENU** over **Quit**.
2. If there are any active requests, you will see the following popup verification window:



Figure 3-20 Console—Quit Window

You can click **SELECT** on one of the following:

- **Quit**, to have the Console kill all active requests before stopping.
- **View Requests**, to display the Request Viewer window.
- **Resume**, to continue running the Console.

3.16.1 Notes

When you quit a Console session, the verification window is displayed by default if there are any active requests. You can choose to have the verification window *always* displayed or *never* displayed—this is specified in the Console

Properties window, under the Miscellaneous category. See the description of the Verify Quit setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

Requesting Data from Agents



<i>Making a One-Time Request for Data</i>	<i>page 4-2</i>
<i>Requesting Periodic Data</i>	<i>page 4-6</i>
<i>Copying Requests</i>	<i>page 4-13</i>
<i>Viewing Incoming Data</i>	<i>page 4-14</i>
<i>Analyzing Stored Data</i>	<i>page 4-22</i>
<i>Modifying the Display of a Graph</i>	<i>page 4-31</i>
<i>Printing a Graph</i>	<i>page 4-33</i>

You can request an agent return values for some or all attributes in a single agent group. Your request can either be for a single, quick snapshot of all the values in the agent group, or it can be a request for periodic reporting of one or more attribute values. For the latter type of requests, you can specify report characteristics such as:

- number of reports from the agent
- interval between reports
- whether the reports should be stored in a file
- whether the attribute values reported should be displayed graphically

This chapter describes how to request data reports from agents and how to view or analyze the returned data.

4.1 *Making a One-Time Request for Data*

A Quick Dump retrieves all the values in an attribute group for a target system. You can initiate a Quick Dump request in one of two ways.

4.1.1 *Quick Dump via the Console Requests Menu*

1. Click **SELECT** over the glyph that represents the target element.
2. Press **MENU** on the Requests button in the SNM Console.
3. Release **MENU** over **Quick Dump** to receive a Request Builder window such as the one shown in Figure 4-1.

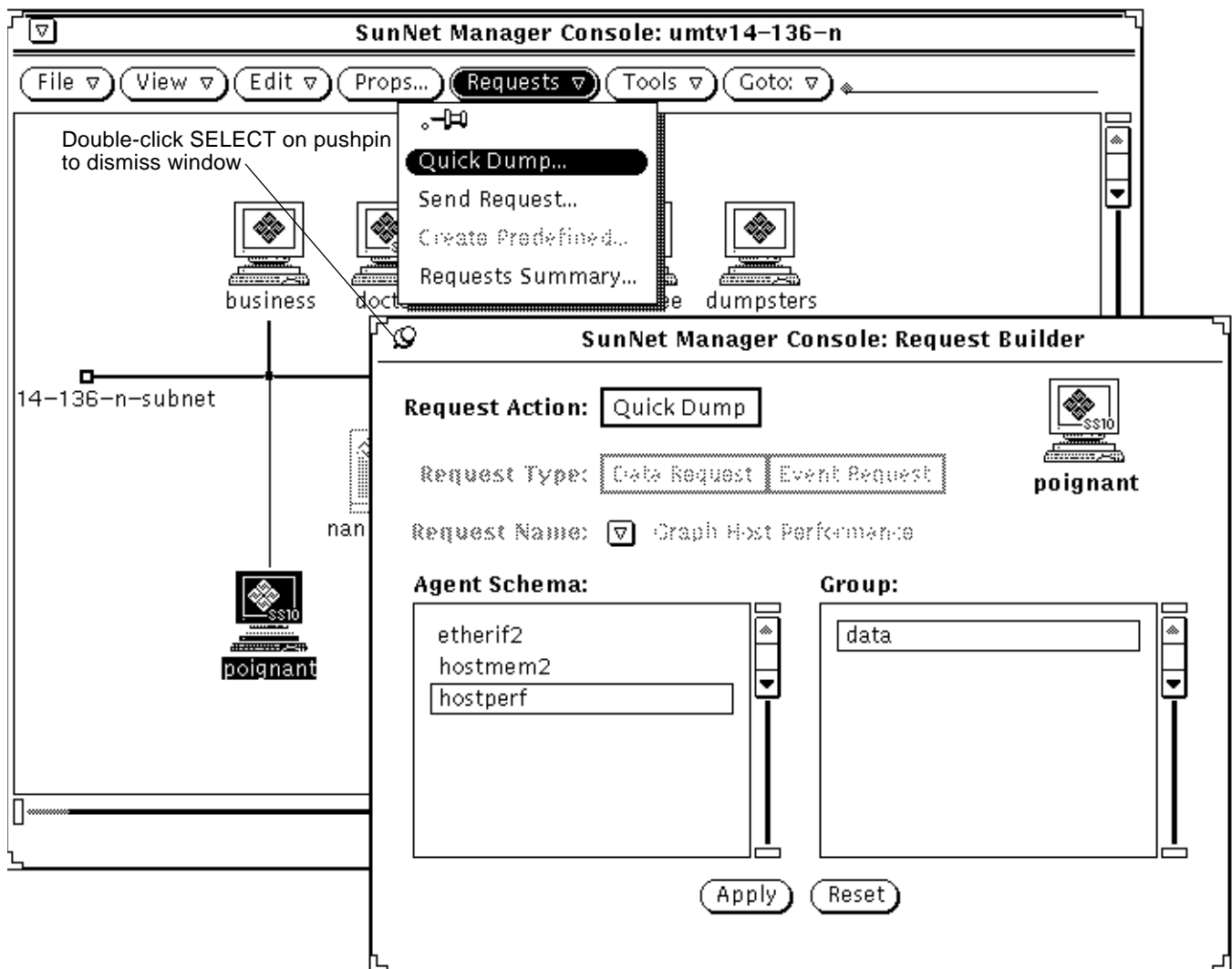


Figure 4-1 Requests Menu—Quick Dump Request

4. In the Request Builder window, click **SELECT** on, first, the Agent Schema, and, second, the Group you want for that schema. Click **SELECT** on **Apply** to send the request.

Clicking on Apply dismisses the Request Builder window. Within seconds you receive a Quick Dump Report window, as shown in Figure 4-3.

5. To dismiss the Quick Dump Report window, double-click **SELECT** on the pushpin in the upper left corner as shown in Figure 4-1.

4.1.2 Quick Dump via the Glyph Menu

The glyph does not have to be highlighted for you to obtain the glyph menu.

1. Press **MENU** over the glyph that represents the target element to open the **Glyph menu** for that element.
2. Press **MENU** over **Quick Dump** and drag right over the desired agent name and attribute group name as shown in Figure 4-2.

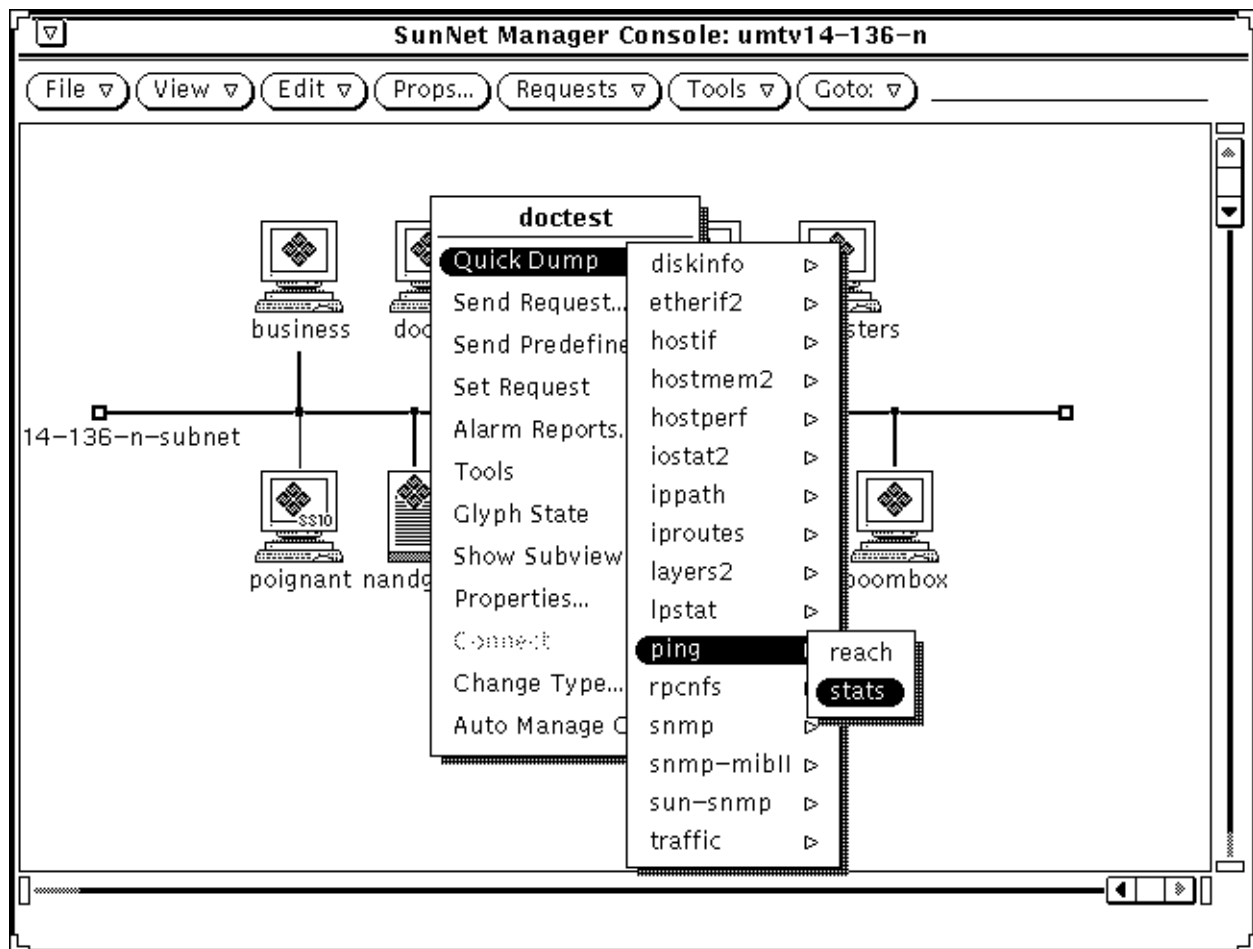


Figure 4-2 Glyph Menu—Quick Dump Request

Releasing MENU on the attribute group name starts the Quick Dump request. Within seconds you receive a Quick Dump Report window, as shown in Figure 4-3.

3. To dismiss the Quick Dump Report window, click SELECT on the pushpin in the upper left corner as shown in Figure 4-3.

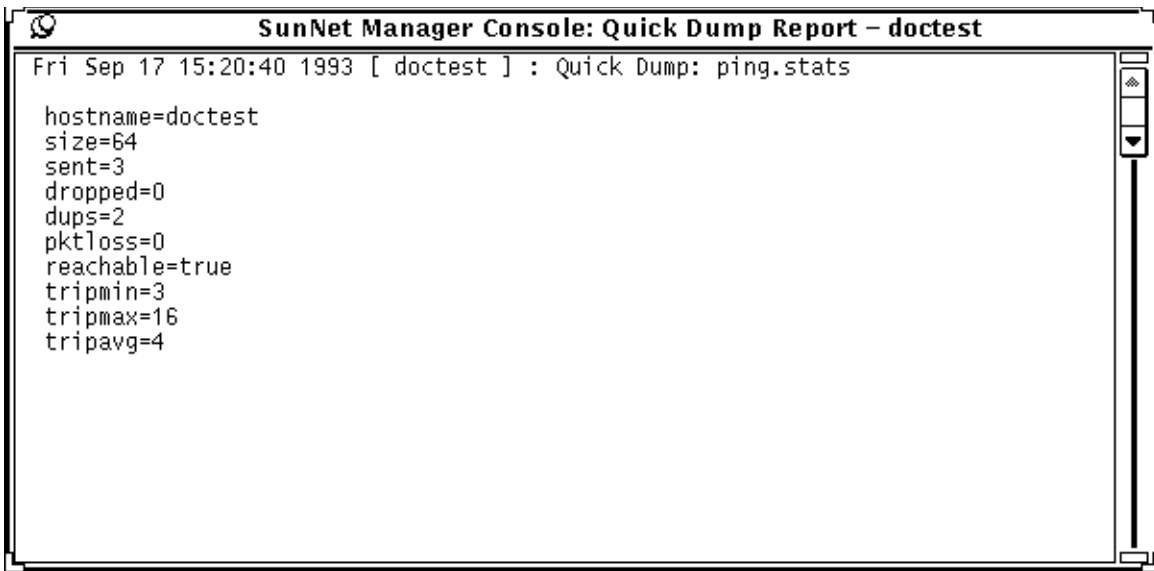


Figure 4-3 Quick Dump Report Window

4.1.3 Notes

Table attributes are displayed in tabular form when possible and the Quick Dump window is automatically stretched if necessary.

Data returned in the Quick Dump window is not stored and is not displayed in the Data Reports window.

The Get operation of the Set Tool returns the same information for SNMP devices as the Quick Dump. The Set Tool is described in Chapter 8 of the *SunNet Manager 2.2.3 Reference Manual*.

4.2 Requesting Periodic Data

A data request causes an agent to automatically report the values of specified attributes for a target system at specified intervals. You can compose your own request, targeting a specific machine for a specific set of information. More conveniently, you can use one of SNM's predefined requests. These requests save you the trouble of composing requests for individual machines.

SNM is shipped with a number of predefined requests that will satisfy many of your network management needs. In the course of making a data request, you can choose one of the available predefined requests, modify a predefined request for a specific need, or build your own request.

4.2.1 Sending a Data Request via the Console Requests Menu

1. Move the mouse pointer over the glyph that represents the target element and click **SELECT**.
2. Press **MENU** on the Requests button in the SNM Console and release **MENU** over **Send Request**.

The window shown in Figure 4-4 will be displayed. The Request Action field is automatically set to Send Request.

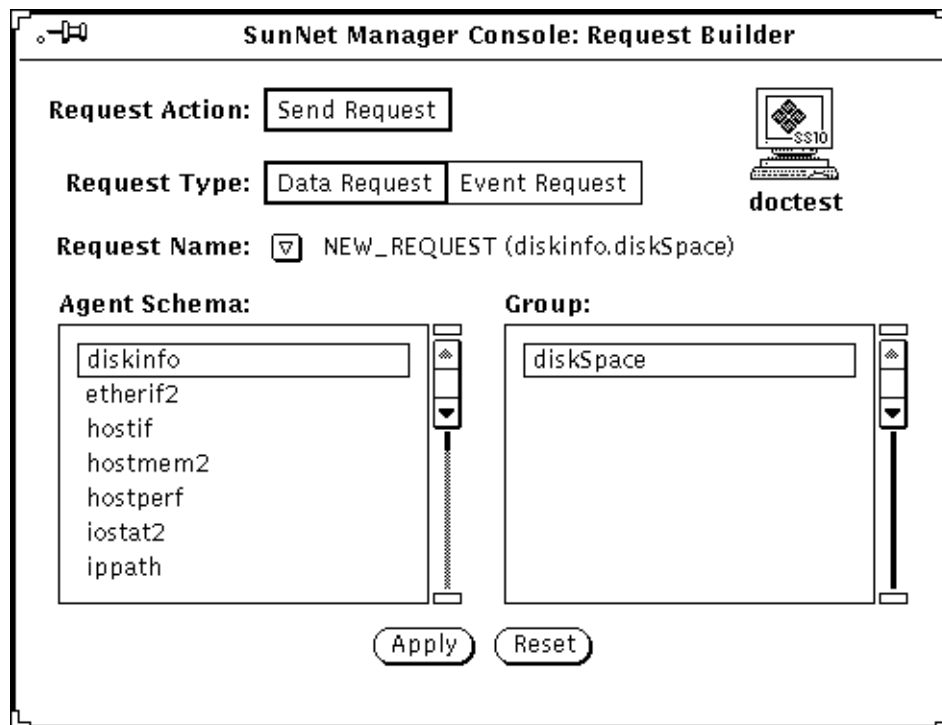


Figure 4-4 Sample Request Builder Window

3. Click **SELECT** on the Request Type you wish to send (data, for our present purposes). Press **MENU** on the Request Name abbreviated menu button. You receive the menu shown in Figure 4-5.

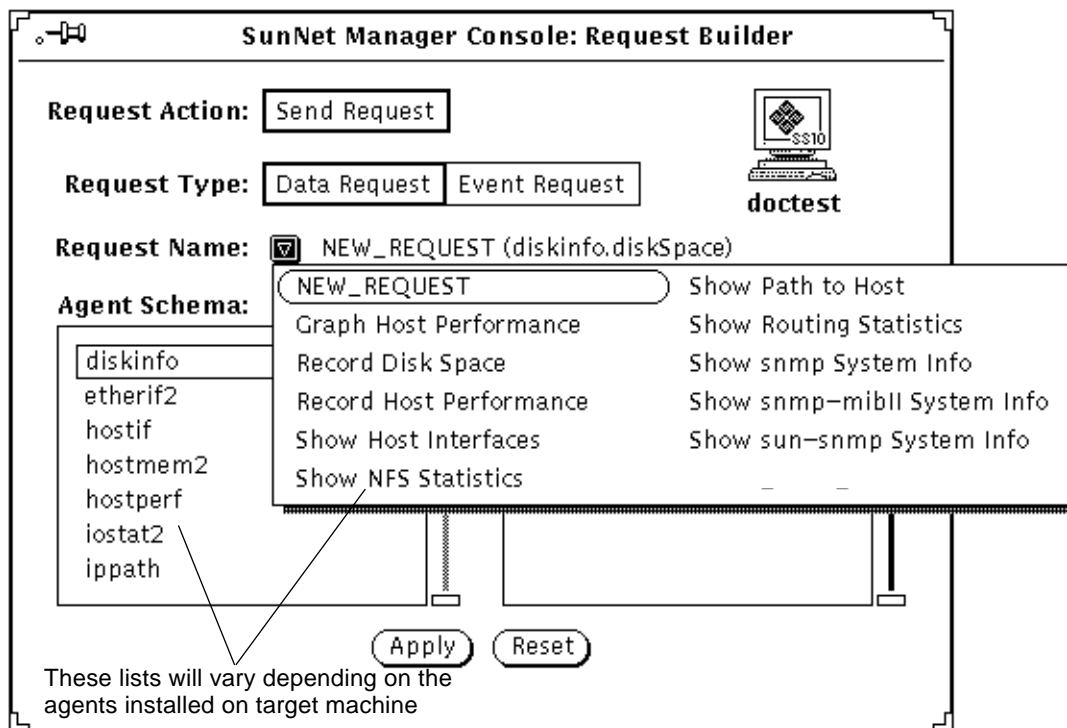


Figure 4-5 Request Name Menu

Choose one of the requests from the Request Name menu. Most users will find it easier to use a predefined request as is or modify a predefined request, rather than creating a new request. If you need to create your own request, do the following:

- a. Click **SELECT** on an agent in the Agent Schema scrolling list
 - b. Click **SELECT** on a group name in the Group scrolling list.
 - c. Choose **NEW_REQUEST** from the Request Name pull-down menu.
4. After choosing either **NEW_REQUEST** or a predefined request name from the Request Name menu, click **SELECT** on the **Apply** button. You receive a Data Request properties window as shown in Figure 4-6.

Help

On-line help is available for this window.

5. Examine the Request Properties window and make any changes you want. Many predefined requests will require little or no modification.

SunNet Manager Console: Data Request (doctest.hostperf.data)

Name: Graph Host Performance

Proxy System: doctest

Interval: 30

Count: 0

Key:

Restart:

Defer Reports:

On Completion: Save Request

Options:

Log to File:

To Program:

Attributes:

- cpu%
- intr
- disk
- ipkts

Attribute: cpu%

Data Log: False

Indicator:

Strip Chart: None

Graph Tool: Absolute Values

Buttons: Start, Hold, Reset, Apply, Reset, Delete

Status Bar: Host performance data | CPU utilization

Figure 4-6 Sample Data Request

The example above shows the predefined data request “Graph Host Performance”.

On the left side of the request window, modify or fill in the report characteristics fields. On the right side of the request window, select (or accept) the attributes on which you want the agent to send data, and how you want to view the data. Press MENU on the Attribute menu button and release MENU over the attribute you want. Click SELECT on Apply to add the attribute to your request. For a description of the fields in the Data Request template, refer to Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual*.

6. After you have selected and applied attributes and their viewing options, click SELECT on the Start button on the lower left side of the window to send the data request to the agent.

4.2.2 Sending a Data Request via the Glyph Menu

This procedure is identical to the preceding procedure except that, instead of selecting a glyph and pulling down the Requests menu, you move the mouse cursor over the glyph and pull down the Glyph menu. In the Glyph menu, release MENU over Send Request. You then receive a Request Builder window, from which you can use a predefined request or create your own request.

The glyph menu has a Send Predefined option, in addition to the Send Request option. The difference between the Send Predefined and Send Request options is that, with the former, you choose a request and send it immediately, without receiving a Request Builder and a request properties window. With the glyph's Send Request (and Console's Requests►Send Request) option you have the intervening steps of the Request Builder and request properties windows.

4.2.3 Sending a Predefined Data Request via the Glyph Menu

SNM is shipped with a number of predefined data requests. These predefined requests save you the trouble of setting and filling in values in a data request.

To send a predefined data request, do the following:

- 1. Over the glyph for the element to which you want to send the request, press MENU over Send Predefined.**
- 2. Pull right over Data Request and continue to pull right to obtain the menu of predefined data requests shown in Figure 4-7.**

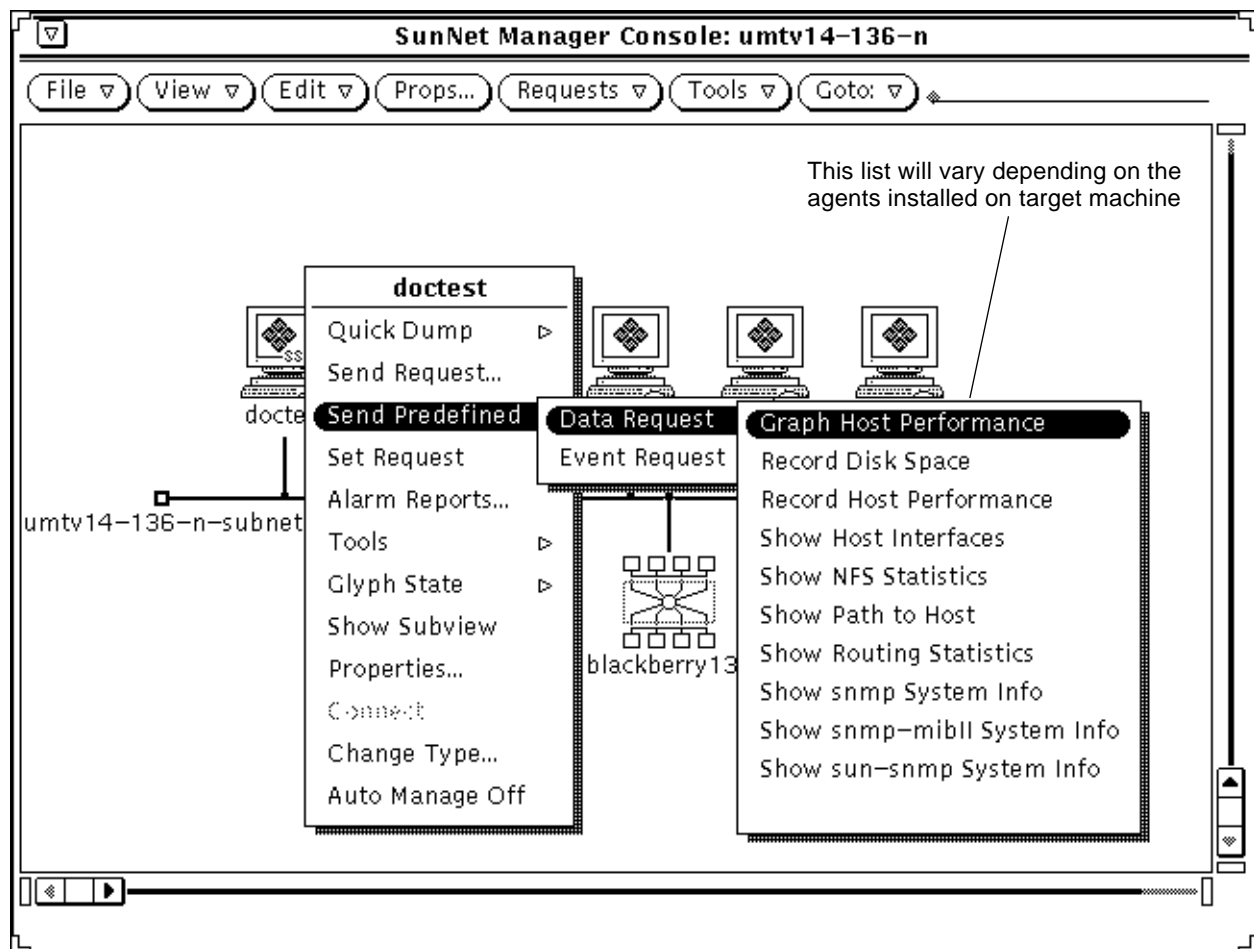


Figure 4-7 Predefined Data Request

3. Release MENU over the predefined request you want.

You receive no properties window for the request; the request is sent immediately following your menu selection.

To view the properties associated with a predefined request, click SELECT on the glyph to which you are sending a request, then in the Console's control area, invoke Requests►Send Request. In the Request Builder window, choose

the name of the predefined request you want from the Request Name menu, then click SELECT on Apply. You then receive the properties window for that predefined request.

Alternative ways to view the properties of a request:

- Double-click on the glyph for the target of your request, then click SELECT on the glyph for the request and click SELECT on the Props button in the Console's control area.
- Invoke Requests ► Requests Summary from the Console's control area. In the Requests Summary window, find and click SELECT on your request, then click SELECT on the Props button in the Requests Summary window. In that window, the Select and Sort menus can be very useful in finding your request.

See Section 6.2, "Viewing and Modifying Properties of a Request," on page 6-3 for instructions on the use of a request glyph and the Requests Summary window.

For further background on predefined requests see Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual*.

4.2.4 Notes

The predefined requests available (and the agents listed in the Agent Schema list in a Request Builder window) for a given machine depend on the agents that have been checked off as present in the properties window for that machine. A machine that has been added to your database by the Discover Tool that does not have the SNMP agents on it has the `hostperf` and `ping` agents checked off. Information is available from a machine without agents through SNMP's proxy feature, just as if the `hostperf` and `ping` agents *were* on that machine. A machine with SNMP agents installed that is added by Discover has the agents checked off that are actually present.

Messages indicating that the request has been started are displayed in the lower left footer of the Console window.

To view or modify the state of a Data Request or its properties, see Section 6.2, "Viewing and Modifying Properties of a Request," on page 6-3.

The default value of the Restart field in the Request Properties window is specified in the Requests category of the Console's Properties window. You access the Console's Properties window by clicking SELECT in the Props button in the Console's control area. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

4.3 Copying Requests

Copying requests will allow you to quickly start the same Data Request for multiple elements. Each request is represented by a glyph that appears in the subview of an element. Because requests are represented by glyphs, copying requests is similar to copying elements.

- 1. Move the mouse pointer over the request glyph that you want to copy and click SELECT to highlight it.**
- 2. Press MENU to open the Edit menu.**
- 3. Drag the mouse pointer down to the Copy option and release.**
- 4. Move the mouse pointer over the target element (in either the same view or a different view). Double-click SELECT to display the subview of the element.**
- 5. In the element's subview, press MENU to open the Edit menu. Drag the mouse pointer down to the Paste option and release.**

4.3.1 Notes

You can also use the keyboard function keys that correspond to Copy and Paste instead of the Console Edit menu.

The Copy function copies the request into the clipboard. Once a request has been copied into the clipboard, it can be pasted into as many views as needed. In the Console window, invoke View ► Clipboard to view the contents of the clipboard.

Pasting a request into the view of an element launches the request for that element. If you specified a name for the original request, the same name is used for the copied request. If you did not specify a name for the original

request, the request name assigned to the copied request is incremented by 1. For example, if the original request uses the name `hostperf.data.0`, then a copied request becomes `hostperf.data.1`.

As an alternative to copying a request, you might find it easier to use the predefined request feature, described in Section 4.2.3, “Sending a Predefined Data Request via the Glyph Menu,” on page 4-10.

4.4 Viewing Incoming Data

You can view Data Request results as they are received by the Console in one of the following ways:

- The Data Reports option of the View menu displays the received data reports in a simple text format. The values of attributes specified in a single Data Request are displayed.
- The Results Grapher displays the values of a specified attribute on a graph. The Grapher is intended to aid in the visual analysis of collected attribute information. You can modify the display of graphs, including specifying graph colors and two-dimensional or three-dimensional displays. Graphs can be merged for comparison of data.
- A Strip Chart can also display the values of a specified attribute in a simple graph. A Strip Chart is a simple graph of a single attribute for a single system. Although Strip Charts can be copied and pasted into different views, you cannot merge multiple Strip Charts. Because each Strip Chart is automatically scaled, it is not very practical to try to compare data among multiple Strip Charts.
- An Indicator displays the last reported value of an attribute for a particular request. If many different Data Requests are active, an Indicator can be a convenient way of seeing the latest reported value of an attribute.

4.4.1 Viewing Incoming Data for All Systems: Data Reports Window

The View►Data Reports window displays reported attribute values sent by the agent in response to a Data Request.

1. **In the Console window, press MENU in the View menu and release MENU over Data Reports as shown in Figure 4-8.**

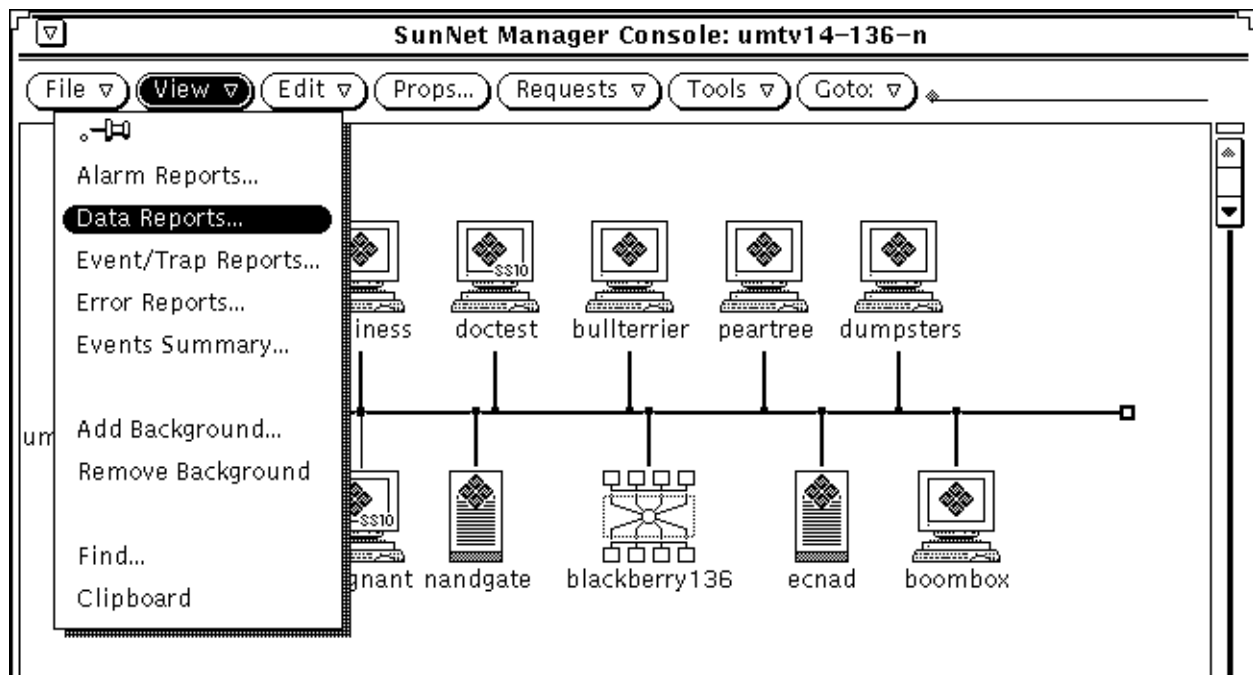


Figure 4-8 View—Data Reports Option

The window shown in Figure 4-9 will be displayed.

2. To examine data reports for a particular system, type in the device name after the Device prompt and press Return.

To see entries for all elements again, press Ctrl-U to clear the Device line and press Return.

An alternative way of viewing reports for a particular system is to click SELECT on the glyph for that system, then invoke View►Data Reports, as described above.

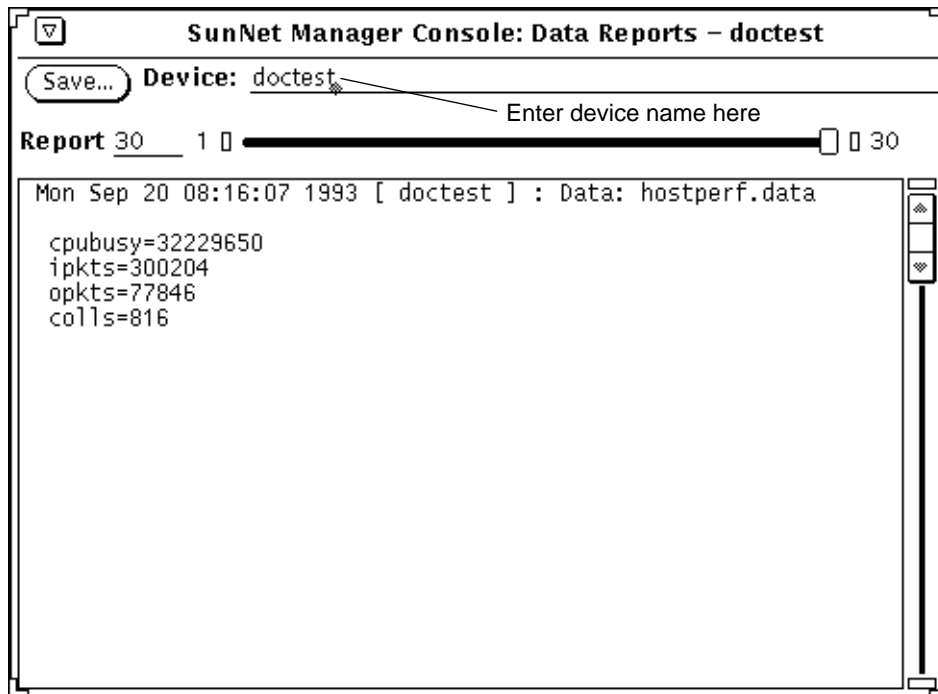


Figure 4-9 Sample Data Reports Window

3. **To save the data reports to a file, click SELECT on the Save button.**
A pop-up Save window appears, where you can enter the path and file name where the data reports are to be stored.
4. **To browse through entries in the window:**
 - Press SELECT on the slider and drag the slider to the left or right.
 - Click SELECT to the left or right of the slider.
 - Click SELECT on either end of the slider bar.
 - Enter the number of a report on the Report line and press Return.

Help

On-line help is available for this window.

4.4.2 Notes

The Data Reports window contains the most recently received data reports for all systems. The currently displayed entry and the total number of entries are identified in the slider bar. When Device is set for a particular element, the slider bar reflects the current and total number of entries for the element.

By default, the maximum number of data reports displayed in the Data Reports window is 1000. When the maximum limit is exceeded, the oldest data report is deleted.

4.4.3 Viewing Incoming Data: Grapher

The Graph Tool (also known as the Grapher) is an application that displays reported attribute values in a graph whose display can be manipulated.

Or, invoke the Grapher from the command line:

```
host% snm_gr
```

1. Open the Data Request Properties window for the target element by either defining a new Data Request or modifying an existing request.

The Data Request window as shown in Figure 4-6 on page 4-9 will be displayed. See Section 4.2, “Requesting Periodic Data,” on page 4-6.

2. Move the mouse pointer over the Graph Tool abbreviated menu button and press MENU. Drag and release on either Absolute Values or Delta Values.

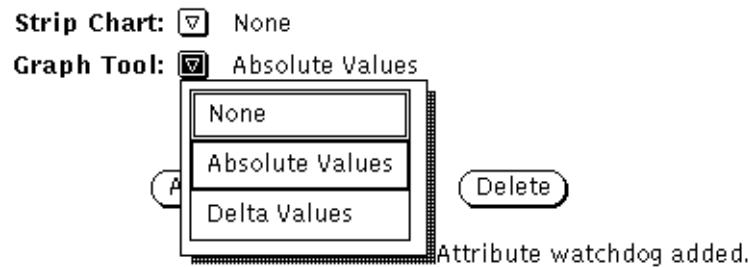


Figure 4-10 Graph Tool Menu

Choose Absolute Values to graph the values as they are reported. In graphs that use absolute values, the graphs use actual numbers, such as packet counts or collisions.

Choose Delta Values to graph the delta (or difference) between a previously reported value and the current reported value. In graphs that use delta values, the graph starts at zero or an arbitrary number and increments by however much it needs to accommodate changes.

Note – The predefined requests that are shipped with SunNet Manager have Absolute Values selected in the Graph Tool field.

4.4.4 Notes

You can modify the display of the graph. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31.

The Results Grapher is automatically started to graph attribute values as they are returned. The Grapher runs as a separate process from the Console and remains running when you quit or close the Console. You can invoke the Grapher from a command line by entering `snm_gr`. See the `snm_gr (1)` man page.

By default, graphs are displayed on a black background. To display graphs on a white background, invoke the Grapher from the command line with the `-b` option. You can also modify the Tools menu to add the `-b` option when invoking the Grapher. See Section 11.4, “Modifying the Console Tools Menu,” on page 11-11.

Graphs can be printed by using the OpenWindows Snapshot utility. Snapshot is available from the Tools menu. See Section 4.7, “Printing a Graph,” on page 4-33 for more information.

4.4.5 Viewing Incoming Data: Strip Charts and Indicators

You can choose the Strip Chart or Indicator options in the Data Request Properties window. These options allow you to monitor the value of a single attribute from the Console view. An Indicator shows the last reported value of an attribute. A Strip Chart is an auto-scaled chart of reported values for a single attribute.

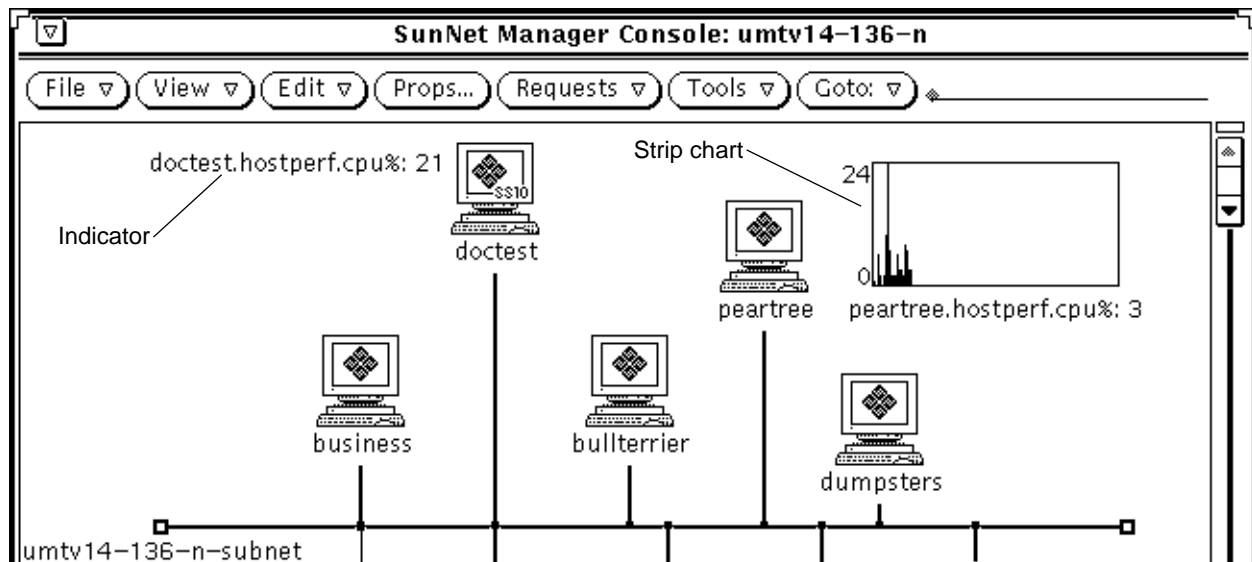


Figure 4-11 Strip Chart and Indicator Samples

1. Open the Data Request Properties window for the target element by either defining a new Data Request or modifying an existing request. See Figure 4-12.

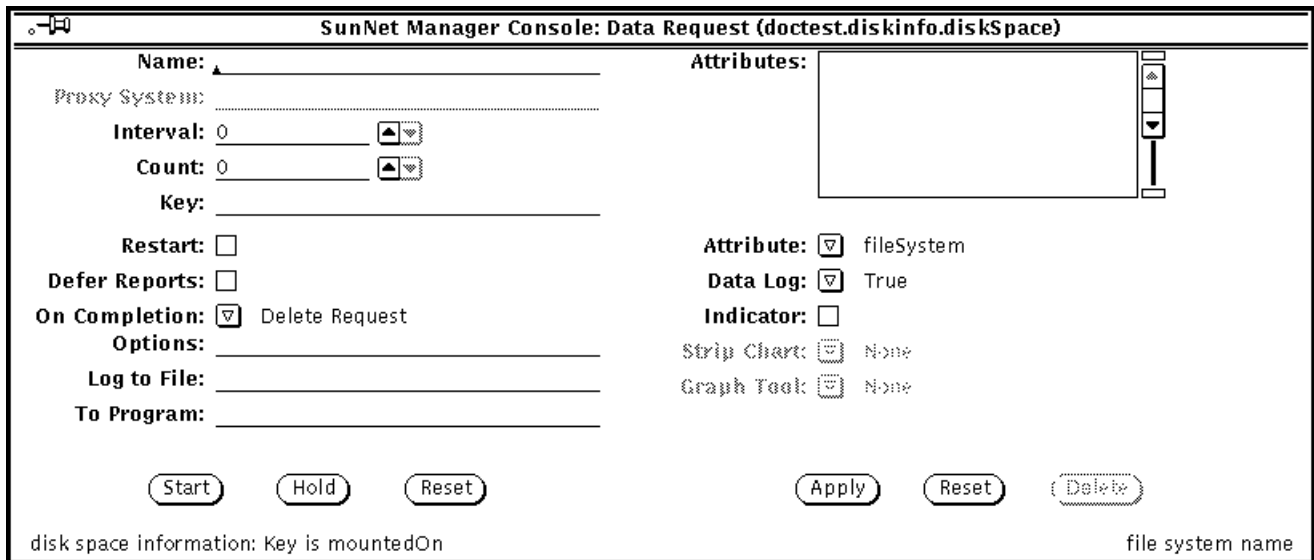


Figure 4-12 Data Request Properties Template

2. To specify that the attribute data be displayed in an Indicator, move the mouse pointer over the box next to the Indicator field and click SELECT. A check mark appears in the box.
3. To specify that the attribute data be displayed in a Strip Chart, move the mouse pointer down over the Strip Chart abbreviated menu button and press MENU. Drag the mouse pointer down to either Absolute Values (chart the received values) or Delta Values (chart the differences between received values).

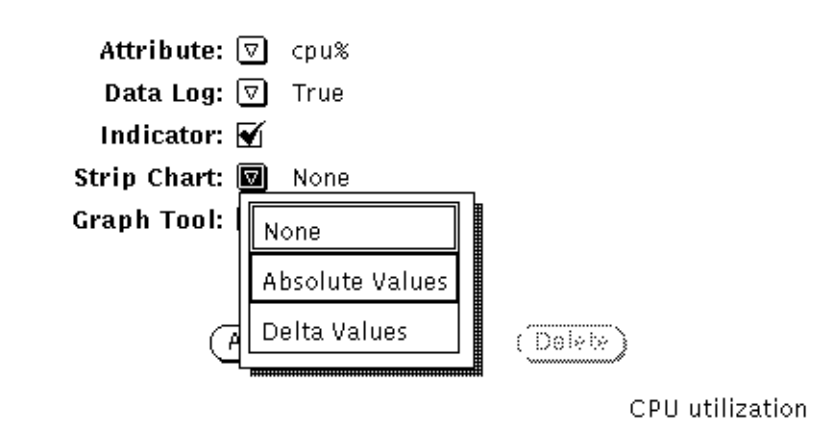


Figure 4-13 Strip Chart Menu

4.4.6 Notes

Indicators and Strip Charts are automatically positioned in the view from which the request is launched. You can move Indicators or Strip Charts within a view, or cut, paste, or copy them into other views.

A maximum of 64 Indicators or 128 Strip Charts can be displayed in the view where the associated request is started.

You can modify certain properties of Strip Charts with their Properties window. For example, you can specify the maximum height and width of a Strip Chart. To modify the properties of a Strip Chart:

- 1. Move the mouse pointer over the Strip Chart you want to modify and press MENU to open its Glyph menu.**
- 2. Drag the mouse pointer down to Properties and release to open the Properties window.**
- 3. Modify the Properties window, as necessary.**
Note that the Properties window for Strip Charts is similar to an Element Properties window. The middle portion of the window, for selecting agent schemas, and the bottom portion, for color selection, do not apply to Strip Charts.
- 4. Click SELECT on the Apply button to modify the Indicator or Strip Chart.**

Help

On-line help is available for this window.

4.5 Analyzing Stored Data

You can analyze data that has been stored into a disk file by using the following tools:

- Results Browser
- Results Grapher

The following types of data files can be analyzed:

- Event/Trap Reports file. Unless a different log directory was specified during installation, this file is located at:
 - `/var/adm/snm/event.log` for Solaris 1.x installations.
 - `/var/opt/SUNWconn/snm/event.log` for Solaris 2.x installations.The log file is defined by the `event-log` keyword in the `/etc/snm.conf` file.
- Data report entries that have been saved to a disk file (see Section 4.4.1, “Viewing Incoming Data for All Systems: Data Reports Window,” on page 4-14).
- Data report files specified with the Log to File field in the Data Request window.
- Any other files that use the data format specified by `snm logfile(5)`.

4.5.1 Analyzing Stored Data: Results Browser

Or, invoke the Browser from the command line:
host% `snm_br`

The Results Browser allows you to retrieve and organize stored data.

1. **Move the mouse pointer over the Tools button and press MENU to open the Tools menu.**

The menu shown in Figure 4-14 will be displayed.

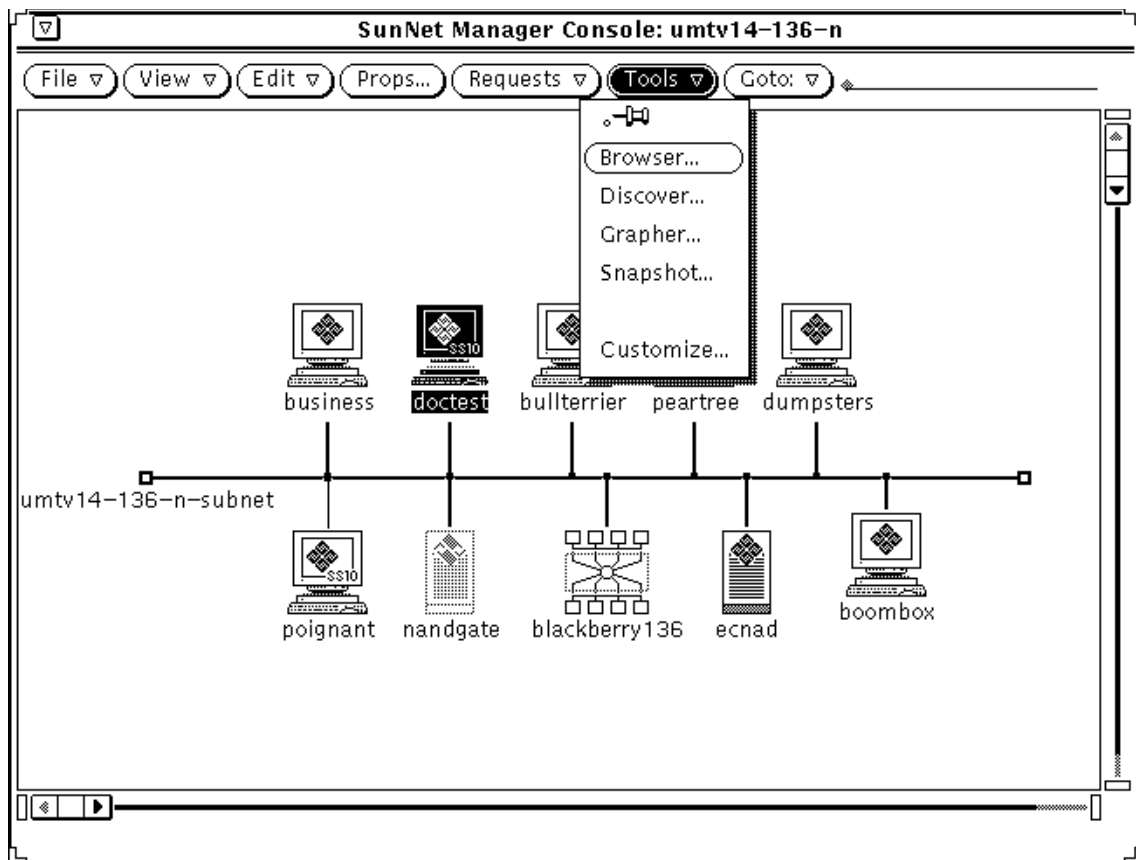


Figure 4-14 Tools Menu

Help

On-line help is available for this window.

2. **Drag the mouse pointer down to Browser and release to open the Results Browser.**
The window shown in Figure 4-15 is displayed.

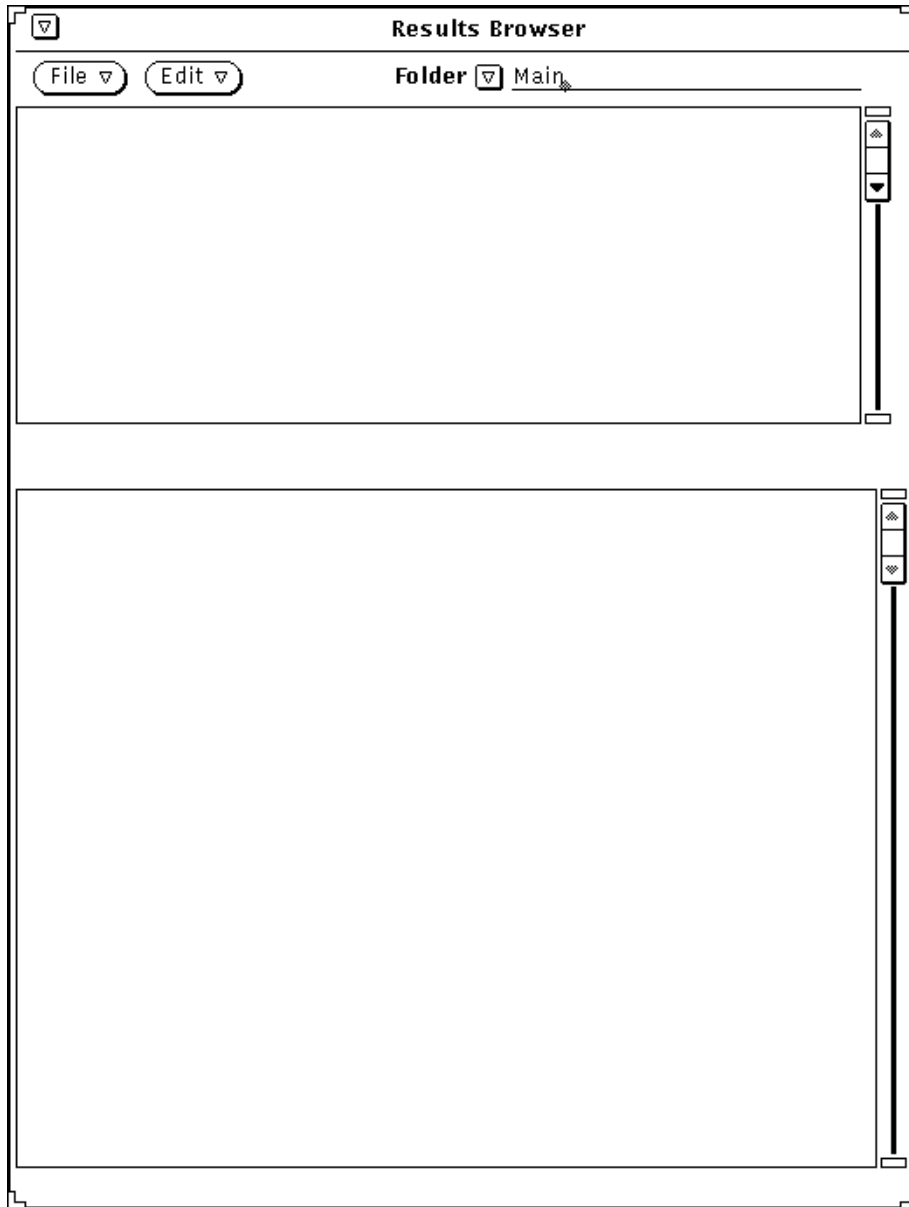


Figure 4-15 Results Browser Window

3. In the Results Browser file menu, move the mouse pointer over the File button and press MENU to open the File menu. Drag the mouse pointer down to Load. You receive the window shown in Figure 4-16.

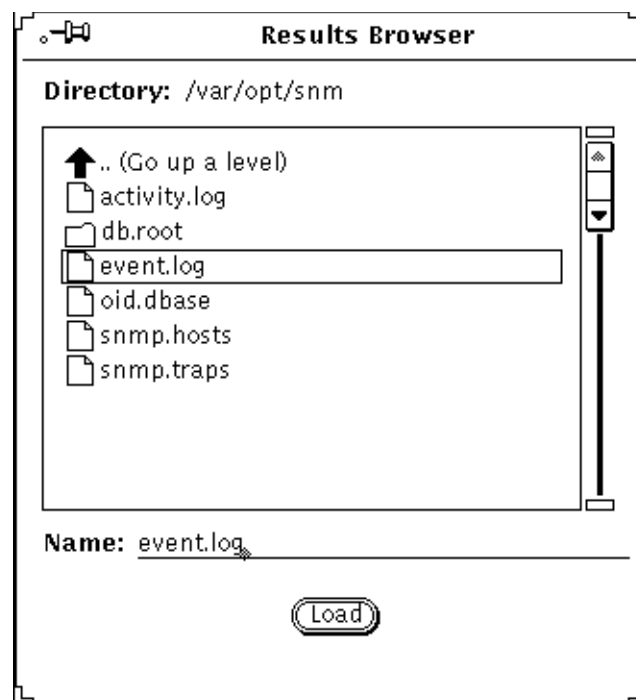


Figure 4-16 File Menu for Results Browser

4. Enter the directory and file name of the file to be loaded and click **SELECT** on the Load button. You receive the window shown in Figure 4-17.

Data loaded into the Browser is automatically organized into report streams and grouped by request and type of data. A *stream* is the set of requests associated with a specific pairing of hostname or IP address and agent name. For example, all of the data reports from the `hostmem2` agent for `poignant` would make up a single stream. The reports from the `layers2` agent for the same machine make up a different stream, as do the `layers2` reports for a different machine.

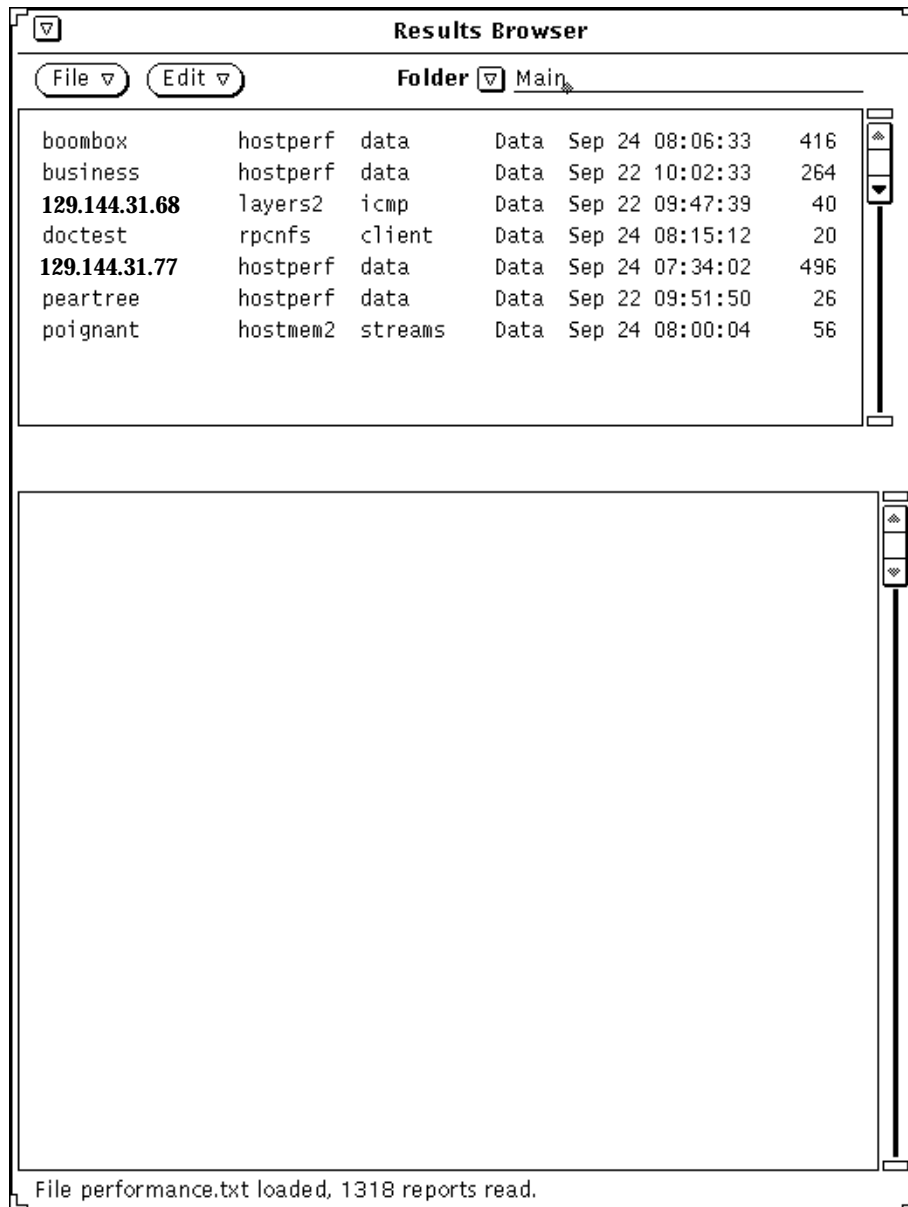


Figure 4-17 Results Browser with Reports Loaded

5. To view individual reports in a report stream, double-click **SELECT** on the line that represents the stream.

4.5.1.1 Notes

See Chapter 6 of the *SunNet Manager 2.2.3 Reference Manual* for a complete description of Results Browser features.

The Browser runs as a separate process from the Console and remains running when you quit or close the Console.

The first column in the Browser scrolling list of streams can contain a hostname or an IP address.

You can invoke the Browser from a command line by entering `snm_br`. When you invoke the Browser from the command line, you can also specify the path and name of one or more data files to be loaded automatically when the Browser's main window is displayed. You can print Browser report streams to a specified printer. To do so:

Or, click **SELECT** on the desired report stream name so that it is highlighted. To select more than one stream, click **ADJUST** on subsequent report stream names.

1. **Select the report streams you wish to print.**
 - a. **Move the mouse pointer into the top portion of the Browser window where the names of the report streams are displayed.**
 - b. **Press MENU to open the Streams menu.**
 - c. **Drag the mouse pointer down to Select, then continue to drag right to By System, By Agent and Group, or By Report Type.**
 - d. **Continue to drag right on the appropriate system name, agent group name, or report type.**
 - e. **Repeat steps a through d until all desired streams are selected.**
2. **Move the mouse pointer over the report streams and press MENU to open the Streams menu.**
3. **Drag the mouse pointer down to Print. (See Figure 4-18.)**

The default printer is `lp`. To change the printer, modify the Browser Properties window as explained in the following summary.

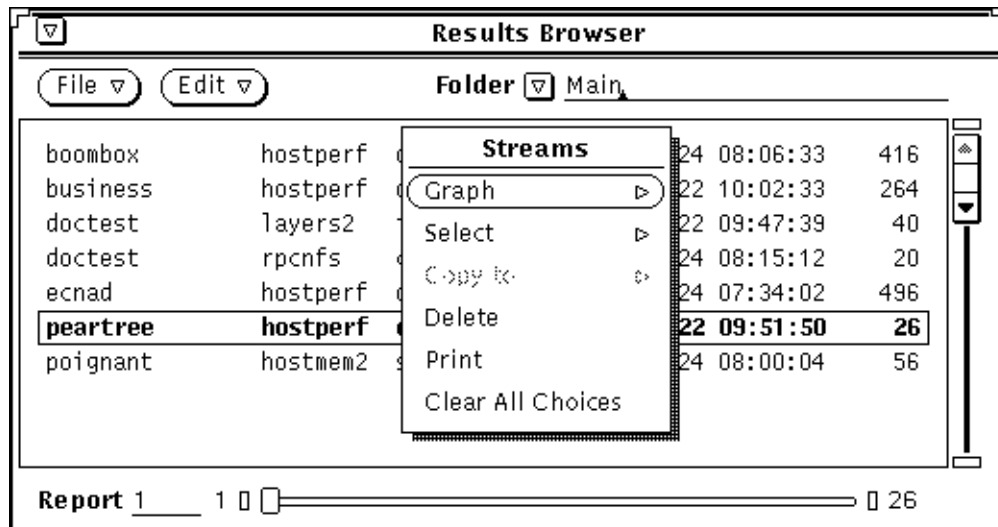


Figure 4-18 Browser Edit Menu

You can modify certain characteristics of the Browser display and the default printer. To do so:

1. Move the mouse pointer to the Edit button of the Browser window and press MENU to open the Edit menu.
2. Drag the mouse pointer down to the Tool Properties option and release. (See Figure 4-19.)

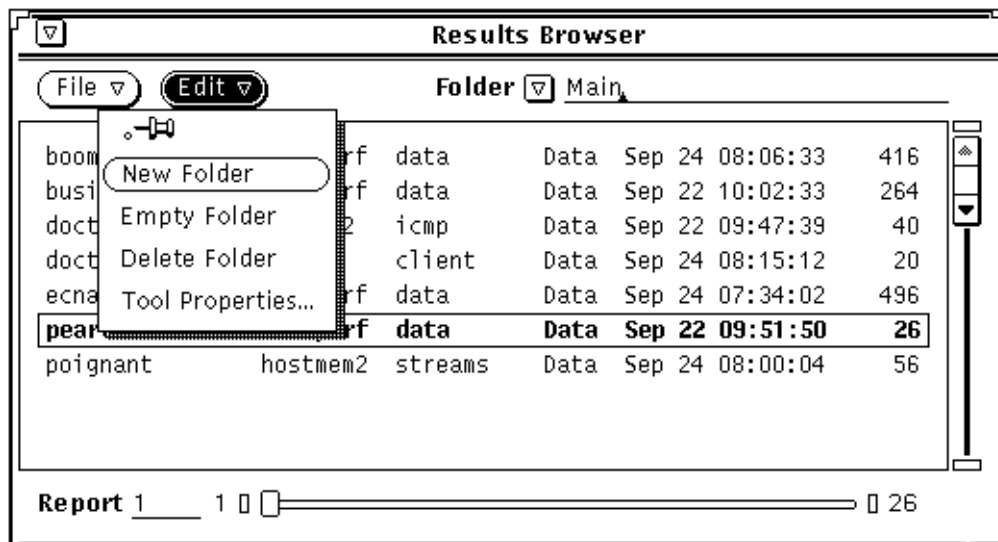


Figure 4-19 Browser Tool Edit Menu

3. **Modify Browser display or print options.** (See Figure 4-20.)

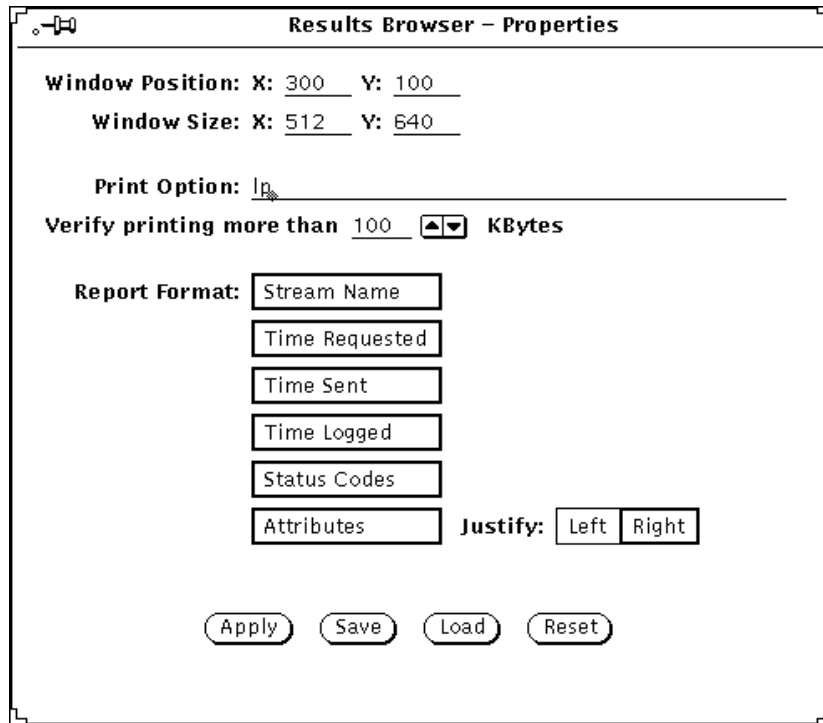


Figure 4-20 Browser Properties Window

4.5.2 Analyzing Stored Data: Results Grapher

The Results Grapher displays reported attribute values in a graph that can be manipulated.

Note – You can invoke the Grapher directly, by selecting **Tools**►**Grapher** in the Console window or by invoking `snm_gr` on a command line. However, the most useful way to use the Grapher is to invoke the Browser, then, from the Results Browser window, invoke the Grapher for a specific set of inputs. The procedure for this is specified below.

Or, invoke the Browser from the command line:
`host% snm_br`

1. **Move the mouse pointer over the Tools button and press MENU to open the Tools menu. Drag the mouse pointer down to Browser and release.**



On-line help is available for this window.

2. **Load the file into the Results Browser.**
 - a. **Move the mouse pointer over the File button and press MENU to open the File menu. Drag the mouse pointer down to Load.**
 - b. **Enter the directory and path name of the file to be loaded and click SELECT on the load button.**
3. **In the Browser window, send the stream(s) that contain the data to be graphed to the Grapher.**
 - a. **Select the stream that contains the data to be graphed.**
 - b. **Move the mouse pointer into the scrolling list in the upper portion of the Browser window and press MENU to open the Streams menu.**
 - c. **Drag the mouse pointer down to Graph and drag right over the desired attribute name.**

4.5.2.1 Notes

You can modify the display of the graph. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31.

The Results Browser and Grapher run as separate processes and remain running when you quit or close the Console.

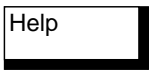
By default, graphs are displayed on a black background. To display graphs on a white background, invoke the Grapher from the command line with the `-b` option. You can also modify the Tools menu to add the `-b` option when invoking the Grapher. See Section 11.4, “Modifying the Console Tools Menu,” on page 11-11 for more information.

Graphs can be printed by using the OpenWindows Snapshot utility. Snapshot is available from the Tools menu of the Console. See Section 4.7, “Printing a Graph,” on page 4-33 for more information.

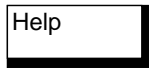
4.6 Modifying the Display of a Graph

You can change the way that each graph is displayed.

- To change the display of the graph:
 - a. **Move the mouse pointer over the displayed graph.**



On-line help is available for this window.



On-line help is available for this window.

b. Press **MENU** and drag the mouse pointer down to **Properties** and release.

c. **Modify the Properties window of the graph.**

- To change the viewing angle of the graph:
 - a. **Move the mouse pointer over the displayed graph.**
 - b. Press **MENU** and drag the mouse pointer down to **Controls** and release.
 - c. **In the Rotation Angles window, adjust the elevation and rotation of the graph by dragging the mouse pointer on the slider buttons.**
- To zoom into a portion of the graph:
 - a. **Move the mouse pointer to a point in the graph along the X-axis and press **SELECT**.**
 - b. **Drag the mouse pointer to another point along the X-axis.**
- To merge multiple graphs:
 - a. **In the Results Grapher main window, click **SELECT** on the names of the graphs you want to merge.**
 - b. **Click **SELECT** on the Merge button.**

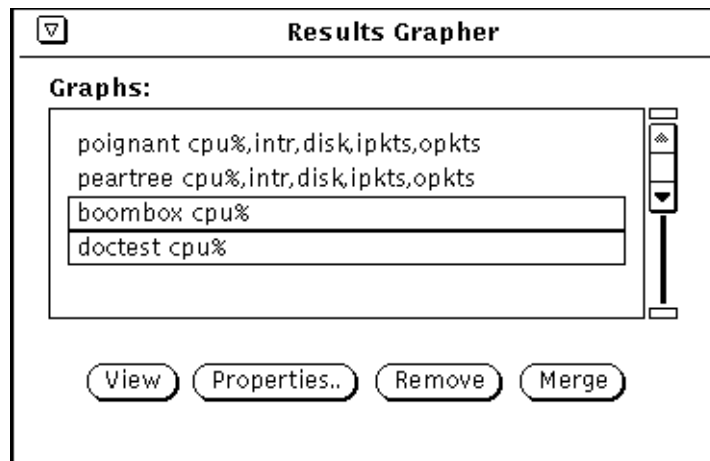


Figure 4-21 Results Grapher Window

4.7 Printing a Graph

You can print graphs (or strip charts) using the OpenWindows Snapshot utility. Snapshot is available from the Tools menu of the Console.

1. Start the Snapshot utility from the Console Tools menu or from the OpenWindows Programs menu.

- In the Console, move the mouse pointer to the Tools button and press MENU to open the Tools menu. Drag the mouse pointer down to Snapshot and release.
- In an open area of your workstation display, press MENU to open the Workspace menu. Drag the mouse pointer right on Programs, then drag down to the Snapshot option and release.
- For more information on the Snapshot utility, refer to the *SunOS 4.x DeskSet Environment Reference Guide*.

2. In the Snapshot window, click SELECT on Window in the Snap Type field, then click SELECT on the Snap button. (See Figure 4-22.)

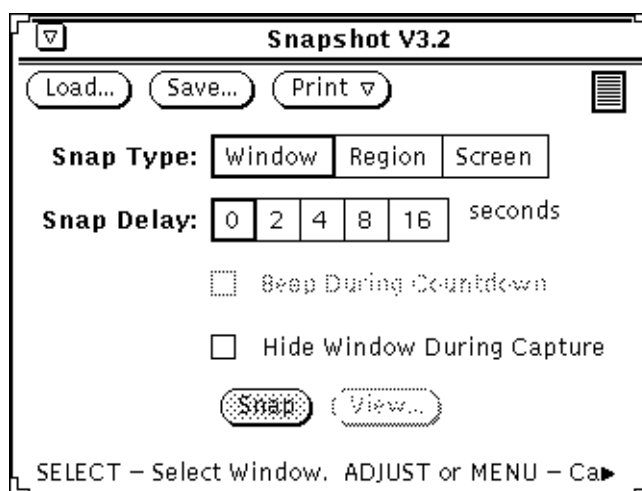


Figure 4-22 Tools—Snapshot Window

3. Move the mouse pointer to the graph to be printed and click SELECT.

Within a few seconds you should see the message “Snap succeeded” at the bottom of the Snapshot window.

4. In the Snapshot window, press MENU on the Print abbreviated menu button.

Drag the mouse pointer down to Print Snap to print the snapshot. Drag the mouse pointer down to Options to set up printer options.

4.7.1 Notes

If the Grapher displays the graphs on a black background, the graphs will print on a black background. To print graphs on a white background, you need to invoke the Grapher with the `-b` option. You can also modify the Tools menu to add the `-b` option when invoking the Grapher. See Section 11.4, “Modifying the Console Tools Menu,” on page 11-11 for more information.

Specifying Events



<i>Specifying an Event</i>	<i>page 5-2</i>
<i>Detecting the Presence of an Event</i>	<i>page 5-9</i>
<i>Checking the Cause of an Event</i>	<i>page 5-10</i>
<i>Changing the State of a Glyph</i>	<i>page 5-12</i>
<i>Changing the Propagation of Glyph State Changes</i>	<i>page 5-14</i>

An event occurs when specified conditions are met. The SNM Console provides a mechanism—described in this chapter—that allows you to specify in the Console the following characteristics that pertain to an event:

- condition(s) that define a particular event;
- visual or audible indications of an event or the action that is to take place when the event occurs;
- whether or not the visual indications of an event are propagated through the view hierarchy of the Console.

When you specify an event, a request is made to the appropriate agent. When an event occurs, the agent sends an event report back to the Console. You can specify various actions for the Console to perform when it receives an event report. For example, you can have the Console display a visual alarm, play an audio file, send a mail message, send the event report to a program, or any combination of these actions.

5.1 *Specifying an Event*

You specify the event conditions, event notification, and actions for individual elements by using the Event Request Properties window.

SNM allows you to compose your own event request, targeting a specific machine for a specific set of information. More conveniently, you can use one of SNM's predefined requests. These requests save you the trouble of composing requests for individual machines.

SNM is shipped with a number of predefined event requests that will satisfy many of your network management needs. In the course of making an event request, you can choose one of the available predefined requests, modify a predefined request for a specific need, or build your own request.

5.1.1 *Sending an Event Request via the Console Requests Menu*

1. **Click SELECT on the glyph that represents the target element.**
2. **Press MENU on the Requests button in the control area of the Console and release MENU over Send Request.**
The window shown in Figure 5-1 will be displayed. The Request Action field is automatically set to Send Request.

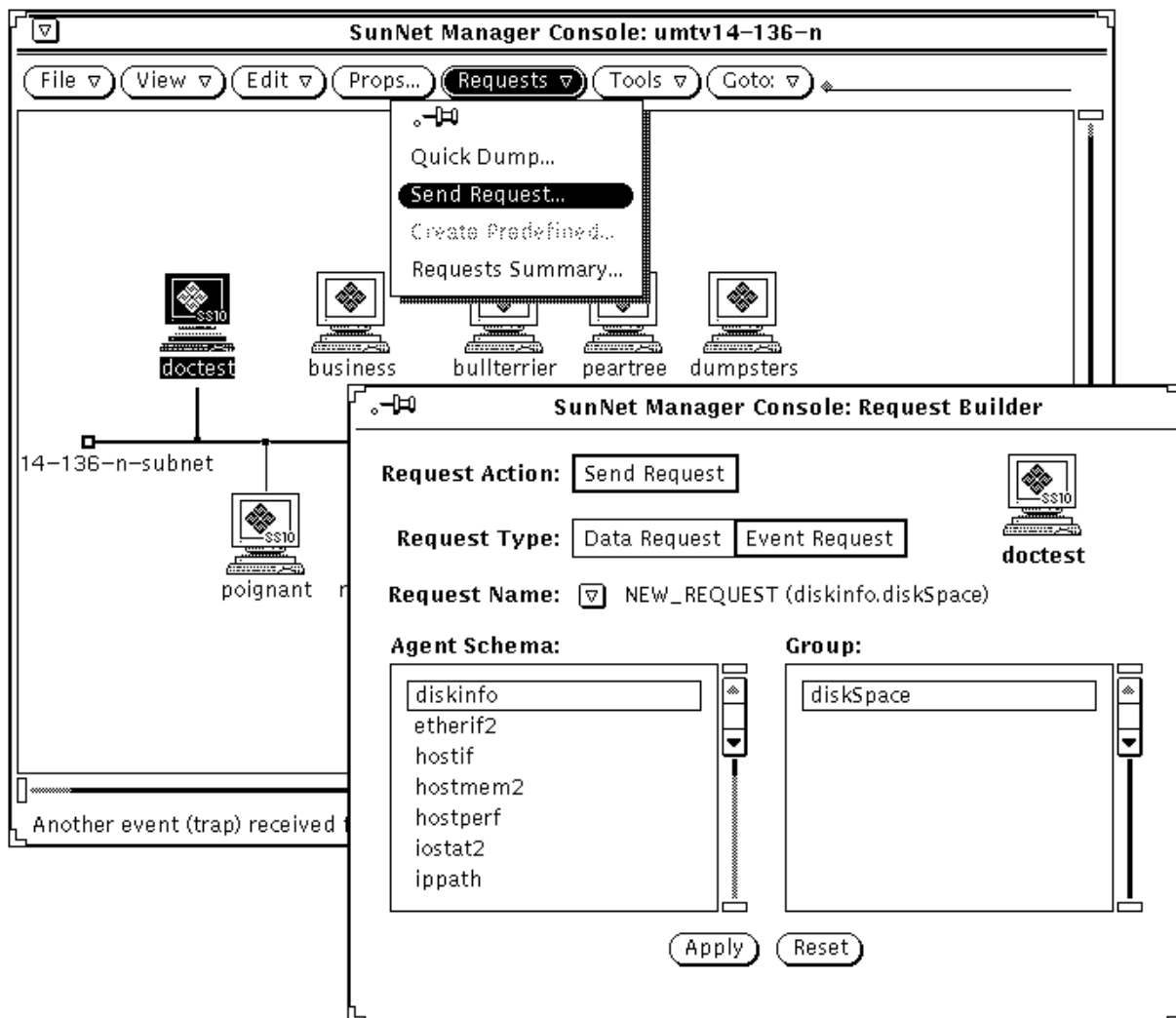


Figure 5-1 Sample Request Builder Window

3. Click **SELECT** on the Request Type you wish to send (event, for our present purposes). Press **MENU** on the Request Name abbreviated menu button. You receive the menu shown in Figure 5-2.

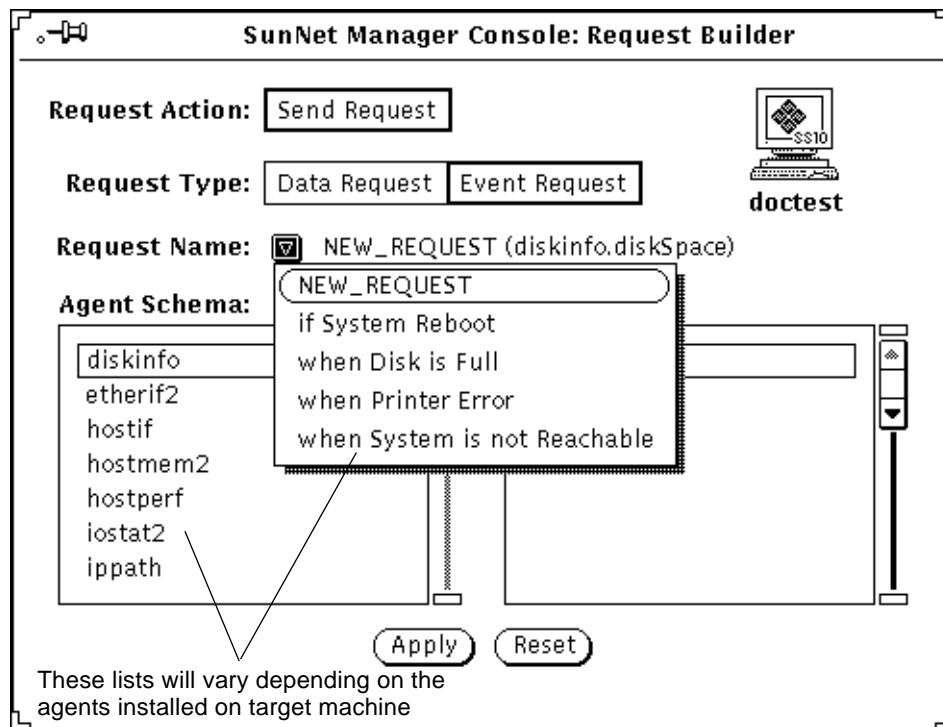


Figure 5-2 Request Name Menu

Choose one of requests from the Request Name menu. Most users will find it easier to use a predefined request as is or modify a predefined request, rather than creating a new request. If you need to create your own request, do the following:

- a. Click **SELECT** on an agent in the Agent Schema scrolling list
 - b. Click **SELECT** on a group name in the Group scrolling list.
 - c. Choose **NEW_REQUEST** from the Request Name pull-down menu.
4. After choosing either **NEW_REQUEST** or a predefined request name from the Request Name menu, click **SELECT** on the **Apply** button. You receive a Data Request properties window as shown in Figure 5-3.
5. **Examine the Request Properties window and make any changes you want.** Many predefined requests will require little or no modification.

Help

On-line help is available for this window.

SunNet Manager Console: Event Request (doctest.hostperf.data)

Name:

Proxy System:

Interval:

Count:

Key:

Restart:

Send Once:

Defer Reports:

On Completion: Save Request

Options:

Attributes:

Attribute: uptime

Relation1: Increased By Less Than

Threshold1:

Relation2: Threshold Not Set

Threshold2:

Priority: Medium

Glyph Effect: Blink Glyph

Audio Effect: None

Audio File:

Mail To:

To Program:

Host performance data CPU utilization

Figure 5-3 Sample Event Request

The example above shows the predefined event request “if System Reboot”.

On the left side of the request window, modify or fill in the report characteristics fields. On the right side of the request window, select (or accept) the attributes on which you want the agent to send data, and how you want to view the data. Press MENU on the Attribute menu button and release MENU over the attribute you want. Click SELECT on Apply to add the attribute to your request. For a description of the fields in the Event Request template, refer to Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

6. After you have selected and applied attributes and their viewing options, click SELECT on the Start button on the lower left side of the window to send the event request to the agent.

5.1.2 Sending an Event Request via the Glyph Menu

This procedure is identical to the preceding procedure except that, instead of selecting a glyph and pulling down the Requests menu, you select the glyph and pull down the glyph menu. In the glyph menu, release MENU over Send Request. You then receive a Request Builder window, from which you can use a predefined request or create your own request.

The glyph menu has a Send Predefined option, in addition to the Send Request option. The difference between the Send Predefined and Send Request options is that, with the former, you choose a request and send it immediately, without receiving a Request Builder and a request properties window. With the glyph's Send Request (and Console's Requests►Send Request) option you have the intervening steps of the Request Builder and request properties windows.

5.1.3 Sending a Predefined Event Request via the Glyph Menu

SNM is shipped with a number of predefined event requests. These predefined requests save you the trouble of setting and filling in values in an event request.

To send a predefined event request, do the following:

- 1. Over the glyph for the element to which you want to send the request, press MENU over Send Predefined.**
- 2. Pull right over Event Request and continue to pull right to obtain the menu of predefined event requests shown in Figure 5-4.**

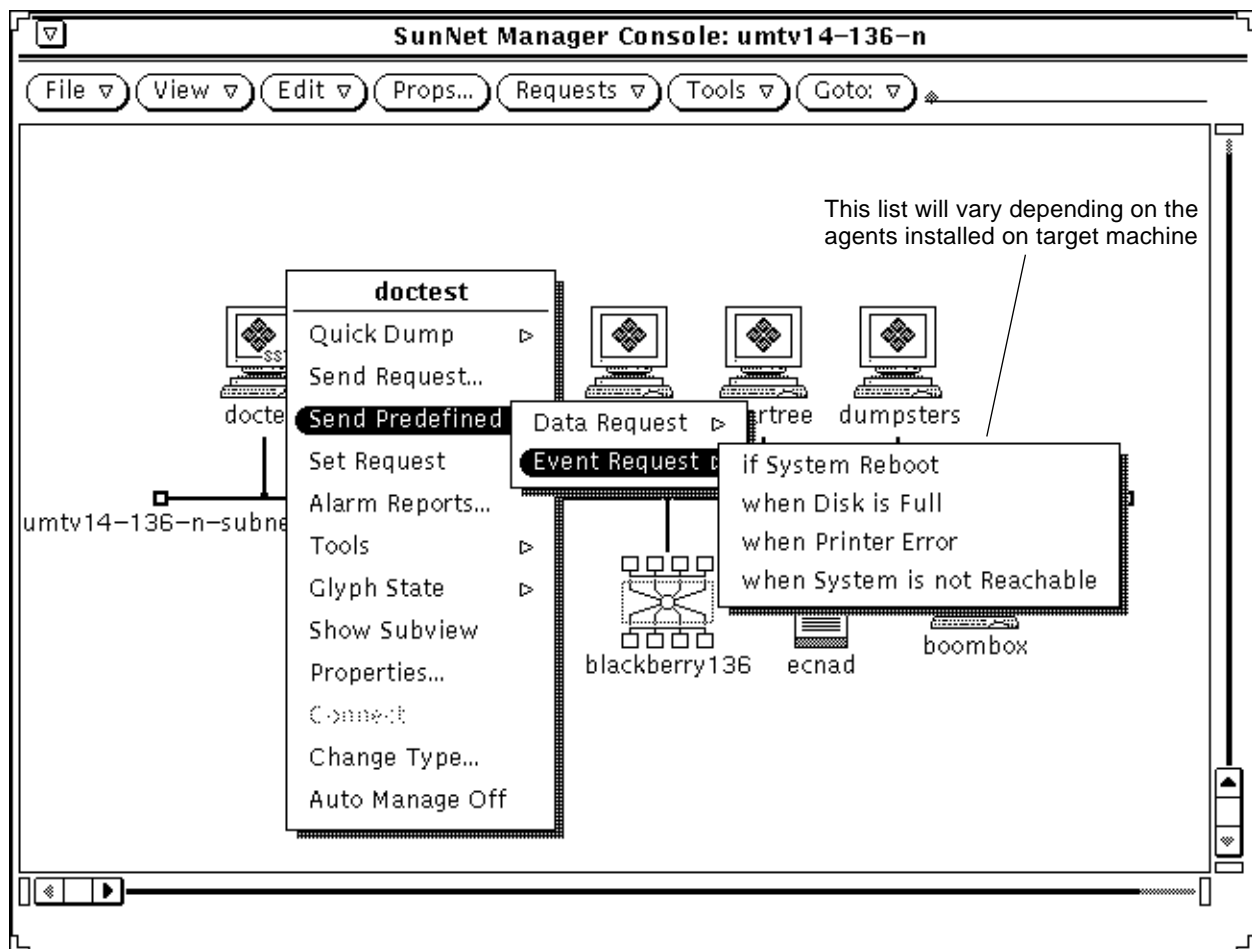


Figure 5-4 Predefined Event Request

3. Release MENU over the predefined request you want.

You receive no properties window for the request; the request is sent immediately following your menu selection.

To view the properties associated with a predefined request, click SELECT on the glyph to which you are sending a request, then in the Console's control area, invoke Requests►Send Request. In the Request Builder window, choose

the name of the predefined request you want from the Request Name menu, then click SELECT on Apply. You then receive the properties window for that predefined request.

Alternative ways to view the properties of a request:

- Double-click on the glyph for the target of your request, then click SELECT on the glyph for the request and click SELECT on the Props button in the Console's control area.
- Invoke Requests ► Requests Summary from the Console's control area. In the Requests Summary window, find and click SELECT on your request, then click SELECT on the Props button in the Requests Summary window. In that window, the Select and Sort menus can be very useful in finding your request.

See Section 6.2, "Viewing and Modifying Properties of a Request," on page 6-3 for instructions on the use of a request glyph and the Requests Summary window.

For further background on predefined requests see Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual*.

5.1.4 Notes

The predefined requests available (and the agents listed in the Agent Schema list in a Request Builder window) for a given machine depend on the agents that have been checked off as present in the properties window for that machine. A machine that has been added to your database by the Discover Tool that does not have the SNMP agents on it has the `hostperf` and `ping` agents checked off. Information is available from a machine without agents through SNMP's proxy feature, just as if the `hostperf` and `ping` agents *were* on that machine. A machine with SNMP agents installed that is added by Discover has the agents checked off that are actually present.

For event reports, the Interval and Count fields simply specify when the agent is to send a report. A report is forwarded to the Console system only if it has been determined that an event has occurred. For agents that are shipped with SNMP, the value reported for an attribute is the value noted at the reporting interval. Thus, it is possible for event conditions to occur *between* reporting intervals which will not generate an event report.

If the Send Once field is off (no check mark appears in the accompanying box), it means that an event report will be sent for every event occurrence. If the Send Once field is on (a check mark appears in the accompanying box), it means that after the first event report is received by the Console, the request is killed. To specify Send Once, click SELECT on the box to display a check mark.

You can choose to have a Console window that is closed to an icon open automatically when an event or trap is received. You specify this in the Console's Properties window, available by clicking SELECT in the Props button in the Console's control area. See the description of the Open on Event or Trap setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

By default, an event's glyph effect options remain in effect for 10 seconds beyond the reporting interval. If another event does *not* occur within this time, the Console cancels the glyph effect. You can increase the 10-second glyph effect overlap time in the Console Properties window. See the description of the Event Effect Overlap Time setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

5.2 Detecting the Presence of an Event

As described in the following section, you can use the Alarm Reports or Event/Trap Reports windows to monitor events. You obtain these from the View menu in the Console's control area (View►Alarm Reports or View►Event/Trap Reports). You can use either of these windows for all elements in a view or for a specific element. An alternative—and for many users, easier—way to detect an event for a specific element is to observe the visual effect of an event as it shows in a glyph.

If an event occurs, a glyph can blink, dim, change color, or remain unchanged. You choose the effect you want in the properties window for an event request at the time you make that request, as described in Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual*.

SNM has a “decay-to-blue” feature that allows you to detect that a condition that caused an event report occurred and that the condition no longer exists. For example, a file server might exceed a threshold you have set for a certain number of NFS transactions, then fall below that threshold. To take advantage of this decay-to-blue feature, you must specify Color by Priority as your Glyph Effect in an event request's properties window. Again, Chapter 3 of the *SunNet Manager 2.2.3 Reference Manual* has details.

See Section 5.4, “Changing the State of a Glyph,” on page 5-12 for instructions on returning a glyph from its “event-occurred” or decayed state back to normal.

5.3 *Checking the Cause of an Event*

When an event occurs, a report is returned to the Console that indicates the cause of the event. The Console gives you two ways to view an event report:

- The Event/Traps Reports window, described in this section.
- The Alarms Summary window (available in the View►Alarm Reports window). This window displays error, as well as event and trap, reports and is described in Section 7.1, “Viewing Alarm Reports,” on page 7-1.

To check the cause of an event in the Event/Trap Reports window, perform the following steps:

1. **In the Console’s control area, press MENU over the View button and Release MENU over Event/Trap Reports. (See Figure 5-5.)**

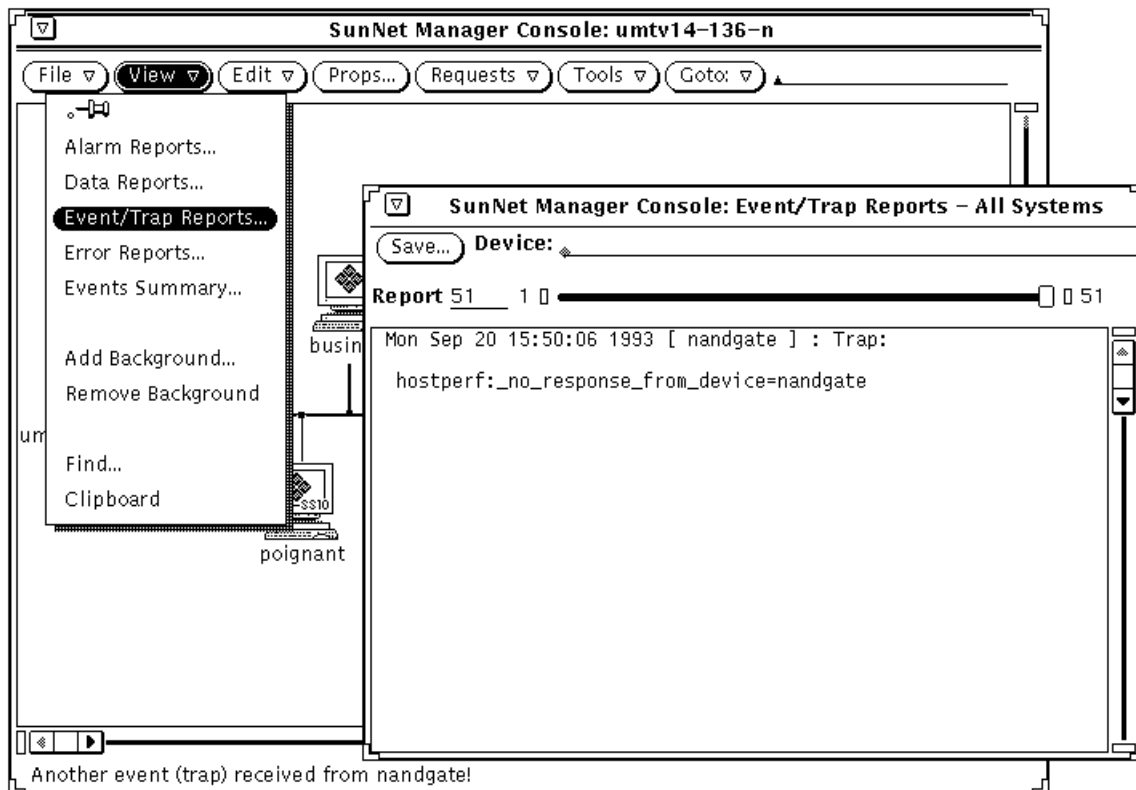


Figure 5-5 View—Event/Traps Window

- To examine event and trap reports for a particular system, type in the device name after the Device prompt and press Return.**
To see entries for all elements again, press Ctrl-U to clear the Device line and press Return.

An alternative way to obtain an element-specific event or trap report is to click SELECT on the glyph in the Console window, then invoke View►Event/Trap Reports.

- To save the event reports to a file, click SELECT on the Save button.**
A pop-up Save window appears, where you can enter the path and file name where the Event/Trap Reports are to be stored.

 Help

On-line help is available for this window.

4. To browse through entries in the log:

- Press SELECT on the slider and drag the slider to the left or right.
- Click SELECT to the left or right of the slider.
- Click SELECT on either end of the slider bar.
- Enter the number of a report on the Report line and press Return.

5.3.1 Notes

Event/Trap Reports entries are time-stamped and show values for all attributes in the specified agent group. The attribute and value that caused the event are flagged with the relational operator and threshold values shown in parentheses to the right.

By default, a maximum of 1000 event reports are displayed in the Event/Trap Reports window. You can change the maximum number in the Console Properties window. To view or change this setting (or any other event- or trap-related setting), click SELECT on Props in the Console's control area, then select Miscellaneous in the Category pulldown menu. See the description of the Maximum Event Reports setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

5.4 Changing the State of a Glyph

A glyph may change its state when an event or a trap is received for the element that is represented by the glyph. For example, if you have specified an event for an element and the notification is "Blink Glyph", the element's glyph state changes from "normal" to "blinking" when the event occurs. Once you have been alerted to the event, you may want to change the state of a glyph back to "normal." This is done using the Glyph State option of the Glyph menu for the element.

1. Over the glyph whose state you want to change, press MENU to open the Glyph menu for the element.
2. Release MENU over Glyph State and drag right to the desired glyph state—Normal, Blink On/Off, or Dim On/Off. (See Figure 5-6.)

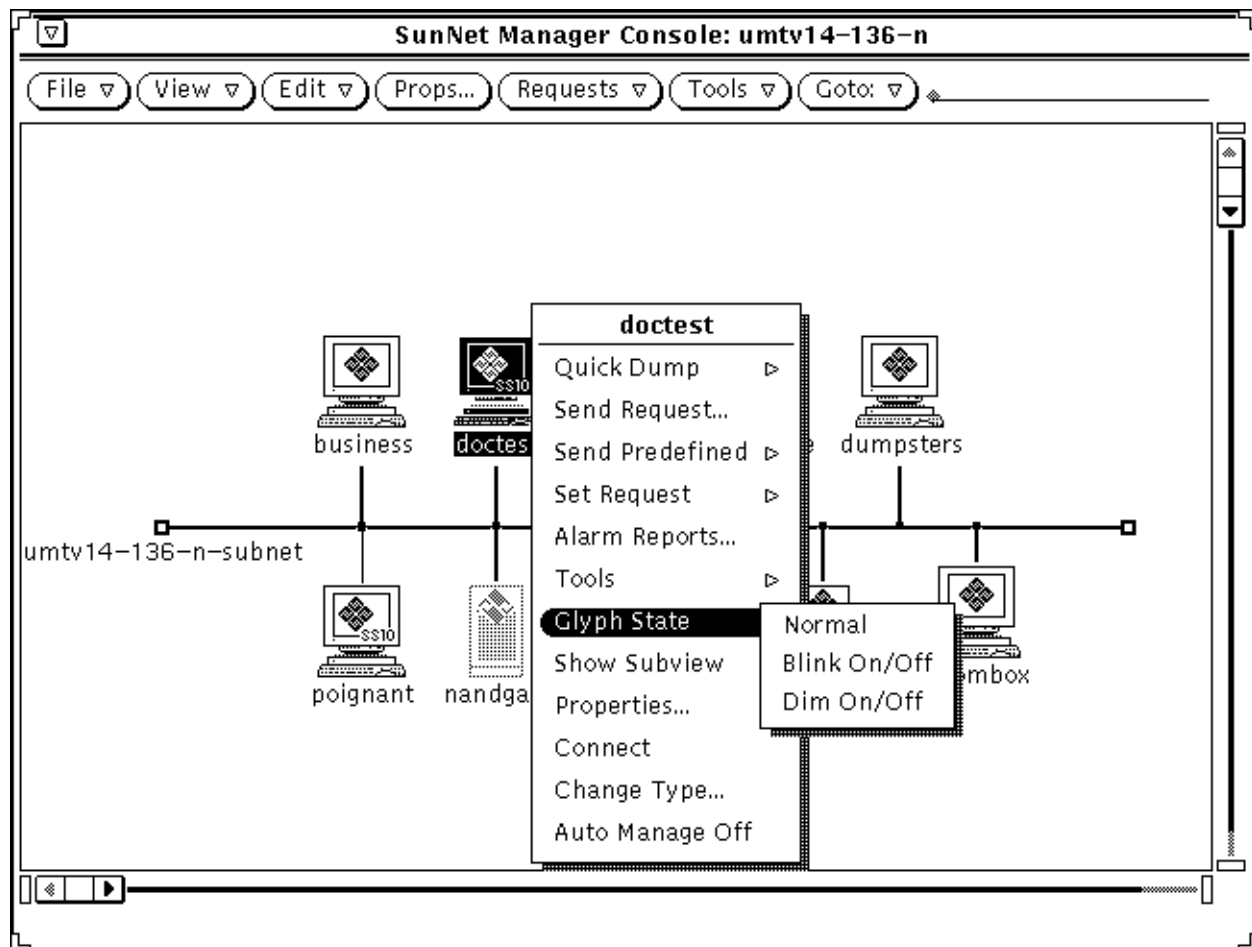


Figure 5-6 Glyph—Glyph State Menu

5.4.1 Notes

Whenever a glyph state is changed as a result of an event or a trap, the glyph state is propagated through the view hierarchy. If a glyph is contained in more than one view, its state is propagated through its multiple view hierarchies. When the Console is closed to an icon, glyph state changes reflected in the Home view cause the Console icon to display question marks.

When you change the state of a glyph, the new glyph state is propagated as though an event had occurred to change the glyph state. For example, if you change the glyph state of an element from “normal” to “blinking,” the glyph state “blinking” propagates as if an event had occurred.

If you have multiple glyph states propagating into a single view and you change the glyph state for the view to “normal,” the glyph states of the elements contained in the view are also reset to “normal.” For example, if you change the glyph state of a view from “blinking” to “normal,” this clears the effects of the event that caused the glyph state to change to “blinking.” This allows you to clear multiple events by resetting the glyph state of a view.

You can also choose to have errors that are received from agents cause a change in the glyph state of an element. By default, this is not enabled. See the description of the Errors category of the Console Properties window in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

5.5 Changing the Propagation of Glyph State Changes

By default, glyph state changes caused by events or traps are propagated through the view hierarchy. You can disable glyph state propagation in several ways.

To disable glyph state propagation for a particular view:

1. **Over the glyph that represents the view, press MENU to open the Glyph menu for the view.**
2. **Release MENU over Properties to open the Properties window for the view. (See Figure 5-7.)**

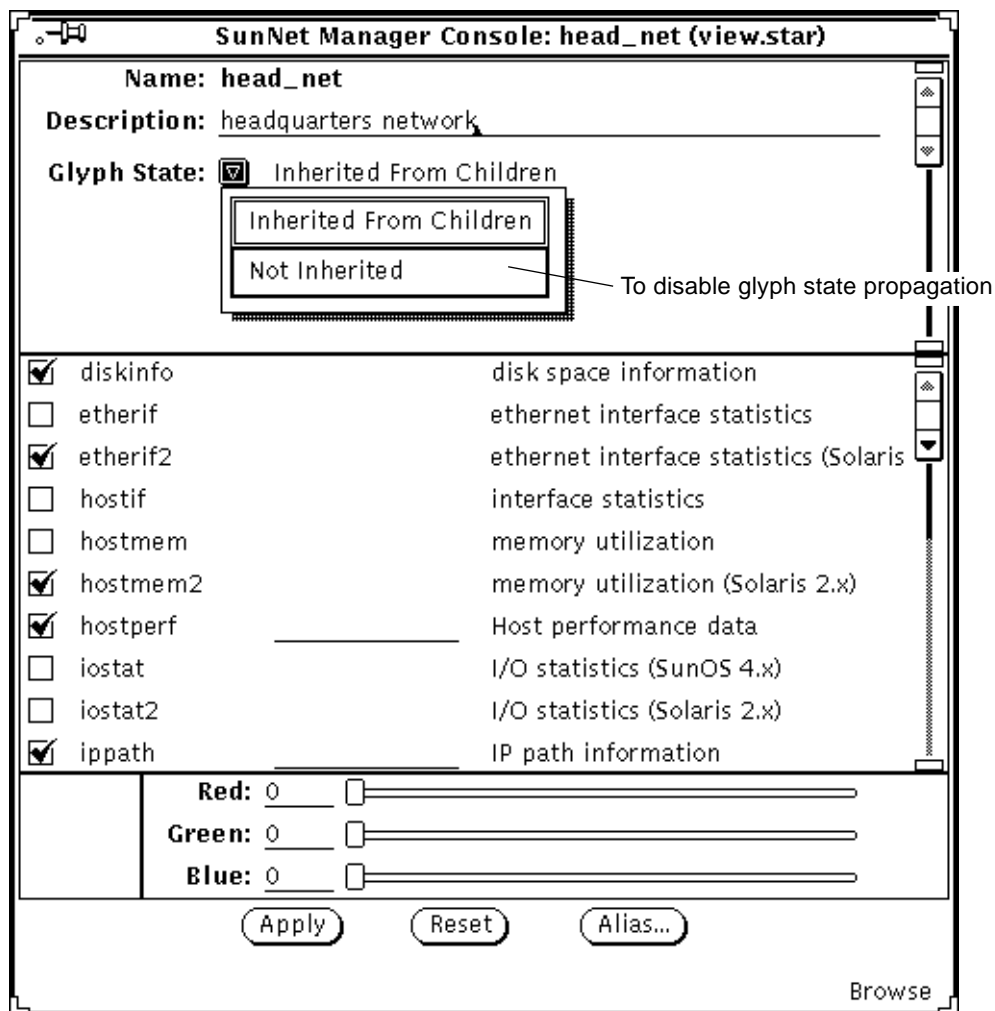


Figure 5-7 Properties Window for a View

3. In the Properties window, press MENU over the Glyph State abbreviated menu button in the top portion of the window. Release MENU over the Not Inherited option.
4. Click SELECT on the Apply button.

To disable glyph state propagation for all views in the database:

1. Click **SELECT** on the **Props** button in the **Console** window.
2. In the **Console Properties** window, press **MENU** over the **Category** abbreviated menu button to open the categories menu. Release **MENU** over **Events and Traps**. (See Figure 5-8.)

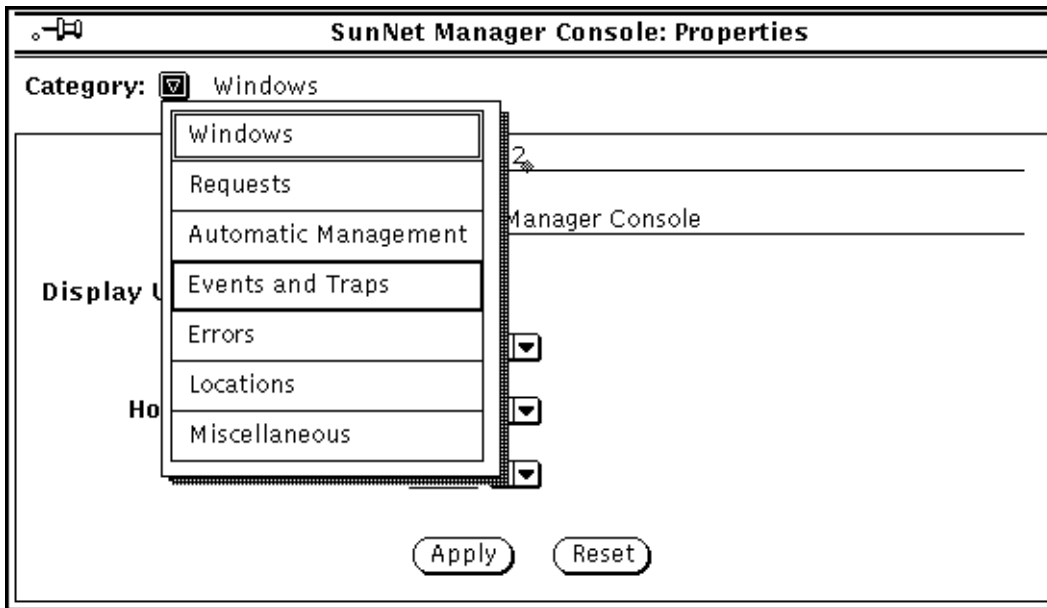


Figure 5-8 Console—Properties—Category Menu

3. In the **Events and Traps** categories window, click **SELECT** in the box next to the **Propagate Event Effect** setting to toggle the check mark off. (See Figure 5-9.)

SunNet Manager Console: Properties

Category: ▾ Events and Traps

Open on Event or Trap:

Upon Opening: ▾ Stay in Current View

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:

Figure 5-9 Properties—Event/Trap Window

4. Click SELECT on the Apply button.

To disable propagation of glyph states caused by traps:

- 1. Open the Events and Traps category settings in the Console Properties window, as described in the previous steps.**

-
- 2. Click SELECT in the box next to the Traps Propagate Effect setting to toggle the check mark off.**
- 3. Click SELECT on the Apply button.**

Viewing and Managing Requests



<i>Viewing the Status of Requests</i>	<i>page 6-1</i>
<i>Viewing and Modifying Properties of a Request</i>	<i>page 6-3</i>
<i>Stopping or Killing Requests</i>	<i>page 6-6</i>

You can view and manage requests in several ways:

- The SNM Console Requests►Summary window allows you to view the status of all requests that have been started from the Console session. From the Requests►Summary window you can stop, kill, or restart multiple requests at a time or modify the properties of a request.
- Each request is associated with a request glyph that resides in the subview of the target element. From the Glyph menu for the request you can modify, stop, or kill the request.

This chapter describes how to view, modify, stop, and kill requests from the Requests Summary window and from the Glyph menu for the request.

6.1 Viewing the Status of Requests

The SNM Console Requests►Summary window allows you to view the status of all active or held Console requests. To receive the Requests►Summary pop-up window:

1. Move the mouse pointer over the Requests button and press MENU to open the Requests menu.
2. Drag the mouse pointer down to Summary and release. (See Figure 6-1.)

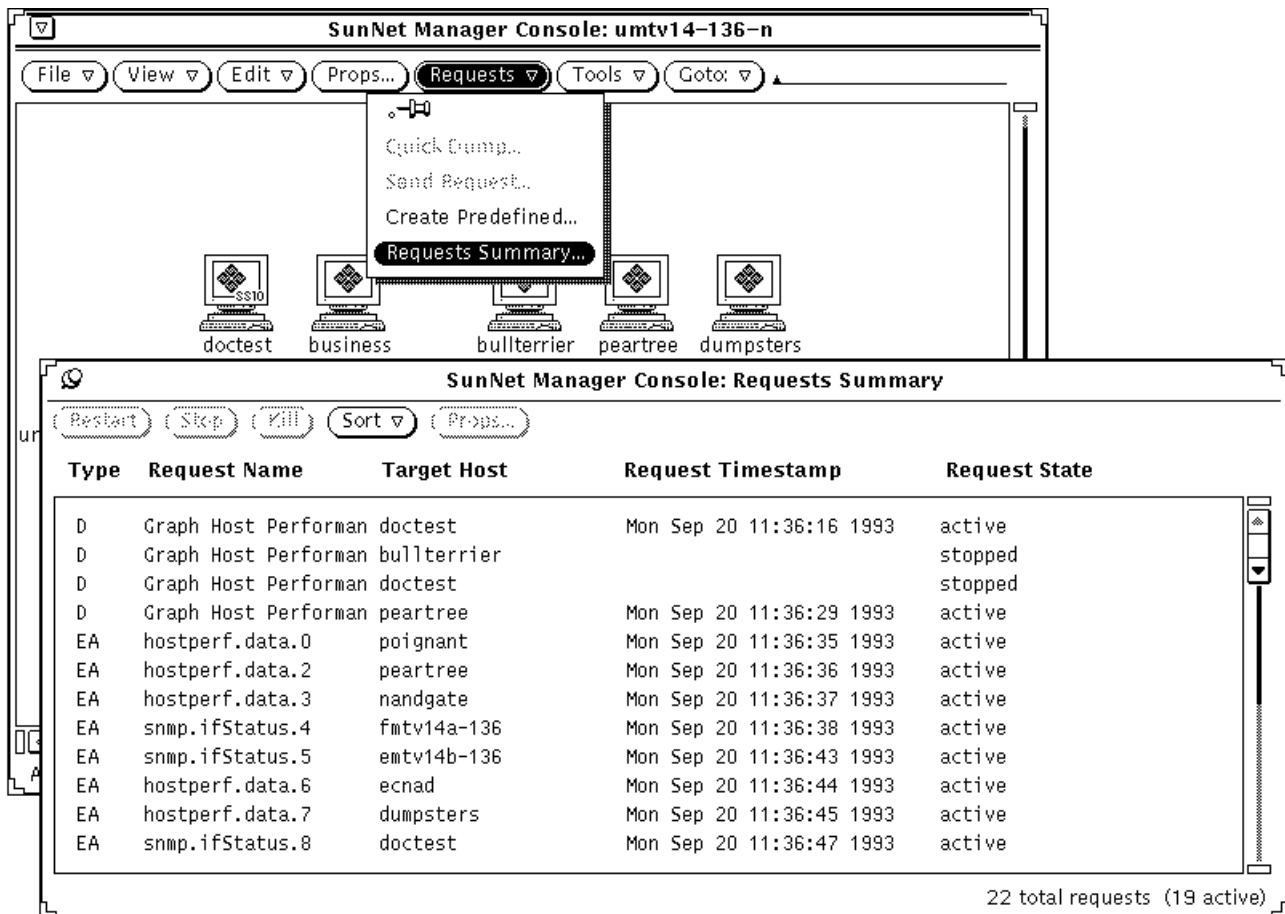


Figure 6-1 Sample Requests—Summary Window

Help

On-line help is available for this window.

3. To display the requests in a different order:
 - a. Move the mouse pointer over the Sort button and press MENU to open the Sort menu.
 - b. Drag the mouse pointer down and release on the desired sort.

6.1.1 Notes

Every active or held Console request is shown in one of several *states*:

- When you start a request (you click SELECT on the Start button on the Properties window for the request), the request state is initially *awaiting activation*. Normally, the request state quickly changes to *being activated*, followed by *active*.
- If an agent error occurs while a request is being activated, the request state changes to *stopped*.
- An active request that is stopped or killed passes through the states *awaiting stop*, *being stopped*, and *stopped*.
- A held request (you click SELECT on the Hold button on the Properties window for the request) is shown in *stopped* state.
- If you specified Delete Request in the Upon Completion field in the Properties window of a request, the request disappears from the Requests►Summary window when the request is completed. If you specified Save Request in the Upon Completion field in the Properties window of a request, the state of the request becomes *stopped* when the request is completed.
- Note that the states *awaiting activation*, *being activated*, *awaiting stop*, and *being stopped* are normally temporary. If you notice that a request seems to be in one of these states for a long time without changing, you should make sure that the target element is reachable by using the ping agent to do a Quick Dump request.

6.2 Viewing and Modifying Properties of a Request

You can modify a data or event request from the Requests►Summary window or from the request glyph.



On-line help is available for this window.

To view the properties of a request from the Requests►Summary window:

1. **Click SELECT on the request whose properties you want to view or modify.**
2. **Click SELECT on the Props button at the top of the window. (See Figure 6-2.)**

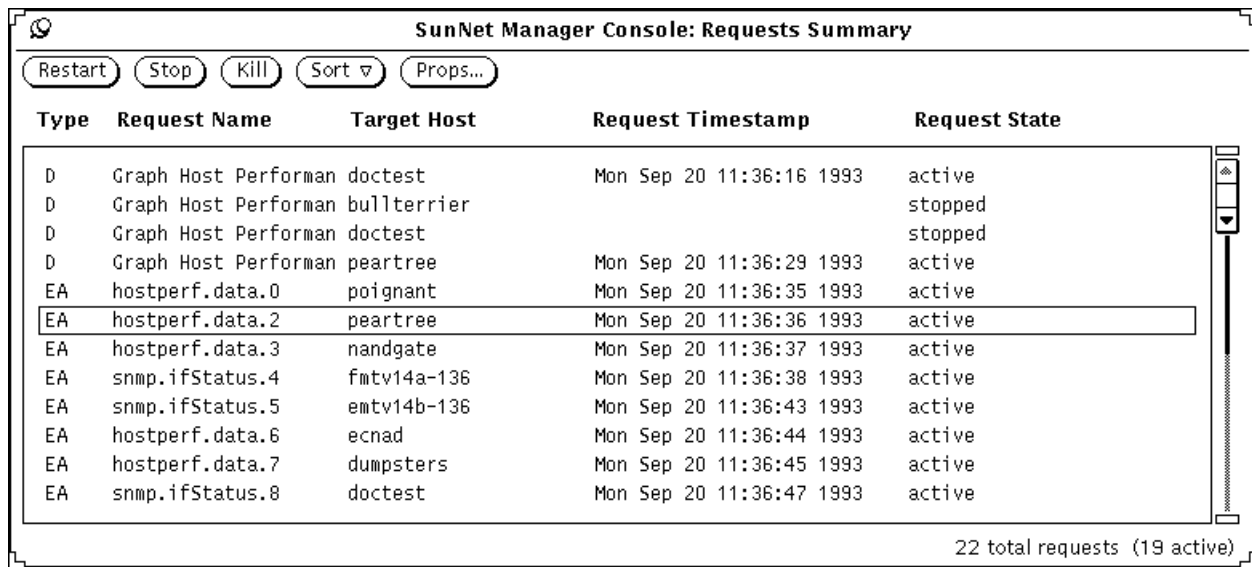


Figure 6-2 Requests—Summary Window

To view the properties of a request from the request glyph:

1. **Move the mouse pointer over the glyph that represents the target element for which you have specified an Event or Data report, and double-click SELECT.**
Data requests are represented by a meter glyph, while event requests are represented by an alarm clock glyph. When a request is active, its glyph appears black or solid. When a request is stopped or held, its glyph is dimmed.
2. **Move the mouse pointer over the glyph that corresponds to the request and press MENU to open the Glyph menu for that request.**
3. **Drag the mouse pointer down to Properties and release. (See Figure 6-3.)**

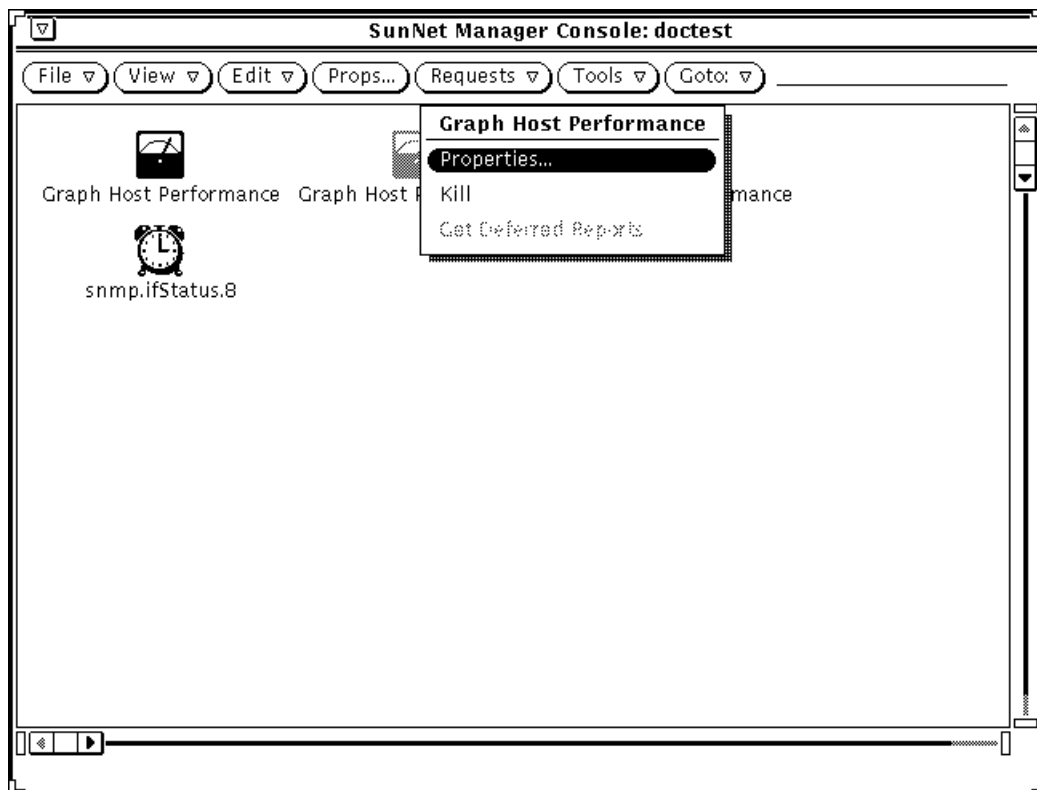


Figure 6-3 Request Glyph Menu

6.2.1 Notes

Once the Properties window for the request is displayed, you can modify request reporting characteristics or the attribute or event specifications.

To change how an attribute is logged or displayed, select the attribute in the Attribute values scrolling list by pointing the mouse at the entry and clicking SELECT. This causes the current values of the event definition to appear in the fields on the right side of the window. If you modify any of these fields, click the Apply button at the bottom of the window. To delete an attribute from a data request, select the attribute from the Attribute values scrolling list and click the Delete button at the bottom of the window.

When you modify a request, you are actually changing the specification for that request, not launching a new one. The original request is stopped and then restarted with the new specifications.

To send the modified request to the agent, click **SELECT** on the Restart button on the lower left of the window. Clicking the Stop button stops the request and saves it only if you have previously specified the Save Request option in the Upon Completion field. Otherwise, the Stop button effectively kills the request.

6.3 Stopping or Killing Requests

Killing a request removes a request from the runtime database. Killing a request removes the request even if you have set the Upon Completion field in the Properties window to Save Request.

If the Upon Completion field in the properties of a request is set to Delete Request, then stopping the request is the same as killing the request. If the Upon Completion field is set to Save Request, then stopping the request saves the request in *stopped* state.

From the Requests►Summary window you can stop or kill multiple requests at the same time. To stop or kill requests from the Requests►Summary window:

1. Select the requests you want to stop or kill.

You can click **SELECT** on one request and click **ADJUST** on other requests that you wish to select.

Or, you can use the Select menu of the Requests►Summary window:

a. Press MENU in the scrolling list area of the Requests►Summary window to open the Select menu.

b. Drag and release on the desired selection type.

2. Click **SELECT on the Stop or Kill button at the top of the Requests►Summary window. (See Figure 6-2 on page 6-4.)**

Viewing Reports



<i>Viewing Alarm Reports</i>	<i>page 7-1</i>
<i>Viewing Error Messages and Error Reports</i>	<i>page 7-7</i>
<i>Viewing Traps</i>	<i>page 7-10</i>

7.1 Viewing Alarm Reports

There are four types of reports returned by SunNet Manager: data, event, error, and trap. Of these four, the Console groups the last three under the heading of “alarms.” SNM allows you to view a summary of alarm reports for all elements within a given view. To do this, perform the following steps:

- 1. Make sure there are no glyphs selected in the Console window.**
- 2. Press MENU on the View button in the Console window and release MENU over Alarms.**

You receive a window such as the following:

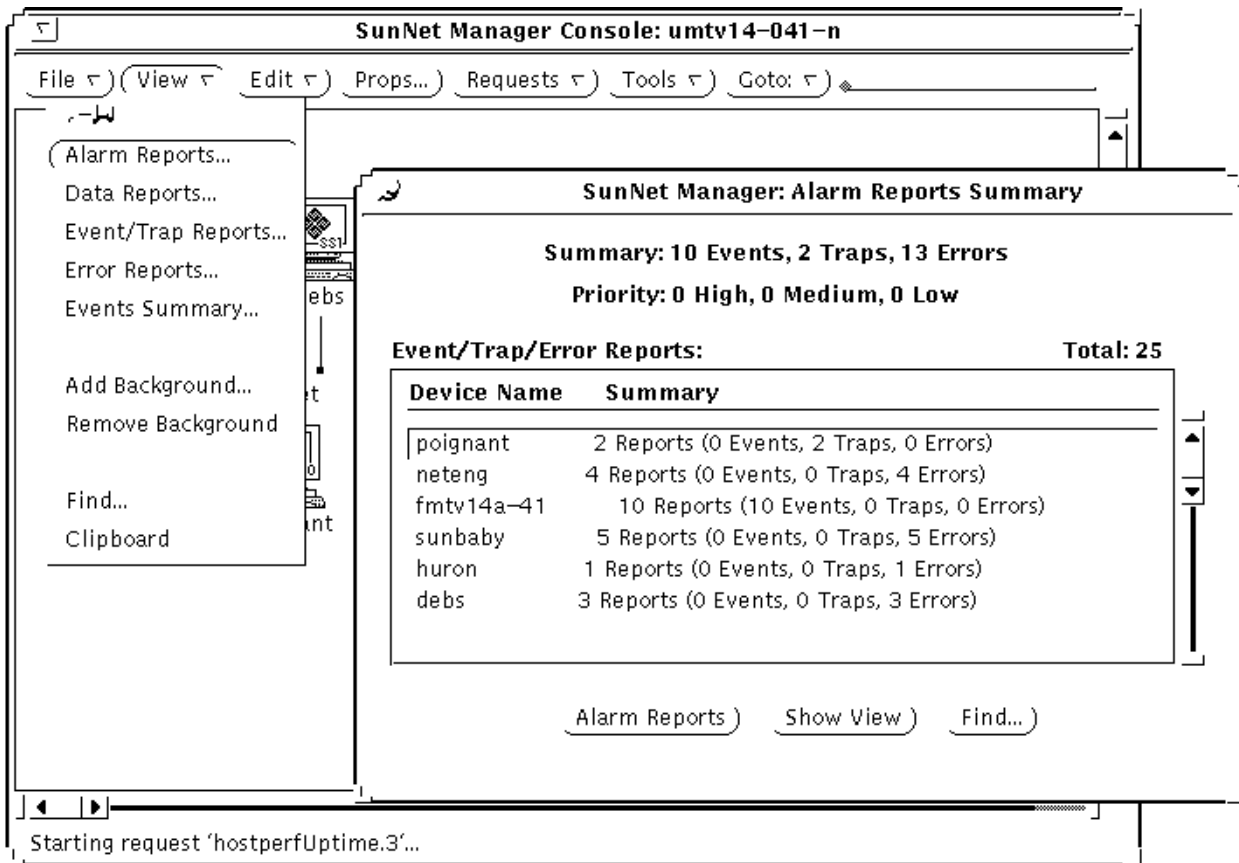


Figure 7-1 Alarm Reports Summary Window

Note – If both the SNM Console Alarm Report Summary window and a device-specific Alarm Summary window are displayed simultaneously and reports continue to arrive for the device, the number-of-reports-received totals for the two windows will differ until the SNM Console Alarm Reports Summary window is next updated (every 30 seconds).

The following subsections describe functions available through the Alarm Reports feature, including (but restricted to) the functions available through the buttons—Alarm Reports, Show View, and Find—at the bottom of the Alarm Reports Summary window.

7.1.1 Finding a Device

To find a device that is not visible in the window's scrolling list, you can scroll through the list or, more conveniently:

1. Click **SELECT** on the **Find** button at the bottom of the window.

After clicking on Find, you receive the window shown in Figure 7-2.

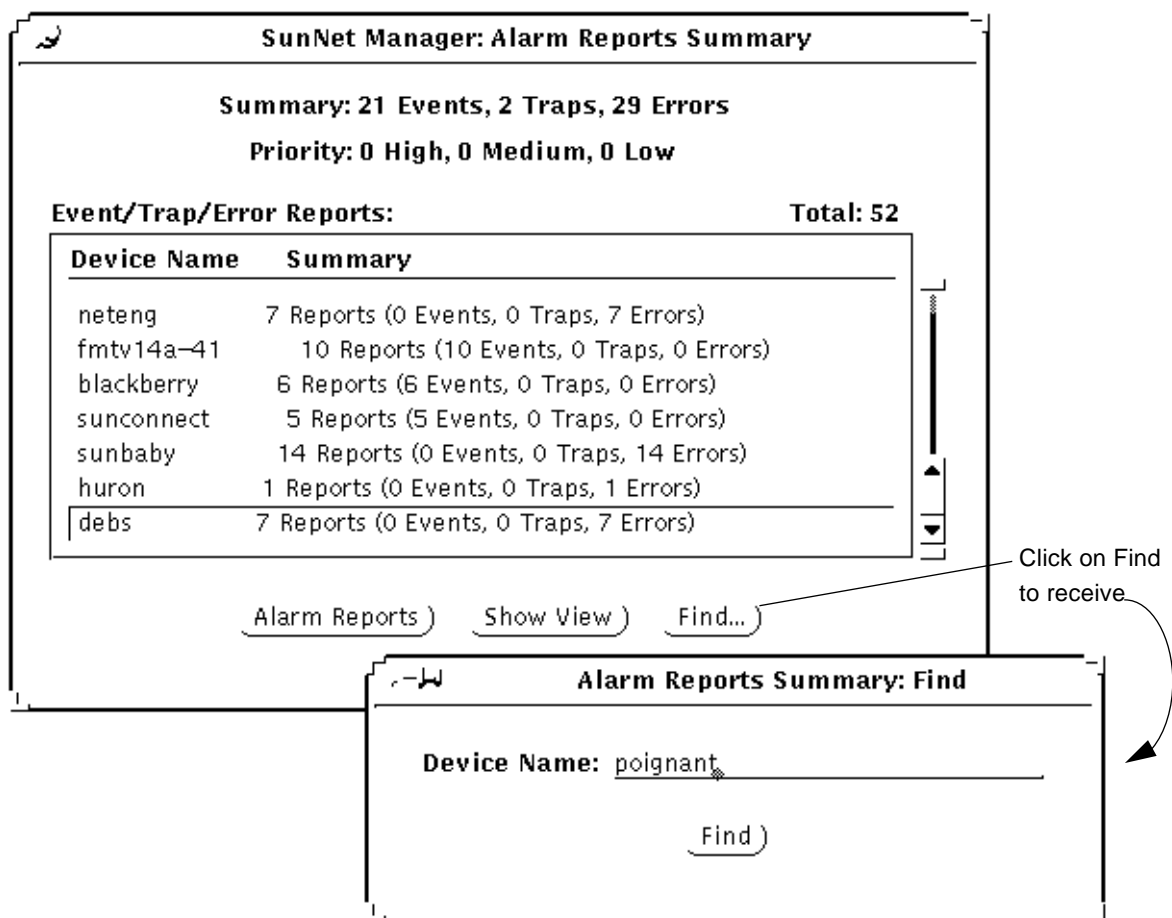


Figure 7-2 Alarm Reports Find Window

2. In the **Device Name** field, enter the name of the network element of the report for which you are looking for.

3. Click SELECT on Find in the Find window.

If a line for a device is present, that line is displayed and highlighted in the Alarm Reports window’s scrolling list. If a line for a device is not present, you receive the message “Device name not found” in a popup window.

7.1.2 Switching Views

Through the Alarm Reports Summary window, SNM allows you to switch views for a specific device. (This function is also available through the View►Find option in the Console window.) To show the current view for a device and to be able to switch views, do the following:

- 1. Select the specific device in the Alarm Reports Summary window’s scrolling list.**
- 2. Click SELECT on the Show View button at the bottom of the Alarm Reports Summary window.**

You receive a window such as the one shown in Figure 7-3.

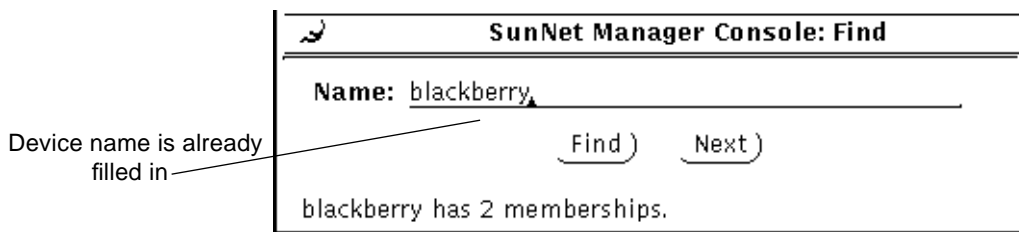


Figure 7-3 Alarm Reports: Show View Window

If a device is in only one view, the Next button in the window above is greyed-out.

- 3. If a device is in multiple views, click SELECT on Next to switch from the current view (as displayed in the Console window) to the next view in which the specified device appears.**

In this context, “next” means the next view on the list of views as displayed by the Console’s Goto menu.

7.1.3 Obtaining Device-specific Alarm Reports

SNM gives you the ability to view further detail for a specific device. To obtain a device-specific report, you can use any of the following methods:

- Double click on the line for a device in the scrolling list in the Alarm Reports Summary window.
- Click SELECT on the line for a device in the scrolling list in the Alarm Reports window, then click SELECT on the Alarm Reports button at the bottom of the window.
- Click SELECT on the glyph for a device and invoke View►Alarm Reports in the Console menu
- Invoke Alarm Reports from an element's glyph menu.

Using any of the preceding methods, you then receive an Alarm Reports window for the specified device, as shown in Figure 7-4.

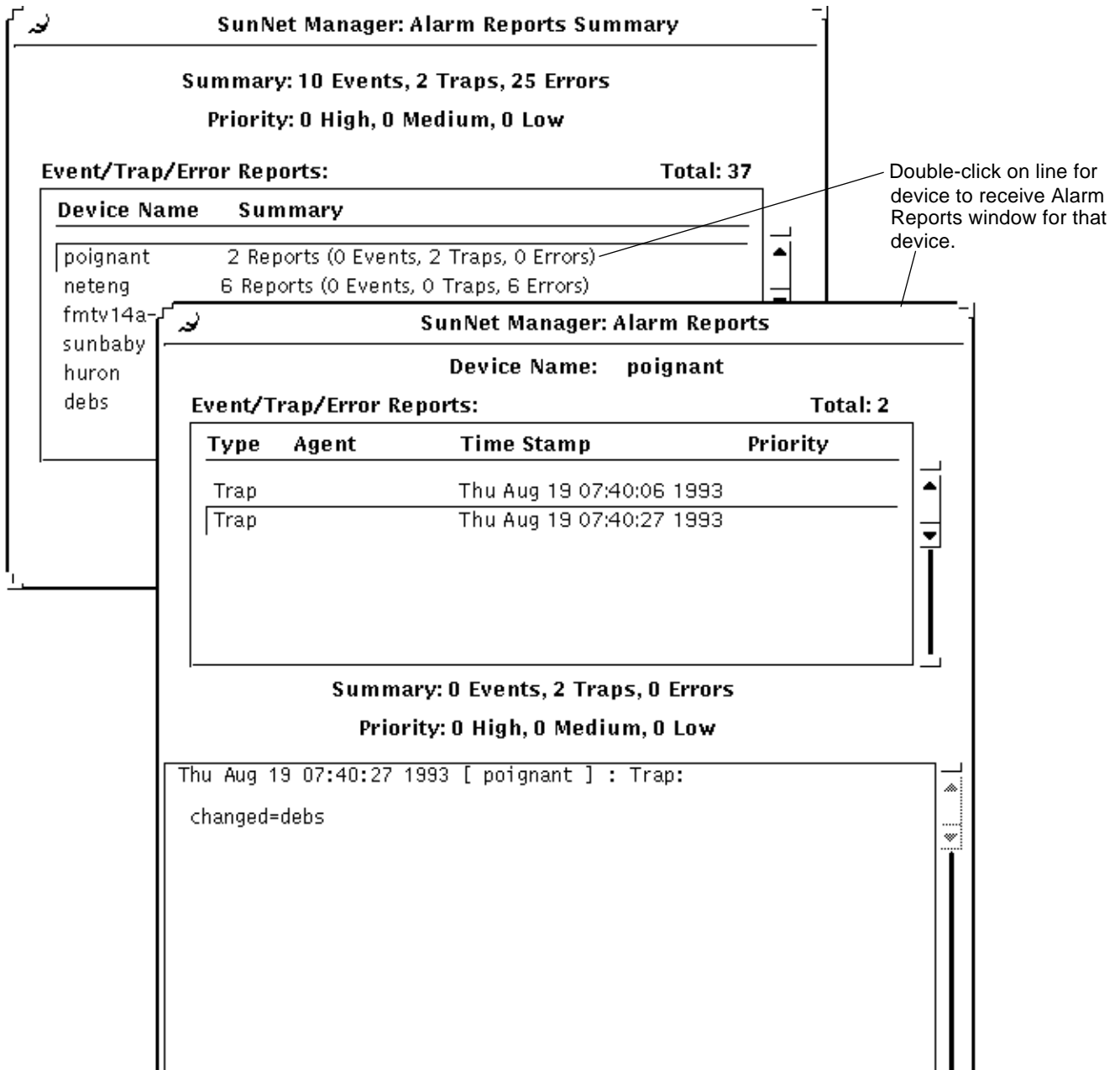


Figure 7-4 Device-specific Alarm Reports Window

7.1.4 Features of Device-specific Alarm Reports Window

A device-specific Alarm Reports window, such as the one shown in Figure 7-4, allows you to:

- sort alarm reports
- filter reports
- find reports associated with a specific agent
- save reports to a file
- print reports

These functions are available through the View, Save, and Print buttons at the bottom of the Alarm Reports window. These functions are described in detail in Chapter 4 of the *SunNet Manager 2.2.3 Reference Manual*.

7.2 Viewing Error Messages and Error Reports

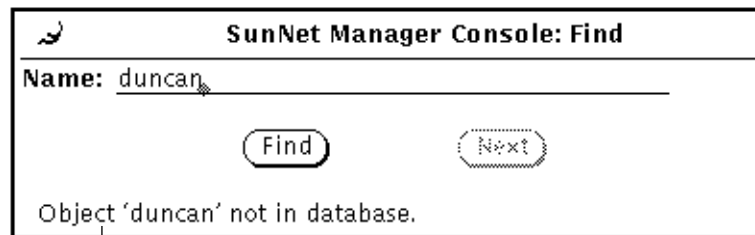
The SunNet Manager Console displays error messages in several locations:

- Footer of the Console window.
These messages are generally brief messages about the status of an operation and are *temporary*. They will be overwritten by subsequent status messages. Because of the brevity of these messages, you are usually directed to the Error Reports window for more information about error messages.



Figure 7-5 Console Window Footer Display

- Footer of the Console pop-up windows or a tool (Results Browser, Grapher, Set Tool) window.
These messages are described in Appendix A of the *SunNet Manager 2.2.3 Reference Manual*.



Pop-up window footer message.

Figure 7-6 Console Pop-up or Tool Window Footer Display

- Error Reports window.
Errors detected by the Console and errors returned by agents are displayed in this window. These messages are described in Appendix A of the *SunNet Manager 2.2.3 Reference Manual* and in the man page for the agent.

To view the Error Reports window:

1. **Move the mouse pointer over the View button and press MENU to open the View menu.**
2. **Drag the mouse pointer down to Error Reports and release MENU. You receive:**

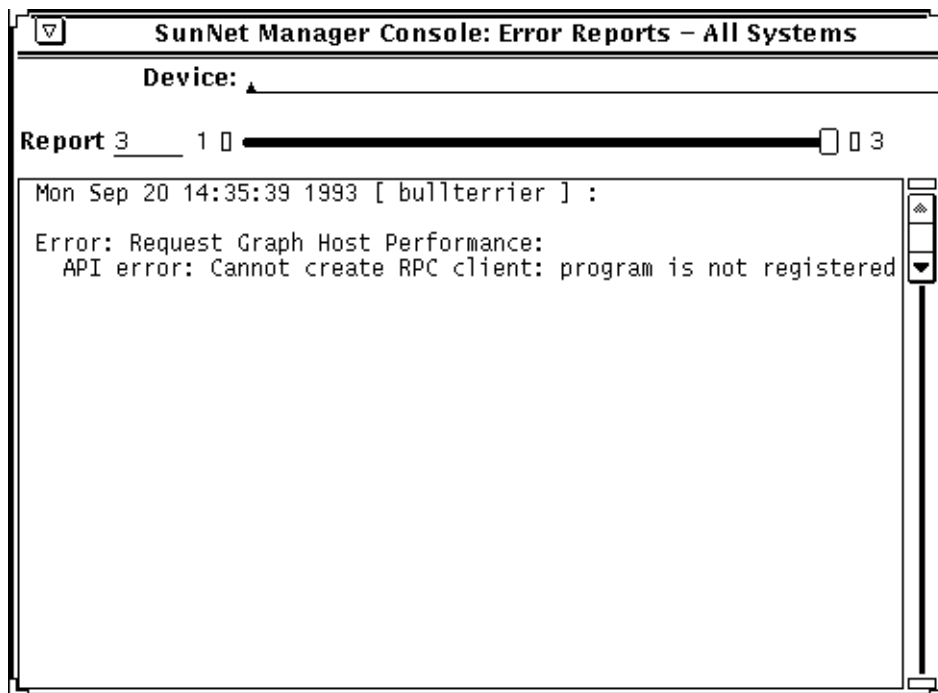


Figure 7-7 Sample Error Reports Window

3. **To examine error reports for a particular system, type in the device name after the Device prompt and press Return.**
To see entries for all elements again, press Ctrl-U to clear the Device line and press Return.
4. **To save the error reports to a file, press MENU in the output portion of the Error Reports window and release MENU over File>Save or File>Store as New File. In the window you then receive, select or enter a directory and enter a file name. Click SELECT on the Save button.**
5. **To browse through entries in the log:**
 - Press SELECT on the slider and drag the slider to the left or right.
 - Click SELECT to the left or right of the slider.
 - Click SELECT on either end of the slider bar.
 - Enter the number of a report on the Report line and press Return.

Help

On-line help is available for this window.

7.2.1 Notes

Two types of agent errors are returned to the Console. Agent-specific errors are errors defined in the agent schema file—these error messages are described in the `man` pages for each agent. There are also “generic” errors, such as “unknown host” or “no threshold value”—these errors are described in Appendix A of the *SunNet Manager 2.2.3 Reference Manual*.

Agent errors can also be classified as “fatal” or “warning.” All generic errors are fatal errors. Agent-specific errors can be either fatal or warning. Fatal errors cause the agent to stop servicing the request. Warnings are for your information only; the agent will continue to return reports.

The Errors category of the Console Properties window allows you to specify signal options and any operations to be started when the Console receives an error from an agent. The default Errors category settings cause the glyph for the target element to be dimmed only if a fatal error is reported for the element. The glyph effect is not propagated. You can change the Errors category settings—for more information, refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

Fatal errors reported by agents, whether agent-specific or generic, are considered in the Console as high-priority errors. The Console treats warnings as low-priority errors. Thus, if you specify Color by Priority in the Glyph Effect setting for the Errors category in the Console Properties window, fatal errors will change an element glyph to red, and warnings will change an element glyph to yellow.

By default, a maximum of 100 error reports are displayed in the Error Reports window. You can change the maximum number in the Console Properties window. See the description of the Maximum Error Reports setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

7.3 Viewing Traps

A trap is an unsolicited report sent from an agent that usually signifies some unexpected error condition. Trap reports are displayed in the Event/Trap Reports window.

When a trap is generated, a trap report is returned to the Console that indicates the cause of the trap. The report is stored in the `event.log` file and may be viewed in the Event/Trap Reports window.

1. In the Console window, press MENU in View►Event/Trap Reports and release MENU. You receive:

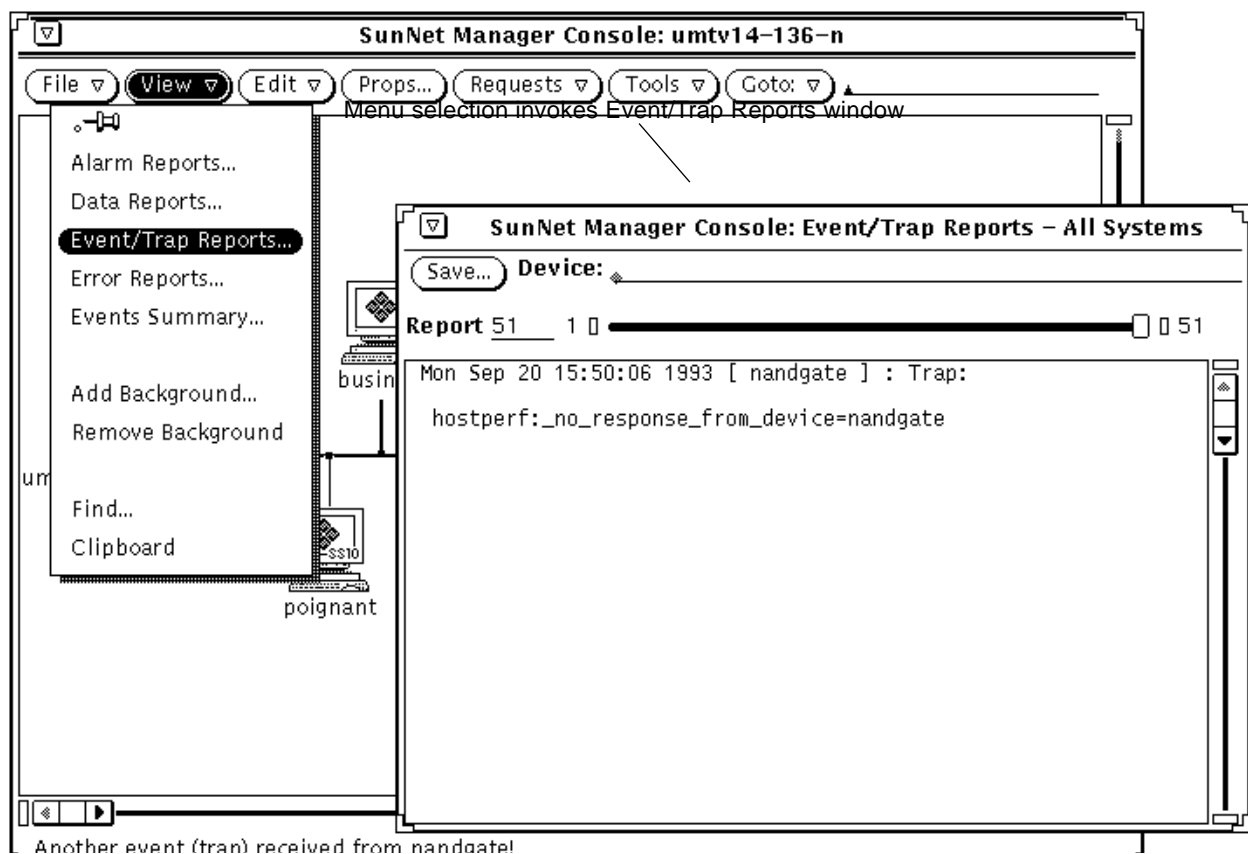
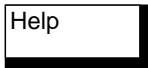


Figure 7-8 View—Event/Trap Reports Window

2. To examine trap reports for a particular system, type in the device name after the Device prompt and press Return.
To see entries for all elements again, press Ctrl-U to clear the Device line and press Return.

An alternative way to obtain an element-specific trap reports is to click SELECT on the glyph in the Console window, then invoke View►Event/Trap Reports.



On-line help is available for this window.

3. To save the Event/Trap Reports to a file, click SELECT on the Save button.

A pop-up Save window appears, where you can enter the path and file name where the event/trap reports are to be stored.

4. To browse through entries in the log:

- Press SELECT on the slider and drag the slider to the left or right.
- Click SELECT to the left or right of the slider.
- Click SELECT on either end of the slider bar.
- Enter the number of a report on the Report line and press Return.

7.3.1 Notes

The Trap Information settings in the Events and Traps category of the Console Properties window allow you to specify signal options and any operations to be started when the Console receives a trap. The default Events and Traps category settings cause the glyph for the target element to blink only if a trap is reported for the element. By default, the glyph effect is propagated. If the Console window is closed to an icon, you can specify that it be opened automatically if an event or trap is received. To view or change event- and trap-related settings, click SELECT on Props in the Console's control area, then select Events and Traps in the Category pulldown menu. For more information on changing Trap Information settings, refer on the Console's Properties window in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

Trap reports are generated when elements are added, changed, or deleted in the runtime database. By default, these traps are ignored by the Console. If you want to have these traps displayed, toggle the check mark off in the Ignore Database Traps setting for the Events and Traps category. If a glyph effect is specified for traps, the glyph representing the system on which the runtime database is located is affected.

Note – With the Ignore-Database-Traps option turned off in the Console's Props►Events and Traps window, when you create an element, the trap report for that element says that the element was “created”. An analogous operation using the database API returns the word “added” rather than “created”.

Traps can be high, medium, or low priority. The Console considers SNMP traps forwarded by the SNMP trap daemon to be high-priority and traps generated by changes to the runtime database to be low-priority. Thus, if you specify

Color by Priority in the Glyph Effect setting for the Events and Traps category in the Console Properties window, SNMP traps will change an element glyph to red and database traps will change an element glyph to yellow.

By default, a maximum of 1000 trap reports are displayed in the Event/Trap Reports window. You can change this maximum number in the Console Properties window. See the description of the Maximum Trap Reports setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

Managing Printers



Through the `lpstat` agent, SNM allows you to check the queue and check the status of remote printers. A printer to be managed can be connected to a machine running SunOS 4.x or Solaris 2.x.

Perform the following steps to allow management of a remote printer:

1. Install the SNM agents on the machine to which the printer is connected (the printer server).

If the machine is running Solaris 2.x, use `pkgadd`; if it is running SunOS 4.x, use `getagents`. See Chapter 4 of *SunNet Manager 2.2.3 Installation Guide* for instructions on installing agents.

2. In the Console window, create an element of category component and type `laserwriter`, `newsprinter`, or `printer`, as appropriate.

See Section 3.5, “Creating Elements,” on page 3-15 for instructions on creating an element. Figure 8-1 shows an example Create Object window.

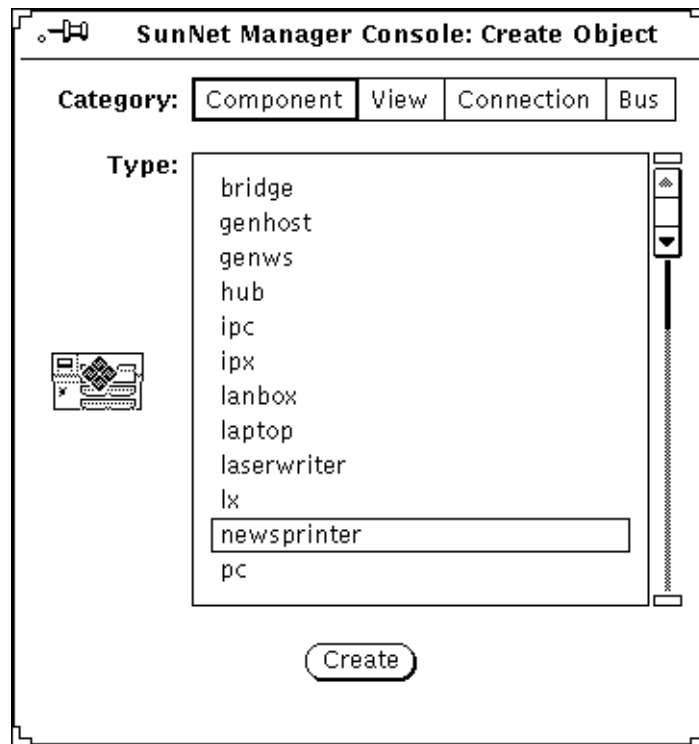


Figure 8-1 Creating a Printer

3. After clicking SELECT in the window above, you receive an element properties window. In this window, do the following:

- a. Enter the name of the printer (print queue name)—*not* the name of the printer server.
- b. Check off the `lpstat` agent.
- c. Enter the name of the connected machine as the proxy.
- d. Click SELECT on Apply.

Do not check off any agents other than `lpstat`. See Figure 8-2 for an example element properties window.

SunNet Manager Console: New component.newsprinter

Name: bc

Contact: _____

Location: _____

Description: _____

<input type="checkbox"/>	ippath	IP path information
<input type="checkbox"/>	iproutes	IP route table and statistics
<input type="checkbox"/>	layers	protocol layer statistics
<input type="checkbox"/>	layers2	protocol layer statistics (for SunOS 5
<input checked="" type="checkbox"/>	lpstat	<u>master</u>	line printer status and queue info
<input type="checkbox"/>	ping	IP connectivity info
<input type="checkbox"/>	rpcnfs	RPC and NFS stats
<input type="checkbox"/>	sample	kernel mbufs agent
<input type="checkbox"/>	snmp	vanilla snmp agent
<input type="checkbox"/>	snmp-mibII	snmp-mibII proxy

Red: 0 _____

Green: 0 _____

Blue: 0 _____

Apply Reset Alias...

Create

Figure 8-2 Properties for New Printer

If you want to receive data or event reports from the printer server, you must create a separate element for that machine. When specifying agents for the printer server, do not check off the `lpstat` agent.

SNM allows you to obtain Quick Dumps and send data and event requests to the printer, just as you would send such requests to a workstation, server, or other type of element. SNM is shipped with a predefined event request so that you can be informed if the printer becomes unavailable. Use of this request is illustrated in Figure 8-3.

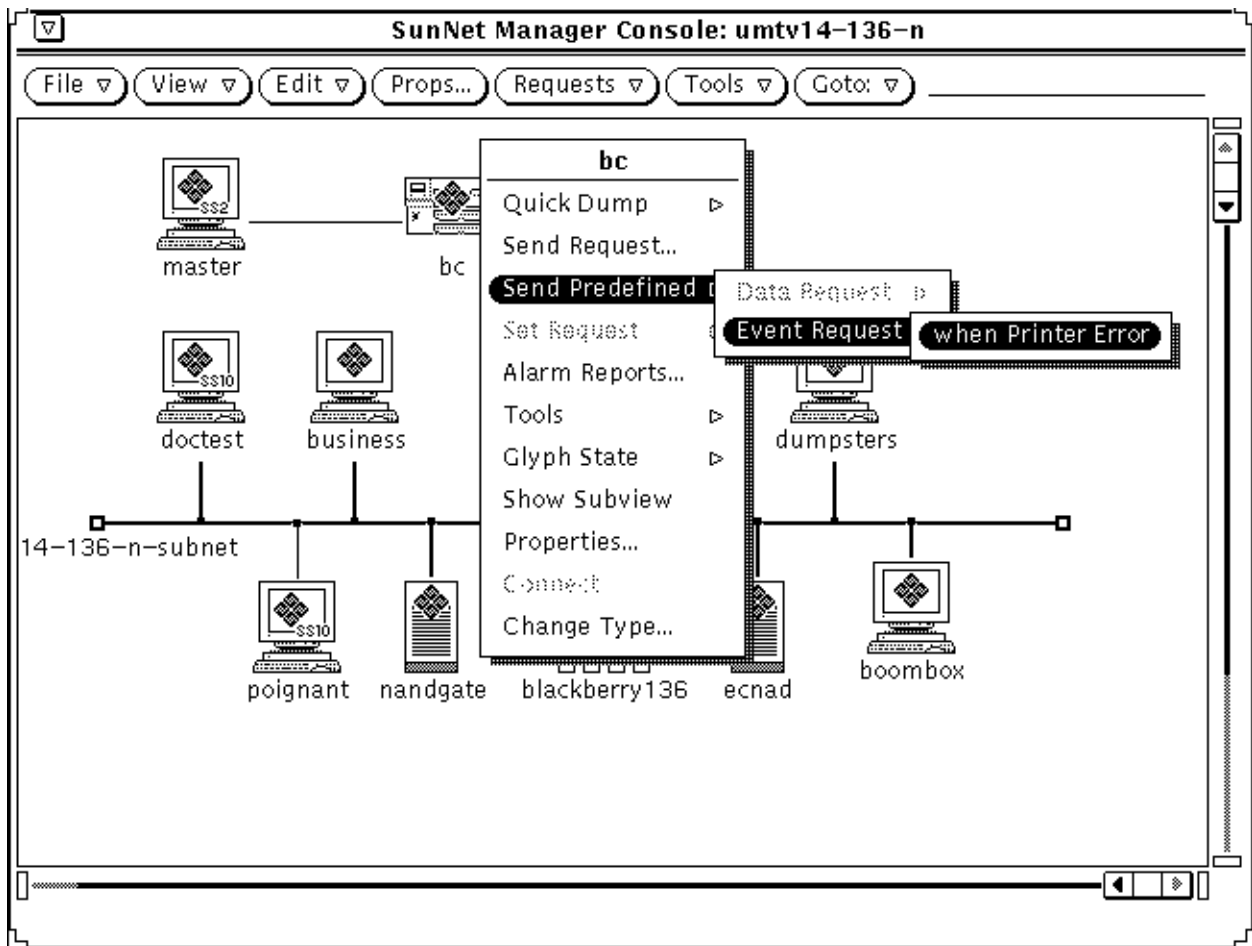


Figure 8-3 Sending Predefined Request to Printer

Through the Quick Dump mechanism (in the printer's glyph menu press MENU on Quick Dump▶lpstat▶queue or ▶status), you can view the current job queue for a printer or obtain the current status. Status is reported as one of the following codes:

- 0 idle
- 1 waiting
- 2 printing
- 3 error

Through the `lpstat` agent, you can obtain a variety of information about print queue and printer status. There are some differences between information returned from printers connected to SunOS 4.x printer servers and that returned from Solaris 2.x print servers. See the `na.lpstat (8)` man page for details.

Managing SNMP Devices



<i>Adding SNMP Devices</i>	<i>page 9-2</i>
<i>Creating an SNMP Element in the Database</i>	<i>page 9-5</i>
<i>Setting Up SNM to Receive Traps from a Device</i>	<i>page 9-10</i>
<i>Using the Set Tool to Retrieve SNMP Attribute Values</i>	<i>page 9-12</i>
<i>Using the Set Tool to Change SNMP Attribute Values</i>	<i>page 9-17</i>

SunNet Manager (SNM) provides a proxy agent that supports the Simple Network Management Protocol (SNMP), the most widely-implemented network management protocol for managing TCP/IP networks. The *SNMP proxy agent* allows you to get data and event information from, and set attribute values for, devices that are manageable through SNMP. The proxy agent can handle requests from the Console for multiple SNMP devices on a network.

The *SNMP trap daemon* receives traps from SNMP devices, filters the traps, and translates the traps into SunNet Manager traps. The trap daemon then forwards the traps to one or more management stations.

Management of SNMP devices is similar to management of non-SNMP devices, with the following exceptions:

- Multiple schemas can be associated with an SNMP device (however, only one schema can be specified in a request).

- While SunNet Manager uses schema files to describe the attributes of a managed object, the SNMP protocol uses a Management Information Base (MIB) to describe the attributes of a managed object.

This chapter describes how to integrate SNMP devices into your SunNet Manager environment so that you can use SNMP to manage those devices. You should have some familiarity with SNMP concepts to proceed with the tasks described in this chapter. Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual* for a detailed description of how the SNMP proxy agent works.

9.1 Adding SNMP Devices

The following is an overview of how to add non-Sun SNMP devices to your management database. Detailed explanations of each step follow in the “Notes” section.

Note – If you are using SNMP to manage Sun workstations that contain the SNM-supplied SNMP agent (`snmpd`), you can skip this task and proceed to Section 9.2, “Creating an SNMP Element in the Database,” on page 9-5.

1. Install the device on the network.

2. Obtain the schema file for the device.

3. Configure the SNMP proxy agent.

The schema file should reside in a directory specified by `na.snmp.schemas` in the `snm.conf` file, for example:

```
# @(#)snm.conf2.36 4/14/94 - SunNet Manager configuration file
# Copyright (c) 1990,1993 by Sun Microsystems Inc.

# Site-specific configuration information

### Keywords for the SNMP proxy agent:
# Directory list for SNMP schema files. Separate each directory
# with a colon.
na.snmp.schemas /opt/SUNWconn/snm/agents
```

4. On the Console system, load the schema file.

Skip this step if you are using the SNMP schema files provided with SNM (`snmp.schema` for MIB I devices, or `snmp-mibII.schema` for MIB II devices). The schema file should reside in a directory specified in the SNM Console Properties window.

5. Create the device in the Console.

See section, Section 9.2, “Creating an SNMP Element in the Database,” on page 9-5, for information pertaining to this step.

9.1.1 Notes

The following is a detailed explanation of each step:

1. Install the device on the network.

Refer to the device documentation for installation information. If the device sends SNMP traps that you want forwarded to the SNM Console, you will also want to set up the SNMP trap daemon and Console for trap handling. See Section 9.3, “Setting Up SNM to Receive Traps from a Device,” on page 9-10 for more information.

2. Obtain the schema file for the device.

SunNet Manager uses schema files to manage objects. You can obtain a schema file in one of several ways:

- The vendor of the SNMP device may provide a SunNet Manager schema file. If the SNMP device sends enterprise-specific traps, the vendor may also supply a file that describes these traps—see Section 9.3, “Setting Up SNM to Receive Traps from a Device,” on page 9-10 for more information about setting up SNM to handle enterprise-specific traps.
- The `snm-server@sun.com` electronic mail server maintains a collection of schema files for various SNMP devices. For information on accessing the mail server, see Section , “SunNet Manager Electronic Mail Distribution Service” in the Preface of this book.
- If the SNMP device adheres to MIB I or MIB II specifications, you can use one of the schemas supplied with SNM—either `snmp.schema` (for MIB I) or `snmp-mibII.schema` (for MIB II). If you installed the SNMP proxy agent with `getagents`, the Sun-supplied SNMP schemas are automatically copied onto the host system with other schemas.

- If you do not have a schema file for the device that you want to manage, you can create a schema file from the MIB for the device with the `mib2schema` utility. Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

Change the name of the schema, if necessary. The schema name is *not* the schema file name. The schema name is specified by the keyword `proxy` in the schema file. If `mib2schema` was used to generate the schema file, this name is derived from the name of the MIB (not the MIB file name). This is the name that will appear in the list of agent schemas for each element. Therefore, you may want to edit this name to ensure that it is meaningful to you.

3. Configure the SNMP proxy agent.

- a. A single proxy agent can handle management requests for many devices. You can allow the SNMP proxy agent on the manager station to handle all SNMP requests. However, you may want to distribute the proxy agent to minimize network traffic—see Section 1.1, “Management Applications and Agents,” for more information.
- b. On the proxy system, make sure that the schema file is available to the SNMP proxy agent. The schema file should reside in a directory specified by the `na.snmp.schemas` keyword in the `snm.conf` file on the proxy system. By default, the `snm.conf` file is located in the following directory:
 - `/etc` for the Solaris 1.1.1 version of SNM 2.2.3
 - `/etc/opt/SUNWconn/snm` for the Solaris 2.3 version of SNM 2.2.3

Note – If you modify the `snm.conf` file while the SNMP proxy agent is running, you need to kill the proxy agent (`na.snmp`) for the changes to take effect. Refer to Appendix A of the *SunNet Manager 2.2.3 Reference Manual* for information on how to kill the agent.

4. On the Console system, load the schema file.

Skip this step if you are using the SNMP schema files provided with SNM (`snmp.schema` for MIB I devices, or `snmp-mibII.schema` for MIB II devices).

To load the schema file into the Console:

- a. Start the Console.

- b. Use the Load ► Management Database option in the File menu to load the schema file.
- c. Make sure that the schema file is located in a directory that is specified by the Schema Directories setting in the Console Properties window.

9.2 Creating an SNMP Element in the Database

The Discover Tool, invoked from the Tools menu in the Console's control area, automatically creates SNMP elements. You can specify an option in Discover that allows you to discover only SNMP elements or SNMP elements in combination with other types of elements. See Chapter 5 of the *SunNet Manager 2.2.3 Reference Manual* for a description of the Discover Tool.

To create SNMP elements one-at-a-time, use the Console's graphical editor. Using this method, creating an element that will be managed with the SNMP proxy agent is essentially the same as creating any element in your database. To define an SNMP element instance in a Console view, you specify SNMP-specific information about that element in the Properties window.

1. **Move the mouse pointer to the Edit button and press MENU to open the Edit menu. Release MENU over the Create option. You receive the Create Object window:**

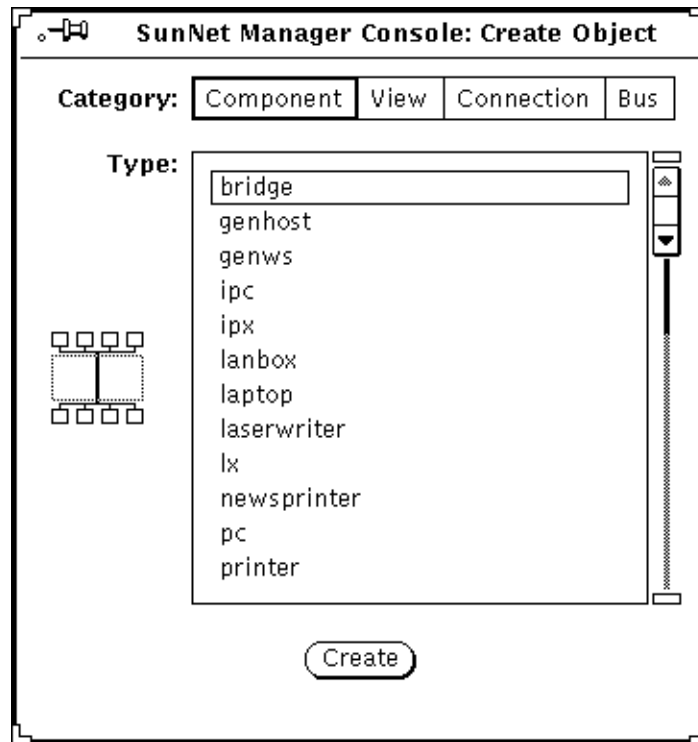
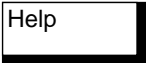


Figure 9-1 Edit—Create Window

2. Click **SELECT** on the category of element and type of element you want. Then click **SELECT** on Create.
3. Fill in the Properties window for the element.



On-line help is available for this window.

The top portion of the Properties window is the element data. You must fill in the Name field; other fields are optional. Specify the SNMP Read Community and SNMP Write Community fields for the element. Although filling in the SNMP fields (including SNMP Vendor Proxy and SNMP Timeout) is optional, you should understand how the proxy agent uses this information—see the “Notes” section for this task.

The middle portion of the Properties window is the list of agent schemas that the Console knows about. Check the schemas that apply to the device. There are three SNMP schemas supplied with SunNet Manager: `snmp` describes the MIB I, `snmp-mibII` describes MIB II, and `sun-snmp` is the

schema file for the SNMP agent (`snmpd`) for Sun workstations. If you loaded any additional schemas into the Console, the names of these schemas appear in the schemas list. Note that the schema name is *not* the schema file name. The schema name is specified by the keyword `proxy` in the schema file. See Section 9.1, “Adding SNMP Devices,” on page 9-2 for more information about setting the schema name.

4. Click SELECT on the Apply button in the properties window.

A glyph for the element you just defined appears with the name you specified.

Figure 9-2 shows a properties window for a new component that has the SNMP schemas checked.

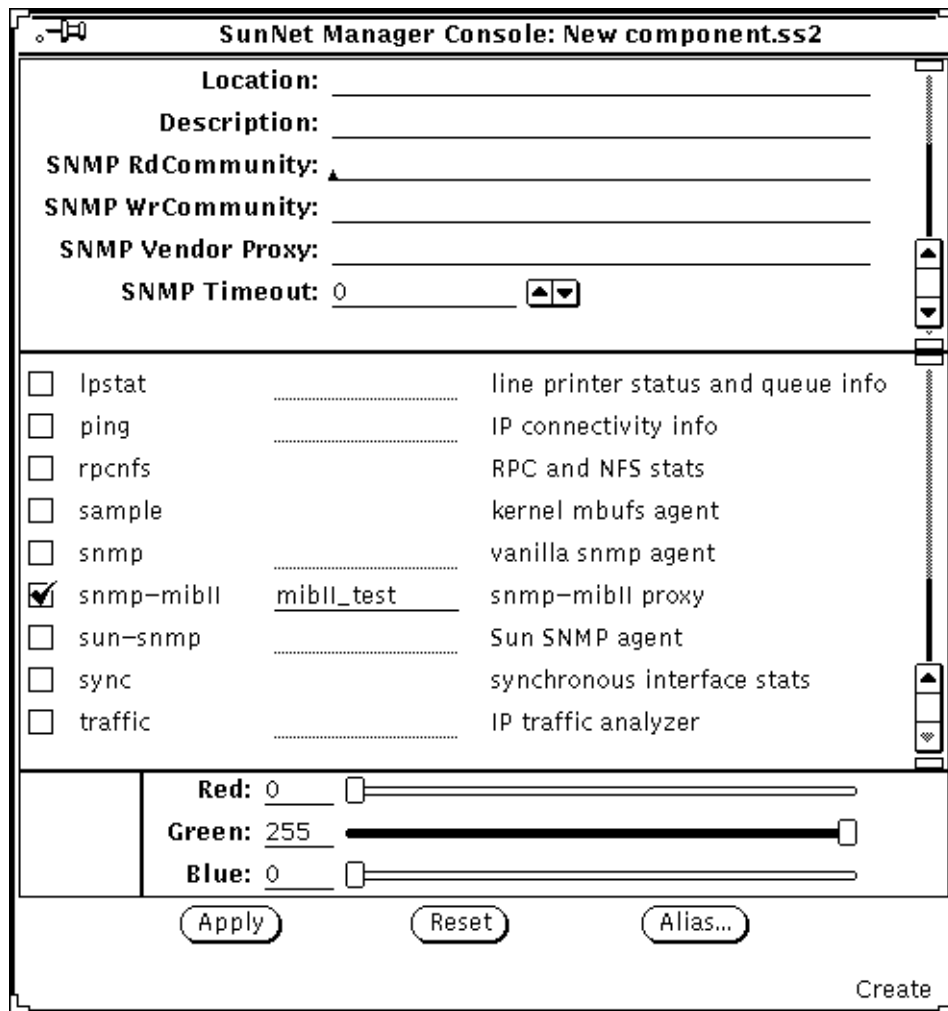


Figure 9-2 Properties Window for a New Component

9.2.1 Notes

The values in the fields SNMP Read Community, SNMP Write Community, SNMP Vendor Proxy, and SNMP Timeout are sent with the request to the SNMP proxy agent. If you do not specify values in the SNMP Read Community, SNMP Write Community, and SNMP Timeout fields, the SNMP proxy agent uses the following values:

- Read community is “public”.
- Write community is “public”.
- Timeout will be the value (in seconds) specified by the keyword `na.snmp.request_timeout` in the `snm.conf` file on the system where the SNMP proxy agent resides. The keyword’s supplied value is 5 (seconds).

SNMP Vendor Proxy is an optional field that specifies the name of a proxy system with which the SNMP proxy agent will communicate. Normally, you do not need to specify a value for this field. If this field is used, the SNMP request is passed through the element to a secondary proxy. This field should *only* be specified when a vendor has supplied an SNMP proxy agent to manage a particular device or set of devices that do not support IP connectivity. The vendor’s SNMP proxy agent communicates with the SunNet Manager SNMP proxy agent through SNMP, but communicates with the element using either SNMP or a different protocol.

You can select multiple SNMP agent schema files for an element. However, only one schema is associated with each request. Merely checking an SNMP agent schema on the Properties window does not make the element manageable through the SNMP proxy agent. SNMP agent software must be installed and running on the SNMP device. The MIB for the device must contain the same data definitions as the schema file used by the Console and the SNMP proxy agent.

The blank lines next to the SNMP agent schema names allow you to specify the name of the system on which the SNMP proxy agent resides. This system name is for a default proxy system. You can specify a different proxy system name for each request. If you do not specify a proxy system in the Properties window or in the report request, the system on which the Console is running is assumed to be where the proxy agent resides.

9.3 Setting Up SNM to Receive Traps from a Device

Many SNMP devices send out unsolicited or unexpected reports called traps. For example, a trap may be sent when a device is restarted. When the SNMP trap daemon receives traps, it will forward all or only selected traps to one or more SNM Consoles.

1. Determine the location of the SNMP trap daemon.

See the “Notes” discussion later on in this section.

2. If the device sends out enterprise-specific traps or if the traps are not to be forwarded to the Console, create trap file entries for these traps.

For example:

```
#
# Example traps
enterprise 1.3.6.1.4.1.42
    1      CPU_Failure
    2      Power_Supply_Failure
    3      Network_Connection_Failure
    4      Over_Heating                discard
    5      RealTimeClock_Failure       discard
```

See the “Notes” discussion later on in this section.

3. Specify where the trap daemon should forward the traps.

The trap daemon can forward traps to one or more Consoles. By default, the trap daemon forwards SNMP traps *only* to the Console on its system. If this is the desired action for the trap daemon, skip this step and proceed to the following step.

Otherwise, add the keyword `na.snmp-trap.rendez <hostname>` in the `snm.conf` file. You can specify more than one host name—separate each host name with a colon (:). (If the keyword is not specified, “localhost” is assumed.) If you modify the `snm.conf` file while the SNMP trap daemon is

running, you need to kill the trap daemon (`na.snmp-trap`) for the changes to take effect. (Refer to Appendix A of the *SunNet Manager 2.2.3 Reference Manual* for information on how to kill the daemon.) For example:

```
### Keywords for the SNMP trap proxy on wordstwo:
# default file name of per-enterprise traps
na.snmp-trap.default-trapfile /var/adm/snm/snmp.traps
#
na.snmp-trap.rendez rubicon
```

4. On the SNMP device, specify that traps be sent to the host where the trap daemon resides.

See the “Notes” discussion below. Typically, you would specify the IP address of the host system. However, this is very device-specific. Refer to the device documentation to find out how to do this.

9.3.1 Notes

A single trap daemon can accept trap messages from many devices. The trap daemon does not need to reside on the SNMP proxy agent system or the Console system. Like proxy agents, the SNMP trap daemon can be distributed in a network to reduce network traffic and distribute the processing load between systems. See Section 1.1, “Management Applications and Agents,” for more information. For example, you might want to have traps from all of the SNMP devices on a subnet sent to one host system. The trap daemon on this system can then forward *some* or *all* of these traps to selected Console system(s).

The SNMP protocol defines six generic types of traps. In addition to returning generic traps, an SNMP device may return enterprise-specific traps, which are defined by the device vendor. (See the device documentation for information on enterprise-specific traps.) Enterprise-specific traps are usually defined in the device MIB. If the MIB for the device contains enterprise-specific traps and you used the `mib2schema` utility to generate a schema file, a trap file is automatically generated. This file may be copied into place or its contents can be appended to the existing trap file. (See the `mib2schema(1)` man page for more information.) Otherwise, create a trap file as described in Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual*.

You may determine that certain generic or enterprise-specific traps do *not* need to be forwarded to the Console. For example, you may decide that a trap does not need to be sent to the Console every time a device is warm-started. You can add the optional keyword “discard” to trap definition entries in the trap file—see the trap file syntax in Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual*.

The default trap file contains trap definitions according to enterprise ID. If multiple devices on the network use the same enterprise ID and all the trap file entries apply to each device, add the trap entries to the default trap file. The default trap file is specified by the keyword `na.snmp-trap.default-trapfile` in the `snm.conf` file on the system on which the trap daemon resides. Normally, the default trap file name is:

- `/var/adm/snm/snmp.traps` for the Solaris 1.1.1 version of SNM 2.2.3
- `/var/opt/SUNWconn/snm/snmp.traps` for the Solaris 2.3 version of SNM 2.2.3

If multiple devices on the network use the same enterprise ID, but the trap file entries apply to only specific device names, define an entry for each device in the SNMP host file. Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual*.

9.4 Using the Set Tool to Retrieve SNMP Attribute Values

You can use the Console to obtain Quick Dumps and data, event, and trap reports on SNMP devices, just as with any other type of device. See Chapter 4, “Requesting Data from Agents,” Chapter 5, “Specifying Events,” and Chapter 7, “Viewing Reports,” for steps on how to get this information.

For SNMP devices you can also use the Set Tool to retrieve SNMP attribute values. Retrieving attribute values with the Set Tool allows you to examine an attribute’s current value before you change it—see Section 9.5, “Using the Set Tool to Change SNMP Attribute Values,” on page 9-17, for information on changing attribute values.

1. **Move the mouse pointer over the glyph that represents the target SNMP device and press MENU to open the Glyph menu.**
2. **Drag the mouse pointer down to Set Request. Drag right over the desired agent schema name and continue to drag right over the desired group or table name. For example:**

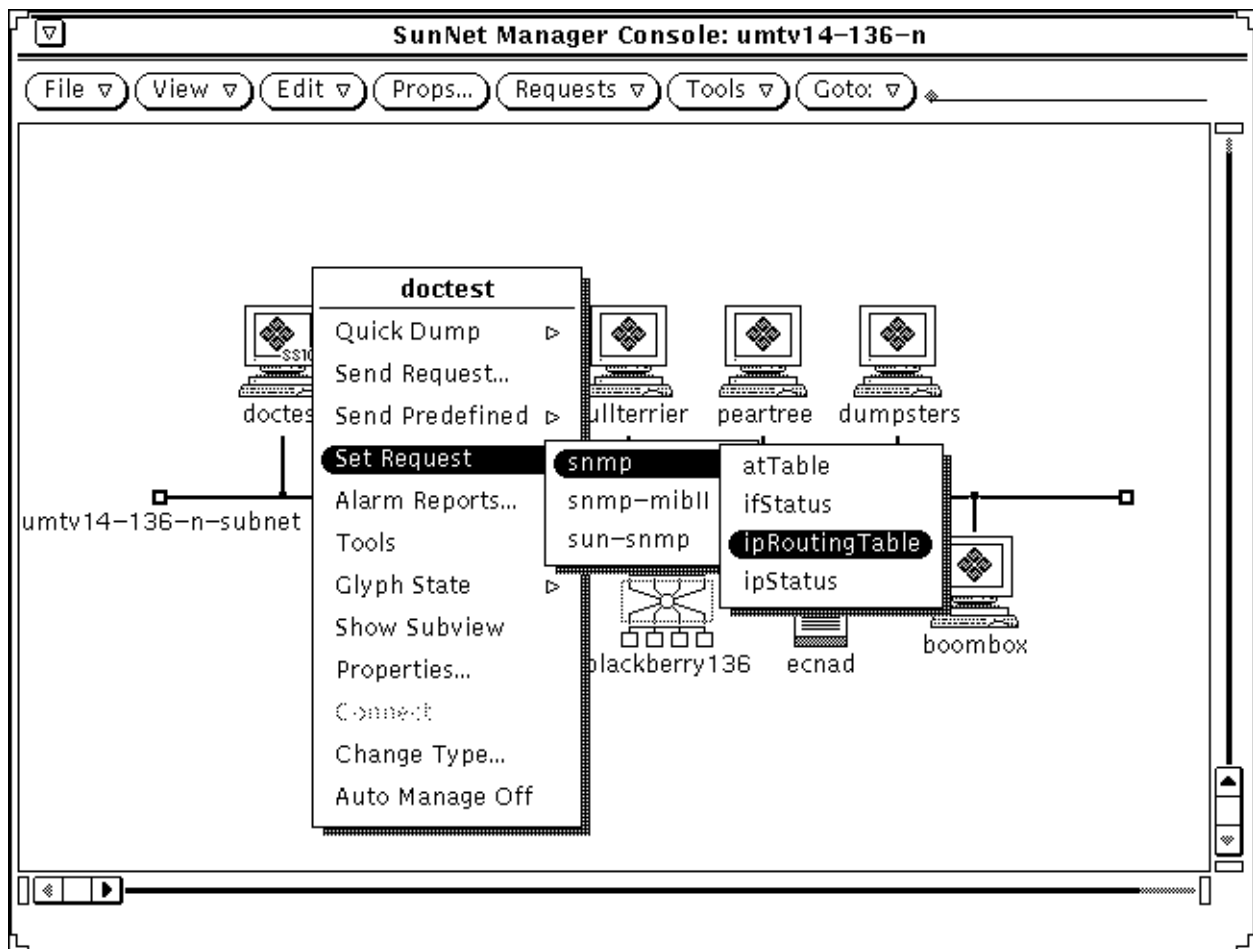


Figure 9-3 Glyph—Set Request Menus

In your response to your menu selection, you receive a window such as the one shown in Figure 9-4.

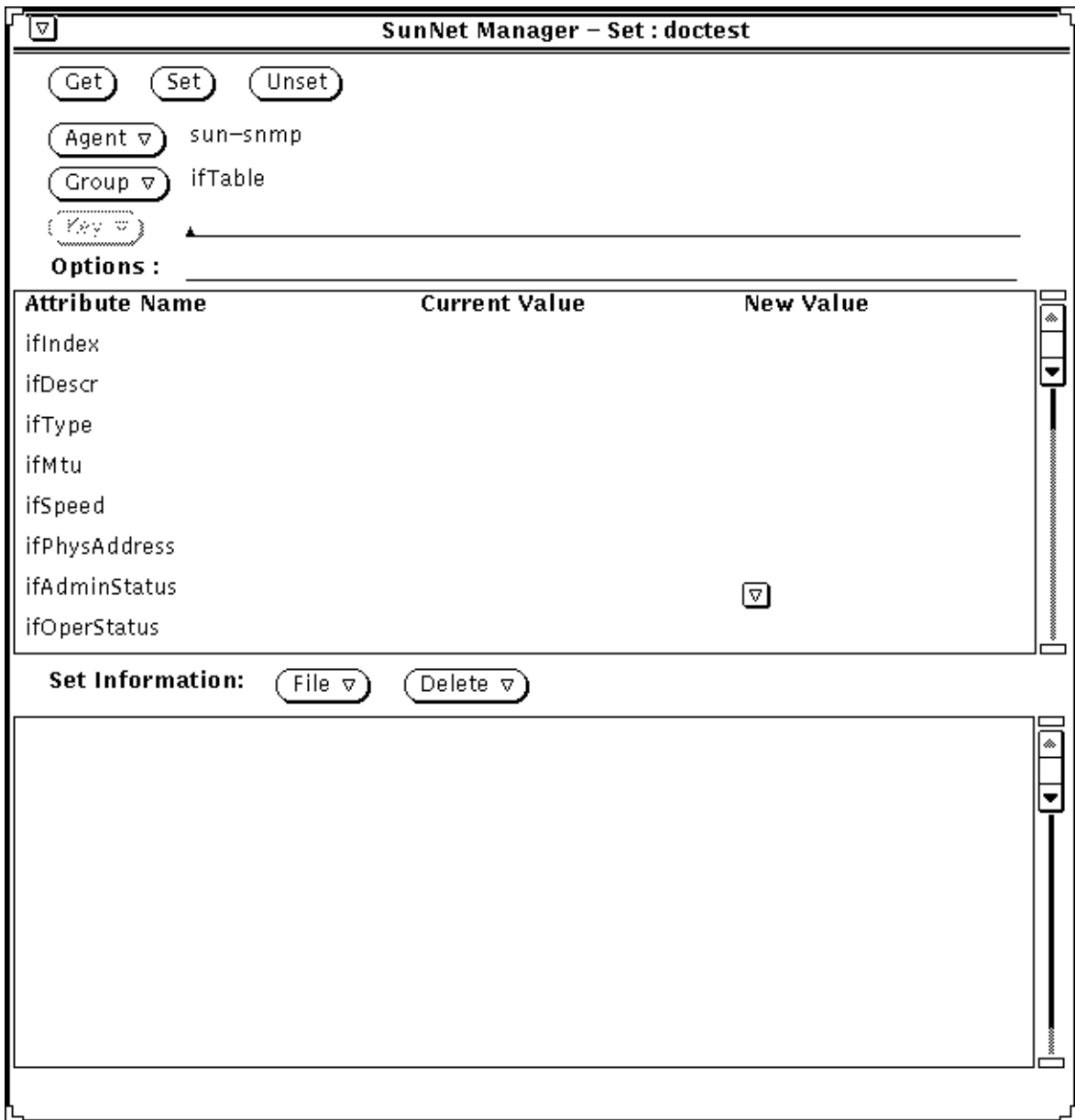


Figure 9-4 Set Tool Window

Help

On-line help is available for this window.

3. In the Set Tool window, specify the key or options for the request.

If the group is a table and you know the key of the row you want, type in the key value in the Key field. If you do not specify a key value, when you SELECT the Get button (in the next step) the first row of the table will be displayed by default and the Key menu generated. You can then choose a value from the Key menu by pressing MENU on the abbreviated menu button.

You can specify an SNMP read-community name in the Options field if it is different from the read-community you have previously specified in the Properties window for the element.

4. Click SELECT on the Get button. The attribute values are displayed in the attribute list.

9.4.1 Notes

In the control panel at the top of the Set Tool window, you can change the attribute group or agent schema name (or both) to retrieve attribute values for other attribute groups or for other agent schemas used by the target device.

- To change the agent schema:
 - a. Move the mouse pointer over the Agent abbreviated menu button.
 - b. Press MENU to open the list of agent schemas available for the target element.
 - c. Drag the mouse pointer to the desired agent schema and release.

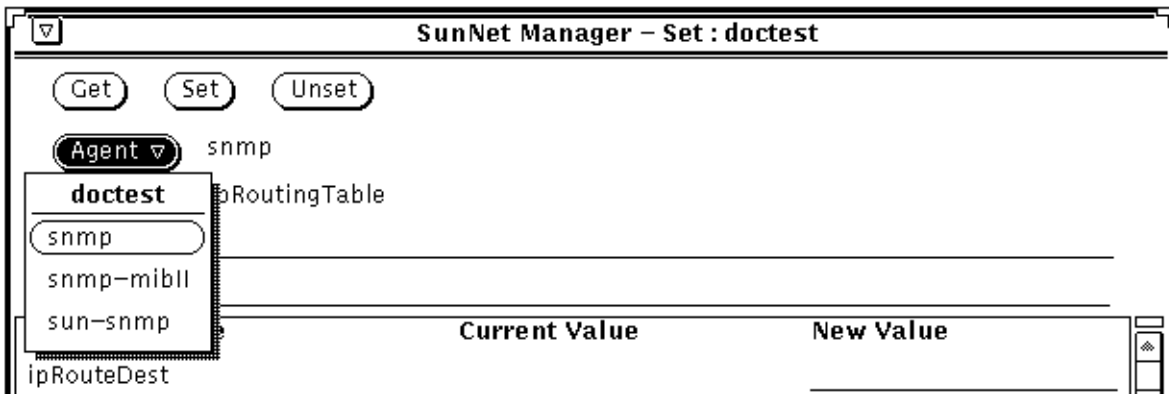


Figure 9-5 Set Tool—Agent Menu

- To change the attribute group:
 - a. Move the mouse pointer over the Group abbreviated menu button.
 - b. Press MENU to open the list of attribute groups specified in the agent schema.
 - c. Drag the mouse pointer to the desired group and release.
 - d. If the group is a table and you know the key of the row you want, type in the key value in the Key field.

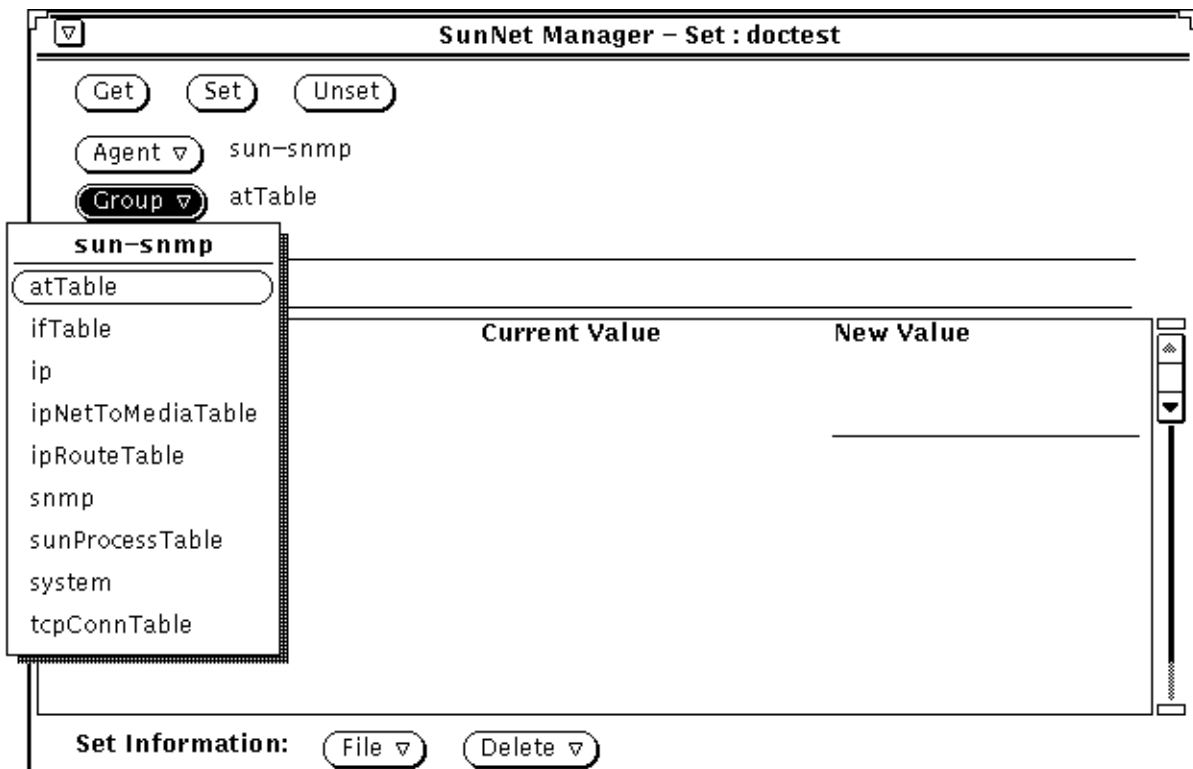
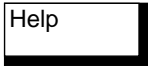


Figure 9-6 Set Tool—Group Menu

9.5 Using the Set Tool to Change SNMP Attribute Values

A set request is used to request an agent to change the value of a particular attribute. With one Set Tool operation, you can send set requests to different agents for multiple attributes with one Set Tool operation.

1. Move the mouse pointer over the glyph that represents the target SNMP device and press MENU to open the Glyph menu.
2. Drag the mouse pointer down to Set Request. Drag right over the desired agent schema name and continue to drag right over the desired group or table name. You receive a Set Tool such as the one shown in Figure 9-4 on page 9-14.



On-line help is available for this window.

- 3. In the Set Tool window, specify the key or options for the request.**
If the group is a table, type in the key value in the Key field. If you do not know the key, retrieve the available key values by clicking SELECT on the Get button.
- 4. Enter the new value on the line provided in the New Value column and press Return. The new value is shown in the lower portion of the window.**
- 5. To change another attribute in a different attribute group or agent schema, use the Group and Agent abbreviated menu buttons.**
All the attributes in the selected group appear in the attribute list. If you want to change the value of an attribute of a row in a table, you must supply the key for that row. You can also click the Get button to display the current values of the attributes.

You can specify an SNMP write-community name in the Options field if it is different from the write-community you have previously specified in the Properties window for the element.
- 6. Repeat the previous three steps until you have entered all the attribute changes you want to make for the target element.**
Note that the new attribute values are collected in the Set Information list. This allows you to view your changes and edit them, if necessary, before the actual set request is made.
- 7. To send the set request with the new value(s), SELECT the Set button at the top of the control panel.**
When the Set request has been successfully completed, the Set Information list is cleared.

9.5.1 Notes

If an attribute is set-able, a line is provided in the New Value column to the right of the Current Value in the attribute list. (Current Value is also provided for non-set-able attributes; however, no lines are provided in the New Value column.) Set-able attributes of enumeration data types have an abbreviated menu button displayed in the New Value column; press MENU on the menu button to choose the desired new value.

How to Create and Manage a Link

<i>Using the Console's Edit Function</i>	<i>page 10-1</i>
<i>Using Discover to Create Manageable Links</i>	<i>page 10-10</i>

This document provides an example of how to use SunNet Manager to manage a link. By “manage,” we mean send event requests to and receive event and trap reports from. For the purposes of this document, a link is an SNM object in the category “connection.”

The easiest way to create a connection is through the Discover Tool, the use of which is described in Chapter 5 of the *SunNet Manager 2.2.3 Reference Manual*. If you need to create only a few manageable links, you should use the Console's graphical editor function, described in the following section. The use of Discover hides the details of link creation; the use of the Edit function requires more intervention on your part.

10.1 Using the Console's Edit Function

You create a link in the same way you create elements of other categories. Invoke the Console's graphical editor function (press Edit►Create in the Console's control area) and click SELECT in the Connection category. For example:

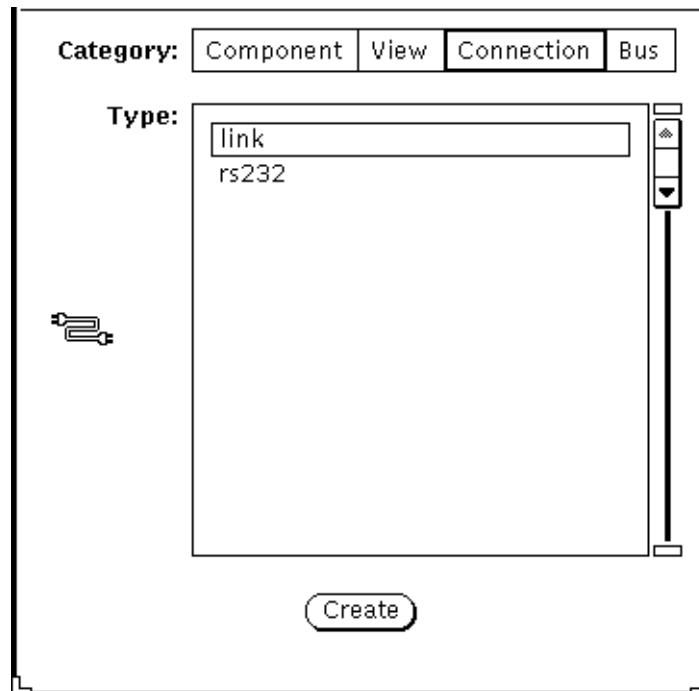


Figure 10-1 Creating a Connection Object

You can manage a connection of any type—types `link` or `rs232`, the types supplied with SNM, or connection types that you add. You can create a link between any two elements. However, realistically, the most useful links are between two components, such as two routers, or a router and a subnet.

After you click `SELECT` in the `Create` button in the window shown in Figure 10-1, you receive a properties window for a new connection as shown in Figure 10-2.

SunNet Manager Console: New connection.link

Name: link_to_fddi_net

Object1: fmtv14a-136

Object2: umtv-eng-fddi-bb-routers

Description: _____

<input type="checkbox"/>	iproutes	IP route table and statistics
<input type="checkbox"/>	layers	protocol layer statistics
<input type="checkbox"/>	layers2	protocol layer statistics (for SunOS 5
<input type="checkbox"/>	lpstat	line printer status and queue info
<input checked="" type="checkbox"/>	ping	IP connectivity info
<input type="checkbox"/>	rpcnfs	RPC and NFS stats
<input type="checkbox"/>	sample	kernel mbufs agent
<input checked="" type="checkbox"/>	snmp	vanilla snmp agent
<input type="checkbox"/>	snmp-mibII	snmp-mibII proxy
<input type="checkbox"/>	snmpv2	snmpv2 agent

Red: 200

Green: 255

Blue: 225

Figure 10-2 Properties for New Connection

Referring to Figure 10-2, Object1 and Object2 are the names of objects in the runtime database. SNM manages the link based on the data returned from Object1. The name of the link (in the Name field) is for your use and cannot be an existing object in the database. For a link, you should have the ping and, if one or both objects support it, the snmp agents checked off.

After you click SELECT on apply your link object is created and is displayed in the Console as shown in the following figure:

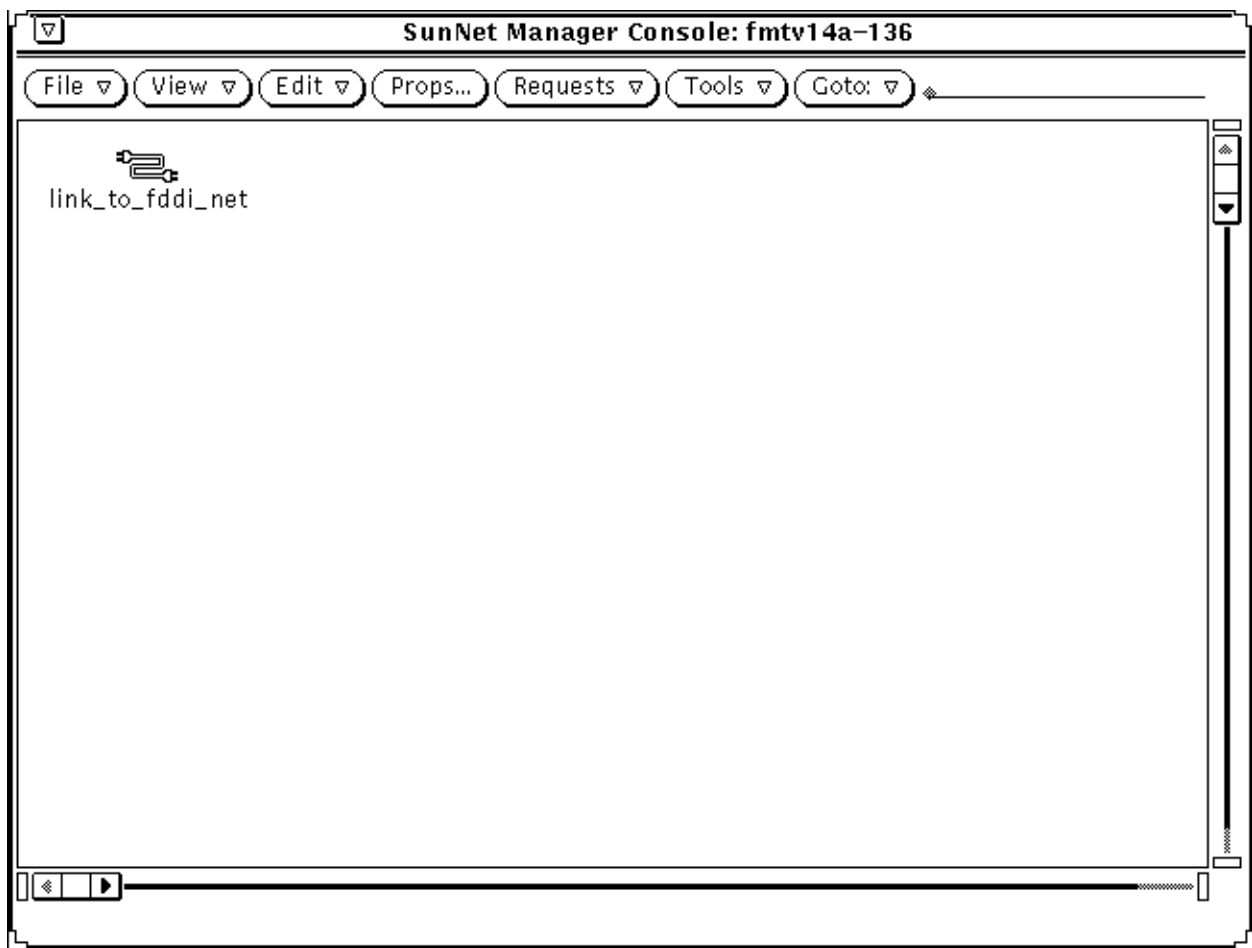


Figure 10-3 New Link in Console

In this example, we display the link in the view for the machine, `fmtv14a-136`, a router that is the first object (Object1) listed in the link properties. This choice of where to locate the object is arbitrary. You might locate the link in its own view, in your Home view, or the view that displays

glyphs for both the router and the subnet to which it connects. For our example, we copy the link object to the view displaying the objects connected by the link:

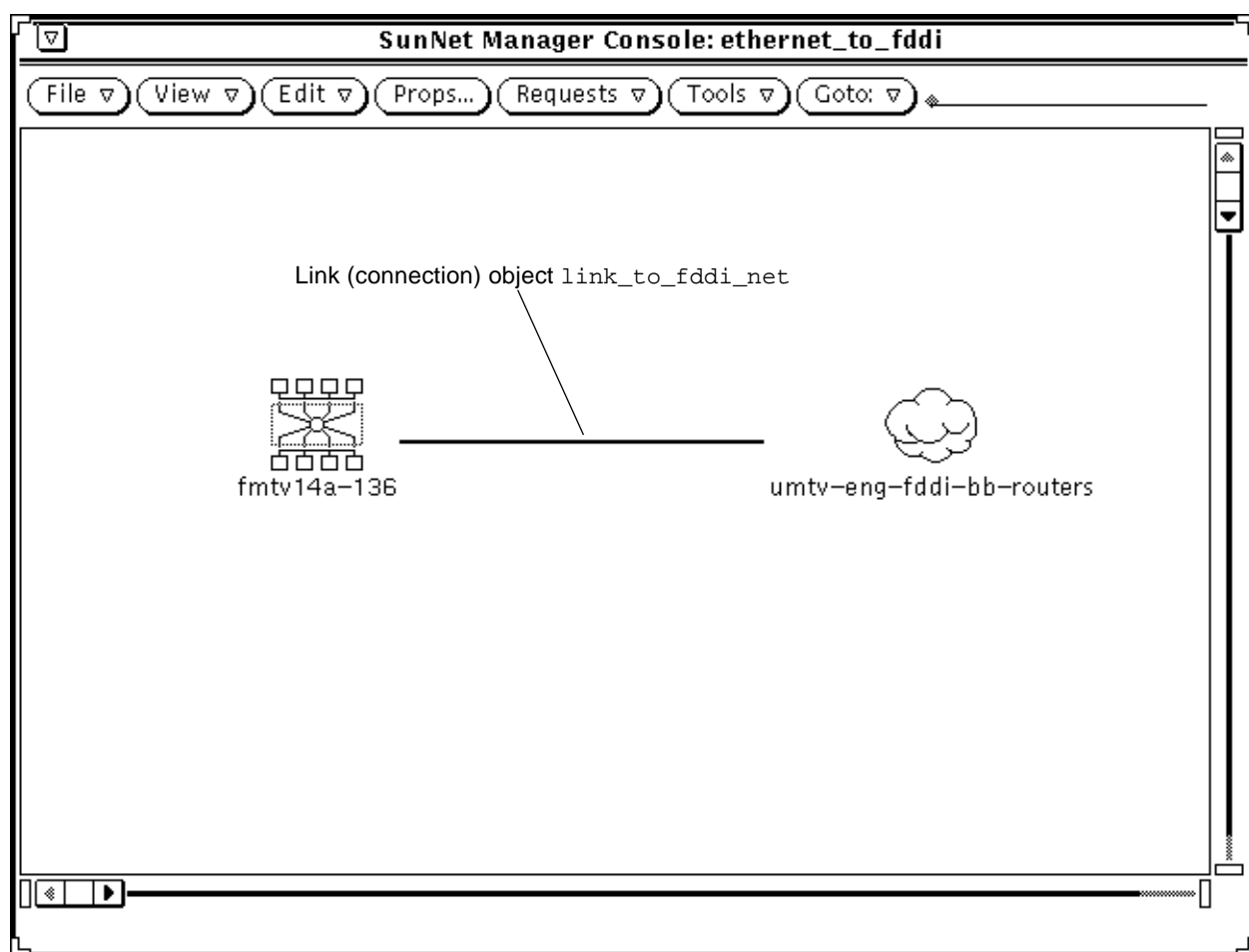


Figure 10-4 Link in View with Connected Objects

In Figure 10-4, note that the link lies between the two objects specified as Object1 and Object2 in Figure 10-2. That is, it connects the router `fmtv14a-136` to the subnet `umtv-eng-fddi-bb-routers`.

Independent of creating the object `link_to_fddi_net` in the Console, if you are creating the link object “by hand”, you must add an entry to the `linkmap` file to identify the new link. The `linkmap` file, described in a man page supplied with SNM, is stored by default in the following directory:

- `/var/adm/snm` for Solaris 1.x
- `/var/opt/SUNWconn/snm` for Solaris 2.x

For the link object `link_to_fddi_net` we create the following entry in the `linkmap` file:

```
fmtv14a-136      2      link_to_fddi_net
```

The first field in this entry (`fmtv14a-136`) corresponds to `Object1` in the link properties sheet. As with `Object1` in the properties sheet, SNM manages the link based on data returned by the element in this first field. The third field (`link_to_fddi_net`) corresponds to the `Name` field in the properties sheet. The second field (`2`) is the interface on the machine specified in the first field. This is the interface over which the connection exists to the object at the remote end of the link. We obtained this number from the Discover Tool, so strictly speaking, we have “cheated” in this example. However, we later describe how to use Discover to perform the same tasks that are described here.

At this point, the link is fully manageable. That is, you can send event requests to it and, if the machine identified in the `linkmap` file is running an SNMP agent, can receive traps from it.

Because a Quick Dump is a form of Data Request, a link cannot respond to a Quick Dump.

Sending an Event Request to a link (a link cannot respond to a Data Request), is the same as sending such a request to a component. For example:

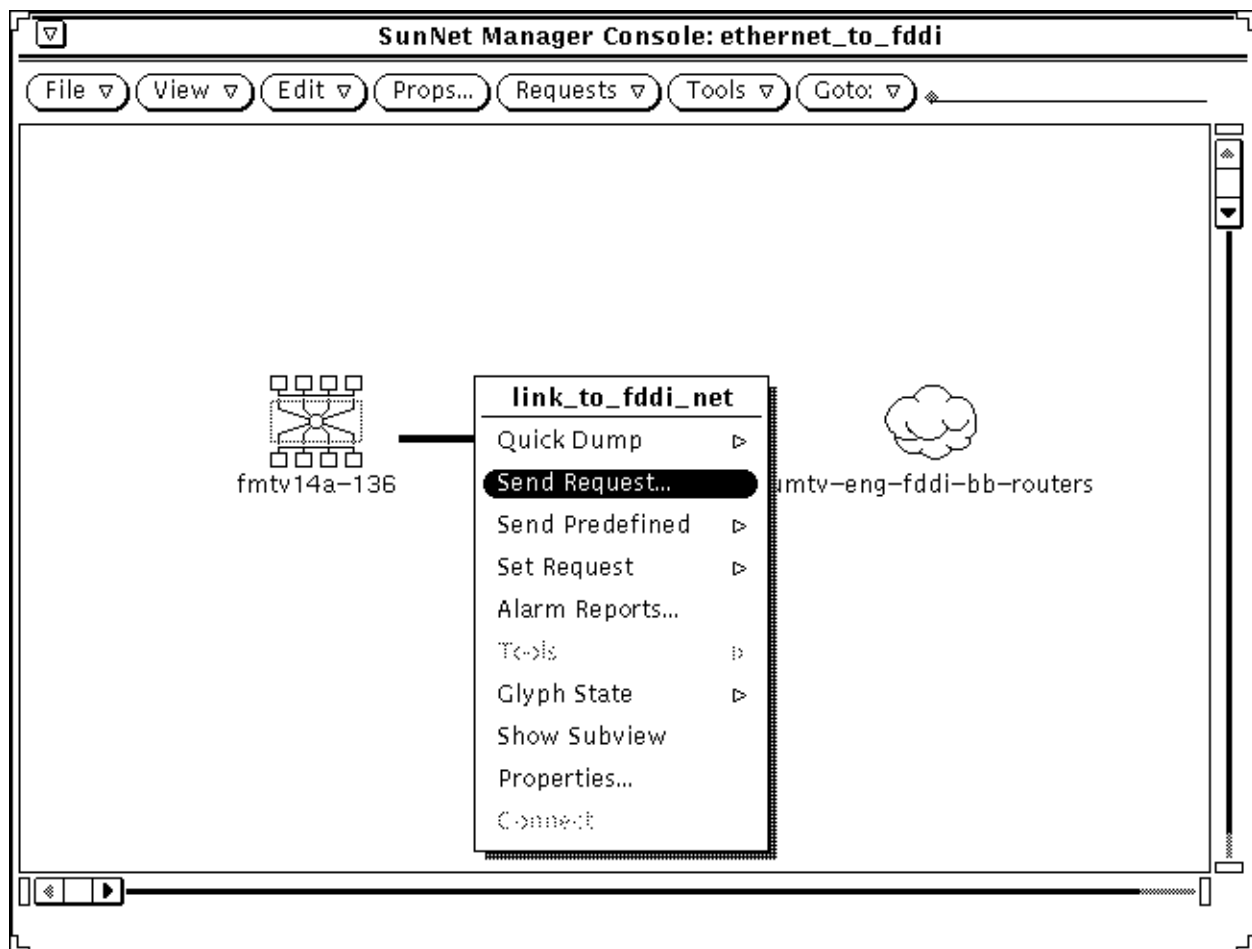


Figure 10-5 Invoking Send Request

After invoking Send Request, as shown above, you receive the Request Builder shown below:

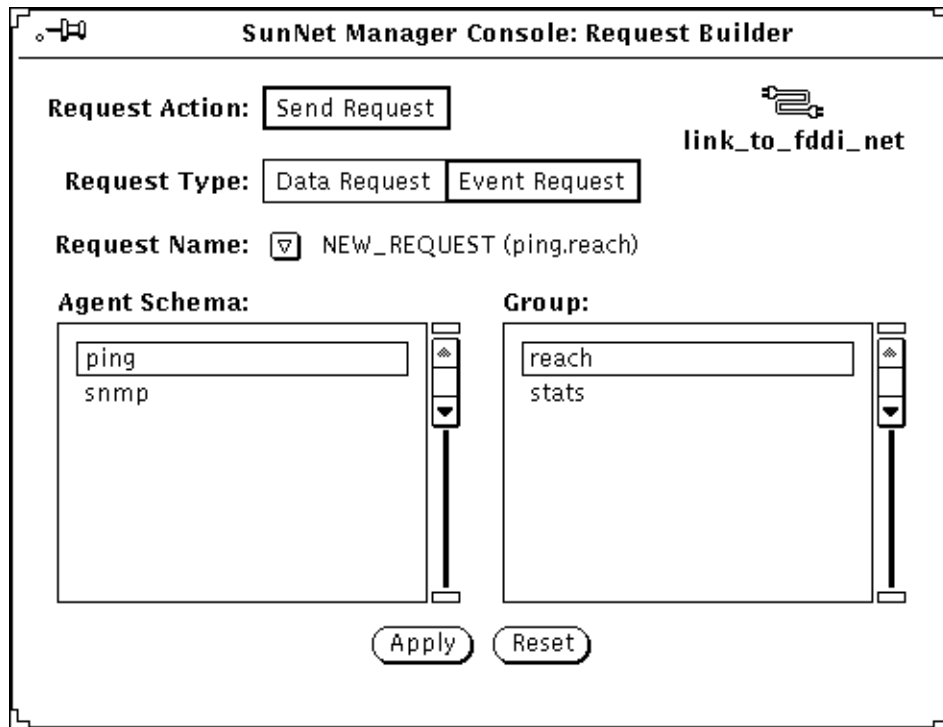


Figure 10-6 Request Builder Window

Click SELECT on Event Request, as was done in Figure 10-6. Choose an agent schema and group, then click SELECT on Apply, as you do for any event request. You receive an Event Request properties window such as the one shown below:

SunNet Manager Console: Event Request (link_to_fddi_net.ping.reach)

Name: ping.reach Attributes:

Proxy System: localhost

Interval: 0 ▲▼

Count: 0 ▲▼

Key: 2 Taken from 2d field in linkmap entry

Restart:

Send Once:

Defer Reports:

On Completion: Delete Request

Options: _____

Attribute: ▼ reachable

Relation1: ▼ Equal To

Threshold1: false

Relation2: ▼ Threshold Not Set

Threshold2: _____

Priority: ▼ Low

Glyph Effect: ▼ Blink Glyph

Audio Effect: ▼ None

Audio File: _____

Mail To: _____

To Program: _____

Start Hold Reset Apply Reset Delete

reachable information whether host is reachable

Figure 10-7 Event Request Properties

As noted in the figure, the Key field in the properties sheet is derived from the interface-number field in the linkmap file. The fact that this number displays correctly is one indication of a valid linkmap entry for link_to_fddi_net. To take advantage of the decay-to-blue feature, you must set the Glyph Effect item, above, to Color by Priority.

To review briefly, the decay-to-blue feature means that if your link goes down (with a resultant change of glyph color to red, orange, or yellow) then comes back up, the glyph color changes to blue and remains blue until reset or until the link goes down again.

If the link goes down (or decays), you observe the glyph effect in the Console, just as you do for an event occurring for any element. The difference with the link management feature is that the link itself displays your specified glyph

effect. When a link changes color, blinks, or dims, it indicates that one or both of the machines at either end of the link is down, or that the link medium itself is disrupted.

10.2 Using Discover to Create Manageable Links

The Discover Tool automates the process of creating manageable links and adding required entries to the `linkmap` file. In this example, we “discover” the same link we created by hand in the previous section.

Invoke Discover by selecting **Tools**►**Discover** in the Console’s control area. In the Discover Tool’s base window, click **SELECT** on **Configuration Options**. In the Discover Configuration window, to find manageable links, click **SELECT** on **Add Object Connections**. The window shown in Figure 10-8 has **Add Object Connections** selected.

Discover Configuration

Category: Discover Required setting for adding manageable links

Net Name/Number: umtv14-136-n Viewname: routers

Netmask: 0xffffffff Add To All Views: Yes No

Maximum Hops: 1 Add Object Connections: Yes No

ICMP Retries: 2 Add Object Coordinates: Yes No

ICMP Timeout: 1 Default Proxy: localhost

SNMP Retries: 3 Objects To Discover:

SNMP Community: public All Objects

SNMP Timeout: 2 snm hosts

Verbose Mode: Yes No SNMP devices

Routers

Networks/Subnets

Figure 10-8 Discover Configuration Window

In addition to the Add Object Connections selection, the non-default selections in the window shown in Figure 10-8 are the Maximum Hops (changed from 0 to 1), the deselection (setting to No) of Add To All Views, the selection of Routers (only) for Objects to Discover. A Viewname of “routers” is specified.

The effect of the selections shown in Figure 10-8 is to tell Discover, “Find only routers 0 or 1 hops away and find all links between those routers. Add all discovered elements to a view named ‘routers’.”

After clicking SELECT on Apply and starting the discover function, you receive a view such as the one shown below.

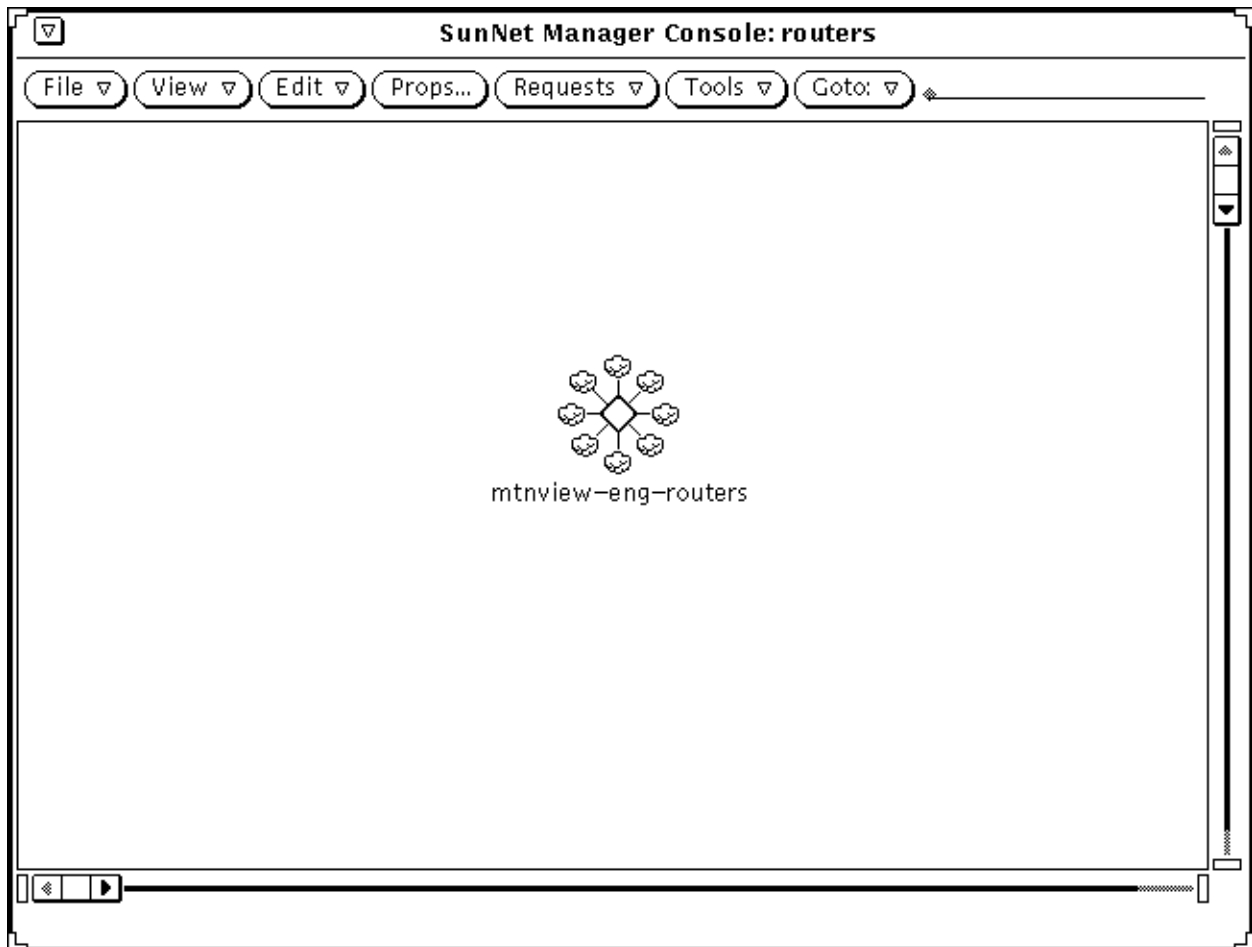


Figure 10-9 Network Icon for View “Routers”

Double-click on the network icon in Figure 10-9 to receive the sub-view shown Figure 10-10.

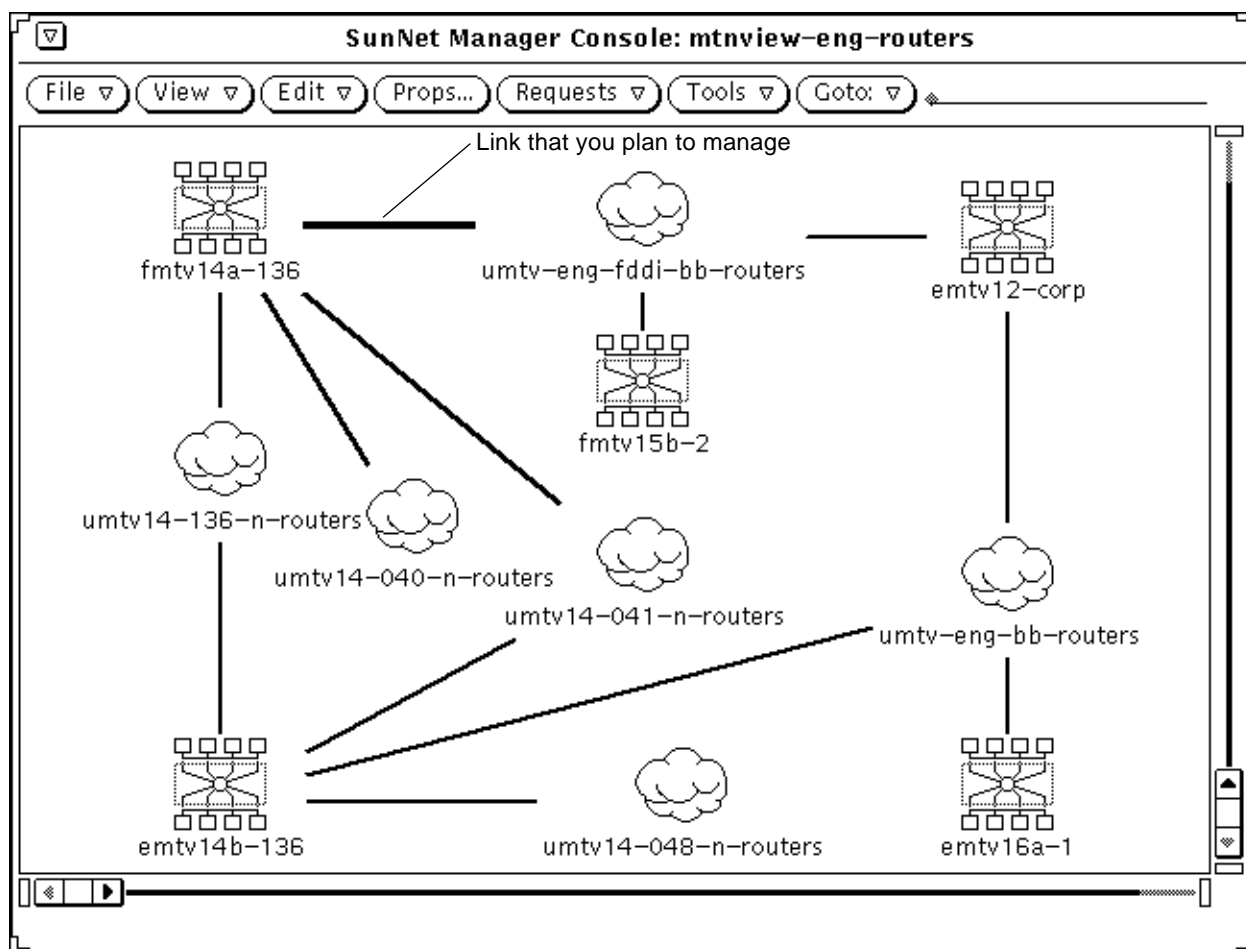


Figure 10-10 View Created by Discover

A difference between the link you created yourself in the previous section and the link created by Discover is the name. The Discover Tool creates a name by combining the names of the two linked objects and appending the string `link`. You can illustrate this by pulling down the glyph menu for the link glyph, as shown below:

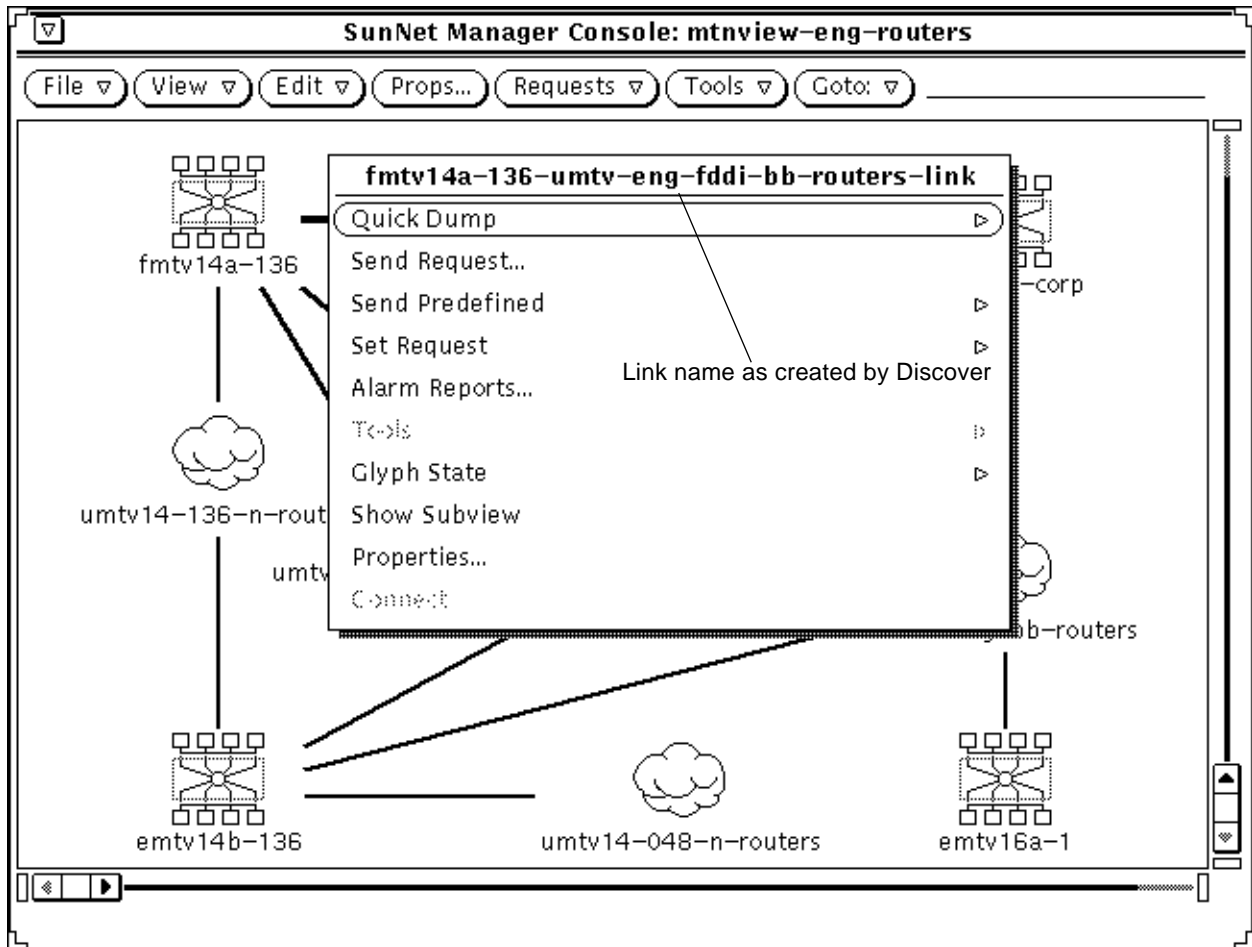


Figure 10-11 Link Name as Created by Discover

Figure 10-12 shows the properties of the “discovered” link. Note that, except for the name, these properties are identical to the properties for the hand-created link, shown in Figure 10-2 on page 10-3.

fmtv14a-136-umtv-eng-fddi-bb-routers-link (connection.link)

Name: fmtv14a-136-umtv-eng-fddi-bb-routers-link

Object1: fmtv14a-136

Object2: umtv-eng-fddi-bb-routers

Description: _____

<input type="checkbox"/>	layers		protocol layer statistics
<input type="checkbox"/>	layers2		protocol layer statistics (for SunOS 5
<input type="checkbox"/>	lpstat	_____	line printer status and queue info
<input checked="" type="checkbox"/>	ping	<u>localhost</u>	IP connectivity info
<input type="checkbox"/>	rpcnfs		RPC and NFS stats
<input type="checkbox"/>	sample		kernel mbufs agent
<input checked="" type="checkbox"/>	snmp	<u>localhost</u>	vanilla snmp agent
<input type="checkbox"/>	snmp-mibII	_____	snmp-mibII proxy
<input type="checkbox"/>	snmpv2	_____	snmpv2 agent
<input type="checkbox"/>	snmpv2-mibII	_____	snmpv2-mibII proxy

Red: 0

Green: 0

Blue: 0

Apply Reset Alias...

Browse

Figure 10-12 Properties of Discovered Link

As with the hand-created link, SNM manages the link based on data returned from the element in the Object1 field. Note that `localhost` is the default for proxy hosts, so the specification of `localhost` for the `ping` and `snmp` agents is equivalent to the empty proxy fields for `ping` and `snmp` shown in Figure 10-2 on page 10-3.

The decision to invoke the Add Object Connections feature in the Discover Tool should be a considered one. While the automatic creation of manageable links might be desirable, there are these disadvantages to consider:

- You lengthen the amount of time Discover takes to find elements and build your database. The time required by the monitor function to detect changes in your database is also lengthened proportionately.
- If your network consists of a set of LANs, you create many links that have little or no value from a network management point of view. With Add Object Connections turned on, the Discover Tool creates links between each machine on a subnet and that subnet. In effect, you have a link that maps to the machine's network interface and its transceiver cable (in the case of Ethernet). This is of no more value than having an element for the machine (or interface) itself.
- Following from the preceding item, you end up with a much larger database than you would otherwise.

Depending on the number of links you want to manage, it might be better for you to use the Console's graphical editor function, as described in the previous section, than to use Discover Tool's Add Object Connections feature.

<i>Adding Background Image to Current View</i>	<i>page 11-1</i>
<i>Creating Types of Elements</i>	<i>page 11-7</i>
<i>Creating a New Glyph for an Element Type</i>	<i>page 11-10</i>
<i>Modifying the Console Tools Menu</i>	<i>page 11-11</i>
<i>Modifying the Tools Menu for an Element Type</i>	<i>page 11-12</i>
<i>Adding Agents and Glyphs</i>	<i>page 11-13</i>
<i>Forwarding Novell's NMS Alarms to SunNet Manager</i>	<i>page 11-14</i>

This chapter describes how to customize views and perform other tasks beyond the routine use of the Console to send requests and gather data.

11.1 Adding Background Image to Current View

You may find it helpful to place elements in views relative to their physical locations to one another. A Console view may be superimposed upon a background image, such as that of a region map or the layout of a building.

- 1. Create the background with your favorite graphics tools (for example, Island Paint).**

The background canvas can be any size. A size no larger than 1120 x 800 is recommended for standard resolution displays. The image should be in raster file format. Icon format is supported if the file ends with the extension `.icon`. Large backgrounds in icon format load much more slowly than raster format files.

2. In the Console window, invoke the **View**►**Add Background** option, as shown in Figure 11-1.

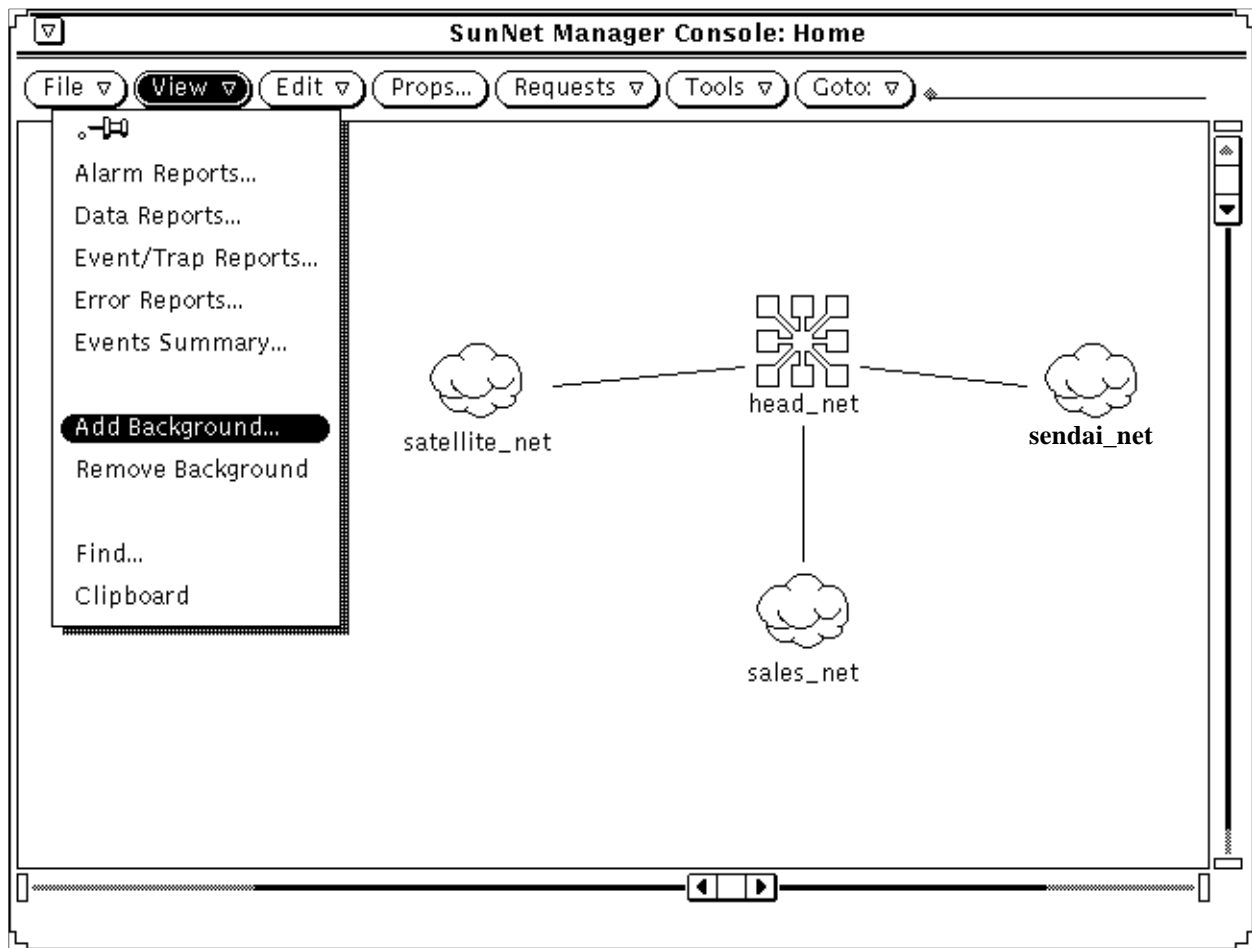


Figure 11-1 Console's Add Background Option

You receive an Add Background file menu, as shown in Figure 11-2.

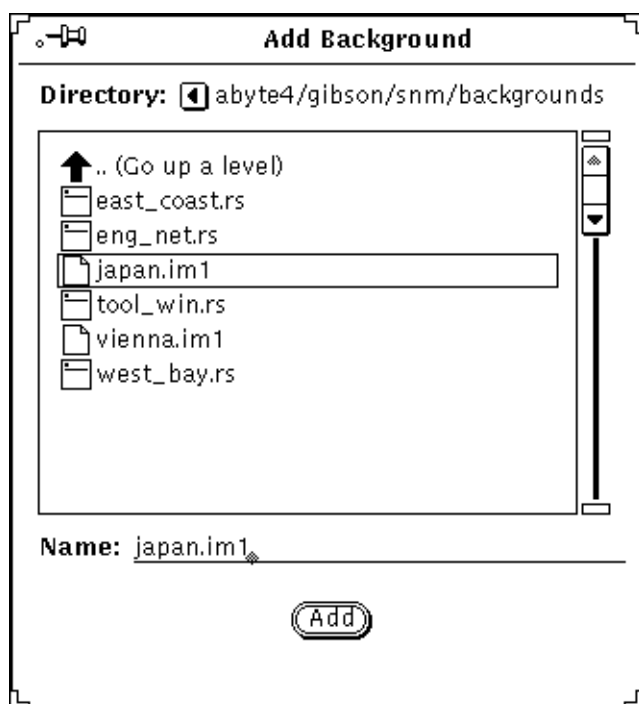


Figure 11-2 Add Background File Menu

3. Double-click SELECT on the file of your choice in the Add Background file menu.

The background contained in the selected file is displayed in the SNM Console, as shown in Figure 11-3.

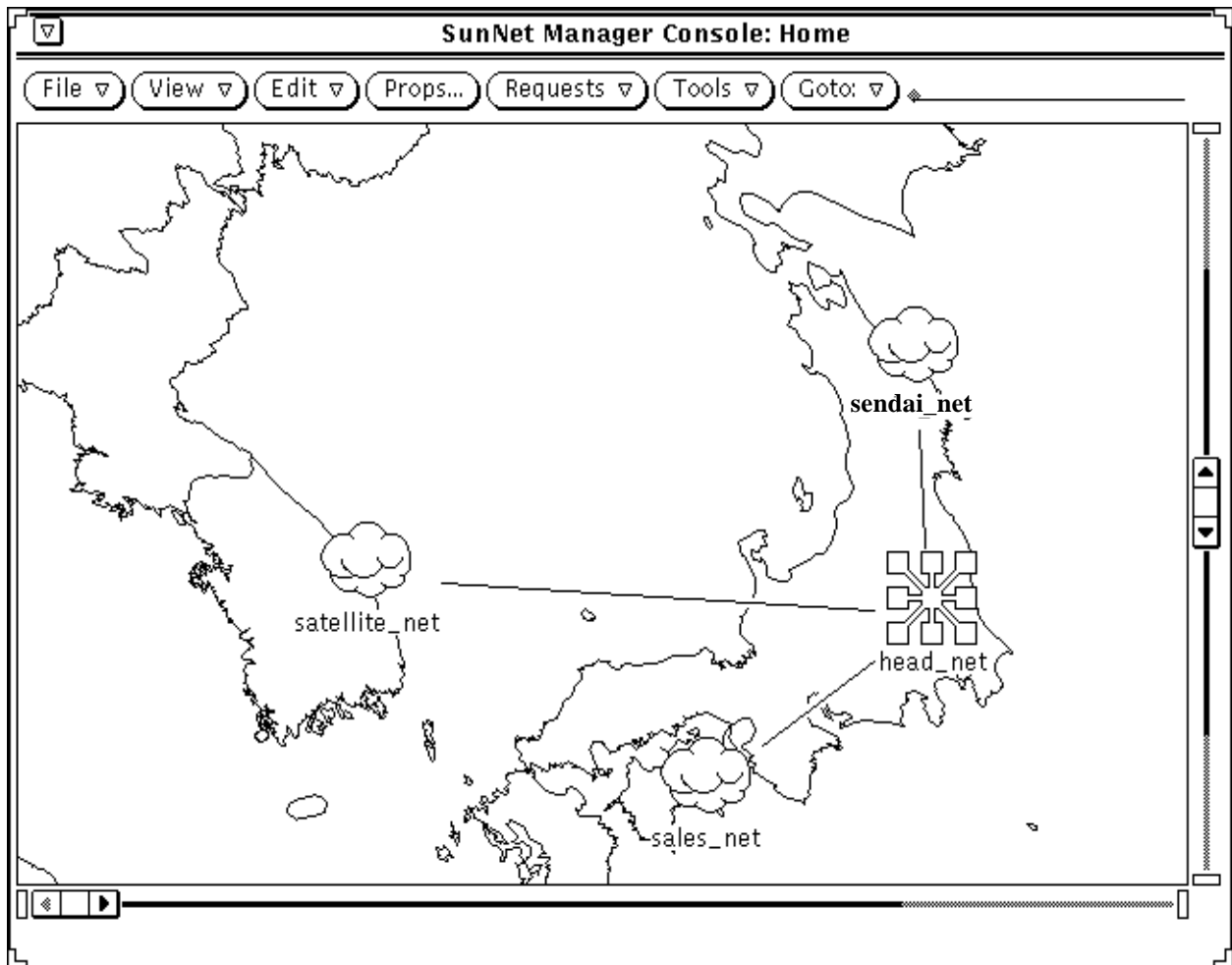


Figure 11-3 Console with New Background

After you save the runtime database to a file, the background you add to a given view is displayed each time you select that view.

To save the runtime database to an ASCII file, do the following:

1. In the Console's File button, press MENU on Save►Management Database and release MENU.

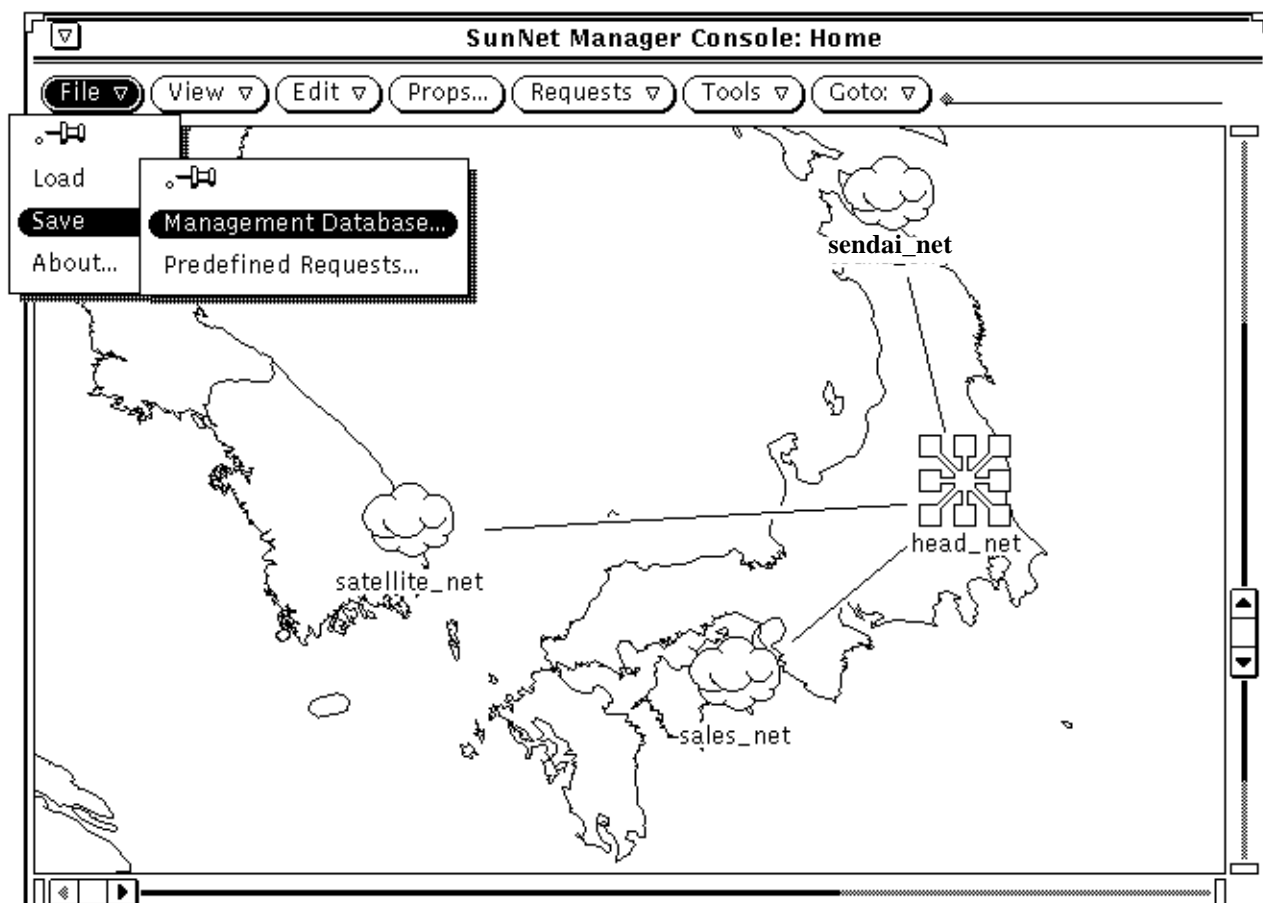


Figure 11-4 Selecting the File—Save—Management Database Menu Item

You receive the file menu shown in Figure 11-5.

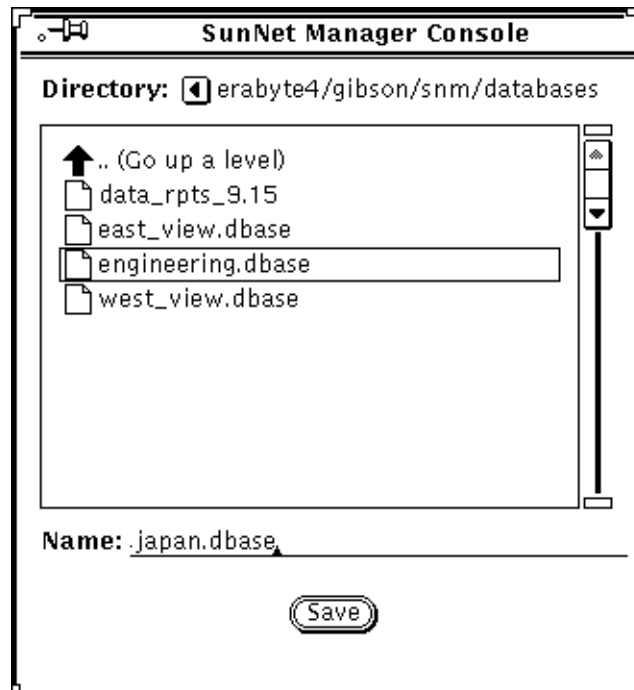


Figure 11-5 File—Save—Management Database Window

2. In the file menu, enter or select the directory and file name of the file you want to save. Click SELECT on the Save button.

When you restart the Console with a command such as the one below, you receive the view with the background that you added.

```
hostname% snm -i $HOME/snm/databases/japan.dbase
```

Note that the pathname specified as an argument to `snm`, above, is an example.

11.1.1 Notes

You can have up to 1024 icon or rasterfiles defined in the runtime database; this includes background images as well as element glyphs.

In addition to changing the background image with the Console option described in this section, you can also edit the ASCII file that contains the runtime database to achieve the same effect. With a text editor, open this ASCII file. Define a `viewBackground` instance record that specifies the name of the view and the path name of the background image.

Database definitions for background images are described in Chapter 10 of the *SunNet Manager 2.2.3 Reference Manual*.

By editing the ASCII file containing a database, you can add a background to a view other than the current view. However, you will find it far easier to use the Console menu item to add or remove a background—even if you have to change views—than it is to edit a file and load the modified database. Also, the Console option is far less prone to error than the file-editing option.

11.2 Creating Types of Elements

The `elements.schema` file provided with SunNet Manager defines many general types of elements, such as SPARCstations and SPARCservers. If necessary, you can create additional element types for your database.

- 1. With a text editor, create a file with the extension `.schema` in a directory specified by the Schema Directories category of the Console Properties►Locations window.**

The default locations for these directories are:

- `/opt/SUNWconn/snm/agents` or `/opt/SUNWconn/snm/struct` for Solaris 2.x
- `/usr/snm/agents` or `/usr/snm/struct` for Solaris 1.x

If you create a schema file in another directory, you should specify the directory in the Console Properties►Locations window. The steps for adding a path to this window are described in Section 11.6, “Adding Agents and Glyphs,” on page 11-13.

- 2. Create a record that defines the element type and the fields that are stored in the database for the element type.**

Database definitions for element types are described in Chapter 10 of the *SunNet Manager 2.2.3 Reference Manual*.

3. **Define a glyph to be used to represent the element type. You can also define the tools that will be available for this element type.**
 See Steps 1-3 in Section 11.3, “Creating a New Glyph for an Element Type,” on page 11-10, for information on creating an icon for the element type. See Steps 1-3 in Section 11.4, “Modifying the Console Tools Menu,” on page 11-11, for information on defining tools for the element type.

An alternative to loading the file into the runtime database is to exit the Console (after saving the runtime database, if you want), then reinvoking the Console (`snm -i`). The new schema file will be automatically loaded in the new Console session.

4. **Load the new element type definition into the runtime database:**
 - a. **In the Console’s File button, press MENU on Load Management Database and release MENU**

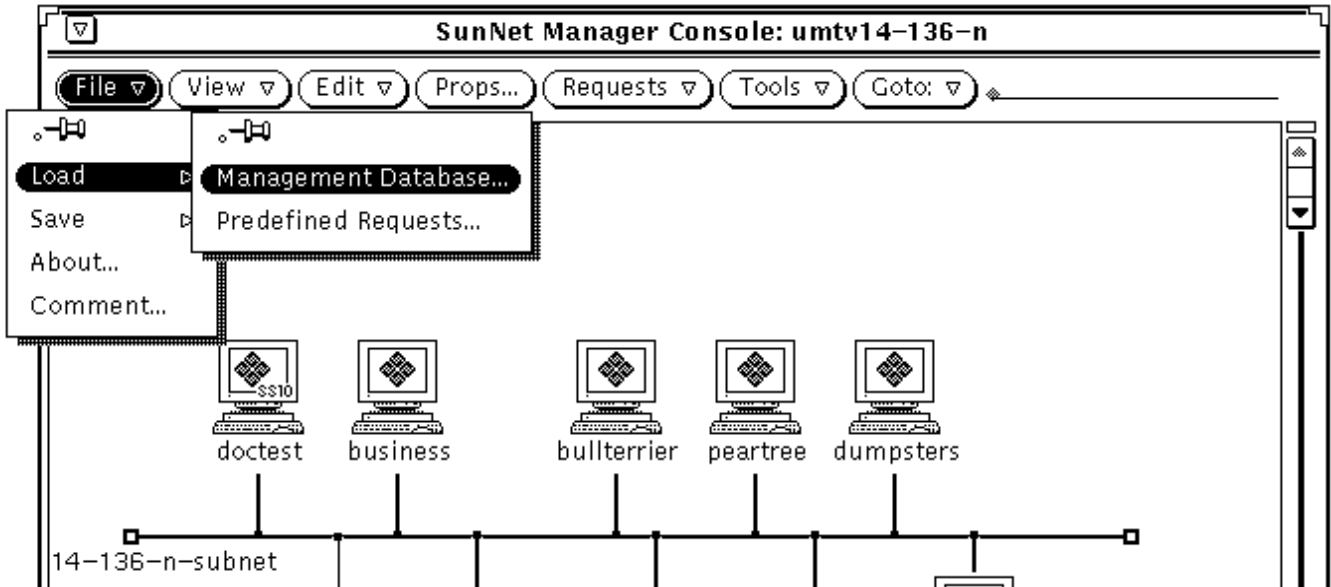


Figure 11-6 Selecting the File—Load—Management Database Menu Item

- b. **In the file menu (shown on following page) you receive, enter or select the directory and file name for the schema file where the new element type is stored and click SELECT on Load.**

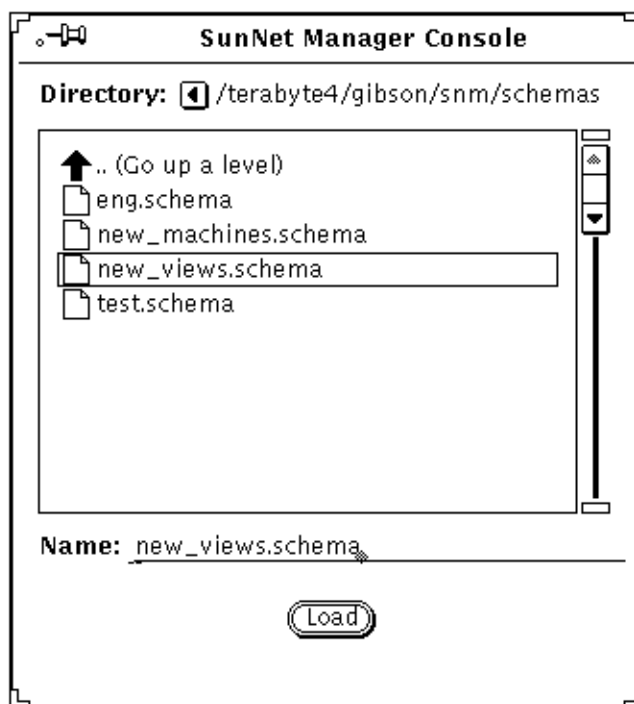


Figure 11-7 File—Load—Management Database Window

5. Create element instances of the newly-loaded element type with the graphical editor.

11.2.1 Notes

There are four categories of elements. You cannot create new element categories. The element categories are:

- **Component.** Includes elements such as workstations, printers, and routers.
- **View.** Includes elements such as subnets and buildings. Views can contain other views or components.
- **Bus.** Includes an Ethernet LAN segment. A bus appears as a line with movable endpoints.

- **Connection.** Includes links and RS-232 lines. A connection connects two other elements and appears as a line between the two elements.

Element types are defined in a record that specifies the element category and the name of the element type. Refer to Chapter 10 of the *SunNet Manager 2.2.3 Reference Manual* for more information about the element type record definition.

11.3 Creating a New Glyph for an Element Type

Each element type defined in the `elements.schema` file is represented by a glyph. The `elements.schema` file is normally located in the following directory:

- `/opt/SUNWconn/snm/struct` for Solaris 2.x
- `/usr/snm/struct` for Solaris 1.x

You can create your own glyphs to represent an element type.

1. Save the runtime database to an ASCII file.

- a. In the Console's File button, press MENU on Save►Management Database and release MENU. (See Figure 11-4 on page 11-5.)
- b. In the file menu, enter or select the directory and file name of the file you want to save. (See Figure 11-5 on page 11-6.)
- c. Click SELECT on the Save button.

2. Create an icon using the OpenWindows Icon Editor or your favorite utility. The icon file name should be `<iconname>.icon`.

Icons shipped with SunNet Manager are 32 by 32 pixels in size. Icons to be used with the Console can be 32, 48, or 64 pixels wide and any reasonable height.

3. You can also define a second icon—the icon mask—to be used as a stencil when coloring or inverting the icon.

This step is optional. The icon mask should be black for bits that you wish colored or inverted. The icon mask should have the path name `iconname.iconmask`. If you do not define an icon mask, a rectangular icon is assumed.

- 4. In the element's schema file, define an `elementGlyph` instance specifying the component or view and its icon path name.**
If the icon path name begins with a slash (/), it is treated as an absolute path. Otherwise, the path name is relative to the directories specified in the Console Properties window. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.
- 5. Restart the Console with the `-i` option and specify the ASCII file in which the runtime database was saved.**

11.3.1 Notes

You can have up to 1024 icon or rasterfiles defined in the runtime database; this includes background images as well as element glyphs.

11.4 Modifying the Console Tools Menu

- 1. In the Console window press MENU in Tools>Customize and release MENU. You receive:**

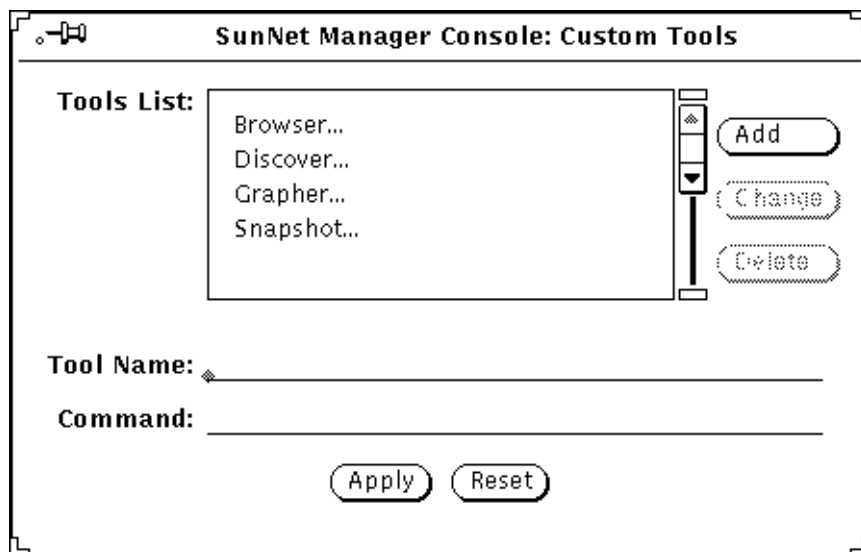


Figure 11-8 Tools—Customize Window

- 2. Add a new entry or modify an entry.**

- a. To add an entry, enter the tool name, as you want it to appear in the Console Tools menu, in the Tool Name line. Enter the tool's complete pathname in the Command line. Click **SELECT** on the Add button to add your entry to the Tools List. Click **SELECRT** on Apply for your change to take effect.
- b. To modify an entry in the Tools List, click **SELECT** on the entry. The tool's name, as it is displayed in the Console Tools menu, appears in the Tool Name line. The tool's full pathname appears in the command line. Make any edits you want and click **SELECT** on Change. Click **SELECT** on Apply to make the change tak effect. Click **SELECT** on Reset to restore the menu to the state it was in when you first invoked the Customize option.

Any changes you make to the Console's Tool menu remain in effect until the next time you invoke `snm` with the `-i` argument. The contents of the Tool menu are part of the runtime database. As such, they are saved when you invoke **File**►**Save**►**Management Database** to save the database to an ASCII file.

11.5 *Modifying the Tools Menu for an Element Type*

A SunOS command can be defined to appear in the Tools menu of an element type.

1. **Save the runtime database to an ASCII file.**
 - a. In the Console's File button, press **MENU** on **Save**►**Management Database** and release **MENU**. (See Figure 11-4 on page 11-5.)
 - b. In the file menu, enter or select the directory and file name of the file you want to save. (See Figure 11-5 on page 11-6.)
 - c. Click **SELECT** on the Save button.
2. **Using a text editor, open the `.schema` file that contains the element type for which you are adding or modifying a user command.**

If you are adding or modifying Tools menu options for an element type that is supplied with SNM, open the `elements.schema` file. The `elements.schema` file is normally located in the following directory:

- `/opt/SUNWconn/snm/struct` for Solaris 2.x

- /user/snm/struct for Solaris 1.x

If you are adding or modifying Tools menu options for an element type that you have created previously, open the appropriate .schema file.

3. **Restart the Console with the `-i` option and specify the ASCII file in which the runtime database was saved.**

11.6 Adding Agents and Glyphs

See Section 11.3, “Creating a New Glyph for an Element Type,” on page 11-10 for instructions on creating new glyphs.

You add agents and glyphs by appending the paths to the directories that contain them to the Schema Directories and Icon Directories items in the Console’s Properties►Locations window. These might be agents and glyphs shipped with another Sun product, such as SunLink X.25, or agents and glyphs provided by a party other than Sun.

1. **In the Console window, click SELECT on Props.**
2. **In the Properties window, press MENU on the Category abbreviated menu button and release MENU over Locations. You receive the window shown in Figure 11-9.**

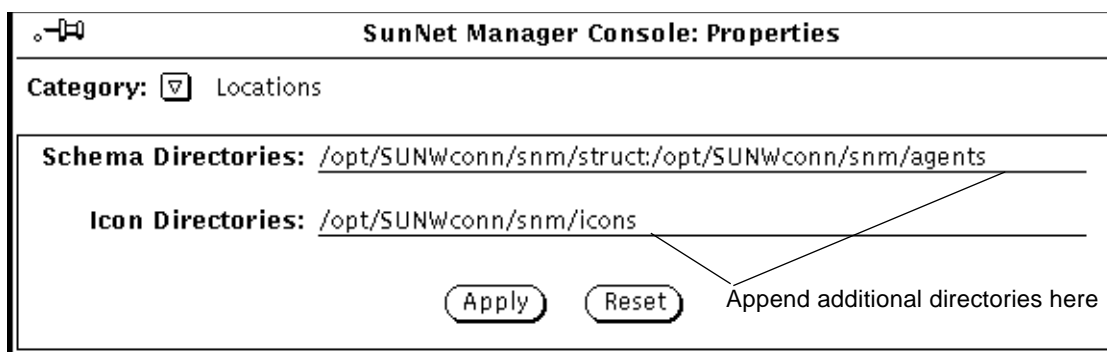


Figure 11-9 Properties/Locations Window

3. **To add a path, append a colon to the last path and enter the path where your agents or icons are stored and then click SELECT on Apply.** Following this, you must quit and reinvoke the Console, to make the new agents and icons available.

An alternative to the procedure described here is to simply copy the agents and glyphs (after ensuring there are no same-name collisions) to the directories already specified in the Properties►Locations window. This alternative is acceptable if you do not want to keep the SNM-supplied agents and glyphs separate from agents and glyphs you obtain from other sources. With either alternative, all agents and glyphs will be available to you whenever you create a new network element, or modify the properties of an existing network element.

11.7 Forwarding Novell's NMS Alarms to SunNet Manager

This section describes how to configure the current release of SunNet Manager and Novell's NetWare Management System (NMS) to forward NMS SNMP alarms from NMS to SunNet Manager over TCP/IP.

11.7.1 Software Requirements

Prior to making the configuration changes described below, verify that the following software requirements are met:

- the current release of SunNet Manager is installed
- for the NetWare Management System server:
 - NetWare Management Agent 1.5 software is installed
 - TCPIP NLM is loaded
 - NW2SNMP NLM is loaded with the GA switch set to ON ("load nw2snmp ga=on")

11.7.2 Configuration Changes Needed to SNM and NMS

To forward alarms from NMS to SunNet Manager, configuration changes are needed on both sides. NMS must be configured to send the alarms to SunNet Manager and SunNet Manager must be configured to understand and interpret the alarm information. These changes are described below.

11.7.2.1 SunNet Manager Configuration Changes

The alarms forwarded from NMS to SunNet Manager are generically referred to as “enterprise-specific traps.” In order for SunNet Manager to handle and interpret the Novell enterprise traps, Novell’s NetWare Server trap MIB (`nwalarm.mib`) must be integrated into SunNet Manager as described in the following steps. For more details, refer to Chapter 11 in the *SunNet Manager 2.2.3 Reference Manual*. In the examples below `<SNM_path>` refers to the location where SNM has been installed. The default location is as follows:

- `/opt/SUNWconn/snm` for Solaris 2.x installations
- `/usr/snm` for Solaris 1.x installations

Obtain a copy of the `nwalarm.mib` file from the NetWare Management Agent Setup diskette.

1. As root, load this file into the `<SNM_path>/agents` directory.
2. As root, run the SunNet Manager `mib2schema` utility on the `nwalarm.mib` file. This will produce three files (`nwalarm.mib.schema`, `nwalarm.mib.oid`, and `nwalarm.mib.traps`) as shown below:

```
hostname# <SNM_path>/bin/mib2schema nwalarm.mib
Translating ....
Translation Complete.
Schema file in "nwalarm.mib.schema"
Oid file in "nwalarm.mib.oid"
Traps in "nwalarm.mib.traps"
```

3. As root, run the SunNet Manager `build_oid` utility. This will update the object identifier database with the information from the `nwalarm.mib.oid` file as follows:

```
hostname# <SNM_path>/bin/build_oid
Parsing <SNM_path>/agents/enterprises.oid
Parsing <SNM_path>/agents/snmp-mibII.oid
Parsing <SNM_path>/agents/snmp.oid
Parsing <SNM_path>/agents/sun-snmp.oid
Parsing <SNM_path>/agents/nwalarm.mib.oid
Writing <database_path>/oid.dbase
```

4. If the `nwalarm.mib.traps` file is the only trap file that you need for your devices, you can copy the contents of that file to the default trap file. On the system where the trap daemon is running, append the contents of `nwalarm.mib.traps` to the end of the file specified in `snm.conf` as the `na.snmp-trap.default-trapfile` file. (The `snm.conf` file is located in `/etc/opt/SUNWconn/snm` for Solaris 2.x; in `/etc` for Solaris 1.x.) Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual* for detailed information on the trap daemon and creating an SNMP host file.

For Solaris 2.x:

```
hostname# cd /opt/SUNWconn/snm/agents
hostname# cat nwalarm.mib.traps >> /var/opt/snm/snmp.traps
```

For Solaris 1.x:

```
hostname# cd /usr/snm/agents
hostname# cat nwalarm.mib.traps >> /var/adm/snm/snmp.traps
```

or:

Create (or update) an SNMP host file by inserting the appropriate entry for the NetWare Management server host and specifying the `nwalarm.mib.schema` and `nwalarm.mib.traps` files (in the `agents` directory) as the schema and trap files respectively. Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual* for detailed information on the trap daemon and creating an SNMP host file.

An example entry added to the `snmp.hosts` file for the NMS server “steam” follows:

```
steam public public 10 <SNM_path>/agents/nwalarm.mib.schema
<SNM_path>/agents/nwalarm.mib.traps
```

11.7.2.2 NMS Configuration Changes

In the Netware Management system, the file `TRAPTARG.CFG` defines the recipients of SNMP traps (alarms).

This file is located in the `SYS:\ETC` directory of servers in which the NetWare Management Agent 1.5 software is installed. The file allows the user to define recipients to receive SNMP traps over IPX and UDP.

To forward traps to SunNet Manager, edit the `TRAPTARG.CFG` file and under the UDP section, add the IP address of the SunNet Manager machine which is to be the recipient of the SNMP alarms. In the following example, the IP address 123.123.34.56 has been added to the UDP section of the `TRAPTARG.CFG` file:

```
Protocol UDP
# In this section you can put SNMP managers that want to receive
# traps from the local node over UDP. Use either IP address or
# logical name. (If you use a logical name be sure the name and its
# corresponding ip address appear in the sys:etc\hosts file.)
# By default, the local node sends traps at least to itself.

127.0.0.1      # send traps to the loopback address
123.123.34.56 # IP address of SunNet Manager system
```

11.7.3 Example Forwarded Trap

Following is a typical trap report which has been generated by SunNet Manager after receiving a forwarded trap from NMS. In this particular example, a supervisor has established a login connection with the server STEAM.

```
Mon Sep 20 15:08:56 1993 [ steam ] : Trap:
sequence=1
receive-time=Mon Sep 20 15:08:56 1993
version=0
community=PUBLIC
enterprise=Novell.mibDoc.nwalarm-mib
source-time=87:09:54.30
trap-type=loginConnection
serverName=STEAM
trapTime=748555591
userName=SUPERVISOR
connectionNumber=1
```


If You Encounter Problems...

<i>Starting the Console</i>	<i>page 12-1</i>
<i>Letting the Discover Tool Build Your Database</i>	<i>page 12-3</i>
<i>Viewing, Creating, and Modifying Elements</i>	<i>page 12-4</i>
<i>Requesting Data from Agents</i>	<i>page 12-8</i>
<i>Viewing Data</i>	<i>page 12-10</i>
<i>Specifying Events</i>	<i>page 12-12</i>
<i>Creating an SNMP Element in the Database</i>	<i>page 12-14</i>
<i>Setting Up SNM to Receive Traps from a Device</i>	<i>page 12-15</i>
<i>Using the Set Tool</i>	<i>page 12-16</i>
<i>Loading Background Images</i>	<i>page 12-18</i>
<i>Creating Types of Elements</i>	<i>page 12-20</i>
<i>Creating a New Glyph for an Element Type</i>	<i>page 12-20</i>

This chapter is intended to provide guidance in case you encounter problems using SunNet Manager. Possible problems are grouped below according to the SNM function or tool where you are having difficulty.

12.1 Starting the Console

- The runtime database cannot be created.

The following message is displayed:

```
Cannot create database directory: <reason>
```

The runtime database cannot be created in the directory specified by the environment variable `SNMDBDIR`. If you did not specify the `SNMDBDIR` environment variable, the runtime database would be created in `/var/adm/snm` for a Solaris 1.1.1 machine or `/var/opt/SUNWconn/snm` for a Solaris 2.3 machine

Usually `<reason>` will indicate the source of your problem. Check that the directory exists and is writable. Make sure that you have at least 1 Mbyte of disk space available in the directory.

- An ASCII database file contains one or more invalid entries.

The Console displays the line number in the file where the error is detected and a brief description of the error. All definitions in the file are backed out of the runtime database. Any other files that do not have errors are correctly read into the runtime database. Edit and fix the particular file that could not be loaded and reload it. There are two ways to reload the file:

1. If the Console is opened, invoke **File**►**Load**►**Management Database**. In the Load window you then receive, double-click **SELECT** on the name of the corrected file.
2. Restart the Console, specifying only the corrected file, by entering:

```
host% snm <corrected_file>
```

This causes the last runtime database (containing only those files that were read correctly) to be loaded, along with the corrected file. If you want to replace the runtime database instead of merging the database in `<corrected_file>`, above, with the runtime database, use the `-i` option as shown in Section 3.2.1, “Startup Commands,” on page 3-3.

- Another user with the same user ID is already running a Console session.

The following message is displayed:

```
snm already running: started <date> on <host> (pid <pid>) by <user> on display <displayname>
```

Multiple Console sessions can be run from a single user ID. For each session, specify a different name by setting the environment variable `SNM_NAME`:

```
host% setenv SNM_NAME "Jack Netman"
```

The name does not need to be a UNIX login name; however, it should not include characters such as `'/'`, `'.'`, or `'..'`.

While multiple Console sessions are supported, it is not the recommended way to use SNM.

- Cannot contact activity or event daemon.

You might receive a message to this effect. In this case, check for the existence of `/etc/inetd.conf`. Make sure that this file contains lines to start `na.activity` and `na.event`. For example, in a Solaris 1.1.1 environment, it would look like this::

```
na.activity/10  tli rpc/udp  wait  root  /usr/snm/agents/na.activity  na.activity
```

<several intervening lines>

```
na.event/10    tli rpc/udp  wait  root  /usr/snm/agents/na.event  na.event
```

```
na.event/10    tli rpc/tcp  wait  root  /usr/snm/agents/na.event  na.event
```

If `inetd.conf` appears to be correct, reinvoke `/usr/sbin/inetd` (in a Solaris 2.x environment; for a Solaris 1.x machine invoke `/usr/etc/inetd`).

12.2 Letting the Discover Tool Build Your Database

- Not enough disk space is available for the runtime database.

This is generally indicated by a message like the following in your system console log:

```
netisam: not enough disk space: unix errno 28
```

Another possibility is a system console (not SNM Console) message: `<filesystem_name> filesystem full`. For either message, see the beginning paragraphs under Section 3.3, “Letting the Discover Tool Build Your Database” for general information about disk space requirements for the SunNet Manager database. For a list of common NetISAM messages and descriptions, refer to Appendix A of the *SunNet Manager 2.2.3 Reference Manual*.

- Element types are not correct.

Discovered devices are classified as either routers, workstations, or servers. To change an element type, see Section 3.9, “Changing Element Types,” on page 3-28.

- Glyph positions are not correct.

In the discover function’s properties window, make sure the Add Object Coordinates item is set to yes.

12.3 Viewing, Creating, and Modifying Elements

12.3.1 Traversing the View Hierarchy

- You have specified a view on the Goto line that is not in the database.

If this happens, the current view remains and the Goto line is cleared.

- You do not want the Console to display empty views.

By default, the Console allows you to go to empty views. You can specify that the Console not display empty views; this is configured in the Miscellaneous category of the Console Properties window. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for instructions.

12.3.2 Creating Elements

- Element name already exists.

If the element instance you are trying to create already exists in the runtime database, the following message appears in the footer of the element Properties window:

```
Cannot create; name already exists!
```

Only one element instance definition can exist for an element name. Once you have created an element instance, you can copy the glyph into different views (see Section 3.13, “Copying Elements,” on page 3-34). To find instances of an element, refer to the instructions in Section 3.7, “Finding Elements,” on page 3-25.

- Desired element type is not listed in Edit menu options.

The `elements.schema` file defines element types that are available from the Edit menu. The `elements.schema` file is normally located in the `struct` directory. (By default the `struct` directory is at `/usr/snm/struct` for Solaris 1.1.1 environments and `/opt/SUNWconn/snm/struct` for Solaris 2.3.) See Section 11.2, “Creating Types of Elements,” on page 11-7 for information on how to create a new element type.

- Desired agent schema is not listed in element Properties window.

The agent schemas that are listed in the Properties window are those files with the `.schema` extension that are located in the directories specified in the Console Properties window. By default, these directories are:

- `/usr/snm/agents` and `/usr/snm/struct` on Solaris 1.1.1 machines
- `/opt/SUNWconn/snm/agents` and `/opt/SUNWconn/snm/struct` on Solaris 2.3 machines

Agent schema files are provided with agent software. If you are using an agent that is not supplied with the SNM package, make sure that the agent schema file is located in a directory specified in the Console Properties window. See the description of the Schema Directories setting in Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual*.

Certain agents, such as the SNMP proxy agent, can use multiple schema files for a single element. These schema files can be Sun-supplied SNMP schema files or schema files created from an enterprise-specific SNMP Management Information Base (MIB) file used to manage a specific device. Refer to Chapter 11 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

12.3.3 Modifying Element Properties

- You want to change the element type of the element instance.
See Section 3.9, “Changing Element Types.”
- You want to change the glyph associated with the element.

Glyphs are associated with element types, not element instances. To create a new glyph for an element type, see Section 11.3, “Creating a New Glyph for an Element Type,” on page 11-10 for more information.

12.3.4 Changing Element Types

- Desired element type is not listed in element type options.

The `elements.schema` file defines element types that are available from the Edit menu. The `elements.schema` file is normally located in the `struct` directory. The default path for the `struct` directory is:

- `/usr/snm/struct` on Solaris 1.1.1 machines
- `/opt/SUNWconn/snm/struct` on Solaris 2.3 machines

See Section 11.2, “Creating Types of Elements,” on page 11-7 for information on how to create a new element type.

12.3.5 Moving Elements from One View to Another

If the following error message appears:

```
Attempt(s) to Drop or Paste into a request.
```

You attempted to paste an element into a request view.

12.3.6 *Deleting Elements*

- The element you tried to delete has an active request, or the element contains another element in its view.

If you attempt to delete an element that has an active agent request associated with it or that contains another element in its view, the following message appears in the Console footer:

```
Cannot cut or delete objects with non-empty subviews. 0
element(s) deleted.
```

You need to kill the agent requests for the element or delete the elements in its view.

- There are multiple instances of an element in a database.

Use the Find option of the View menu to locate all instances of an element—see Section 3.7, “Finding Elements,” on page 3-25. Within each view, delete the element.

12.3.7 *Saving the Management Database*

- The path you specified does not exist or is not writable.

If the specified path is not a writable path, the following message appears in the footer of the Console:

```
Cannot open <file> - save failed.
```

Verify that the path exists and is writable.

- The file name you specified does not have write permission.

If the file is not writable, the following message appears in the Console footer:

```
Cannot open <file> for writing
```

Make sure the directory has the appropriate permissions for access.

12.4 Requesting Data from Agents

12.4.1 Making a One-Time Request for Data

- Quick Dump option is not available from the Glyph menu.

If there are no readable attributes for any agent on the target system, the Quick Dump item in the Glyph menu is dimmed.

- Agent software is not installed on target system.

The specified agent may not be installed on the target system if the request is stopped and the following message appears in the Error Reports window:

```
Error: Request <request_name>: API error: Cannot create RPC
client: program=<number>, version=10: RPC. Program not registered
```

See Chapter 4 of the *SunNet Manager 2.2.3 Installation Guide* for instructions on installing agents.

If an agent is a proxy agent, the agent software does not need to be resident on the target system (the proxy agent software needs to be installed only on the proxy system). SNM-supplied proxy agents are `hostperf`, `ippath`, `lpstat`, `ping`, `traffic`, and SNMP proxy agents.

12.4.2 Requesting Periodic Data

- Expected reports are not returning.

Check the request to make sure that the Defer Reports field is off (no check mark appears in the accompanying box).

- Agent software is not installed on target system.

The specified agent may not be installed on the target system if the request is stopped and the following message appears in the Error Reports window:

```
Error: Request <request_name>: API error: Cannot create RPC
client: program=<number>, version=10: RPC. Program not registered
```


Run the `getagents` program to install the agent software and libraries from the manager station. For instructions on running `getagents`, see Chapter 4 of the *SunNet Manager 2.2.3 Installation Guide*. If an agent is a proxy agent, then the agent software does not need to be resident on the target system (the proxy agent software needs to be installed only on the proxy system). SNM-supplied proxy agents are `hostperf`, `ippath`, `lpstat`, `ping`, `traffic`, and SNMP proxy agents.

12.4.3 Copying Requests

- No agents were specified in the Properties window of the target element.

The following message indicates that agent software has not been installed on the target system.

```
Attempt(s) to Drop or Paste to an element accepting no requests
```

Run the `getagents` program on the target system.

- The agent in the copied request is not associated with the target element.

The following message indicates that the agent specified in the copied request is not associated with the target element.

```
Attempt(s) to Drop or Paste a request unknown to an element
```

Check that the agent is appropriate for the target element and install the agent software on the target system, if necessary.

- You cannot paste requests into the Home view.

The following message indicates that you tried to copy a request to the Home view.

```
Attempt(s) to inappropriately Drop or Paste into Home
```

You can only copy a request to an element subview.

12.4.4 Viewing Incoming Data

- The maximum number of entries in the Data Reports window is exceeded.

If you have a large number of incoming data reports, it is not unusual for the maximum number (1000) of data reports in the Data Reports window to be reached. When this happens, the total number of entries in the Data Reports window will not increment, although new reports are added. You can change the maximum number of entries by modifying the Maximum Data Reports setting in the Miscellaneous category of the Console Properties window. Refer to Chapter 9 in the *SunNet Manager 2.2.3 Reference Manual* for more information.

12.5 Viewing Data

12.5.1 Viewing Incoming Data with the Grapher

- Attribute is not graphable.

Only attributes of data types integer, float, counter, gauge, timestamp, or UNIX time can be graphed.

- Data scale is distorted.

By default, the vertical axis of a graph is plotted using Absolute values. The minimum and maximum values of the vertical axis are the smallest and greatest values among all the data sets that are being graphed. If you graph different attributes on the same graph, data sets can sometimes virtually disappear in the graph display. You should probably change the graph display to use Relative data scale values. The maximum and minimum values of the graph will then vary according to the maximum and minimum values of each data set. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31 for more information.

- Time scale is distorted.

By default, the horizontal (time) axis of a graph is plotted using Absolute values. The minimum and maximum values of the horizontal axis are the earliest and latest times among all the data sets that are being graphed. If you graph different time periods on the same graph, data sets can sometimes virtually disappear in the graph display. You should probably change the graph display to use Relative time scale values. The maximum

and minimum values of the graph will then vary according to the maximum and minimum values of each data set. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31 for more information.

12.5.2 Viewing Incoming Data with Strip Charts and Indicators

- Indicators and Strip Charts display in wrong view.

When a request is loaded from an ASCII file and the Restart field of the request has previously been set to True, Indicators and Strip charts associated with the display of the returned attribute values appear in the view from which the request was originally started. This occurs even if you moved the Indicator or Strip Chart into a different view before saving the runtime database to an ASCII file. (The reason for this is that Strip Charts and Indicators are not saved when you perform a save-database operation.)

12.5.3 Analyzing Stored Data with the Grapher

- Data streams are not selected in the Results Browser window

If you see the following message in the footer of the Results Browser window, you need to select the report streams to be graphed before you can send data to the Grapher.

No Streams Selected

See Section 4.5.1, “Analyzing Stored Data: Results Browser,” on page 4-22 for information about selecting report streams.

- Attribute is not graph-able.

Only attributes of data types integer, float, counter, gauge, timestamp, or UNIX time can be graphed.

- Data scale is distorted.

By default, the vertical axis of a graph is plotted using Absolute values. The minimum and maximum values of the vertical axis are the smallest and greatest values among all the data sets that are being graphed. If you graph different attributes on the same graph, data sets can sometimes virtually disappear in the graph display. You should probably change the graph

display to use Relative data scale values. The maximum and minimum values of the graph will then vary according to the maximum and minimum values of each data set. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31 for more information.

- Time scale is distorted.

By default, the horizontal (time) axis of a graph is plotted using Absolute values. The minimum and maximum values of the horizontal axis are the earliest and latest times among all the data sets that are being graphed. If you graph different time periods on the same graph, data sets can sometimes virtually disappear in the graph display. You should probably change the graph display to use Relative time scale values. The maximum and minimum values of the graph will then vary according to the maximum and minimum values of each data set. See Section 4.6, “Modifying the Display of a Graph,” on page 4-31 for more information.

12.5.4 Printing a Graph

- Graph does not print or the graph does not print in color.

Check the printer options in the Snapshot window to make sure that they match the characteristics of the printer.

12.6 Specifying Events

12.6.1 Sending an Event Request

- The agent software is not installed on the target system.

The specified agent may not be installed on the target system if the request is stopped and the following message appears in the Error Reports window:

```
Error: Request <request_name>: API error: Cannot create RPC
client: program=<number>, version=10: RPC. Program not registered
```

Install the agent software on the target system. (See Chapter 4 of the *SunNet Manager 2.2.3 Installation Guide* for instructions for running `getagents`.) If an agent is a proxy agent, then the agent software doesn't need to be resident on the target system. SNM-supplied proxy agents are `hostperf`, `ippath`, `ping`, `traffic`, and SNMP proxy agents.

- The target system does not support SNMP or the SNMP agent for the target system is not running.

If you are trying to send a request to a target system through the SNMP proxy agent and the proxy is unable to communicate with the target system, the following messages appear in the Console footer and Error Reports log, respectively.

```
Cannot start request `snmp.<group>.<#>'--will retry later. See error log for details.
```

```
Error: Request snmp.<group>.<#>: API error: Remote procedure call timed out: Cannot send request: Retrying.
```

Refer to Chapter 9, “Managing SNMP Devices,” for more information about using the SNMP proxy agent.

- No threshold has been set in the event specification.

If you attempt to send an event specification to an agent without specifying the conditions of the event, the following message is displayed.

```
No threshold is set, request is not sent.
```

Make sure that you click SELECT on the Apply button after specifying any thresholds.

12.6.2 Viewing the Status of Requests

Note that the states *awaiting activation*, *being activated*, *awaiting stop*, and *being stopped* are normally temporary. If you notice that a request seems to be in one of these states for a long time without changing, you should make sure that the target element is reachable by using the ping agent to do a Quick Dump request.

12.6.3 Viewing and Modifying the Properties of a Request

- Modifications to the request did not take effect.

Make sure that you have clicked SELECT on the Apply button after modifying an attribute display.

- Expected reports are not returning.

Check the request to make sure that the Defer Reports field is off (no check mark appears).

12.7 Creating an SNMP Element in the Database

- Element name already exists.

If the element instance you are trying to create already exists in the runtime database, the following message appears in the footer of the element Properties window:

```
Cannot create; name already exists!
```

Only one element instance definition can exist for a given element name or alias. You can modify the properties of an existing element to specify the SNMP-related information (refer to Section 3.8, “Modifying Element Properties,” for more information). Once you have created an element instance, you can copy the glyph into different views (refer to Section 3.13, “Copying Elements,” for more information). To find instances of an element, refer to Section 3.7, “Finding Elements,” for more information.

- Desired element type is not listed in Edit menu options.

With the alias feature, a given element instance definition might have multiple, database-unique names.

The `elements.schema` file defines element types that are available from the Edit menu. Refer to Section 11.2, “Creating Types of Elements,” for information on how to create a new element type.

- Desired agent schema is not listed in the Properties window of the element.

The agent schema names that are listed in the Properties window are defined by the keyword `proxy` in a schema file. The schema name is not necessarily the same as the schema file name.

Make sure that you have loaded the schema file into the runtime database. This is done with the Load►Management Database option of the Console’s File menu.

On the Console system, schema files (files with a `.schema` extension) must be located in the directories specified by the Schema Directories setting in the Locations category in the Console Properties window. These directories normally are `<SNM_path>/agents` and `<SNM_path>/struct`, where `<SNM_path>` is `/usr/snm` for Solaris 1.x environments and `/opt/SUNWconn/snm` for Solaris 2.x environments.

12.8 Setting Up SNMP to Receive Traps from a Device

- Traps are not being received by the Console.

Check the value of the `na.snmp-trap.rendez` keyword in the `/etc/snm.conf` file on the system on which the trap daemon resides. Add the keyword if it does not exist. Make sure the host name of the Console system is defined correctly. Multiple host names should be separated by colons (:).

- Traps are not being signaled in the Console.

The Console can be configured to signal, send mail, or fork a program when a trap report is received. If trap reports are being displayed in the Event/Trap Reports window, but the Console is not signaling the receipt of the trap report, check the settings for Trap Information in the Events and Traps category of the Console Properties window. If a glyph effect is being propagated, make sure that glyph state propagation has been enabled for the Console view that is being displayed.

12.9 Using the Set Tool

12.9.1 Using the Set Tool to Retrieve SNMP Attribute Values

- No value is returned for an attribute.

If the message “(No value retrieved)” appears under the Current Value column for an attribute, either the value is not available at the time the get request is made or an error occurred. (Refer to the error message at the bottom of the screen.)

- The proxy agent cannot find the schema or group specified in the request.

If the SNMP proxy agent cannot find the schema file for the target system or the schema file on the proxy system is not the same as the one loaded in the Console, the following message appears:

```
Error(Get): Invalid object group:group
```

This can happen if you are attempting to use a schema file that is not a “standard” schema file supplied by Sun (the schema file has been supplied by another vendor, or you have created your own schema file). Make sure that the schema file on the SNMP proxy system is located in a directory specified by the `na.snmp.schemas` keyword in the `/etc/snm.conf` file on the proxy system. If you change the keyword value while the SNMP proxy agent is running, you need to kill the proxy agent for the change to take effect. Make sure that the schema file on the proxy system is the same as the schema file on the Console.

- The SNMP proxy agent encounters an error while performing the request.

Any error messages that are prefixed by `Error(Get):` are messages returned by the SNMP proxy agent; see the `na.snmp(8)` man page for more information about the error.

- The community name defined in the request does not match the community name associated with the SNMP device.

This is likely to be the case if either of the following messages appear:

```
No response from system: <system>
This variable not available for set
```

An authenticationFailure trap is typically sent by SNMP devices in this situation.

Read and write community names are defined for the element in the element's Properties window. In the Set Tool window, you can also specify a community name value in the Options field for each request. If you do not specify community name values in the Properties window for the element or in the Options field of the request, the SNMP proxy agent uses "public" for both community names.

12.9.2 Using the Set Tool to Change SNMP Attribute Values

- The proxy agent cannot find the schema or group specified in the request.
If the SNMP proxy agent cannot find the schema file for the target system or the schema file on the proxy system is not the same as the one loaded in the Console, the following message appears:

```
Error(Get): Invalid object group: <gro>
```

This can happen if you are attempting to use a schema file that is not a "standard" schema file supplied by Sun (the schema file has been supplied by another vendor, or you have created your own schema file). Make sure that the schema file on the SNMP proxy system is located in a directory specified by the `na.snmp.schemas` keyword in the `/etc/snm.conf` file on the proxy system. If you change the keyword value while the SNMP proxy agent is running, you need to kill the proxy agent for the change to take effect. Make sure that the schema file on the proxy system is the same as the schema file on the Console.

- The SNMP proxy agent encounters an error while performing the request.

Any error messages that are prefixed by `Error(Set)` are messages returned by the SNMP proxy agent; see the `na.snmp man` page for more information about the error.

- The community name defined in the request does not match the community name associated with the SNMP device.

This is the likely to be the case if either of the following messages appear:

```
No response from system: <system>
This variable not available for set
```

An `authenticationFailure` trap is typically sent by SNMP devices in this situation.

Read and write community names are defined in the Properties window for the element. In the Set Tool window, you can also specify community name values in the Options field for each request. If you do not specify community name values in the Properties window of the element or in the Options field of the request, the SNMP proxy agent uses “public” for both community names.

12.10 Loading Background Images

- **The background file cannot be found.**

An image file you specified in the Add Background file menu does not exist or is not in the directory you specified.

If you added a background by editing the ASCII file that contains the runtime database and the Console cannot locate the background image file you specified in the `viewBackground` instance, the following message appears:

```
Cannot find icon/rasterfile <file>
```

If the icon path name begins with a slash (/), it is treated as an absolute path. Otherwise, the path name is relative to the directories specified by the Icon Directories setting in the Console Properties Locations category. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

- The background image file is not in the correct format.

If the background image file is not in rasterfile format, the following message appears:

```
Bad rasterfile: <file>
```

Icon format is supported if the file ends with the extension `.icon`.

- The background image file is a color file, but the Console is currently running on a black and white monitor.

If the following message appears, the background image file can only be loaded on color systems.

```
Cannot load color rasterfile on B&W monitor
```

- Too many icons and rasterfiles are already loaded into the runtime database.

If the following message appears, you need to reduce the number of icons or rasterfiles in the runtime database.

```
Cannot load more than 1024 icons/rasterfiles
```

- The view instance cannot be found.

If you added a background by editing the ASCII file that contains the runtime database and the view instance for the background image is not defined, the following message is displayed:

```
Unknown <viewname>
```

Make sure that the view instance definition exists and that it is loaded *before* the `viewBackground` instance.

12.11 Creating Types of Elements

- The schema file you created does not load.

If the following message appears, make sure that the schema file is readable.

```
Cannot open <file> - load failed
```

If loading the schema file fails because of a syntax error in the schema file, a message like the following appears in the Error Reports window:

```
line x: syntax error
```

Check the line indicated in the `.schema` file. Make sure that record entries have beginning and ending paragraph braces `()`. The field names in the element definition must *not* contain blanks—use underscores instead. The underscores will be displayed as blanks in the Properties window for the element.

The schema file may fail to load if the specified icon cannot be found. If the icon path name begins with a slash (`/`), it is treated as an absolute path. Otherwise, the path name is relative to the directories specified in the Console Properties window. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

12.12 Creating a New Glyph for an Element Type

- The icon file cannot be found.

If the Console cannot locate the icon file you specified in the `viewBackground` instance, the following message appears:

```
Cannot find icon/rasterfile <file>
```

If the icon path name begins with a slash (/), it is treated as an absolute path. Otherwise, the path name is relative to the directories specified in the Console Properties window. Refer to Chapter 9 of the *SunNet Manager 2.2.3 Reference Manual* for more information.

- Too many icons and rasterfiles are already loaded into the runtime database.

If the following message appears, you need to reduce the number of icons or rasterfiles in the runtime database.

```
Cannot load more than 1024 icons/rasterfiles
```


Index

Symbols

/etc/snm.conf file, 4-22, 12-15, 12-16, 12-17
/var/adm/snm directory, 3-10, 3-37, 12-2
/var/opt/SUNWconn/snm directory, 12-2

A

Add to All Views field, 3-12
adding SNMP devices, 9-2
adding Tools for element type, 11-12
agent configuration, 1-7
agent directory, 11-13
agent schema files, 1-6
agents
 adding, 12-5
 correlation between presence and requests available, 5-8
 definition of, 1-1
 how to access information on, 2-9
 procedure to add ..., 11-13
agents, shipped with SNM
 summary of, 2-8
alarm report
 definition of, 7-1

 features of device-specific .. window, 7-7
 obtaining device-specific, 7-5
alarms
 forwarding NMS .. to SNM, 11-14
alias feature
 description of, 3-22
aliases
 use in managing multiple network interfaces, 3-24
analyzing data reports
 Results Browser, 4-22
 Results Grapher, 4-30
ASCII database file
 specifying in SNM command line, 3-4
attribute values
 changing, 9-17, 12-17
attributes, 1-2, 1-6

B

background image
 adding to current view, 11-1
 comparison of means of adding, 11-7
BasicStart button, 3-8
Browser, 4-22

C

- cause of events, 5-10
- changing an attribute value, 9-17, 12-17
- changing element types, 3-28
- changing glyph state, 5-12
- changing SNMP attributes, 9-17
- clipboard
 - function in copying elements, 3-34
 - function in deleting elements, 3-35
 - function in moving elements, 3-31
- color
 - specifying the .. of an element, 3-20
- Color by Priority
 - role in decay-to-blue feature, 5-9
- configuration, 1-7
- connecting elements, 3-32
- connections
 - distinction between manageable and simple .., 3-33
- Console
 - introduction to, 1-4
 - quitting, 3-38
 - rules for control-area functions, 3-8
 - starting up, 3-3
- Console configuration, 1-7
- Console graphical editor, 3-2
- Console Requests viewer, 6-1
- Console views, 3-14
- Console window
 - configurability of, 3-8
- copying elements, 3-34
- copying requests, 4-13
- creating a background canvas, 11-1
- creating an SNMP element, 9-5, 12-14
- creating element types, 11-7
- creating elements, 3-15
- creating glyphs for element types, 11-10
- creating SNMP elements, 9-5
- critical nodes
 - using event requests to monitor, 2-12

D

- daemon configuration, 1-7
- data files, 4-22
- data report, 1-5
- Data Reports window, 4-14
- data request
 - analyzing results, 4-22
 - building, 2-27
 - copying, 2-29
 - how to send, 4-6
 - modifying, 6-3
 - Quick Dump, 4-4
 - viewing results, 4-14
- database directory, 3-10
- decay feature
 - use with manageable connections, 10-9
- decay-to-blue feature, 5-9
- deleting elements, 3-35
- disabling glyph state propagation, 5-14
- Discover
 - Add to All Views field, 3-12
 - configuring, 3-12
 - Maximum Hops field, 3-12
 - Objects to Discover field, 3-12
- discover function, 3-9
- Discover Tool
 - distinctions among element types, 3-30
 - extent of default search, 3-12
 - introduction to, 3-2
 - monitor function, 3-9
 - setting of properties window for discovered elements, 5-8
 - use for element-specific searches, 3-2
 - used to create manageable connections, 10-10
- disk space for database, 3-10

E

- element glyph state
 - changing, 5-12

- propagation, 5-14
- element instances, 1-6
- element properties, 3-26
- element Properties window, 3-17
- element schema
 - defining an icon mask, 11-10
- element schema file, 1-5
- element type
 - adding Tools for, 11-12
 - creating glyphs for, 11-10
 - modifying Tools for, 11-12
- element type definitions, 1-5
- element types
 - creating, 11-7
 - restrictions for changing, 3-30
- elementGlyph, 11-11
- elements
 - changing type of, 3-28
 - connecting, 3-32
 - copying, 3-34
 - creating, 3-15
 - creating SNMP elements, 9-5
 - deleting, 3-35
 - finding, 3-14, 3-25
 - modifying properties of, 3-26
 - moving between views, 3-31
 - moving within a view, 3-30
- elements.schema file, 1-5
- environment variables
 - SNMDBDIR, 3-10
- error messages, 7-7
- Error Reports window, 7-8
- event, 1-5
 - detecting presence of, 5-9
 - specifying, 5-2
- event glyph changes, 5-12
- event report request, 5-2
 - attribute values, 5-9
- event reports
 - modifying maximum number, 5-12
 - obtaining, 5-10
- event request
 - modifying, 6-3

- properties sheet, 2-18
- sending, 5-2
- sending to a link, 10-8
- specifying, 2-14

event.log file, 4-22

Event/Trap Reports window, 5-10, 7-10

events

- checking cause, 5-10
- SNM response to, 5-1

F

- finding elements, 3-14, 3-25
- footer message, 7-8

G

- get requests, 9-12, 12-16
- glyph directory, 11-13
- glyph menu
 - send request option, 5-6
- glyph state
 - changing, 5-12
 - propagation, 5-14
- Glyph State option, 5-12
- glyph states, 5-9
- glyphs, 3-1
 - procedure to add ..., 11-13
 - use of for multiple elements, 3-20
- glyphs for element types, 11-10
- Goto button, 3-15
- Graph Tool, 4-17
- Grapher, 4-14, 4-30, 4-31
 - invoking from Browser, 2-31
- graphical editor, 3-2
- graphs
 - modifying, 4-31
 - printing, 4-33

H

- HeadStart button, 3-8
- Home view, 3-14
- hostperf proxy agent, 3-20

I

- icon directory, 11-13
- icon mask, 11-10
- incoming data
 - problems viewing, 12-10
 - viewing, 4-14
- Indicator, 4-14
- Indicators, 4-19
- instances of elements, 1-6
- IP address
 - using as name of an element, 3-17

K

- killing requests, 6-6

L

- link creation
 - using Console's editor, 10-2
- link management
 - description of, 10-1
- link naming convention, 10-13
- linkmap file
 - use in link management, 10-6

M

- mail server information, xxi
- man command
 - for information on SNM agents, 2-9
- manageable connection
 - properties of, 10-3
- management application, 1-1
- management database, 1-5
- management station, 1-1
- managing printers, 8-1
- managing requests, 6-1
- managing SNMP devices, 9-1
- modifying a data request, 6-3
- modifying an event request, 6-3
- modifying graphs, 4-31
- modifying Tools for element type, 11-12

Monitor

- using to update management database, 2-36

monitor function, 3-9

moving elements, 3-30, 3-31

N

- Name field
 - in element property sheet, 3-17
- NMS alarms
 - forwarding to SNM, 11-14
- Novell's NetWare Management System
 - forwarding alarms to SNM, 11-14

P

- PATH environment variable
 - adding SNM to, 3-2
- ping proxy agent, 3-20
 - using to monitor availability, 2-13
- planning
 - for network management, 2-1
- predefined data requests
 - how to make, 4-8
 - introduction to, 4-7
 - sending from glyph menu, 4-10
 - summary of, 2-23
- predefined event request
 - example of, 2-14
- predefined event requests
 - example of, 5-5
 - sending from glyph menu, 5-6
 - summary of, 2-12
- printers
 - how to manage, 8-1
- printing a graph, 4-33
- propagation of glyph state, 5-14
- properties
 - finding .. of a request, 4-12, 5-8
 - properties of a request, 6-3
 - properties of an element, 3-17, 3-26
- proxy agent, 1-2, 1-3
- proxy agents supplied with SNM, 12-9

proxy feature
ability to access hostperf and ping
information, 5-8

Q

-q option
to snm command, 3-8

Quick Dump
for router interface status, 2-21
how to make .. request, 4-2

Quick Dump request, 4-4

Quick Start window
how to suppress, 3-8
introduction to, 3-6

quitting a Console session, 3-38

R

read community, 9-6

receiving SNMP traps, 9-10, 12-15

request glyph, 6-1

request properties, 6-3

request status, 6-1

requests
copying, 4-13
killing, 6-6
managing, 6-1
stopping, 6-6
viewing, 6-1

Requests Summary window
use in finding a request, 4-12, 5-8

Requests viewer, 6-1

requests, types of, 2-12

Results Browser, 1-5, 4-22
using, 2-29

Results Grapher, 1-5, 4-14, 4-22, 4-30, 4-31

retrieving current attribute values, 9-12,
12-16

retrieving SNMP attributes, 9-12

routers
adding names for multiple
interfaces, 3-22
interface status, 2-21

RPC protocol, 1-2

runtime database
clearing and initializing, 3-4
difference between .. and stored
ASCII file, 3-37
guideline for size requirement
for, 3-10
location of, 12-2
overview of, 3-2
replacing rather than merging, 12-2
saving, 3-36
saving to an ASCII file, 11-4
use of Discover Tool to build, 3-9
value of saving to ASCII file, 1-6

runtime management database, 3-1

S

saving runtime database
value of, 1-6

saving the runtime management
database, 3-36

schema file for agents, 1-6

schema file for element type, 1-5

set request, 9-17
problems with, 12-17

Set Tool, 9-12, 9-17

setting SNMP attributes, 9-17

Snapshot utility, 4-33

SNM agents
indicating presence on a
machine, 4-12

snm command
options to, 3-5

SNM hosts view, 3-12

SNM mail server, xxi

snm.conf file, 1-7, 9-2, 9-4, 9-9, 9-10, 9-12

SNMDBDIR
environment variable for runtime
database, 12-2

SNMDBDIR environment variable, 3-10

SNMHOME environment variable
requirement for, 3-3

SNMP
 ifOperStatus event request, 2-19
 managing with, 9-1
 sysUpTime event request, 2-17
SNMP attributes
 getting, 9-12
 setting, 9-17
SNMP devices
 adding to database, 9-2
SNMP element
 creating in database, 9-5, 12-14
SNMP get request, 9-12, 12-16
SNMP proxy agent, 1-2, 9-1
SNMP read community string, 9-6
SNMP set request, 9-17, 12-17
SNMP timeout, 9-6
SNMP traps, 9-10, 12-15
SNMP Vendor Proxy, 9-6
SNMP view, 3-12
SNMP write community string, 9-6
snmp.traps file, 9-12
snm-server, xxi
specifying events, 5-2
startup window, 3-6
state changes of glyph, 5-12
status of requests, 6-1
stopping requests, 6-6
Strip Charts, 4-14, 4-19
Sun SNMP agent (snmpd), 2-10
SunNet Manager
 command-line options for, 3-5
 requirement if installed in non-
 default location, 3-3
switching views
 Alarm Reports window, 7-4

T

timeout, 9-6
Tools menu for element type, 11-12
trap glyph changes, 5-12
trap reports, 7-10

traps
 receiving, 9-10, 12-15
type of element, 1-5
type of elements, 3-28

V

view hierarchy, 3-14
View menu, 4-14
viewBackground instance record
 for background image, 11-7
viewing data, 4-14
viewing data in Graph Tool, 4-17
viewing data in Indicators, 4-19
viewing data in Strip Charts, 4-19
viewing Data Reports window, 4-14
viewing error messages, 7-7
viewing requests, 6-1
viewing trap reports, 7-10
views
 adding background images, 11-1
 glyph state propagation, 5-14
 moving elements between, 3-31
 moving elements within, 3-30
 navigating, 3-14
 SNM hosts, 3-12
 SNMP agents, 3-12
 SNMP devices, 3-12
views, switching, 7-4

W

write community, 9-6

Copyright 1995 Sun Microsystems, Inc., 2550 Garcia Avenue, Mountain View, Californie 94043-1100 USA.

Tous droits réservés. Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie et la décompilation. Aucune partie de ce produit ou de sa documentation associée ne peuvent être reproduits sous aucune forme, par quelque moyen que ce soit sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il en a.

Des parties de ce produit pourront être dérivées du système UNIX[®], licencié par UNIX Systems Laboratories Inc., filiale entièrement détenue par Novell, Inc. ainsi que par le système 4.3. de Berkeley, licencié par l'Université de Californie. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

LEGENDE RELATIVE AUX DROITS RESTREINTS : l'utilisation, la duplication ou la divulgation par l'administration américaine sont soumises aux restrictions visées à l'alinéa (c)(1)(ii) de la clause relative aux droits des données techniques et aux logiciels informatiques du DFAR 252.227- 7013 et FAR 52.227-19.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevet(s) américain(s), étranger(s) ou par des demandes en cours d'enregistrement.

MARQUES

Sun, Sun Microsystems, le logo Sun, Solaris, SunSoft, le logo SunSoft, SunOS, OpenWindows, DeskSet, ONC, SNM, and NFS sont des marques déposées ou enregistrées par Sun Microsystems, Inc. aux Etats-Unis et dans certains autres pays. UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays, et exclusivement licenciée par X/Open Company Ltd. OPEN LOOK est une marque enregistrée de Novell, Inc., PostScript et Display PostScript sont des marques d'Adobe Systems, Inc.

Toutes les marques SPARC sont des marques déposées ou enregistrées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. SPARCcenter, SPARCcluster, SPARCcompiler, SPARCdesign, SPARC811, SPARCengine, SPARCprinter, SPARCserver, SPARCstation, SPARCstorage, SPARCworks, microSPARC, microSPARC II et UltraSPARC sont exclusivement licenciées à Sun Microsystems, Inc. Les produits portant les marques sont basés sur une architecture développée par Sun Microsystems, Inc.

Les utilisateurs d'interfaces graphiques OPEN LOOK[®] et Sun[™] ont été développés par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique, cette licence couvrant aussi les licences de Sun qui mettent en place OPEN LOOK GUIs et qui en outre se conforment aux licences écrites de Sun.

Le système X Window est un produit du X Consortium, Inc.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" SANS GARANTIE D'AUCUNE SORTE, NI EXPRESSE NI IMPLICITE, Y COMPRIS, ET SANS QUE CETTE LISTE NE SOIT LIMITATIVE, DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DES PRODUITS A REpondre A UNE UTILISATION PARTICULIERE OU LE FAIT QU'ILS NE SOIENT PAS CONTREFAISANTS DE PRODUITS DE TIERS.

CETTE PUBLICATION PEUT CONTENIR DES MENTIONS TECHNIQUES ERRONEES OU DES ERREURS TYPOGRAPHIQUES. DES CHANGEMENTS SONT PERIODIQUEMENT APPORTES AUX INFORMATIONS CONTENUES AUX PRESENTES, CES CHANGEMENTS SERONT INCORPORES AUX NOUVELLES EDITIONS DE LA PUBLICATION. SUN MICROSYSTEMS INC. PEUT REALISER DES AMELIORATIONS ET/OU DES CHANGEMENTS DANS LE(S) PRODUIT(S) ET/OU LE(S) PROGRAMME(S) DECRITS DANS CETTE PUBLICATION A TOUS MOMENTS.



Adobe PostScript

