ServerWORKS™ Manager

Overview and Installation

Part Number : ER-4QXAA-UA. G01

Digital Equipment Corporation

December 1997

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that might appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license. No responsibility is assumed for use or reliability or software or equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Preface

This document explains how to use DIGITAL ServerWORKS Manager network management product to manage DIGITAL servers. It also provides detailed procedures for installing, configuring, and using the ServerWORKS Manager components.

Audience

This guide is intended for the network administrator or server administrator.

Prerequisites

To use ServerWORKS Manager effectively, you should be familiar with the operational requirements for managing a network using the Simple Network Management Protocol (SNMP).

Terminology

The terms “Select" and "Choose" are used frequently in the procedures presented in this guide to perform operations. Both terms refer to specific mouse pointer or keyboard operations:

- Select—Move the mouse pointer to an item (icon, command, name, and so on) and single-click the mouse button, or use the specified set of keyboard keys.
- Choose—Move the mouse pointer to an item (icon, command, name, and so on) and double-click the

operational mouse button, or use the specified set of keyboard keys.

Related Information

DIGITAL ServerWORKS Manager Documentation

In addition to this user's guide, ServerWORKS Manager includes extensive online help and other online-readable information.
See Appendix A for references to additional sources of information.

DIGITAL ServerWORKS Manager Order Information

For information about upgrading ServerWORKS Manager or other DIGITAL software products, contact your DIGITAL Sales Representative or Channel Partner.

Keyboard Conventions

To Do This:	**Press These Keys:**
Scroll one window up or down	PAGE UP or PAGE DOWN
Go to the beginning of the list	CTRL+HOME
Go to the end of the list	CTRL+END
Move focus left or right	LEFT or RIGHT ARROW
Move focus one line up or down	UP or DOWN ARROW
Move to next window	CTRL + TAB
Move to previous window	CTRL+SHIFT+TAB
Go to the next field	DOWN ARROW or TAB
Go to the previous field	UP ARROW or SHIFT+TAB
Go to the next group	CTRL+DOWN ARROW
Go to the previous group	CTRL+UP ARROW
Move the focus up or down without affecting the state of the previous line (to add or remove lines from a selected set)	SHIFT+UP ARROW or SHIFT+DOWN ARROW
Toggle the state of the focus item	SPACEBAR
Display Help	F1
Display Help (from a console window)	CTRL+ALT+F1

Table of Contents

Preface

Introduction

Installation and Configuration

ServerWORKS Manager Console

Managing Servers Using SNMP-Based EnterpriseManagement Systems

Getting the Data You Want

Reference Information

Table of Figures

Table of Tables

Introduction 1

What is DIGITAL ServerWORKS Manager?

DIGITAL ServerWORKS Manager lets network and server administrators monitor and manage:

- DIGITAL servers, Alpha-based systems, and desktop and mobile PCs
- Non-DIGITAL servers
- Other network components, such as bridges, routers, hubs, printers, and so forth

ServerWORKS Manager’s easy-to-use Windows-based interface and multi-language support makes performing many common server and network management tasks much easier.

From a single management console, you have access to your entire network through the ServerWORKS Manager's client/server architecture. ServerWORKS Manager uses the Simple Network Management Protocol (SNMP) for its primary communication with servers running a wide range of operating systems and the Desktop Management Interface (DMI) for its primary communication with desktop and mobile systems. Both these industry-standard protocols are used to monitor the network and its components for early signs of problems, thus avoiding expensive downtime.

Why Install DIGITAL ServerWORKS Manager?

As a server or network administrator, you need to identify and address system and network problems as soon as possible. You would prefer to solve problems before they cause costly downtime to your users. In your business environment, DIGITAL ServerWORKS Manager helps you handle a wide variety of situations and tasks:

- **Looking at your network configuration** —Before you can manage your network and its components efficiently, you need to know the elements that make up your network. ServerWORKS Manager provides the ability to discover your network and its current configuration—including multi-vendor servers and DIGITAL and NT clusters—and displays the information in a hierarchy (tree view) or a topological map. Changes to hardware, such as upgrades to DIMMs or Pentium IIs, are displayed in the System Browser. You can customize views or create new ones to organize the view of your network to reflect your corporate structure or job responsibilities. You can query individual components of the network.
- **Providing minimal health thresholds for environmental conditions** — ServerWORKS Manager alarm agents establish the first line of defense against failures by monitoring power supplies, voltage, fans, and temperature for your specific hardware. When alarm conditions are met, traps are sent to alert you about potential and/or actual problems.
- **Monitoring usage**—ServerWORKS Manager can provide baseline information on parameters such as network adapter statistics, disk storage, and CPU use. It lets you set alarms to notify you when the value of a parameter exceeds a threshold that you define, allowing you to make adjustments before minor problems grow into critical problems. By monitoring network traffic, disk storage use, CPU use, and more, you can determine how to better balance the system load and place resources where they are needed most.

- **Monitoring intelligently**—ServerWORKS smart agent polls for many conditions locally, on the managed system, and only notifies the ServerWORKS Management Console when an alarm threshold is reached, saving considerable network bandwidth.
- **Managing assets**—ServerWORKS Manager can help the IS team manage the asset inventory. You need to know not only what systems are on your network, but how they are configured and whether components such as memory and hard disks are adequate for present use and future software upgrades.
- **Monitoring clusters**—ServerWORKS Manager discovers and manages Microsoft NT clusters and DIGITAL NT clusters on DIGITAL X86 processor-based and Alpha processor-based servers. ServerWORKS Manager sees the servers and identifies them as cluster members.
- **Automatically rebooting servers**—ServerWORKS Manager offers the optional WatchDog Timer. WatchDog Timer detects when servers running NT, SCO UNIX, or NetWare are down and reboots them automatically.
- **Viewing alarms and events in the Windows NT Event Viewer**—ServerWORKS Manager gives you the choice of using the Alarm Viewer or the Windows NT Event Viewer to check on alarms.

The following sections show how you might use ServerWORKS Manager to solve some typical problems that arise in network management.

Looking at the Network: IP Discovery and More

The network at Desktop, Inc. has grown enormously. Various groups are equipped with their own collection of workgroup servers from multiple vendors. Many individuals have several PCs and even their own hubs and routers.

Sophia works for the network administration organization, which manages the overall network and plans for future growth. Sophia uses ServerWORKS Manager's IP Discovery tool to build a topological map of the network. She can view and manage the entire network from ServerWORKS Manager, an option she does not have with most other network management packages. By simply defining an object type and assigning appropriate MIBs and icons, she can manage non-DIGITAL network elements, for example, a Compaq server. She chooses to create a map of only the hubs and routers so she can get a better picture of the pieces of the network she controls. Figure 1-1 shows a portion of this map.

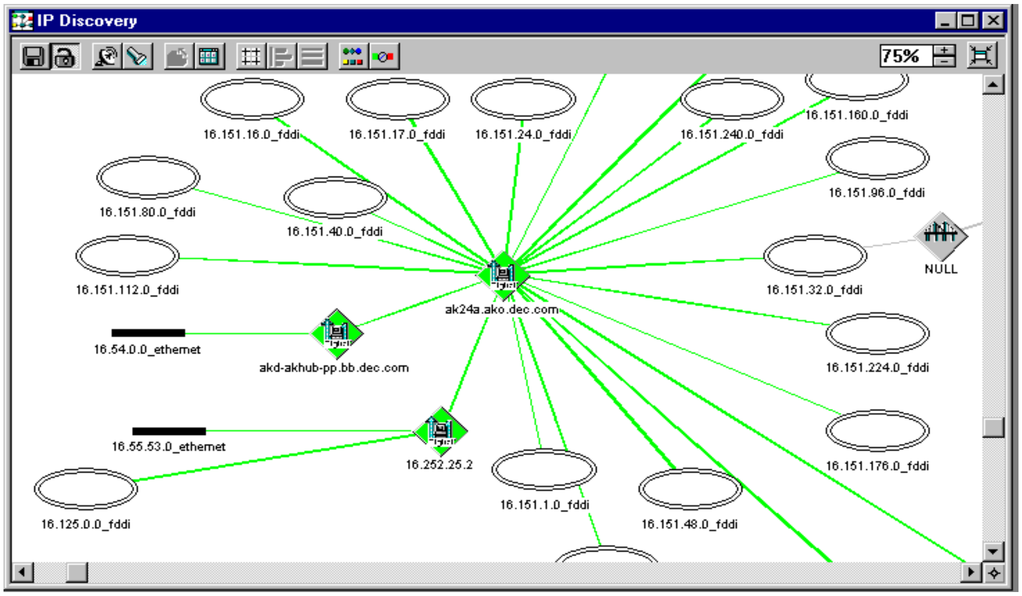


Figure 1-1 IP Discovery Map

Monitoring Performance: CPU Utilization

General Mercantile runs several CPU-intensive applications on a variety of servers. Balancing the CPU load is an important part of Rebecca's responsibilities. She uses ServerWORKS Manager to set an alarm if CPU utilization exceeds 80%. When CPU utilization reaches this point, she may decide to balance the CPU loads by switching applications from one server to another server. Rebecca sets the alarm so that once it is triggered, it will not be re-enabled until CPU use drops to 60%.

Rebecca also creates monthly snapshot reports and graphs of the CPU utilization for each of the servers when the applications are running. She provides her management with these reports. Last year, the IT organization used these reports to persuade General Mercantile management to add 25 DIGITAL servers to the network.

Monitoring the Network: Locating Network Interface Problems

At AKO Chemical, the IT group is having performance problems with a particular host's Ethernet adapter. The host can handle 10,000 packets per second, but anything more could be a problem.

Andy uses ServerWORKS Manager to set an alarm to notify him when the number of packets the host is handling reaches this critical level. Since Andy normally works at his desk, he chooses to be notified of the alarm through electronic mail. ServerWORKS Manager sends the alarm whenever the network Interface Inbound Packets reach or exceed 10,000 packets.

To further isolate the problem, Andy sets an alarm on the Inbound Errors to understand if the slowdown on the host is caused by errors and hence retransmissions by the higher layer protocol. He also sets an alarm on Inbound Packet Discards to determine if the slowdown is caused by the Inbound Packet not being delivered to a higher layer protocol because of buffer limitations or other transmission errors.

Because only a single protocol is being run at AKO Chemical, the company has a homogeneous environment. Andy can take advantage of this homogeneity and set an alarm on Network Interface Unknown Protocol to isolate random traffic produced by a device on the network.

Andy discovers that incoming bad packets are causing the problem. He uses the source address of the packets to track down and replace the device that is producing the bad packets.

Managing NT and Netware Resources: Server Administration from a Single Console

Two companies merged to form Freeform Engineering. The new company still uses two different networks, and Diego has to manage both of them. He does this from a single console by installing ServerWORKS Manager on a Windows NT system.

One fourth of Diego's users are on DIGITAL servers running Novell NetWare. Using the NetWare tools from within ServerWORKS Manager, he sets up new clients, manages the print queues, and performs other network management tasks.

The remainder of the company uses DIGITAL servers running Windows NT. The network includes several NT clusters. Because Diego installed ServerWORKS Manager on a Windows NT system, he can use ServerWORKS Manager's NT Server Management from the same management console to set up print queues and create domain or server user accounts.

Managing the Desktop: Checking Clients for Software Upgrade

Quick Electronics plans to upgrade all of its desktops to a new version of the operating system, which requires at least 1 GB of hard disk storage and 16 MB of memory. Laura uses ClientWORKS MIF Browser in combination with Microsoft System Management Server (SMS) to check all the desktop systems she manages. Although she is responsible for 500 such systems, she is able to obtain this information in only a few hours. She learns that 10 percent of the systems need additional memory and 15 percent need hard disk upgrades before the new operating system can be installed.

Managing Storage: Setting Alarms on File Utilization

Disk storage is a problem at the Sometime Electric Company. Users frequently exceed the disk storage capacity and suddenly find themselves unable to access the server. John, the server administrator at Sometime Electric, uses ServerWORKS Manager to set an alarm when file system utilization reaches 95%. Because he is not always at his desk, John uses ServerWORKS Manager's paging feature. John could also specify destination consoles where he or others could view alarms forwarded from his usual management console. When file system utilization reaches 95%, John is automatically notified and he can run his cleanup procedure to reclaim disk space.

John sets the threshold of the alarm at 95% with an automatic re-enable at 80%. Thus, once the alarm is triggered, it is disabled until it reaches the re-enable setting. In this way, John triggers only one alarm when the danger level is reached and provides for automatically re-enabling when the cleanup process is complete.

DIGITAL ServerWORKS Manager Features

ServerWORKS Manager components help you discover, view, and manage your network, monitor the network objects using SNMP operations, and set and view alarm conditions.

Discovering Your Network

When you start ServerWORKS Manager for the first time, you can open ServerWORKS Explorer. When you expand the Explorer's root object, the Explorer displays the root objects that make up your network. If you have Novell NetWare networks or Microsoft networks, they will appear here automatically, and they will be discovered automatically when you open the object.

Information about server objects (DIGITAL hosts) and SNMP objects must be placed into the database before it can be viewed. Information can be inserted into the database manually, or you can use the IP Discovery Wizard to automatically search and locate all objects on your network or on some segment of the network. The IP Discovery Wizard searches the network for TCP/IP and SNMP objects and builds a database of information from that network.

IP Discovery can be configured to search a default subnet, only the local network, or to find devices in locations other than your local network. It can locate all object types or filter the information to include only specified types, such as hubs, concentrators, or routers.

After the discovery is complete, the information is written to a database and displayed graphically in a map view. The Wizard also creates a report that you can view with Notepad, print, or save to a file. This report includes information about potential address and configuration problems that exist on your network.

You can run the IP Discovery Wizard whenever you need to add new information. After discovery is completed, the database is updated and the new information is displayed in the IP Discovery map or in another custom map.

Looking at Your Network

Once IP Discovery has run, you can use ServerWORKS Manager to monitor and manage the discovered objects.

Map View: IP Discovery

The Map View displays a graphical representation of your network's layout. The Map Viewer uses the ServerWORKS database to build the map, also called the logical topology, and automatically positions objects. When this map is complete, you can reposition the objects manually and save the changes so they will be preserved in any subsequent discovery that writes to the map view. Multiple discoveries can be run and the objects saved in the same map, or in different map views.

Hierarchical View: The ServerWORKS Explorer

The ServerWORKS Explorer is your main entry point into ServerWORKS Manager. The ServerWORKS Explorer opens with a tree view that consists of root objects for each of the object types in your network. From the hierarchical view, you display your Windows NT and Novell NetWare networks, if they exist. You can display DIGITAL servers and SNMP objects found during the discovery process in either map view or hierarchical view. SNMP objects are displayed with color to represent status and alarm bells to indicate unacknowledged alarms.

Customized Views

You can create your own map and hierarchical viewers to reflect your environment and needs. For example, you might want:

- A separate map viewer for each segment of your network
- A separate map viewer for each logical component of your network, such as Floor 1, Floor 2, Floor 3 or Manufacturing, Engineering, Personnel, or Sales
- A customized hierarchical viewer that includes only the Windows NT servers, NT clusters, and workstations that are in your building
- A map that includes only the hubs, routers, and bridges that make up your network

Monitoring Your Network

ServerWORKS Manager provides a variety of tools to help you monitor and manage your network and the systems in it, including three network browsers: the System Browser, the MIB Browser, and the MIF Browser. The MIF Browser is described in the section titled ClientWORKS Integration in this chapter.

The System Browser for DIGITAL Hosts

The System Browser displays and monitors information about the DIGITAL hosts on your network. With the System Browser, you can monitor information about the CPU, the storage, the network interfaces, and the environmental sensors. The exact information available varies according to the equipment, software, and sensors installed on the device you are monitoring.

In addition to viewing a static snapshot of the device, you can create a dynamic graph to monitor certain data over time. Data you can look at this way includes CPU load, file system utilization, network statistics, and readings from the thermal and voltage sensors.

Refer to the online help or the tutorial for more information about the System Browser and graphs.

The MIB Browser for SNMP Objects

ServerWORKS Manager provides the MIB Browser, which gives you the following capabilities for SNMP devices:

- Query SNMP agents to retrieve Management Information Base (MIB) variables, such as the system name, system ID, and up time for a router, hub, or bridge from the standard MIB II groups or any other MIB enrolled with the MIB database.
- View and set MIB variables

ServerWORKS Manager also provides tools to let you create, view, and modify MIB groups, associate a MIB grouping with an object, compile standard MIB definition files, and enroll new MIB groups into the ServerWORKS database.

Checking Network Status

ServerWORKS Manager uses color in both map and hierarchical viewers to indicate each object's operational status: whether it is up, not responding, or down. By default, the color green indicates that the object is operational, while red shows that the object has gone down. Magenta means that the system is not responding and should be looked at. You have the option of changing these colors.

Setting Alarms

While checking the status of network objects is useful, it does not notify you of potential problems. ServerWORKS Manager’s alarming and notification feature lets you set alarms to warn you of specific events that are important in your environment and specify how you want to be notified.

You can set four types of alarms:

- System (interface) status alarms that report when a system or interface changes status (for example, a workstation goes down)
- SNMP trap alarms that are triggered when a particular SNMP trap is generated
- Component status alarms that report the operational status of a DIGITAL server or DIGITAL node objects (for example, a fan fails)
- Component threshold alarms that are triggered when some characteristic of a DIGITAL host meets a specified condition (for example, the temperature reaches some upper limit)

When an alarm is triggered, the Alarm Counters on the management console’s status bar are updated. After an alarm is triggered, it is disabled. You can define a value at which the alarm will automatically be re-enabled. Rebecca at General Mercantile uses this threshold and re-enable feature to set an alarm that is triggered when CPU load reaches 80% and re-enabled when CPU load drops to 60%.

In addition to displaying alarm information on the management console's screen, you can request that the alarm be sent to an electronic mail address or to a pager number. You can also automatically trigger an action that you define. You can display a help file that tells the system manager what the alarm means and what should be done about it. You can even take action to correct the problem. For example, John at Sometime Electric might want to execute a script that would delete all the files from the /TEMP directory of the server that triggered the alarm.

Refer to the online help or to the tutorial for more information on setting alarms, re-enabling thresholds, and receiving notification.

Viewing Alarms

ServerWORKS Manager views alarms in two ways:

- Alarm bells displayed next to the name of an object in any viewer indicate a device that triggered an alarm.
- The Alarm Counter buttons, located on the status bar at the bottom of the ServerWORKS Manager window, show both the status of your network objects and the number of unacknowledged alarms of high, medium, or low severity.

More detailed alarm information is available from the Alarm Viewer. Double-click on an alarm counter button to view alarms of the specified severity. Double-click on an alarm entry to view a detailed alarm message. Alarms can also be filtered by an area of interest: object, date, time, severity, status, and alarm type. For example, if you have not assigned an action to Status or Threshold alarms on environmental conditions, you can view these alarms through filtering by the alarm type SNMP Trap.

You can also view many alarms and events in the Window NT Event Viewer. You must enable this feature. Refer to the section "Troubleshooting" in Chapter 2 for the procedure.

Managing Microsoft Windows NT Domains

If you have a Microsoft Windows NT network as part of your networking environment, you can use ServerWORKS Manager NT Server Management to manage it. NT Server Management allows you to administer your Microsoft network from the single interface of the ServerWORKS Manager rather than from the multiple windows and multiple utilities required by Windows NT.

ServerWORKS Manager automatically discovers your NT domains and lets you display the contents and properties of objects in the Explorer or as part of a custom collection or view. You can drag and drop objects such as users from one domain to another or to a server and otherwise take advantage of the single consistent interface. You can perform group operations easily. For instance, you could select several groups and modify their privileges.

You must install ServerWORKS Manager on a console that is running Windows NT to use NT Server Management. You must also have the appropriate administrator privileges for the particular task you want to perform, since ServerWORKS Manager security is based on Windows NT security. You are denied access without the privileges.

Refer to the ServerWORKS Manager NT Server Management online help for more information.

Managing NT Clusters

ServerWORKS Manager also finds Microsoft NT clusters and DIGITAL NT clusters on DIGITAL servers. As with DIGITAL clusters, a cluster icon appears in the hierarchy or map views next to the cluster member. The System Browser can supply you with other information, such as the cluster to which the server belongs, the cluster members, and cluster groups. Figure 5-3 shows a map view of a network that contains NT cluster servers.

Managing Novell NetWare Servers

If you have Novell NetWare file servers on your network, you can list those servers in the ServerWORKS Explorer and perform management tasks by accessing the NetWare utilities on those servers. When you select a NetWare server, icons for the following NetWare utilities are displayed on the ServerWORKS Manager toolbar: Filer, Pconsole, Printcon, Rconsole, Syscon, Userdef, and NWAdmin. To start a utility, click on the button.

Integration with Enterprise-Level Network Management Tools

Because ServerWORKS Manager uses the SNMP protocol, it can work with other enterprise network tools that use this protocol. ServerWORKS Manager can obtain information about all devices that follow the SNMP standard; likewise, DIGITAL MIBs can be compiled into another network management tool and DIGITAL hosts can then be browsed from that tool.

The DIGITAL Server Agent component of ServerWORKS Manager uses the operating system’s native SNMP protocol stack and extendible SNMP agent. You can set up the DIGITAL server's SNMP agents to send traps to a network management system such as ServerWORKS Manager. Traps can be forwarded from ServerWORKS Manager to an enterprise manager, such as HP OpenView NT or Tivoli TME 10.

Refer to the section entitled "Managing Servers Using SNMP-Based Enterprise Management Systems" in Chapter 4 for more information.

Integration of Companion and Other Applications

ServerWORKS Manager includes companion applications that are integrated into ServerWORKS Manager. These applications include:

- ***Global Array Manager (MYLEX GAM)***—MYLEX's client/server package used to monitor and manage the disk array subsystems attached to a MYLEX RAID controller.
- ***StorageWORKS Command Console (SWCC)***—This client/server package is used to monitor, manage, and troubleshoot large storage subsystems attached to a DIGITAL StorageWORKS RAID controller.
- ***Remote Server Manager (RSM)***—This package provides out-of-band management of X86 processor-based servers and includes both hardware and software components, purchased separately. The software component can be purchased separately and is included on the ServerWORKS CD. The RSM software is installed on a Windows NT management console and is able to manage remote DIGITAL servers that contain RSM hardware.

When the RSM software is installed on your ServerWORKS Manager console, it automatically integrates into ServerWORKS Manager. This integration means that all of the RSM functions can be performed from within ServerWORKS Manager. Because RSM uses a modem to connect from the management console to the remote server, RSM can still run even when the network is down.

- ***Remote Management Console (RMC)*** —This package is used to monitor and manage Alpha-based systems that have either:
  - KCRCM option hardware installed
  - RMC functionality built into the system

  When RMC software is installed onto the ServerWORKS Manager console, RMC automatically integrates into ServerWORKS Manager. This integration means that all RMC capabilities are available from within ServerWORKS Manager. For example, you can monitor the power supplies, temperature, and fans. You can also halt and power off an Alpha-based system. Because the connection from the management console to the remote system is through a modem, the RMC functionality can be used even when the network is down.

- ***Third-party applications***—Integration of other third-party applications is explained in a document available from the web. The document is located in the DIGITAL Windows Enterprise Computing web site at the following address:

```
http://www.windows.digital.com/products
  /server/svr_wrks_mgr_abstract.asp
```

ClientWORKS Integration: MIF Browsing Using DMI

ClientWORKS, the DIGITAL implementation of the Desktop Management Interface (DMI) standard, allows you to retrieve information both locally and remotely.

DMI uses Management Interface Format (MIF) files to provide detailed information on the hardware and software components of desktop, server, and mobile computers. Each component, peripheral, or application that has an associated MIF file can be browsed by a DMI-enabled application, such as the ClientWORKS MIF browser. This information can be displayed to users and administrators alike.

Integration into Microsoft's SMS

The MIFMaker program, also installed as part of ClientWORKS, is used to create up-to-date snapshots of MIF information that can be used with asset management and software distribution tools like Microsoft SMS to allow you to manage hardware and software for your entire enterprise—for example, to determine how many of your servers have 64 MB of memory or more.

SMS obtains information for its database by reading a Windows system's MIF file. The MIF information is pushed to the SMS server when the desktop SMS script is executed, generally when the user logs in. The ClientWORKS MIFmaker component automatically generates MIF snapshot files at set intervals that you, the administrator, define. Your SMS administrator can use tools in SMS to control MIFmaker and collect the MIF snapshot files in its database.

Supported Platforms – SNMP Agents

The SNMP agents running on DIGITAL systems provide the communication channel to the management console. The SNMP protocol is used over an IP network. These agents provide real-time system and performance data along with information about alarms. The DMI agents provide configuration data on DIGITAL servers or mobile systems.

The following table indicates the SNMP and DMI agents that are provided with ServerWORKS Manager V3.2 (See footnotes for exceptions).

Table 1-1 SNMP and DMI Agents

Minimum OS Version Supported	Host Resource SNMP Agent	X86 processor-based DIGITAL Server SNMP Agent	Alpha processor-based DIGITAL Server SNMP Agent	DIGITAL DMI Agent
NetWare® V3.12 and V4.1 (X86 processor-based DIGITAL servers only)	✓	✓	N/A	N/A
Windows NT ® V3.51 and V4.0 workstation and server (for all DIGITAL servers)	✓	✓	✓	✓
SCO® UNIX Open Server V5.0 (X86 processor-based servers only)	✓	✓	N/A	N/A
DIGITAL UNIX V3.2d-1[1] and greater (for Alpha processor-based servers)	✓	N/A	Future	N/A
DIGITAL OpenVMS V6.2[2] (Alpha processor-based servers only)	✓	N/A	Future	N/A
Windows 95 [3] (X86 processor-based DIGITAL servers only)	✓	N/A	N/A	✓
OS2/Warp 3.0 [4] (X86 processor-based DIGITAL servers only)	✓	N/A	N/A	N/A

[1] Shipped on ServerWORKS CD for V3.2d-1 agent; provided as part of the operating system for later versions.

[2] Available with DIGITAL TCP/IP Services for OpenVMS Version 4.1 (also known as UCX).

[3] Provided with ClientWORKS on DIGITAL mobile computers.

[4] Provided as part of OS/2 operating system.

Installation and Configuration 2

Introduction

This chapter explains how to install ServerWORKS Manager. The chapter is divided into sections that explain the installation of multiple components and the migration from previous versions. The following table describes the contents of each section:

In this section	**Find information about**
Prerequisites	Minimum hardware and software requirements for the management console, agents, and clusters
Installation Options	The components you can install
Pre-Installation Considerations	Component-specific information
Before You Begin	Required tasks and recommendations
General Installation Instructions	Locating any component on the CD-ROM and beginning its installation
Component Installation Instructions	Specific instructions for installing Agents, ServerWORKS Manager, RAID Storage Management applications, and Remote Management services
Post-Installation Options	Options for successful migration from earlier versions of ServerWORKS, ClientWORKS, and ManageWORKS
Troubleshooting	Solutions for unsuccessful installations

Prerequisites

ServerWORKS Manager has minimum requirements for the management console hardware and software, the agent hardware and software, and DIGITAL and Microsoft NT clusters.

Management console refers to the system on which ServerWORKS Manager console is installed and from which the servers are managed. This system can be a server.

Management Console Hardware

You need the following hardware to run ServerWORKS Manager.

Component	Minimum Requirements
Processor	Pentium 133MHz
Storage Devices	1 GB hard drive CD-ROM drive 3.5-inch diskette drive
Network Interface Card	Network adapter with TCP/IP support installed
Monitor	SVGA 800 x 600 (1024x768 resolution recommended on an 18" monitor)
Memory	32 MB

Table 2-1 Minimum Hardware Requirements for ServerWORKS Manager Console

Management Console Software

You need the following software to run ServerWORKS Manager:

Component	Minimum Requirements
Operating System	One of the following: • Windows NT V4.0 (on X86 processors) • Windows 95
Management Protocol	SNMP service [5]—Install the SNMP provided with the operating system
Transport and Network Protocols	TCP/IP—Install the TCP/IP provided with the operating system. TCP/IPX[6]—Install the TCP/IPX provided with the operating system

Table 2-2 Minimum Software Requirements for ServerWORKS Manager Console

[5] ServerWORKS Manager requires SNMP service only if a DIGITAL system SNMP agent is being installed on the management console machine.

[6] The IPX stack is required only if the NetWare OMM is needed. In addition, Novell's IP stack must be used; others may not work.

Agent Hardware

You need the following minimum hardware to support ServerWORKS agents. However, some options in the system parameter area, such as assets or FRU information, remain hardware dependent.

Component[7]	**Minimum Requirements**
X86 processor-based Prioris DIGITAL servers	LX, MX, XL, HX and ZX Servers; DIGITAL 1100, 3000, 5000, and 7000 family of servers
Alpha-based systems	AlphaServer 300, 400, 800, 1000, 1000A, 1200, 2000, 2100, 2100A, 4000, 4100, 8200, and 8400, DIGITAL Server 3000, 5000, 7000 (Windows NT)
Desktop computers [8]	Venturis FX, Venturis GL-6xxx,[9] Venturis 486, Venturis 486 LP, Venturis Pentium, Venturis Pentium LP, Celebris XL 6xxx, DIGITAL PC 5500, and DIGITAL PC 5400
Notebook computers[10]	HiNote Ultra 2000
Network Interface Card	X86 processor-based DIGITAL servers — TCP/IP adapter (Ethernet, Token Ring, or RAS)
	Alpha-based systems—All TCP/IP network adapters

Table 2-3 Minimum Hardware Requirements for Agents

[7] Note that ServerWORKS software is shipped only with DIGITAL products.

[8] Desktop computers may not support environmental parameters, RSM, or RMC.

[9] Venturis GL 6xxx is equivalent to the DIGITAL PC 3400. The DIGITAL PC 3400 is not available in all areas.

[10] Notebook computers may not support environmental parameters, RSM, or RMC.

Agent Software

You need the following software to run ServerWORKS agents:

Component		**Minimum Requirements**
Network Operating System	X86 processor-based DIGITAL servers	Novell NetWare[11] V3.12 or V4.1 SCO UNIX V5.0, V5.01, V5.02, V5.04 (not on clusters) Windows NT V3.51, V4.0 OS/2 3.0
	Alpha-based systems	Digital UNIX V3.2D-1 or greater OpenVMS 6.2 Windows NT V3.51, V4.0 for Alpha-based systems (for agents only)
Network Protocol		SNMP TCP/IP IPX (on NetWare servers only)

Table 2-4 Minimum Software Requirements for Agents

[11] Also known as IntranetWare.

Network Cluster Support

You need the following software to use ServerWORKS Manager to manage clusters.

Cluster Type	Requirements
DIGITAL Clusters V1.0	Windows NT V3.51 with Service Pack 3 running on DIGITAL servers DIGITAL Cluster MIB (already compiled into ServerWORKS Manager database
DIGITAL Clusters V1.1	Windows NT 4.0 with Service Pack 3 running on DIGITAL servers DIGITAL Cluster MIB (already compiled into ServerWORKS Manager database)
Microsoft NT Clusters	Windows NT V4.0 with Service Pack 3 running on DIGITAL servers Microsoft Cluster Server (MSCS)

Table 2-5 Minimum Software Requirements for Network Cluster Support

Installation Options

The ServerWORKS Manager CD-ROM contains the following components.

- ServerWORKS Manager Agents — Provides DIGITAL extension agents for enhanced SNMP capabilities and S.M.A.R.T. agent activity on managed systems. Install from the component screen onto the machine to be managed.
- ServerWORKS Manager Console — Provides ServerWORKS Manager SNMP-based management software for the management console. Install from the component screen onto the management console machine.
- ClientWORKS — Provides DMI browsing for the ServerWORKS management console. Install from the component screen on the management console machine.
- RAID Storage Management — Provides the client and server software for managing disk arrays that are connected to RAID controllers. You can choose from the following applications:
  - StorageWORKS Command Console (SWCC) — Monitors, manages, and troubleshoots large storage subsystems attached to a DIGITAL StorageWORKS RAID controller. Install from the component screen.
  - Mylex Global Array Manager (GAM) — Monitors and manages the disk array subsystems attached to a Mylex RAID controller. Install from the component screen.
- Remote Management Integration — Integrates remote management tools with ServerWORKS Manager Console.
  - Remote Server Manager (RSM) — Provides out-of-band management of X86 processor-based servers. Includes both hardware and software components.
  - Remote Management Console (RMC) — Monitors and manages Alpha-based systems.

- Tutorial—Explains how to get started with ServerWORKS Manager. You can view the tutorial from the CD-ROM before you install any component. It is installed with ServerWORKS Manager Console and includes Adobe Acrobat reader.
- Documentation—Contains viewable .pdf documents for all components. You can print the documents from Adobe Acrobat. The documentation is installed with the software.

Pre-Installation Considerations

The following sections provide background information about the components and their interaction with other software.

ServerWORKS Manager Agent Software

The ServerWORKS Manager CD-ROM includes the SNMP extension agents for various server operating systems. The SNMP agents on the ServerWORKS Manager CD-ROM must be installed even if the operating system comes with SNMP agents.

Note: *You must reinstall the Microsoft Service Pack after you install an agent on a system (as per recommendations from Microsoft Corporation for Service Packs).*

The following is a list of operating systems Management SNMP Agents that are supported by ServerWORKS Manager. The (✓) indicates that the agent is resident on the ServerWORKS Manager CD-ROM while the ( ) indicates that the agent is available elsewhere.

Operating System	**Supported on X86 processor-based DIGITAL servers**	**Supported on Alpha-based systems**
NetWare[12]3.12 or 4.x	✓	
SCO UNIX 5.0 or greater	✓	
DIGITAL UNIX 3.2D-1 (see note 3)		✓
Windows NT 3.51 or greater	✓	✓
IBM OS/2 Warp 3.0 (see Note 1)		
OpenVMS (see Note 2)		

Table 2-6 Operating System Management SNMP Agents

Note 1: In the current implementation of ServerWORKS Manager, OS/2 DIGITAL Servers are discovered as "server" objects, and not as "server.Digital. "In order to manage OS/2 DIGITAL Servers, it is necessary to manually change the server by first selecting the server, then selecting "Properties" from the "Actions" pull-down Menu. The server is displayed in the "Selected Objects" list box. From the "Properties" list box, select "General Information." (Interface Information is the default selection.) In the "type list" box, search for "server.Digital" and select it. Select "OK" to exit the dialog box.

Note 2: The OpenVMS SNMP agent for Alpha-based systems is included in the DIGITAL TCP/IP Services for OpenVMS product V4.1 or greater (this is a component of the NAS Client/Server Package). The SNMP agent is installed when TCP/IP is installed. The package also contains installation instructions for TCP/IP.

[12] Desktop computers may not support environmental parameters, RSM, or RMC.

Note 3: Agents for DIGITAL UNIX 3.2D and higher are supplied with the operating system. Refer to the instructions provided with the operating system to ensure the SNMP agent is enabled.

ServerWORKS Manager Console

Do not install ServerWORKS Manager Console software *and* agent software on a server running Windows NT 3.51 Server or Workstation. On NT 3.51, Microsoft's SNMP agent locks port 162 and does not relinquish it. The ServerWORKS Manager Console must have access to port 162.

At the beginning of the installation, ServerWORKS Manager Console Installation checks to see whether a version of ServerWORKS Manager Console exists on the system. If so, you have the following options:

- Preserve the database—Merges an existing V3.x database into a new Microsoft Access database, retaining all the information from the old version. Converts an existing 2.x version to a V3.x version.
- Remove the previous version—Deletes the old version of ServerWORKS Manager Console, including the companion database.

If you preserve the old database, the database remains on the system, even if the version of ServerWORKS Manager is removed. It is found in the directory:

```
<install drive>:\program files\digital\swmgr\database\old
```

A duplicate copy of the new database is kept in:

```
<install drive>:\program files\digital\swmgr\database\empty
```

You can copy the duplicate database to the default directory:

```
<install drive>:\program files\digital\swmgr\database
```

to start with a clean database.

You can restore the links between the database and ServerWORKS Manager Console. Refer to “Reusing a Previous Version of ServerWORKS Manager Console” in this chapter. If you have other V2.x databases to convert from previous installations, refer to the section "Converting a ServerWORKS Manager Database to Access."

Unless you have a compelling reason to install in another directory, install all components in the default directories. Maintaining two versions of ServerWORKS is not recommended. If you want a second version, first rename the files of the older version in the Start Menu directories. Use the following procedures:

For Windows NT 4.0 or Windows 95:

1. From the Desktop, choose Start→Settings→Taskbar.
2. Select the Start Menu Programs tab and click the Advanced button.
3. Choose Tools→Find→ Files and Folders. Then enter Start in the Named: field.
4. Browse the directory tree for the ServerWORKS, ClientWORKS or ManageWORKS directories and rename the files.

For Windows NT 3.51

You must have administrator privileges in the startup groups.

1. From the Program Manager, choose Startup.
2. Remove or rename the files.

ServerWORKS Manager Console and OpenVMS Management Station can be installed and run *separately* on the same machine. Continue to use ManageWORKS as the interface for the OpenVMS Management Station.

If you are installing ServerWORKS Manager Console software on an X86 processor-based server running NT 4.0 on which you also want to install an agent for local monitoring, install the agent software first, then install ServerWORKS Manager Console. If you install the ServerWORKS Manager Console first, you have to uninstall ClientWORKS before installing the agent software.

Do you have ManageWORKS installed?

If you do not have ManageWORKS installed, you can skip this section.

Only ManageWORKS V2.2 is supported for upgrading to ServerWORKS Manager 3.x. The installation checks to see whether ManageWORKS is installed. If it is, you can preserve the IP Discovery maps from ManageWORKS V2.2. Only IP objects in the IP Discovery View are preserved. User preferences and custom SVN views from ManageWORKS must be reapplied to new hierarchical views that you create in ServerWORKS Manager. Other ManageWORKS views, alarm and polling information, application launch information, or default actions are not preserved. If you do not remove ManageWORKS after upgrading to ServerWORKS Manager, you can continue to use it *separately* from ServerWORKS Manager.

After Upgrading to ServerWORKS Manager

You can expect the following conditions:

- The first time you run ServerWORKS Manager after upgrading from ManageWORKS V2.2, the message “Database inconsistency detected” appears. Choose the Ignore button. On the next dialog, choose the Ignore Forever button to prevent seeing the message each time you run ServerWORKS Manager.
- When you are discovering a network using the IP Discovery Wizard after upgrading, you are asked to choose a map view for the discovery results. The map views are equivalent, so you can select either one.
- If you preserve the ManageWORKS database, a read-only viewer named Browser is created. You cannot delete the Browser.
- To initialize a ManageWORKS database after upgrading to ServerWORKS Manager V3.x, first close all ServerWORKS Manager components (Event Logger, Event Dispatcher, Poller, Ping Server, and the Data Collector). Then initialize using the ServerWORKS Manager DB Utility with this procedure:

    1. From the Start menu, choose Programs→ServerWORKS DB Utility.
    2. Select "Entire Database except MIB."
    3. Click Initialize.
    4. Choose OK to exit from the utility.

- If you preserve the ManageWORKS V2.2 version and execute it without the full command line (including the initialization file SWMGR.INI), you will get incorrect database path pointers from the new version in addition to the following messages:

  ```
  CODEBASE ERROR
  Wrong DB version 0.0.0
  Expected DB version 2.0.X
  ```

  If you do not remove the ManageWORKS menu items from the Start menu, you may experience similar behavior.

ClientWORKS

If you do not have ClientWORKS installed, skip this section.

ClientWORKS may have been installed

- At the factory
- During the installation of the Windows NT agent
- During a previous ServerWORKS Manager installation

Do not install ClientWORKS on a server running Windows NT 3.51.

The version of ClientWORKS that is installed by the NT agent or that is factory installed, provides the remote and local browsing capability. The ClientWORKS installed by ServerWORKS Manager Console is configured for remote browsing only. ServerWORKS Manager Console can use ClientWORKS as it is configured for the agents.

To install ClientWORKS through the NT agent installation, you must uninstall any existing ClientWORKS software before starting the agent installation.

In most cases, the factory-installed ClientWORKS and the ClientWORKS installed as part of the NT agent installation can be used directly by the ServerWORKS Manager Console. The existing ClientWORKS is not replaced with the one from ServerWORKS Manager Console installation. As a result, ClientWORKS offers both the local and remote DMI browsing.

If a previous version of ClientWORKS is not compatible with ServerWORKS Manager Console, the installation procedure either removes it or asks you to remove it. If the installation is successful in removing ClientWORKS, it is replaced with a new version of ClientWORKS that supports only remote browsing.

The DIGITAL Windows NT Agent software contains the ClientWORKS software for browsing your X86 processor-based server. ServerWORKS Manager Console software contains the ClientWORKS software to browse other PC servers and clients remotely, but not to browse the local machine.

If you exit from the ClientWORKS installation that is launched by the ServerWORKS Manager Console installation and later decide to install ClientWORKS, you can do so by reinstalling ServerWORKS Manager Console. During the reinstallation, ServerWORKS Manager Console will install ClientWORKS.

RSM

Skip this section if you are not installing Remote Server Manager.

RSM consists of hardware and software components. They are installed on X86 processor-based DIGITAL servers running Window NT or Windows 95. In order to integrate RSM with ServerWORKS Manager console, the RSM software must be installed on the same machine as the ServerWORKS Manager Console software.

RSM software should be installed on an X86 processor-based DIGITAL server into its default directory:

```
        <windows drive>:\rs_mgr
```

A separate integration tool is provided to integrate RSM into ServerWORKS Manager Console. The integration is automatic if RSM was installed into its default directory.

If RSM was installed elsewhere, the RSM integration tool will ask for the destination directory where RSM was installed.

RMC

Skip this section if you are not installing Remote Management Console.

This section describes how to access the Remote Management Console (RMC) on an Alpha processor-based system. After configuring the RMC, you can start it from ServerWORKS Manager.

The RMC is a hardware/firmware feature of Alpha processor-based servers. The RMC allows you to control and monitor an AlphaServer system from a remote location. RMC commands are used to reset, halt, and power the monitored system on or off.

The control logic for the RMC is part of the system hardware in AlphaServer 800, 1200, 4000, and 4100 systems. Refer to the user documentation for these systems for instructions on configuring and using RMC. The AlphaServer 1000 and 1000A systems provide the RMC through a hardware option, the KCRCM AlphaServer Remote Console Module, which can be ordered separately. The KCRCM module is connected to an EISA/ISA slot on the AlphaServer 1000 or 1000A system. Refer to the documentation provided with the module for installation and configuration instructions.

To run RMC from ServerWORKS, use Terminal (TERMINAL.EXE) on Windows NT V3.51 or Hyperterminal (HYPERTRM.EXE) on Windows NT V4.0 and Windows 95. To integrate RMC into ServerWORKS Manager Console, Hyperterminal must be installed in the default directory selected by the operating system installation. Install as directed for Windows 95 and Windows NT.

AlphaServer systems identified during IP Auto Discovery display a purple icon on the toolbar when they are selected. Clicking on the icon for the system causes you to be prompted for the telephone number you configured for the modem connected to the AlphaServer. Entering the telephone number connects you to the remote AlphaServer and allows you to use the RMC.

When the RMC integration is complete, the installation confirms that the links between RMC and ServerWORKS Manager Console were successful. Refer to the section “Reusing a Previous Version of ServerWORKS Manager Console” for more information.

StorageWorks Command Console

Skip this section if you are not installing StorageWorks Command Console (SWCC).

StorageWorks is installed from the CD-ROM. The StorageWorks client can be installed on a management system. The StorageWorks agents can be installed on managed servers to which a RAID controller is connected. If StorageWorks cannot be automatically installed on the system, more information is displayed.

A previously installed version of StorageWORKS that was used with ServerWORKS Manager Console V2.x cannot be used with ServerWORKS Manager Console V3.x. StorageWorks must be reinstalled with the version provided on the ServerWORKS Manager CD-ROM (or a more recent version). Earlier versions are not compatible with ServerWORKS Manager Console 3.x.

Mylex Global Array Manager

Skip this section if you are not installing Mylex Global Array Manager (GAM).

GAM is installed from the CD-ROM. If GAM cannot be automatically installed on the system, information on how to install it is displayed.

A previously installed version of Mylex GAM that was used with ServerWORKS Console V2.x cannot be used with ServerWORKS Manager Console V3. Mylex GAM must be reinstalled with the version provided on the ServerWORKS Manager CD-ROM or a more recent version. Earlier versions are not compatible with ServerWORKS Manager Console 3.x.

Tutorial

The ServerWORKS Manager Tutorial is installed as part of the ServerWORKS Manager Console software. This tutorial contains basic information about ServerWORKS Manager. You can complete the tutorial in about 20 minutes. If you are a first-time user, DIGITAL recommends that you use the tutorial to get started.

Documentation

During the ServerWORKS Manager Console installation, the readme.txt and install.txt files are copied to the root of the installation directory. Online help is installed with the products. You can view or print the documents from the CD-ROM using Adobe Acrobat.

Before You Begin

Read the following section for suggestions and perform the required tasks before installing any component of ServerWORKS.

- You must install SNMP on the managed systems and configure a trap destination if you want to receive trap messages. Refer to the section “Configuring SNMP Agents” in the next section.
- After you install SNMP on Windows NT, make sure you reinstall the latest Windows NT Service Pack. Failure to do so may cause SNMP to crash. Contact Microsoft support for more information about the Service Packs.
- Shut down any other applications that are running before you install or integrate any component. Shut down SNMP services before you install ClientWORKS.
- Use the latest version of Microsoft ODBC. You must have the file ODBCJT32.DLL, V3.5 or greater. If you are in doubt whether you have the latest version, install the Microsoft Data Access Pack as offered with the installation.

- If you are installing a new version of ODBC, be aware that the ODBC datasource is unique to the installer’s user name in the current domain (\\domain\username). If you install under a different username or domain, ODBC creates a different set of ODBC datasources.
- Remove previous versions of ServerWORKS and ClientWORKS before you install a new version of either. You can remove them through the Control Panel→Add/Remove Programs applet or from the ServerWORKS Manager Console→unInstallShield menu item.
- If you have a version of ClientWORKS 2.90 or older, manually remove the ServerWORKS and ClientWORKS applications. The README.txt file contains complete instructions for removing ClientWORKS V2.90 or older.
- Remove ServerWORKS, ClientWORKS, and ManageWORKS menu items from the Startup menu because startup tasks may interact or interfere with the installation of newer ServerWORKS Manager components. The best way to remove them is through the Start→Taskbar→Start Menu Programs.
- You need 75 Mb of temporary disk space to install. The installation uses the directory set by your TEMP variable, or if TEMP is not defined, the Windows directory. For the environment variable ‘TEMP,’ specify a directory with a minimum 75 MB of storage to hold the temporary files used during installation. In addition, specify a TEMP directory that is not in your PATH. Otherwise, unpredictable results may occur. On Windows NT, use the Control Panel applet System Properties→Environment to modify the TEMP variable.
- Upgrade Microsoft Access V2.0 or earlier to Access V7.0 before the ServerWORKS Manager Console is installed. Otherwise, the complete version of ODBC is not installed and database updates are incomplete.
- Install the ServerWORKS components in the order in which they appear on the component screen. For example, install the agents before you install ServerWORKS Manager Console.
- If you stop an installation before it is complete, close the installation program completely and start over. For best results, use the Control Panel→Add/Remove Programs applet to remove any files from the incomplete installation before you attempt another installation. The uninstall program only removes files that were changed the last time an installation was run. Changed files from previous installations are not removed.

- The system files copied to your operating system's Windows system directory are not deleted when ServerWORKS Manager Console is uninstalled. They are retained to avoid a problem with InstallShield's Uninstall, which removes Windows system files no longer used by any other running program without asking for confirmation. If the ServerWORKS uninstall program were to delete the system files, some required DLLs would be removed, causing problems later when other programs are started.
- To use RMC install TERMINAL.EXE on Windows NT V3.51 or HYPERTRM.EXE on Windows NT V4 and on Windows 95. Because HYPERTRM.EXE is an option during the installation of Windows 95 or Windows NT 4.0, you may not have it installed. You can install if from the operating system kit before you begin installing ServerWORKS.
- Install RSM and RMC integration after ServerWORKS Manager Console V3.x is installed.
- Install StorageWorks Command Console (SWCC) after ServerWORKS Manager Console is installed.
- Install Mylex Global Array Manager (GAM) after ServerWORKS Manager Console and StorageWorks is installed.
- Choose one language to install and uninstall. Only one copy of the uninstall program is kept in your Windows directory. Therefore, it is always in the language selected during the last install on that system.
- Shut down all ServerWORKS Manager background processes (Event Logger, Event Dispatcher, Poller, Ping Server, Data Collector) before you install or integrate any third-party applications.
- To install ServerWORKS Manager on a system that has TME 10 NetView installed, first shut down the NetView daemons. Daemons continue to run in the background after you exit NetView. To stop the daemons, select the menu item Server Management from the NetView program group. Then select Stop Server to stop the daemons.

- Make sure you have administrator privileges if you are installing and configuring ServerWORKS with Windows NT. Remember that Windows NT administration rules and restrictions for Groups and Users continue to apply when you work from ServerWORKS Manager NT Server Management. For example, if you create a Local group remotely, the group does not have non-default privileges, such as Log On Locally, unless the administrator assigns the right. Refer to the Windows NT 4.0 Books Online volume *Basics and Installation Microsoft Windows NT Server, Version 4.0* on the MSDN CD-ROM for complete background on Windows NT.

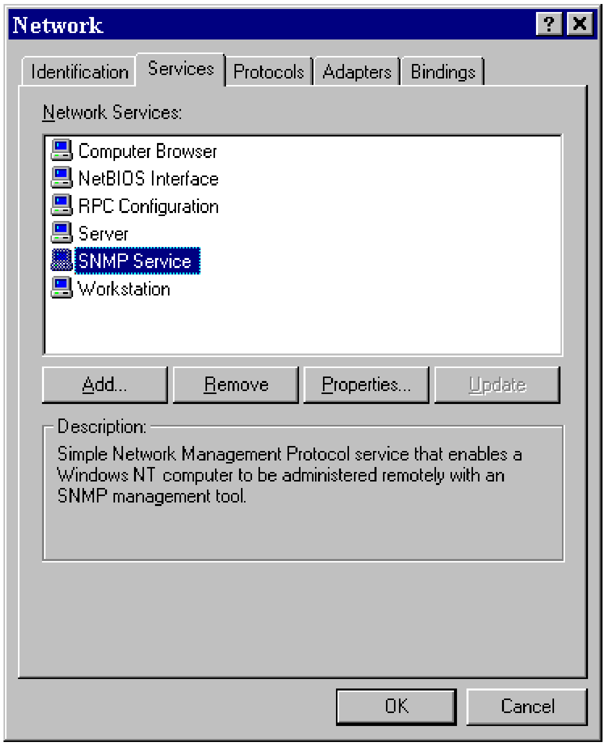
Configuring SNMP Agents

You must install the SNMP agent (also referred to as a service) on the server (managed system) and configure it with the address of the destination client(s) that will receive traps. The destination is the management console running an application such as ServerWORKS Manager. ServerWORKS Manager issues a warning message if you attempt to set a component or threshold alarm but you do not have SNMP installed and configured with a trap destination.

Configuring the SNMP Agent on Windows NT 4.0

Install and configure the SNMP agent on the Windows NT 4.0 server with the IP address or name of the client that will receive the traps.

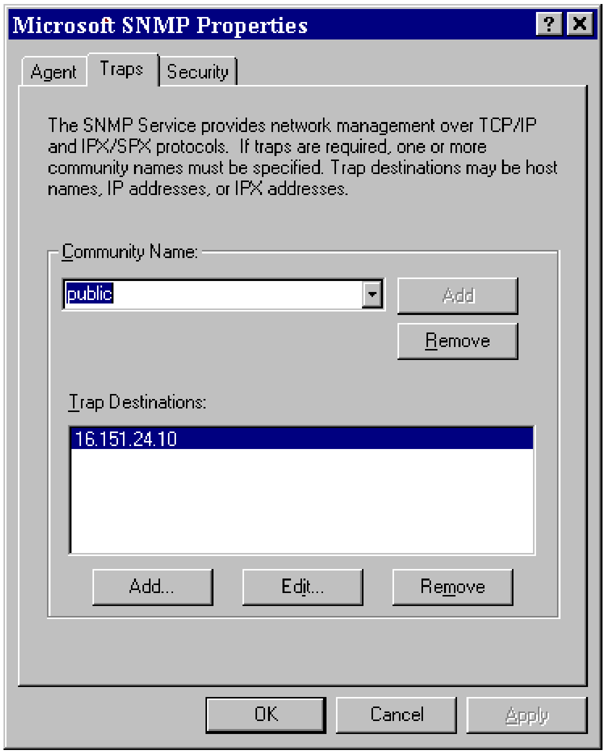
1. Using the Windows NT Control Panel, select the Network item.
2. Select the Services tab of the Network property page.
3. Select the SNMP Service item from the list of services as shown in the figure that follows. (If the service does not appear on the list, load the SNMP service from the operating system installation disks.)



Simple Network Management Protocol service that enables a Windows NT computer to be administered remotely with an SNMP management tool.

Figure 2-1 Selecting SNMP Agent from the Network Services Page

4. Click the Properties button.
5. Select the Traps tab.
6. Select the community name that you want to modify, or enter a new community name and click the Add button. (Public is the Windows NT default community name).



The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses, or IPX addresses.

Community Name: public

Trap Destinations: 16.151.24.10

Figure 2-2 Trap Destination Specified on the Traps Property Page

7. Click the Add button under the Trap Destinations list box. The trap destination represents a node running an application (such as ServerWORKS Manager) that is listening for traps on a port specified in the /Windows/Services file (typically port 162).

8. Enter the unique IP or IPX address of the host that will receive traps for this community. Do not use a subnet address.

9. Click the Add button on the Service Configuration dialog.

10. According to Microsoft recommendations, reinstall the latest Service Pack.

Check that the SNMP service is running. Use Control Panel→Services on Windows NT or Control Panel→Network→Services on Windows 95. Do not start the SNMP Trap service on the management console.

Configuring the SNMP Agent on Windows 95

Install the SNMP agent and configure the SNMP trap destination on the Windows 95 server.

Installing SNMP Software

1. From the Control Panel, click the Network icon.
2. Click the Add button on the Network option.
3. In the Select Network Component Type dialog box, double-click on Service.
4. In the Select Network Service dialog box, click the Have Disk button.
5. In the Install From Disk dialog box, type the path to the ADMIN\NETTOOLS\SNMP directory on the Windows 95 compact disc, and then click OK.
6. In the Select Network Service dialog box, click Microsoft SNMP Agent in the Models list and click OK. If you are prompted to specify the location of additional files, specify a path to the files on the CD-ROM or shared network drive.
7. Restart the computer.

Configuring the Trap Destination

You can also configure the trap destination on Windows 95 with the System Policy Editor. The Policy Editor is not a standard installed component for Windows 95.

1. From the Start menu, choose Control Panel.
2. Choose Add/Remove Programs and click on the Windows Setup tab.
3. Click on Have Disk and specify the path \ADMIN\APPTOOLS\POLEDIT. Click OK.
4. Select System Policy Editor from the Component list box and click Install and exit from the Add/Remove Programs tool.
5. From the Start menu, click Run and enter the command

   ```
   poledit
   ```
6. Choose OK to start the program.

7. In the System Policy Editor, choose File→Open Registry.
8. Double-click on Local Computer.
9. On the Local Computer Properties dialog box, double-click on the Network icon.
10. Double-click on SNMP to display the properties for the SNMP agent. Then set the community, permitted managers, (the IP or IPX addresses that are allowed to get information from an SNMP agent), and trap destinations for the Public Community (the IP or IPX address of hosts in the Public community to which you want SNMP to send traps).

Notes: *To send traps to a community other than Public, you must edit the Registry directly. That procedure is explained in detail in your Microsoft Windows 95 documentation and is beyond the scope of this manual.*

Configuring the SNMP Agent on Windows 3.51

Configure the SNMP agent on the Windows 3.51 server with the address or name of the client that will receive the traps.

1. From the Control Panel, click the Network icon.
2. On the Network Settings dialog box, choose SNMP Services.
   - If SNMP does not appear in the list of services, use the Add Software button and install the SNMP service from the operating system diskettes.
3. Choose the Configure button.
4. In the Send Traps with Community Name list box, enter the community name and click Add.
5. In the Trap Destination list box, enter the IP or IPX address of the trap destination and click Add.
6. Choose OK to close.

According to Microsoft's recommendations, reinstall the Service Pack.

First Steps for Installing All Components

Every component installation begins from the main screen after you select an installation language. The following steps open the main screen.

1. Insert the CD-ROM into the CD-ROM drive of the appropriate machine for the component. For example, insert into the CD-ROM drive of a managed system if you are installing agents. (You cannot install from a network drive.)
2. On Windows NT or Windows 95 systems, as soon as the CD-ROM is engaged the main screen appears. If it does not (for example, on a Windows NT 3.51 system), do the following:
   - From the desktop, click the Start menu.
   - Choose Run. Enter the path as follows:

     On Windows systems: `<cd-rom drive>:\Autoplay.exe`

     On Alpha systems: `<cd-rom drive>:\Alpha\Autoplay.exe`

     Double-click on Autoplay.exe to open the language selection screen.
3. Choose your preferred language. The selected language remains the default the next time you install or uninstall any component from the CD-ROM. The main screen opens.
4. On the main screen you have the following options:
   - ***Welcome***—Displays overview information about the product.
   - ***Install***—Displays the components you can install.
   - ***Tutorial***—Runs the online tutorial. You can install the tutorial or view it at any time from the CD-ROM.
   - ***Documentation***—Displays the manuals and other hardcopy documentation using the Adobe Acrobat reader located on the CD-ROM. (You do not need to install Adobe Acrobat on your system.) You can open the manual from the CD-ROM. Online help is installed with the applications.
   - ***Finish***—Closes the installation and offers to start ServerWORKS Manager Console (if it was installed) or to exit.

Do one of the following:

- Click on Install to open the component screen. From this screen you can navigate to any of the components to install them. Skip to the section "Component Installation Instructions" for details about each component.
- Click on any of the other options and follow the prompts to navigate through the option. For example, click on the Tutorial to open the tutorial and view it. When you exit from the tutorial, you are returned to the main screen where you can choose to install a component or exit.

Component Installation Instructions

Use the step-by-step instructions in the following sections to install specific components. If this is the first installation of ServerWORKS Manager, begin by installing the ServerWORKS agents. Then install ServerWORKS Manager Console.

If you are reinstalling any of the components from an earlier version, read the section “Pre-Installation Considerations” if you have not done so.

Installing ServerWORKS Manager Agents

Install the agents before you install any other component. Install the agents on the remote machines that you will manage from the ServerWORKS Manager Console. The installation provides only the agents that are appropriate for the operating system and platform on which you are running the ServerWORKS Manager CD-ROM.

Installing ClientWORKS with the Agents

ClientWORKS is installed when you install NT agents on DIGITAL servers. This installation of ClientWORKS is configured for local and remote browsing. (Refer to the section "ClientWORKS" in this chapter for more information.) You do not need to reinstall ClientWORKS when you install ServerWORKS Manager Console.

Note: *After you install an agent on Windows NT, reinstall the latest Service Pack. (When you install a system component on a system that has a Service Pack installed, you must reinstall the Service Pack, following Microsoft's recommendations.)*

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.

3. From the component screen, click ServerWORKS Manager Agents.
4. Follow the messages in the prompts to complete the agent installation.
   - To install NT agents on DIGITAL servers, click Install.
   - To install agents on other operating systems, click Read to learn more about specific instructions. Follow the prompts. When the agent installation is complete, click Close.
5. 5. On the component screen, choose the next component to install. If you are not installing other components, click Close and then click Finish on the main screen.

Do you plan to monitor your management console?

You can install an agent and the console software on a management console running Windows NT 4.0. Use the preceding instructions for the agent installation.

Installing ServerWORKS Manager Console

Install the ServerWORKS Manager Agents before you install the ServerWORKS Manager Console. (The ClientWORKS installation is also included with the ServerWORKS installation, and you have the option of installing it as soon as the ServerWORKS Manager Console installation is complete.) Install the console software on the machine from which you will manage other systems and servers. Typically, this is your desktop or lab administration machine.

If previous versions of ClientWORKS or ManageWORKS are installed, the installation may perform additional tasks, according to your responses or what it finds on your system. Always follow the instructions in the prompts.

If you are reinstalling, refer to the section “Before You Begin” for helpful suggestions and required tasks.

To install ServerWORKS Manager Console

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the component screen, choose ServerWORKS Manager Console.

4. Do one of the following on the intermediate installation screen:

   – On Windows NT, if you have already installed the NT agent, skip Step 1.

     At Step 2, click Read to learn more about ODBC and the Data Access Pack.

     At Step 3, click Install to install the Microsoft Data Access Pack if you do not have ODBC V3.5 or greater installed. You need to install all the Data Access Pack components. Follow the instructions in the prompts.

     At Step 4, click Install to install ServerWORKS Manager and open the component screen. Then click Next.

   – On Windows 95, at Step 1 click Read to learn more about ODBC and the Data Access Pack.

     At Step 2, click Install to install the Microsoft Data Access Pack. You need to install all components of the Data Access Pack. Follow the instructions in the prompts.

     At Step 3, click Install to install ServerWORKS Manager Console. Then click Next.

4. On the Welcome screen, click Next to agree to the licensing information.

5. If the installation cannot locate a previous registration, register your name and organization on the ServerWORKS Manager Console screen, follow any prompts, and click Next.

6. On the Choose Destination Location screen, click Next to place the files in the specified default directory. Avoid installing a new version over a previous version. (On a subsequent installation, you may have problems sharing files between the two versions if one version resides in another directory.) If you want to change the directory, use the Browse command to select the location and return to the Choose Destination Location screen. Then click Next to proceed.

7. If this is the first installation, skip to Step 8. If you are reinstalling, do one or both of the following:

   – Select "Use the existing database." This option preserves the current database and merges it into a new database. If you do not select this option, the old database is saved in:

   ```
   \Program Files\Digital\SWMgr\database\old
   ```

   – Select "Remove previous versions of ManageWORKS and ServerWORKS." Follow any messages in the prompts regarding uninstalling previous versions of the software.

   Then click Next.

8. Specify whether you want the background tasks to start automatically or to start only when you run ServerWORKS Manager. If your console is dedicated to ServerWORKS and administration, you may want to run them automatically. Then click Next to proceed.

9. Continue to follow the prompts until the ServerWORKS Manager installation is complete.

Installing ClientWORKS

After ServerWORKS Manager has been installed successfully, the ClientWORKS installation begins automatically. This installation of ClientWORKS is for remote browsing only. Refer to the section "ClientWORKS" in this chapter for more information.

If SNMP services are running, you are prompted to stop them during the installation. Follow the messages in the prompts to shut down and restart the SNMP service.

1. Proceed with the ClientWORKS portion of the installation. Continue to follow any prompts. Then click Next.

2. On the first licensing acknowledgment screen, click Next. On the second licensing screen, click Yes.

3. On the ClientWORKS components screen, select the option(s) and then click Next.

4. On the language option screen, choose the same language that you used to install ServerWORKS Manager and click Next to proceed.

5. Choose the destination for ClientWORKS and click Next.

6. Choose the default folder name or enter your own folder name. Then click Next. Follow any prompts regarding SNMP service.

   When ClientWORKS is successfully installed, ServerWORKS Manager Console integrates ClientWORKS with ServerWORKS.

7. The option “View README.TXT” is selected so that you can read the information immediately. If you do not want to view the README.TXT, deselect the option and click Finish. Follow the messages to close any remaining dialog boxes. The intermediate installation screen appears. Click Close.

8. On the component screen, click Close again to return to the main screen.

9. On the main screen, click Finish.

10. On the next prompt, select "Start ServerWORKS Manager immediately" or click Exit.

11. On exiting you are returned to the component screen. If you do not plan to install any other components, click Close.

12. On the main screen, click Finish.

Installing RAID Storage Management

Skip this section if you are not installing RAID controller management applications.

Installing StorageWorks

StorageWorks consists of a client for the management console and agents for the managed servers. The StorageWorks client is installed on a Windows NT or Windows 95 node. The StorageWorks agents are installed on servers that are connected to a StorageWorks Raid controller running Windows NT, NetWare, or SCO UNIX.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."

2. Click Install to open the component screen.

3. From the component screen, choose StorageWorks Command Console.

4. On the next screen, click on Agent or Client and follow the prompts to return to the main screen.

5. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Installing Mylex GAM

Mylex GAM consists of a client that is installed on the management console running Windows NT or Windows 95 and agents that are installed on servers that are connected to Mylex GAM RAID controllers.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the components screen, choose Mylex GAM.
4. On the next screen, click Install and follow the prompts to return to the main screen.
5. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Installing Remote Management Integration

Skip this section if you are not installing remote management integration.

Your selection for remote management depends on the operating system of the management console where you are installing the component.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the components screen, choose a remote management service for your system.
4. Follow the prompts and click Finish when the integration is successful.
5. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Post-Installation Options

Several features of ServerWORKS are manually installed or configured after ServerWORKS is installed.

WatchDog Timer on Multiple Platforms

WatchDog Timer is an option you can install after ServerWORKS Manager is installed. The Watchdog Timer is a utility that automatically recovers a hung operating system by rebooting the server. The Watchdog Timer is disabled by default at installation. For security reasons this release supports enabling/disabling this feature at the agent from the system prompt.

On the NT, NetWare, and SCO UNIX operating systems, ServerWORKS Manager offers Watchdog Timer support for Prioris ZX6, HX6, MX6 and XL6 servers and the DIGITAL Server 3000, 5000, and 7000 series.

To enable WatchDog Timer:

1. Open the system prompt.
2. Enter the program name followed by a space and the number of minutes to wait before rebooting of the system occurs. For example:

   On an NT system:

   ```
   sw_wdt 4
   ```

   On a NetWare system:

   ```
   load ServerWORKS_wdt 4
   ```

   The system provides a message describing the result. For example, an NT system displays the message “WatchDog enabled for 4 minute wait before reset after system hang.”

To disable WatchDog Timer:

1. Enter the program name at the system prompt
2. Omit the number of minutes.

Using sw_wdt sets the Watchdog Timer permanently on a server. If the Watchdog Timer causes a system to be reset, the last shutdown reason includes a message confirming this. You can choose from a one to four-minute wait.

WatchDog Timer on SCO UNIX

You can enable WatchDog Timer at installation when you install ServerWORKS agents on SCO UNIX systems. In response to the prompt, enter the number of minutes to wait before rebooting occurs. You must be logged in as /root or as an administrator to enable WatchDog Timer on SCO UNIX.

Reusing a Previous Version of ServerWORKS Manager Console

You can use a previous version of a ServerWORKS Manager Console and its database. If the previous version was ServerWORKS Manager Console V2.x or V3.x , do the following:

1. Find the ServerWORKS Manager section in the WIN.INI file. This section is labeled:

   [ManageWORKS user info]

2. In this section, find the line within this section that begins:

   ```
   INI file=
   ```

   The line specifies the current location of ServerWORKS Manager. You will need to change the line to:

   ```
   INI file=<full path to ServerWORKS Manager Console to use> \SWMGR.INI
   ```

3. For ManageWORKS V2.2, edit the line to:

   ```
   INI file=<full path of previous installation>\MWORKS.INI
   ```

Converting a ServerWORKS Manager Console Database to Access

ServerWORKS Manager Console V3.x uses an Microsoft Access database to store information. Version 2.x ‘ini’ files such as swextomm.ini are no longer used. All information is now stored in the database. If you want to use an V2.x database, it must be converted to be used with V3.x. This is done automatically by the installation procedure.

Assume ServerWORKS Manager Console is installed at:

```
<install drive>:\program files\digital\swmgr:
```

If a previous installation was found and the database was preserved, a copy is placed at:

```
<install drive>:\program files\digital\swmgr\database\old
```

```
The installation converts the ServerWORKS Manager Console V2.x
database in DB4 format to a Microsoft Access database format
automatically
```

As part of an installation, ServerWORKS Manager Console installs a pre-initialized V3.x database at:

```
<install drive>:\program files\digital\swmgr\database\empty
```

If this is a new installation or if the previous database is not being preserved, this is the initial database.

Note: *During the installation, if the current version is installed in the same directory as the previous version, the previous version is deleted first. Installing a new version in the same directory as a previous version is not recommended.*

Troubleshooting

This section describes common occurrences when an installation is unsuccessful and suggests solutions. Review the list for your particular situation if you are dissatisfied with the installation. If you have not yet installed, reviewing the list before you proceed is recommended.

Condition: The alarm settings do not work correctly after upgrading Windows NT 3.51 to Windows NT 4.0. Most likely, the version of ODBC needs upgrading.

Action: Install ODBC 3.5 from the ServerWORKS CD-ROM by running \ODBC35\dataacc.exe.

Condition: ServerWORKS Manager does not launch. The last exit from ServerWORKS Manager or another component that uses the file PCMGR.MDB may have been abnormal or system shutdown may have been improper (for example, a power outage).

Action: The .MDB database file may need repair. To do this, follow the instructions:

1. Start the ODBC management utility from the Control panel.
2. Click on the user DSN page.
3. Select SWMgrDB.
4. Click on the Configure button.

5. Click on the Repair button.
6. Choose OK to exit.

Reboot and try ServerWORKS Manager again.

Condition: Memory resources are being reduced.

Action: Running ServerWORKS Manager for long periods of time (more than a day) and receiving large numbers of SNMP traps or alarms of any type, progressively consumes memory and eventually can cause the console system to run out of virtual memory. The problem is caused by memory leaks that occur with some versions of ODBC and Jet drivers. If this problem occurs, update the console's ODBC and Jet versions to 3.5. You may also need to tune the system using information from the Microsoft problem report Q154384 (see below).

The Version 3.5 ODBC and Jet drivers are available on the ServerWORKS Manager CD, in the \ODBC35 directory, in a file named dataacc.exe. Simply execute the file. This is an InstallSHIELD application that installs the drivers. There is also a readme.txt file in this directory. Both are Microsoft files that can be found in the April '97 Microsoft Developer Network SDK CD Disk 1.

Another source for the drivers is the Microsoft web page, http://www.microsoft.com/support/products/backoffice/odbc.

Select MS ODBC Drivers 3.5, then ODBC Desktop Database Drivers 3.5. This downloads the file, WX1350.exe, which contains the drivers. In addition to upgrading the ODBC and Jet drivers to Version 3.5, it may be necessary to tune the console to prevent database applications from consuming excessive memory. Microsoft has published two problem reports, Q153797 and Q154384, describing memory leak problems. Report Q154384 provides detail on how to tune a system's ODBC and Jet 3.x drivers for best memory usage and performance. It is recommended that you read these documents.

If ServerWORKS Manager is already installed when you update the ODBC drivers, the next time ServerWORKS Manager is started, it may display the message, "Can't Find Database" (Windows NT V4.0), or "Database Inconsistency Error" (Windows 95). To proceed, click OK to continue. ServerWORKS Manager will start up normally and the message will not reappear.

Condition: The ServerWORKS Manager Event Logger does not record events as expected.

Action: If unacknowledged events fill up the log, the log can terminate prematurely. Increase the buffer file size using the ServerWORKS Manager DB Utility.

If the Event Logger terminates abnormally, new events are not recorded and existing events are not acknowledged. Rebooting your management console may alleviate this.

The Event Logger recognizes community names from SNMP traps of only up to six characters. Longer names are truncated. Review the documentation for your operating system for information on setting community names.

Condition: Alarm events are not appearing on the Windows NT Event Viewer.

Action: You can use NT Event Viewer only on systems running Windows NT. To use the Event Viewer, modify the initialization file (`swmgr.ini`) to enable NT Event Viewer logging. Use the following procedure:

1. From the Start menu, choose Find→Files or Folders.
2. In the Name field, enter

   ```
   swgmr.ini
   ```

   Then click Find.
3. When the search is complete, double-click on the file.
4. Search the file for the parameter section [Setup]
5. Change the following parameter to a value as shown:

   ```
   WriteTrapMsgToNTEventLog=1
   ```
6. Close the swgmr.ini file and restart the ServerWORKS Manager Console.

Condition: The SNMP service does not start from the installation program or from the NET START SNMP command.

Action: First check the Event Viewer and look for either of the following messages:

On NT 3.51: The SNMP Service terminated with server-specific error 1.

On NT 4.0: The SNMP Service is ignoring trap destination <node name> because it is invalid.

If you see these messages, use the following procedure:

1. Remove the offending node from the trap destination list in the SNMP Service Configuration dialog.
2. Start SNMP from the DOS prompt using the NET START SNMP command. Repeat this procedure for every failing node in the list.

If there are many Trap Destinations listed, do the following:

1. From a DOS Prompt, type NET STOP SNMP to insure that SNMP service is stopped.
2. Start the service using SNMP command.
3. Check the Event Log for errors and remove from the trap destination list any nodes that timed out.

There are other SNMP errors that cause the service-specific error 1 to be posted to the event log. If the previous procedure does not change the condition, consider the following alternatives:

- Check your DNS and WINS settings. Make sure that LMHOSTS lookup is enabled if you intend to resolve the problem using LMHOSTS.
- A single invalid destination can cause a time-out if the network is running slowly. Waiting for multiple time-outs will cause this problem on a healthy network.

Condition: An NT Local group member does not have rights on the machine on which the group was created, for example, the right to log on locally.

Action: In NT administration, the administrator must explicitly assign rights. The administrator can do this in NT Management or through ServerWORKS Manager NT Server Management. In NT administration, this is accomplished in the User Manager→Policies→User Rights→Log on Locally. In ServerWORKS Manager NT Server Management, this is accomplished from the User Rights tab. Refer to the section "Using NT Server Management for NT Domains" in Chapter 5 for a sample NT Server Management procedure.

Condition: The installation continues to fail despite attempts to remove all ServerWORKS, ManageWORKS, and ClientWORKS from the system.

Action: There are numerous keys in the Registry relating to the applications. You should first remove the software using the Control Panel→Add/Remove Programs applet. Some earlier versions of these products cannot be completely removed without intervention in the Registry. You can find the Registry in the following locations.

Table 2-7 Location of the Windows Registry

Operating System	**Registry Editor**
Windows NT	\Windows\Regedt32.exe
Windows 95	\Windows\Regedit.exe

Refer to Appendix A for a list of Registry keys.

ServerWORKS Manager Console 3

Introduction

ServerWORKS Manager Console is designed to manage DIGITAL servers, desktop PCs, and mobile devices. It may also be used as an interface for administrative tasks for Microsoft NT or Novell NetWare[1] servers.

The contents of this section are as follows:

- ***Discovery***—collect information about the objects on the network
- ***Viewers***—display the objects that can be managed
- ***Browsers***—set or display specific parameters on objects
- ***Alarming and Actions***—set alarms for user-defined events and start appropriate actions
- ***Monitoring and Status***—display color-coded information on the objects
- ***Reports***—generate specific information

Each of these is briefly discussed in the following sections. For more information on any particular topic, refer to the Windows-based online help integrated into ServerWORKS Manager Console.

[1] Novell NetWare is also known as IntraNetWare.

Discovery

Discovery is the process used to discover objects on the network. There are three methods used to discover objects on the network:

- NT Server Management Discovery
- Novell NetWare Discovery
- IP Discovery

The first two processes are done dynamically every time an object is expanded from ServerWORKS Explorer. For example, each time the NT Server Management (Microsoft Networks) object is expanded, a discovery is done.

The third method is IP Discovery. This is done in a separate process using the IP Discovery tool and is initiated by the user in order to minimize the amount of IP network traffic.

NT Server Management Discovery

NT Server Management Discovery lists the Microsoft Network objects (those running LAN Manager V3.0 Protocol). ServerWORKS Explorer displays the root object, which may be expanded to show the entire Microsoft Network. Objects found may include more objects than just NT servers (such as OS/2 or Windows 95). The systems that respond may not have the full functionality of Windows NT, and as a result may not have all its capabilities. In addition, you need the DIGITAL agent installed on an NT machine you are monitoring to get complete information on the NT machine. Therefore, NT Server Management tools may be used to administer some tasks on those systems, but not necessarily all.

NT Server Management Discovery information is not stored in the database, but is obtained each time that the NT Server Management object is expanded.

Novell NetWare Discovery

Novell NetWare discovery is similar to the NT Server Management discovery in that it is started by expanding the root NetWare object in the ServerWORKS Explorer. This results in dynamically finding the NetWare objects on the LAN. Note that NetWare V3.x and V4.x systems have different capabilities.

NetWare Discovery information is not stored in the database, but is obtained each time that the Novell NetWare object is expanded.

IP Discovery

The IP Discovery wizard finds TCP/IP and SNMP objects on the network and places information about these devices in the database. After discovery is complete, the IP Discovery tool uses the information in the database to create a default network map (IP Discovery Viewer).

ServerWORKS Manager offers two methods of discovery. If you know your network, you can use the Start Host method, which begins a fast discovery of the network segment from a logical starting point like a router or name server. If you choose this method, you must name the starting point. (You may experience unpredictable behavior if you do not name the Start Host). You can achieve more thorough discovery through Ping Spray. You can also use the methods simultaneously.

In addition to finding devices on the network, discovery also assigns an **object type** to each device. A device is defined according to information that the discovery tool receives when it “discovers” the device. The object type defines what the device is, for example: a router, server, bridge, or hub.

The IP Discovery wizard also finds object types that you define, such as non-DIGITAL servers. For example, if your network contains a Compaq server, you can define a type called Server.Compaq, assign Compaq MIBs to the object type, and provide icons to use in the hierarchical and map views. Refer to the section "Creating Custom Object Types and Profiles" in Chapter 5 for more information.

Subsequent Discoveries

The Discovery process may be incremental—it may be run repeatedly on a viewer to update the information in the database and subsequently, in the map. If more than one map exists, a specific map may be selected to be updated with the discovery results.

When an incremental discovery is done, the following occurs:

- New connections and nodes are added to the specified map(s).
- Configuration information for previously existing nodes is updated only if there is a change.
- Customized maps are preserved.

Adding Devices Manually

The IP Discovery wizard does not have to be used to populate a viewer. IP devices may be manually added to the database and to the map and hierarchical viewers.

Viewers

Viewers are used to display objects and may also illustrate the relationship between these objects. ServerWORKS Manager Console provides two types of viewers:

- ***Hierarchical***—listing of the objects under the applicable root object
- ***Map***—topological representation of objects and the connections between objects

Map Viewers

Map viewers are graphical displays of the network topology at various levels. If the map is at its highest level, clicking on an object results in that object opening up and displaying the next level of detail. Once at the lowest level, an object such as a DIGITAL server or a router can be selected and then monitored either by using the pull-down menus or by double-clicking on the object to bring up its default browser.

Hierarchical Viewers

Hierarchical viewers display all local and network resources by using a tree structure. Different levels of the tree can be expanded or collapsed using the “+” and “-” tree controls. One hierarchical viewer is the ServerWORKS Explorer. This viewer is displayed when you choose File→Open Viewer→Explorer after ServerWORKS Manager Console is initially started.

ServerWORKS Explorer

ServerWORKS Manager Console comes with a default hierarchical viewer known as the ServerWORKS Explorer. ServerWORKS Explorer is a viewer that displays all network resources and management tools.

ServerWORKS Explorer is read-only—it cannot be deleted or renamed. In addition, the order of its contents and the way in which the objects are organized cannot be changed.

By default, there may be up to four root objects listed under the ServerWORKS Explorer. These are:

- Server Objects
- SNMP Objects
- NT Server Management—listed only if the management console is running Microsoft NT for Servers
- NetWare File Servers—listed only if the management console is running Novell NetWare

Objects may be listed under one or more root objects. For example, a DIGITAL server running Microsoft Windows NT would be an object in the tree structure under Server Objects, SNMP Objects, and NT Server Management. It is listed under all three categories because it fulfills the requirements of each of these categories. The specifications for the categories are described in the following sections.

Server Objects

The Server Objects category includes DIGITAL servers with the following characteristics.

- X86 processor-based DIGITAL server running NT (with DIGITAL SNMP Extension Agents)
- X86 processor-based DIGITAL server running Novell (with DIGITAL SNMP Extension Agents)
- X86 processor-based DIGITAL server running SCO UNIX (with DIGITAL SNMP Extension Agents)
- X86 processor-based DIGITAL server running OS/2[2] (with OS/2 SNMP agents installed; at a minimum, Host Resources Agent must be installed)
- Alpha-based system running NT (with DIGITAL Agents)
- Alpha-based system running DIGITAL UNIX
- Alpha-based system running OpenVMS

You can find similar information about non-DIGITAL servers running NT and the DIGITAL NT agent, whose sets of MIB II variables are enrolled in the ServerWORKS Manager database. Refer to the section "Creating Custom Object Types and Profiles" in Chapter 5.

SNMP Objects

This category includes all devices running the SNMP protocol, such as:

- Bridges
- Routers
- Hubs
- Servers
- Desktop systems
- Printers
- Token Ring networks

[2] DIGITAL servers with OS/2 are manually discovered.

- Ethernet networks
- FDDI rings

Microsoft Windows NT Server Manager

This category includes all DIGITAL servers on a LAN running the Windows NT operating system. This category can also include non-DIGITAL servers whose MIB II variables are enrolled in the ServerWORKS database. Most NT Server administration tasks may be performed for systems in this category. The integration is such that ServerWORKS Manager Console menus and dialog boxes may be used to perform Microsoft NT Server Management tasks.

Note: *The NT Server Management tools are available only if the management console has Windows NT Workstation or Microsoft NT Server installed. If neither is installed, the NT Server management object is not included in the ServerWORKS Explorer tree structure.*

Novell NetWare Server Manager

This category includes all DIGITAL servers that are on a LAN running the Novell NetWare operating system and that can be managed using the NetWare Management tools.

Note: *The NetWare Server Management tools are available only if the management console is running Windows NetWare Client from Novell. If Windows NetWare Client is not running, the NetWare Server management object is not included in the ServerWORKS Explorer tree structure.*

Customizing Viewers

ServerWORKS Explorer is the starting point for customizing viewers by serving as a source of objects to copy into other views.

Both hierarchical and map viewers may be customized to meet specific requirements. A customized view may be updated by running a discovery and selecting that view to be updated.

Several different viewers may be created to serve different purposes. For example, one view may contain all of the servers in the organization, while another may display files and applications on multiple servers, while a third may display the TCP/IP topology. Any type of information may be grouped in a view, regardless of its source or content.

Manually Placing Objects into Views

There are four ways to manually add objects into viewers:

- Using Insert from the Edit menu
- Using the map palette to insert objects into the map viewers
- Using the mouse to drag and drop objects from one viewer to another viewer
- Cutting, copying, and pasting objects between views or within a view

In addition to putting objects into a view, viewers may also be customized by changing the format, layout, and colors assigned to certain objects. A background may also be specified for a topological map view.

For more information on viewers and how to customize them, refer to the ServerWORKS Manager Console online help.

Browsers

ServerWORKS Manager Console provides three different browsers that may be used to query and set parameters on objects. These browsers are:

- System Browser
- MIB Browser
- MIF Browser

System Browser

The System Browser provides information on both static and dynamic parameters found in DIGITAL objects such as servers, desktop systems, and mobile devices. The System Browser uses information provided by DIGITAL SNMP agents loaded on the server, desktop, or mobile system. The information supplied may be:

- Static information—details the system's configuration
  - System firmware descriptions and revision levels
  - CPU and memory expansion board configurations
  - Power supply and fan configurations
  - Disks
  - Network Interface Cards (NICs)
  - Asset management information for Field Replaceable Units (FRUs)
- Dynamic information—details the current state of an object located on a server
  - CPU utilization
  - Disk utilization
  - Network statistics
  - Thermal and voltage readings and/or states
  - Fan and power supply states
  - Error status for the Error Correction Code (ECC) on the SIMMs/DIMMs
  - Reads and writes of the Operator Control Panel (OCP)

The System Browser also provides detailed reports and the ability to graph certain parameters such as CPU utilization, network statistics, and thermal and voltage readings. These graphs may be useful for fault management and performance management.

MIB Browser

The Management Information Base (MIB) Browser is used to query (**get**) and modify (**set**) MIB parameters on SNMP compliant objects on the network.   After an SNMP object is specified, the MIB Browser lists all of the applicable MIB groups for that object type, as well as the MIB variables in each group. For example, suppose the object parvin.ako.dec.com is selected. The MIB Browser would then list all of the applicable MIB groups for that object type, as well as the MIB variables in each group

The MIB Browser provides the following capabilities:

- Perform SNMP **set** operations against one or more SNMP agents
- View the properties of any MIB variable (for example, the variable's data type or object identifier, access status, and description)
- Access the MIB Profiler to modify or create MIB profiles (see "Additional Tools" in this chapter)
- Access the MIB Enroller to enroll new MIB groups into the ServerWORKS database or modify existing groups (see "Additional Tools" in this chapter)

For SNMP objects other than DIGITAL servers, the MIB Browser is the default management action. It is started from the Map Viewer, the toolbar, or the Tools Menu.

Some of the MIB variables are Read/Write, thereby allowing the variable to be “set” as well as read. For example, sysLocation is a Read/Write variable, which means that a new location can be entered for the system whenever the system is moved. The change is actually made in the MIB itself. A Read/Write variable may also be changed by other individuals using another network management system.

Note: ***Set*** *operations change the value of the parameter in the device and are usually only allowed for non-critical parameters. This is because SNMP Version 1.0 provides limited security capabilities and is unable to determine whether a set request is coming from an authorized user or system.*

MIF Browser

The Management Information Format (MIF) Browser is used in a similar fashion to the MIB Browser. It is used on desktop and mobile systems and may also be used on systems running Windows NT or Windows 95. With the DMI service layer running on the system to be browsed, you can see an inventory of various system software, hardware, settings, and configurations. This information can be passed on to Microsoft System Management Server (SMS) through the MIF Maker program.

The MIF browser is available through an icon on the tool bar.

Alarming and Actions

This section covers the following alarm topics:

- Creating Actions
- Configuring alarms
- Viewing alarms
- Actions to take when an alarm occurs

Creating Actions

Actions are similar to scripts that define what is to be done when an alarm or event occurs. The actions are stored independently of the alarm settings and may be reused for different types of objects (such as servers or hubs) as well as for different types of alarms. Actions can be created before the alarms that may use them. This is done through the “Actions Directory Setup” component of the Alarm Configuration Tool.

Actions may take three forms:

- Dial a paging device and supply a numeric message
- Send an email message
- Start an application

Examples of applications are:

- Running a .wav file to notify individuals who are in the vicinity of the console that a problem exists
- Opening a troubleshooting window to guide an administrator through an unfamiliar procedure
- Proactively fixing the problem without operator intervention (for example, if the system fills up with temporary files, the application can delete files in a temporary directory)

Configuring Alarms

The Alarm Configuration Tool is used to set alarms on network objects, including DIGITAL or other servers, desktop computers, and mobile systems. The same alarm can be configured simultaneously for more than one object as long as the system parameter on which the alarm is set is also present on the hosts that were selected for alarm configuration.

Traps and alarms are received on destination management consoles. You must configure SNMP, naming at least one destination on each device where a ServerWORKS agent is installed, and you must have SNMP configured on the management console for the traps to be received. From the management console, you can also forward traps to other management consoles using the Trap Forwarding utility.

Alarms that are not standard SNMP traps can be converted to trap format and forwarded as traps to the management console to reduce the amount of network traffic.

Alarms can be set for status or threshold events.

- **Threshold alarms** are triggered when a preset value is reached. For example, an alarm may be set for File Utilization with the threshold set for 85%. Threshold alarms may be set for the following:
  - CPU Utilization
  - File System Utilization
  - Disk storage used
  - Voltage
  - Temperature
  - Cooling, fans

  - Memory SIMM/DIMM ECC status
  - Total Packets
  - Inbound Errors (errors while receiving data)
  - Outbound Errors (errors occurring when transmitting data)
  - Inbound Packets (number of packets received)
  - Inbound Packet Discards (number of received packets that are discarded)
  - Unknown Protocol Errors (packets received with unknown protocols)

- **Status alarms** are set when a device fails, issues a warning, or comes back online. For example, fan sensors failing may result in a status alarm. The following are the categories for which status alarms can be set:
  - Processors
  - Disks
  - Fans Sensors
  - Voltage Sensors
  - Power Supply Sensors
  - Temperature Sensors
  - Memory Status
  - Cluster Group Status
- System status alarms to show whether a system is up, down, or not responding.
- SNMP Trap alarms for any SNMP device on the network. The alarms are set on traps occurring as the result of status changes.

Viewing Alarms

The Alarm Viewer is used to display the alarms that have occurred on objects. It allows:

- Viewing of unacknowledged alarms
- Acknowledging of alarms
- Searching for alarms based on specified criteria (filters)
- Displaying alarm criteria on alarms that have been set

Checking Unacknowledged Alarm Status and Count

The alarm counter buttons located on the status bar at the bottom of the ServerWORKS window display the number of unacknowledged alarms of high, medium, low, or informational severity.

To list all unacknowledged alarms of a particular severity, click the alarm counter button of the desired severity (High, Med, Low, or Info). The Alarm Viewer window appears, listing all unacknowledged alarms of that severity.

Additional SNMP Tools

There are additional SNMP tools that you can use. These are:

- ***Properties***—provides information about objects
- ***MIB Compiler***—adds new MIBs to ServerWORKS Manager Console
- ***MIB Profiler***—associates MIBs with an object type

Properties

ServerWORKS Manager Console's SNMP device tool provides the ability to view properties for any SNMP device. The tool is available from the Actions menu. It is also available when performing any of the other types of management functions such as NT Server or NetWare Server Management.

MIB Compiler

The MIB Compiler is used to load new MIB group and MIB variable definitions into the database.

The MIB compiler takes a MIB definition file in standard ASN.1 format (to describe the information exchanged in a format independent of the communicating systems), compiles the file, and links the resulting MIB information into the database.

MIB Profiler

The MIB Profiler is used to associate MIBs with an object type. For example, a DIGITAL server object type has certain MIBs that have been defined to be associated with that object type.

If the MIBs associated with an object need to be modified, this is done using the MIB Profiler. The MIB profiler:

- Assigns MIB groups to an object type.
- Deletes (de-assigns) MIB groups from an object type.

The MIB Profiler saves the MIB group assignments in the database so they can be referenced by the MIB Browser. For example, after a particular SNMP object is selected, the MIB Browser obtains the object type and uses this information to display all the associated MIB groups from the database. Only the applicable MIB groups are listed in the MIB Groups field of the MIB Browser window. Then either a group or one or more variables from that group may be chosen to perform get and set operations against the specified object.

Monitoring and Status

A primary indication of a problem with an object is indicated by one of the following:

- A color change to its circle icon
- A color change to the map icon background
- A bell appearing next to the object

The circle and icon background color are indications of the ICMP (Internet Control Message Protocol) status or SNMP polling, and the bell indicates alarms and traps.

Status Changes

Status changes in objects are indicated by color changes on the viewers. On a hierarchical viewer, the status is indicated by a circle to the left of the object. On a map viewer, status is indicated by the background color of the object icon. The meanings of the colors are as follows (note that these are the default colors):

- Green—is the result of either an ICMP or SNMP poll and indicates that the device is up
- Yellow—is the result of an SNMP poll and indicates that the device may be partially up or that one interface may be down
- Red—is the result of an SNMP poll and indicates that the device may be in the process of going down (may be intentional)
- Magenta—is the result of either an ICMP or SNMP poll and indicates that the device is not responding

Status is detected by either polling or “pinging” an object. If the poll or the ping is successful, the status color is green. Otherwise, the status color of the object is magenta. The colors yellow and red are seen only in limited circumstances.

Alarms

The alarm bell is used to indicate alarms occurring on objects. On a hierarchical viewer, the bell is on the left side of the object, while on a map viewer, the bell is in the upper right corner of the object icon.

The conditions that cause the bell to appear are the triggering of a trap or an alarm. The conditions for alarms are determined by what has been previously set using the Alarm Configuration Tool.

Reports

There are two types of reports available. These are:

- Discovery Report—generated by IP Discovery and contains information about the objects discovered
- IP Address Report—generated by the IP Address Report Utility and provides information on Media Access Control (MAC) addresses

Discovery Report

When a Discovery operation completes, a Discovery report is created that lists any newly discovered IP hosts, configuration changes, duplicate IP addresses, and misconfigured devices. All past reports are saved in the directory:

```
<installation Directory>\database\IPREPORT
```

The file name format is:

```
<month><date><hour><minutes>.txt
```

For example:

```
04071917.txt        =           (April 7th at 5:17pm)
```

IP Address Report Utility

The IP address report is created from the database after a discovery is completed. The information contained in the report is address, name, and MAC address of each discovered object. This report is generally used to find conflicting IP addresses associated with their unique MAC addresses.

The IP Address Report Utility is located on the Tools pull-down menu.

Background Tasks

The background tasks associated with ServerWORKS Manager Console are:

- Poller—Sends messages out at timed intervals to all objects with the intent of initiating a response from the object
- Data Collector, Event Logger, and Event Dispatcher—Background processes that are associated with the ability to receive alarms and to perform further actions
- Ping Server—Performs user-initiated “polls” of one object

Poller

The Poller periodically requests status information (up, down, or no response) from specified network objects and their interfaces. The objects that may be polled are all interfaces belonging to network objects that have an SNMP agent or that have IP support (for example, routers and end nodes).

By default, the Poller is automatically started after IP discovery is done. Using the default settings, all objects that are listed in the database are polled at the same interval.

Polling may also be done on a user-defined group. A group may consist of a collection of objects that would be polled at the same intervals.

Status Changes

When the Poller detects a status change, it forwards the information to the management console.

When a hierarchical or map viewer receives the Poller status change information, it updates the status color in the viewers (icon background in the map viewer and the circle next to object in the hierarchical viewer). The meanings (default) of the colors are:

- Green—up
- Red—down
- Magenta—no response

The colors may be customized.

The Poller may also be configured to send SNMP trap information to an enterprise-level network management system. Refer to Chapter 4 for more information.

Data Collector, Event Logger, and Event Dispatcher

Both the Event Dispatcher and Event Logger must be running to receive alarms, notification of alarms, or to automatically run a script when an alarm threshold is reached. In addition, the ServerWORKS Manager Console Data Collector must also be running to receive alarms.

If these three utilities are not placed in the Windows NT or Windows 95 Startup Group, the Event Dispatcher and Event Logger are automatically initiated when ServerWORKS Manager Console is started.

Ping Server

ServerWORKS Manager Console has the capability to "ping" devices on the network.

Database and Associated files

ServerWORKS Manager Console Database

The database is composed of a set of files that are stored on the management console. Information gathered from IP Discovery, Polling, Alarm Configuration, Alarm Viewer, and other utilities are written to the database. If an alarm is added on a server or the MIB Enroller is used to add a MIB, these additions are reflected only in the database on the management console. They do not alter any of the information on the device.

Some changes are not written to the database but may affect systems on the network. For example, if NetWare Server Management or NT Server Management tools are being used, the information is not written to the database but directly affects the servers being managed.

ServerWORKS Database Files

The ServerWORKS database consists of the following files located in the \database directory:

- pcmgr.mdb file—contains SNMP information about the devices on your network
- snmpomm.ini, .dat—contains the configuration of SNMP components and database validation entries
- swmgr.ini—contains the configuration settings for the ServerWORKS Manager applications
- class.pod, .idx—contains display information about viewers and objects
- contain.pod, .idx—contains display information about viewers and objects
- object.pod, .id**x**—contains display information about viewers and objects

In addition, the directories under <ServerWORKS-Installation-Directory>\database have the following purpose:

- Backgrnd—contains “.bmp” files for map viewer backgrounds
- Bitmaps—contains the bitmaps
- Empty—files that represent the initial state of the ServerWORKS database
- Ipreport—contains the IP discovery reports
- Mail—temporary storage for actions that use mail
- Pager—temporary storage for actions that use paging

Managing Servers Using SNMP-Based Enterprise Management Systems 4

This chapter explains how to use SNMP V1.0 (Simple Network Management Protocol) and SNMP management tools with ServerWORKS Manager.

About SNMP

ServerWORKS Manager uses the SNMP V1.0 protocol for its primary communication with servers running a variety of operating systems. ServerWORKS Manager implements SNMP-based MIBs and an SNMP agent extension component that allows:

- Remote control of systems through SNMP Set and Get operations
- Setting of SNMP agent traps and alarms for the objects being managed using ServerWORKS agents
- Polling of SNMP variables to create console-based threshold alarms

SNMP System Components

SNMP retrieves data through one or many *Management Information Bases* (MIBs) that describe the manageable objects on that host. In addition to system-supplied MIBs, vendors can define additional MIBs that allow vendor-developed devices to be monitored and managed by SNMP management consoles.

A MIB includes the following information about every object it describes:

- An object identifier that uniquely identifies the managed object on the network
- A definition of the data type used to define the object

- A textual description of the object
- An index method used for objects that are of a complex data type
- The read or write access that is allowed on the object

A *manager* is a program that requests data from other computers on the network. An *SNMP management console* is any computer running SNMP management software. When an administrator at the management console requests information about a managed object, the SNMP management program requests information about the object using its object identifier.

The *agent* is the program that receives management requests and then sends the requested information back to the SNMP management program that initiated the request.

The agent performs four operations:

- **Get** and **Get Next** retrieve information about the managed object and return it to the management console.
- **Set** changes the value of a managed object variable. Only variables whose object definitions allow read/write access can be set.
- **Trap** sends messages to the SNMP management console when a change or error occurs in a managed object. The trap is the only operation initiated by the agent without a specific request from a management program.

An *extension agent* is software that extends the functionality of the system agent. When the agent receives a request for information about one of the objects handled by an extension agent, it passes the request to the extension agent for processing. The extension agent returns the information to the SNMP agent, which returns it to the management console that requested the information, as shown in Figure 4-1.

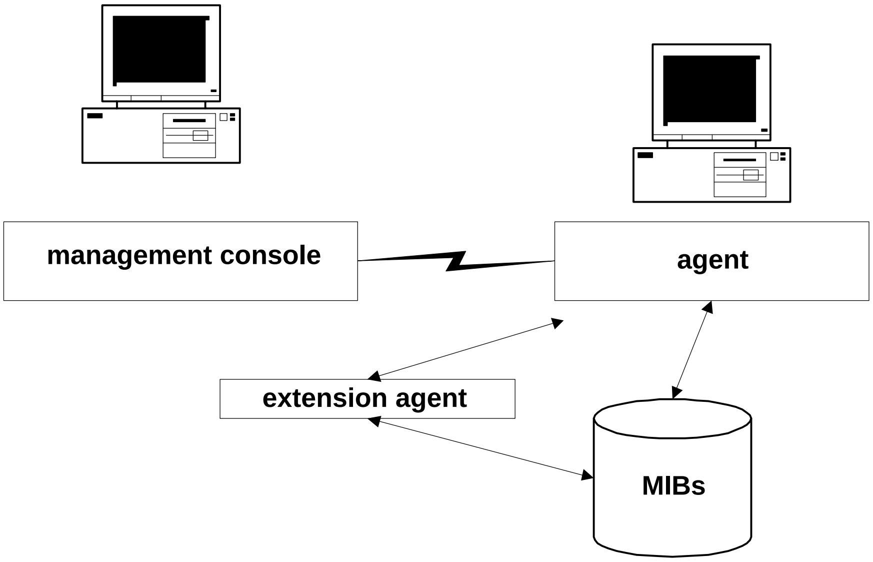


Figure 4-1 Extension Agents in SNMP

The DIGITAL SNMP Extension Agent

Most operating systems provide SNMP agent subsystems that allow you to construct extension modules for specific hardware and software. The DIGITAL server agent uses the operating system's native SNMP protocol stack and distribution mechanisms to return information about DIGITAL hardware and software and to export traps to other systems.

An SNMP agent must be configured to send its traps directly to any SNMP management console, including ServerWORKS Manager Console, or to enterprise management systems, such as HP OpenView or Tivoli TME 10, that use SNMP as their trap and alarming mechanism.

How ServerWORKS Manager Console Uses SNMP

ServerWORKS Manager Console functions as a management console without the SNMP trap service. Because it uses its own SNMP stack for decoding SNMP traps, it does not require that SNMP be installed on the console machine. However, systems that are to be viewed by the management console *must* have SNMP agents installed and configured. If the management console will be used to view the system on which it is installed, then SNMP must be installed and configured on the management console as well.

ServerWORKS Manager Console relies on the operating system SNMP components to provide the IP port number of the SNMP trap (usually 162). This entry can be found in the services file. On a Windows NT system, this file is usually at c:\winnt\system32\drivers\etc\services. On a UNIX system, this file is at /etc/services.

ServerWORKS Manager attempts to use the trap port if it is not already in use. The ServerWORKS Manager Event Dispatcher receives traps from the SNMP trap port, so in order to run an enterprise manager on the same system as ServerWORKS Manager, you must close the Event Dispatcher process.

Note: *Some Windows 95 and Windows NT systems may have the snmp-trap entry removed. Make sure the following line is in the services file:*

```
snmp-trap  162/udp     snmp
```

Configuring SNMP for Trap Forwarding

SNMP is a connectionless protocol. If the agent system and the management console system do not agree on the trap port number and other details about the exchange, no messages will pass between the two systems. No error will be detected and no exception message will be generated.

A system running Windows operating systems does not have the SNMP service installed by default. You must add the SNMP service explicitly from the Control Panel and then configure the SNMP agent with the correct security and access. You need to do this for both the management console and the system that will be generating the traps. You will not receive traps at the destination console if you do not configure the SNMP services correctly.

You find the SNMP setup in the Control Panel, under the Network icon. You need to configure the SNMP service and specify a trap destination on the server (the managed system). Refer to the section "Configuring the SNMP Agents" in Chapter 2 for instructions for Windows NT and Windows 95.

The screens differ in the two versions, but both require the same information:

- The community name or names you will be using
- The network name or the IP address of each SNMP management console that will be the destination for trap messages generated within a specific community

The following sections explain these items in more detail.

Configuring SNMP Security

The SNMP security service uses *community names* to authenticate messages. All SNMP messages must contain a community name. The SNMP agent that receives the message checks the community name against the list of names with which the SNMP service is configured. If the message contains a known community name, the message is processed. If no known community name matches the one in the message, the message is rejected. The "Send Authentication Trap" check box in the setup window determines whether the SNMP service sends a trap message to the requesting server when such an authentication failure occurs.

The default community name when the SNMP service is installed on a Windows NT-based computer is "public." You can add or remove community names as necessary. Note that if you remove all community names, including the default name, the SNMP service on that computer will authenticate and process SNMP messages containing any community name.

There is no relation between community names and domain or workgroup names. Community names function as a shared password for groups of hosts and you should select and change them as you would any other password.

Only agents and managers that are configured with the same community name can communicate with each other. If the agent does not recognize the community name contained in the SNMP messages from the management console, it will not accept any messages from the management console.

Configuring SNMP Traps

The SNMP agent generates trap messages, which are sent to an SNMP management console called the *trap destination.* If you want a system to forward SNMP traps to a management console, you must make sure both systems are properly configured:

- The community name on the management console must be the same community name set on the agent system.
- The agent system must specify the management console system as a trap destination.

If you set up an alarm without having configured the SNMP services, you are prompted to configure SNMP and an SNMP trap destination on the managed system before proceeding. Refer to the section "Configuring the SNMP Agents" for details.

When an agent trap condition occurs on the sending system, the agent sends the appropriate SNMP trap message to the management console system. If you do not configure both systems properly, no traps are passed.

Traps typically notify the management console about events such as a service starting or stopping, the existence of a serious error condition, or other event that is important to the agent. The SNMP agent or extension agent and its associated MIB defines what conditions cause a trap message to be generated, but the user controls where the message is sent.

The trap destination must be a host that is running an SNMP manager program, such as ServerWORKS Manager or an enterprise manager. Although you can identify the trap destination by its unique name, the numeric IP address is most efficient. DHCP is not recommended due to the uncertainty of DHCP address translation. Do not use a subnet address.

Getting the Data You Want 5

An installation and IP Discovery with ServerWORKS Manager presents volumes of information on all the network objects. The advantage of using ServerWORKS Manager is that you can adjust and filter this information in ways that help you interpret or present data based on your information requirements. This chapter explains several procedures that allow you to take advantage of the versatility of ServerWORKS Manager.

Discovering Your Network

IP Discovery finds TCP/IP and SNMP objects on the network and places the information in the ServerWORKS Manager database. The database information is used to create the maps and views that illustrate the network. Before you search for network objects on a large network, it is helpful to know the subnet and subnet mask.

How Discovery Finds Objects

Discovery identifies objects using a specific sequence. First, Discovery queries for the SNMP MIB II System Descriptor (the sysDescr). Discovery also checks to see whether a DIGITAL agent is running on the object. If the agent is running, Discovery looks for the DIGITAL base agent system descriptor string (svrSystemDescr). On finding this string, Discovery identifies the object as a Server.Digital.

Discovery continues to query the object and determines the following:

- If the object is a server, Discovery determines whether the object is a cluster server.
- If the object is a cluster server, Discovery determines whether the object is a DIGITAL or DIGITAL NT cluster.
- If Discovery does not find any of the preceding information, the object is identified as a Node.Generic. (Most objects appear as generic nodes because SNMP is not running.)
- If an object has multiple adapters, and is not running the DIGITAL agent, the object is identified as a Router.

To discover a network:

1. From ServerWORKS Manager, choose Actions→Discover IP Objects.
2. On the Networks to discover dialog, your subnet is the default network address to discover. You can specify other subnets and find objects in any or all of them.
3. Select any Network Address you want to discover. To add to the list:
   - In the Network field, enter a subnet IP address or unique IP address (to discover a known object and place it in a view)
   - In the Netmask field, enter the subnet mask range of addresses to scan. Click Add to place the new network or machine on the list. Then click on the subnet you added to select it. To select multiple subnets, hold down CTRL and click on each subnet you want to discover.
4. Click Next.
5. On the Types to discover dialog box, do one of the following:
   - Click on Next to discover All Types of objects on the selected network(s).
   - Select the specific types of objects you want to discover; for example, you can specify Server.Digital or SERVER.MSNTCluster. Then click Next.
6. On the Discovery options dialog box, choose the discovery method. Unless you are familiar with your subnet and can specify a Start Host for beginning the discovery, choose Ping Spray. If you have created hierarchical views or maps, select one for the results of the discovery from the list in the "Select a map viewer for discovery results:" list.
7. Click Finish. When the discovery is done, you can read the discovery report and add new objects to the current view. You can also choose to view the IP Discovery Report.

Customizable Options for a View or Map

Once you have a map or view, you can modify it. Because a network can include many different object types, you may want to view data differently or act on the objects differently.

To get basic information quickly

You can launch an application such as the System Browser or the ClientWORKS MIF Browser. ServerWORKS Manager has already associated servers and cluster objects with these applications. Double-click on a network object to display the associated browser. The System Browser gives you a snapshot of object vital statistics, such as the IP address and name, the cluster name for cluster servers, a hardware description, and storage capability.

To create a logical network map

You may want to manage particular network objects on a map as a group because they have similar usage or for organizational purposes. You can isolate them easily. Simply drag the network objects from map to map.

To view vital statistics on a map

You can add a label to a network object to display specific information on the map. For example, you may want to see the IP address and name and netmask of an object.

1. From the Tools menu, choose Options→Object Display.
2. From the Hidden list, select the information you want to display in a label.
3. Click Show. If you want to put the labels in a specific order, select each label and choose Before or After until the labels are positioned.
4. Click Close.

To modify the menus for the work you do

You can edit the Tools menu to add or delete programs. For example, you can create a menu command that runs a batch file. To customize the Tools menu:

1. From the Tools menu, choose Options→Tools.
2. Do one of the following:
   - Click Add to add another application to the Tools list. Enter the tool name (for example, Notepad) and the Path (for example, c:\windows\notepad.exe) and click OK.
   - Select an application and click Remove to delete the application.
   - Select an application and click Change to modify the display name or path of the tool.
3. Click Close.

To manage network objects as a group

You can select a logical group of network objects and apply the same alarms and options to them.

First, create the group:

1. From a map view, select the object(s) by doing one of the following:
   - Hold down the CTRL key and click on each object you want to add to the group.
   - Click and drag across the map to draw a selection rectangle around the objects you want to add to the group.
2. From the Tools menu, choose Group Management.

3. Do one of the following:
   - Click Add Group to create a new group containing the selected objects. Enter a group name, polling properties and the community name for SNMP Get and Set operations in the Group Properties group.
   - Select one of the existing groups. Copy its polling properties and community name into the new group and modify them as needed.
4. Select from Objects not in group and click Add to place them on the Objects in group list. To remove objects from the group, select them and click Remove.
5. Click OK.

Working with the ServerWORKS Manager Database

The ServerWORKS Manager database is PCMGR.mdb. It is a Microsoft Access database that you can view in Access. The database is installed in the subdirectory named `database` of the ServerWORKS Manager Console kit. If you chose the default directory at installation the location is:

```
/Program Files/DIGITAL/SWMgr/database/PCMGR.mdb
```

The database contains all the information about objects discovered on your network, alarm and alarm configuration information, and event data.

If you are familiar with Access and database structure, you can modify records in the database to create query reports, use scripts, or perform specialized SNMP operations. Information in the tables may be easier to view in the database table records than in the actual MIB files.

Note: Use Access 95 Version 7.0. Do not use Access 97 Version x.

The following list describes the most commonly accessed databases tables:

This Table	Contains records about
APPL_GR	All integrated third-party applications. A record exists for each integrated application.
EVT_LOG	The alarm log table. All alarms and events, object IDs, and messages associated with each event are stored here.
MIB_CLAS	MIB class name and the group the MIB belongs to, for all MIBs compiled in the database.
MIB_DESC	A description of each MIB variable.
MIB_NAME	Names of the MIB groups.
MIB_PROF	Object type and subtype profile for each MIB.
MIB_TABL	The internal MIB variable ID for all MIB groups that are compiled in ServerWORKS. The ID is useful for joining this table with other tables.
OBJ_DEF	Actual name and the polling interval of each machine.
OBJ_IP	Global name information (including the IP address, alternate address or subnet, and netmask) of each machine.
OBJ_SNMP	SNMP community names.
TRAP_ENT	Trap definitions and enterprise OID for all MIBs compiled in the database.

The following table lists the prefixes used to name the database tables.

Prefix	Table Information
ALM	Alarm configuration
APPL	Third-party application integration
AUTO	Auto-discovery information
COL	Data Collector information
DB	ServerWORKS database information
EVT	Event log data
GR	Group information
LOG	Event log data
LTBL	Reserved for future use
MIB	MIB II variable information
NMDB	Maximum counters for database fields
NOTF	Notification information
OBJ	Object type information that ServerWORKS uses
POD	Reserved for future use
SUBT	Object subtype information
SYS	Mapping of SYSOID and subtype information for MIB II variables
TRAP	Trap information
TYPE	Object type information
USR	User information
VIEW	Map and hierarchical view information
VWER	Internal viewer information

Using the DB Utility

The DB Utility accomplishes several database maintenance tasks. You use the DB Utility in the following situations:

- If you suspect the database or some portion (table) is corrupted.
- If you want to erase a table and start over. For example, you do not like the thresholds you set for alarms and you want to change the levels on all of them. (The cleanup erases everything in the selected table, so be certain you want to recreate the information in ServerWORKS Manager).
- If you want to modify the alarm log table. For example, you set a "false" alarm that sent numerous messages for a non-alarm condition and you want to clear the log of excess entries. You can also change the size of the log table (the number of lines).

Shut down ServerWORKS Manager Console, including the background tasks, before you start the DB Utility.

To open the DB Utility

1. From the Start menu, choose Programs→ServerWORKS Manager Console→ServerWORKS DB Utility.
2. Do one of the following:
   – In the Database Table to Clean Up group, select one table and click Initialize.
   – In the Alarm Log Table, enter the maximum lines you want in the table (up to 10,000, but note that 10,000 log entries consume disk space and memory).
3. Choose File→Exit.

Creating Custom Object Types and Profiles

ServerWORKS Manager lets you create custom object types and assign MIB groups of variables for non-DIGITAL servers. For example, Sophia of Desktop, Inc., could use this process to view her network of servers from multiple vendors.

To create the object type and assign the variables, you must complete the following tasks. Each of these tasks is composed of several smaller steps. When you have completed the tasks, you can manually add the object to your network map and begin managing it immediately.

- Define the object type so ServerWORKS recognizes objects on your network that match the description
- Enroll the MIB groups
- Assign the MIB groups that focus on information you want about the object type

Use the following procedure as a guide to creating an object type and profile for any network element. This example creates an object type for the Compaq ProLiant 2500 Server, assigns MIB groups, and explains how to add the object type to your network map manually and by discovery.

Defining the New Object Type

1. From the ServerWORKS Tools menu, choose Tools→Object Types and click the Add button. The Add SNMP Object Types dialog box opens. This is where you enter the object definition. (See Figure 5-1.)
2. In the Add SNMP dialog box, enter or select:
   - The object type name, for example, Server
   - The object subtype name, for example, Compaq
   - Bitmaps to represent the object icons (see Figure 5-1)
   - The icon's background shape (for example, endnode)

   Then click Apply.
3. Click Close. A message warns you to exit from ServerWORKS Manager. Then choose File→Exit.

About naming objects

You can name an object anything you want. For example, if you plan to view the network by organization, you might have object types named Server.Finance or Node.Sales1, Node.Sales2.

About selecting bitmaps

You can create your own bitmaps or you can select them from the ServerWORKS bitmaps collection and modify them slightly to represent a new object.

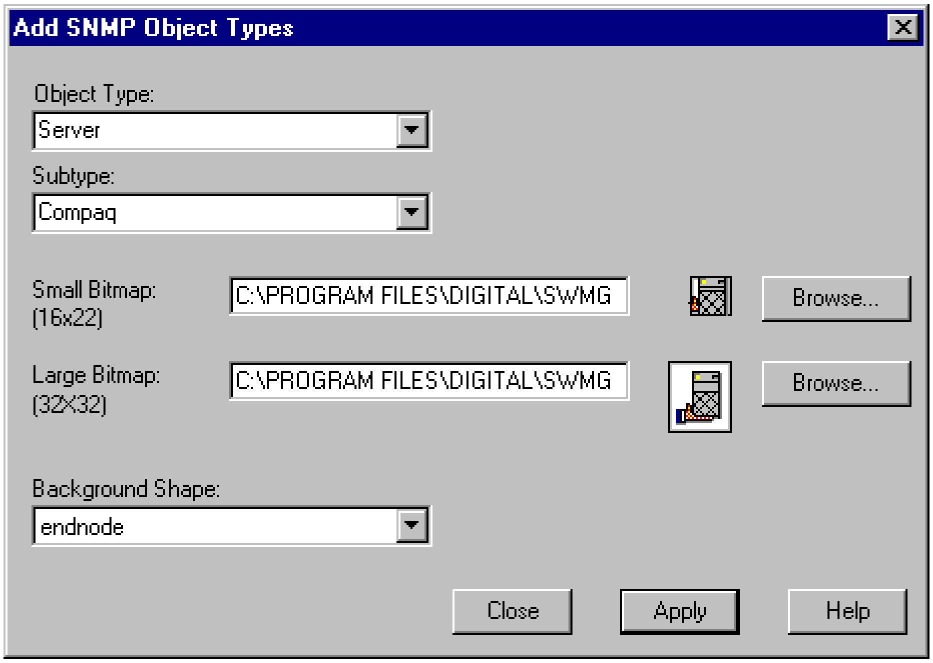
You can find the ServerWORKS bitmaps at:

```
<ServerWORKS directory>:\database\bitmaps
```

A color change to the bitmap is sufficient and is accomplished easily in a tool such as Paint. The sample bitmaps `serverg.bmp` and `server32.bmp` provide a good starting point for modifying bitmaps because they are the correct size. Modify and rename the bitmaps in Paint. For example, for a Compaq object, use serverc16.bmp and serverc32.bmp and store them with the ServerWORKS bitmaps.

About the background shape

Each network element that appears in the object list (server, node, bridge, and so on) has a default shape for the icon. Use the default.



Add SNMP Object Types

Object Type: Server

Subtype: Compaq

Small Bitmap: (16x22) C:\PROGRAM FILES\DIGITAL\SWMG

Large Bitmap: (32X32) C:\PROGRAM FILES\DIGITAL\SWMG

Background Shape: endnode

Figure 5-1 Entries in the Add SNMP Object Types Dialog Box Define an Object Type

Enrolling MIBs in the ServerWORKS Database

Before an object type can be used in ServerWORKS Manager Console, MIB groups associated with the object must be enrolled in the ServerWORKS database. ServerWORKS Manager has already enrolled hundreds of MIB groups that are ready for assignment to new object types. For example, if the object type Node.Finance is a DIGITAL server, you can assign DIGITAL MIBs already enrolled for the server.Digital object type. (For the convenience of Compaq server administrators, the Compaq MIB variables are already enrolled in the ServerWORKS database.)

However, if you are creating an object type with MIBs you have acquired from a vendor, a Web site, or a bulletin board service, you must enroll (compile) them into the ServerWORKS database first.

1. From the ServerWORKS menu, choose Tools→ MIB Enroller. The SNMP MIB Enroller dialog box opens.
2. From the Compile menu, choose MIB Compiler.
3. Choose File→Open to browse for the MIB on your system.
4. Select the MIB. The MIB text appears in the MIB edit box.
5. Click the Enroll button. Enter a name for the MIB and choose OK.
6. Choose OK again at the prompt “Do you want to store this MIB in the permanent database?”

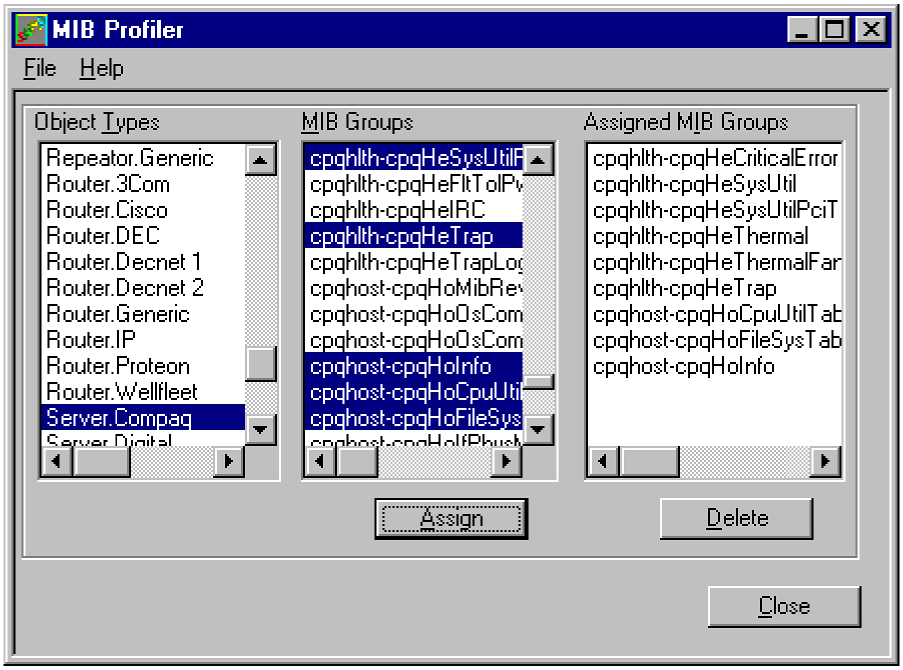
About MIB group variables and their purpose

How do you know which MIB group to choose? Each group variable is explained for you. To learn more about a group's variables, choose the group from the MIB groups list. Select a MIB variable and click on the MIB Info button to display an explanation of the variable. You can also add to the definition and save your comments.

Assigning MIB Groups to the Object Type

1. From the ServerWORKS menu, choose Actions→ Browse MIB→MIB Utilities.
2. From the MIB Browser menu, choose MIB Utilities→MIB Profiler.
3. Select the new object name from the Object Types list, as illustrated in Figure 5-2.
4. Scroll through the MIB Groups list and select the groups of variables to assign to the object type. In this case, Compaq MIBs are identified with the cpq prefix.

5. Choose Assign to add the groups to the Assigned MIB Groups list.
6. Click Close.



Object Types:
Repeator.Generic
Router.3Com
Router.Cisco
Router.DEC
Router.Decnet 1
Router.Decnet 2
Router.Generic
Router.IP
Router.Proteon
Router.Wellfleet
Server.Compaq
Server.Digital

MIB Groups:
cpqhlth-cpqHeSysUtilF
cpqhlth-cpqHeFltTolPv
cpqhlth-cpqHeIRC
cpqhlth-cpqHeTrap
cpqhlth-cpqHeTrapLog
cpqhost-cpqHoMibRev
cpqhost-cpqHoOsCom
cpqhost-cpqHoOsCom
cpqhost-cpqHoInfo
cpqhost-cpqHoCpuUti
cpqhost-cpqHoFileSys
cpqhost-cpqHoIfPhysM

Assigned MIB Groups:
cpqhlth-cpqHeCriticalError
cpqhlth-cpqHeSysUtil
cpqhlth-cpqHeSysUtilPciT
cpqhlth-cpqHeThermal
cpqhlth-cpqHeThermalFar
cpqhlth-cpqHeTrap
cpqhost-cpqHoCpuUtilTab
cpqhost-cpqHoFileSysTab
cpqhost-cpqHoInfo

Figure 5-2 MIB Groups are Assigned to the New Object Type

Scrolling Quickly Through ServerWORKS Manager Lists

MIB groups and variables number in the hundreds. To reduce the searching time, click anywhere on the list and then type the first letter or two of a group name to move to the section of the list that contains the variables. For example, type s in the Object Types list to display the server objects, type cp in the MIB Groups list to find the Compaq groups.

Manually Adding the Object to the Network Map

Adding a network element manually is the fastest and least complex way to begin managing the objects.

1. From the ServerWORKS Manager menu, choose File→New Viewer to create a new map or choose File→Open Viewer to open an existing map where you will add objects of the new object type—in this case, the Server.Compaq type.
2. Choose Edit→Insert and select the object type (Server) from the Insert dialog box list.
3. In the Insert: Server dialog box, enter a display name, for example Compaq1. This name is also the default IP Name. You can change the IP name. Choose a network object type from the Type list. For this example, it is Server.Compaq.
4. Click on Get Addr to display the IP Address.
5. Click OK. An auto-discovery is started to insert the new object into the view you selected.

Checking for the Object

From the map, double-click on the object to open the MIB Browser. The new object is identified with the Compaq name as part of the system descriptor. After you run IP Discovery, view the Discovery Report to see the list of new Compaq objects.

Figure 5-3 shows the map view of a network with the new object type. In the lower right corner, serv19.dec.com and serv24.dec.com, two Microsoft NT cluster members were discovered. One has experienced an alarm condition.

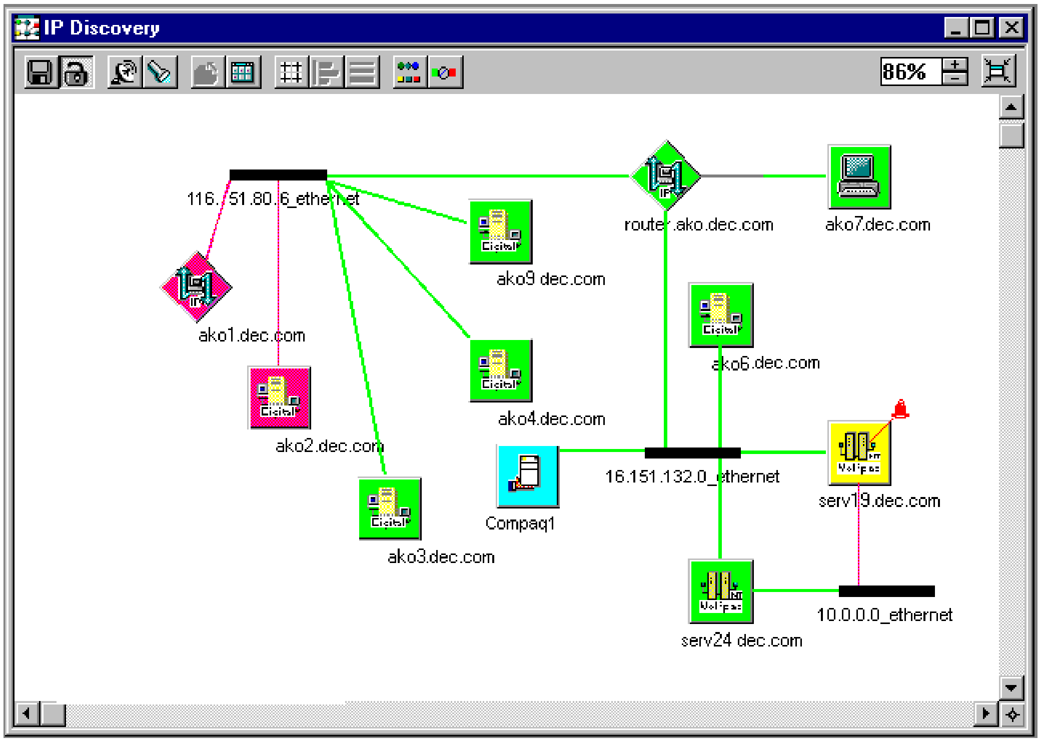


Figure 5-3 New Object Type Discovered in Map and Hierarchical Views

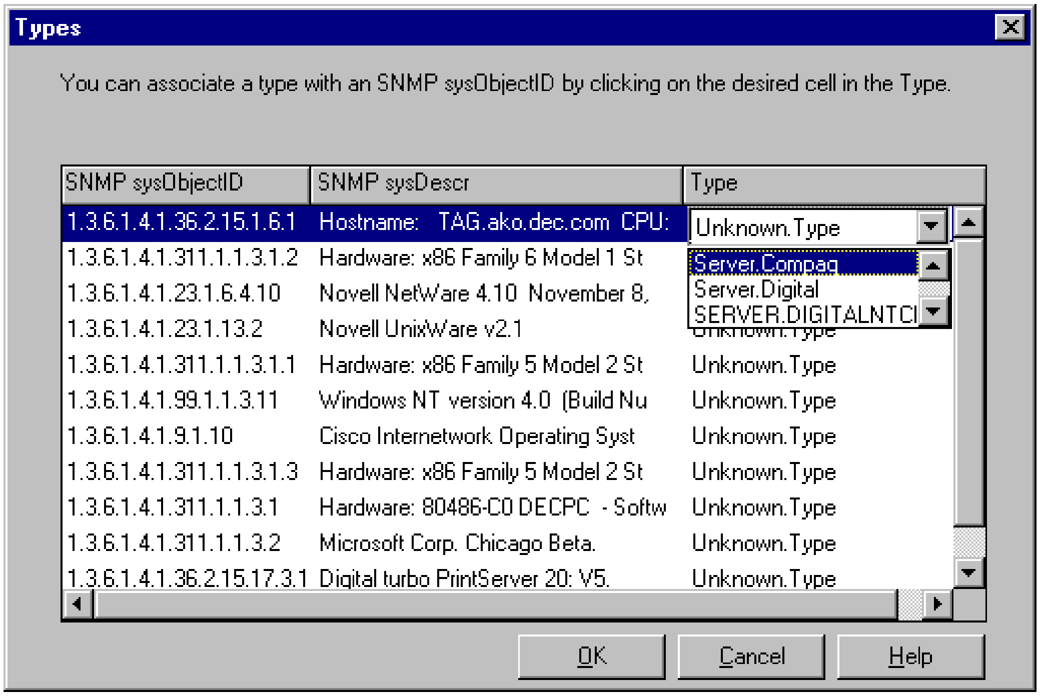
Associating Unknown Objects with Known Object Types

When SNMP is running, Discovery might also find objects that are not associated with a known object type. These objects are named Unknown.Type. The sysObjectID for the object is not mapped to a existing object type so the appropriate MIBs are not applied to the object.

To create the association, you must map the unknown object type to an existing network object. You can perform the mapping when you run a new Discovery.

1. From the ServerWORKS Manager window, choose Actions→Discover IP Objects.
2. On the Networks to discover dialog box, select the network and netmask. Then click Next.

3. On the Types to discover dialog box, click the Types button.
4. On the Types dialog box, you can view the list of Unknown.Type objects.
5. Select an object to associate with a type. You can identify the object by the sysObjectID or the SNMP sysDescr. (Double-click on the object in a map to open the MIB Browser and find the information.)
6. Click on the Unknown.Type label in the object’s row. A drop-down list appears with the list of existing object types. Select the object type. Because you have created the object Server.Compaq, the name appears on the list.



Types

You can associate a type with an SNMP sysObjectID by clicking on the desired cell in the Type.

SNMP sysObjectID	SNMP sysDescr	Type
1.3.6.1.4.1.36.2.15.1.6.1	Hostname: TAG.ako.dec.com CPU:	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.2	Hardware: x86 Family 6 Model 1 St	
1.3.6.1.4.1.23.1.6.4.10	Novell NetWare 4.10 November 8,	
1.3.6.1.4.1.23.1.13.2	Novell UnixWare v2.1	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.1	Hardware: x86 Family 5 Model 2 St	Unknown.Type
1.3.6.1.4.1.99.1.1.3.11	Windows NT version 4.0 (Build Nu	Unknown.Type
1.3.6.1.4.1.9.1.10	Cisco Internetwork Operating Syst	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.3	Hardware: x86 Family 5 Model 2 St	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1	Hardware: 80486-C0 DECPC - Softw	Unknown.Type
1.3.6.1.4.1.311.1.1.3.2	Microsoft Corp. Chicago Beta.	Unknown.Type
1.3.6.1.4.1.36.2.15.17.3.1	Digital turbo PrintServer 20: V5.	Unknown.Type

Figure 5-4 Types Dialog Box for Associating Unknown Objects with Existing Objects

7. Click OK. From the Types to discover dialog box, click Next.
8. On the Discovery Options dialog box, select the view or map to hold the discovery and click Finish.

When the Discovery is complete, the unknown object appears on the map as the new Server.Compaq object. Double-click on the object to view details in the MIB Browser.

Editing the Registry to Recognize the New Object

Manual insertion is a quick way to insert one or two objects, but if you are adding multiple objects of a type, you might prefer to use IP Discovery. On NT systems, IP Discovery uses a key in the NT Registry to identify objects. You can change the key to reflect a unique characteristic of the object for a particular map view (for example, a hardware-specific identifier or an organizational identifier).

1. Open the Registry editor regedit.exe. (Using Start→Find→Files or Folders is one way to locate the file.)
2. In the Registry, find the entry

```
HKEY_LOCAL_MACHINE\
        HARDWARE\
                DESCRIPTION\
                        System\
                                CentralProcessor\
```

3. Double-click on the Identifier value and prepend the string with Compaq, as follows:

```
REG_SZ: Compaq - x86 Family 6 Model 1 Stepping 7
```

4. For this example the expression Compaq uniquely identifies the server object type.
5. Click OK and exit from the Registry.

Editing the Registry with a Batch File

Creating a new object type temporarily changes the Registry. Because the change is not permanent, you can write a batch file to make this change each time you reboot. Use the Windows NT Resource Kit regcgh.exe to get the key value for the Registry. The following is an example of a batch file you can use as a guideline:

```
if "%1"=="" goto error
set tmpfile=C:\temp.reg
echo REGEDIT4>%tmpfile%
echo.>>%tmpfile%
echo [HKEY_LOCAL_MACHINE
        \HARDWARE
            \DESCRIPTIONS
                \System
                    \CentralProcessor
                        \0]>>%tmpfile%
echo "Identifier"="Compaq Server">>%tmpfile%
call regedit %tmpfile%
del %tmpfile%
goto exit
echo Set of Compaq MIB II System Descriptor failed
:error
pause
:exit
```

Integrating with Other Managers

One of the advantages of ServerWORKS Manager is its capability to enroll other vendor's MIBs into its database and to provide DIGITAL MIBs to other manager applications that allow them to see DIGITAL servers.

You can launch ServerWORKS applications from HP OpenView, NetServer Assistant, or Tivoli TME 10.

Receiving ServerWORKS Traps in Enterprise-Level Managers

By default, a trap forwarded from ServerWORKS Manager to an enterprise-level manager will be displayed as an unknown trap. To allow an enterprise manager such as HP OpenView or Tivoli TME 10 to display information about DIGITAL servers, you need to follow these basic steps:

- Enroll DIGITAL MIBs in the enterprise system.
- Create the appropriate device class (object types and subtypes).
- Customize the alarm view, if you wish.

The specific steps will vary depending on which enterprise-level manager you use. This section uses examples taken from Tivoli TME 10 NetView to illustrate the process.

Enrolling DIGITAL MIBs in a Non-DIGITAL System

Most network managers allow you to compile a new MIB. After you compile a MIB, the same information displayed in the MIB Browser can be displayed using another workgroup manager's or enterprise manager's browser.

If you choose to enroll the DIGITAL-specific MIBs, you enable the user to get and set MIB variables from the systems on which the DIGITAL SNMP extended agents are running. A number of DIGITAL MIBs are found in the ServerWORKS Manager directory. You can integrate any or all of the following MIBs into your SNMP management system:

MIB Name	Description
NTCMGT.MIB	DIGITAL NT Cluster MIB
RFC1514.MIB	Host Resource MIB
SVRMGT.MIB	DIGITAL Server Management MIB
SVRSYS.MIB	DIGITAL System MIB
MLXGAM.MIB	Mylex Global Array Manager MIB

To add a DIGITAL MIB to Tivoli TME 10 NetView on the target system, select MIB from the Tools menu. Select Load. The MIB Loader opens. Select the MIBs you want to load. If you choose the Server System MIB, you need to include RFC1213 (MIB II) as well, because the Server System MIB references variables in RFC1213.

Launching ServerWORKS System Browser from an Enterprise-Level Manager

ServerWORKS Manager offers integrated application launch. Most enterprise managers, such as HP OpenView and Tivoli TME 10, allow you to add user-defined applications. When you install ServerWORKS Manager on a system where Tivoli TME 10 NetView for Windows NT is installed, the ServerWORKS Manager installation automatically installs into TME 10 NetView and registers the ServerWORKS Manager System Browser so that TME 10 NetView can be used with DIGITAL servers. When you select a DIGITAL host in the NetView IPMap, the System Browser entry in the TME 10 NetView Tools pull-down menu is activated, as shown in Figure 5-5.

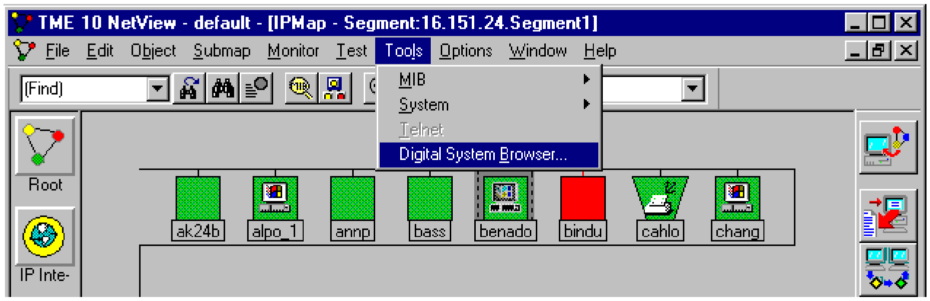


Figure 5-5 Launching the System Browser from TME 10 NetView

Creating Alarms and Notification Actions

You can associate an action with an alarm or event. You can reuse the action for different types of objects or for different types of alarms. The following section describes how to create an alarm and set up a notification action for it. First create the alarm. Then define the action for the alarm. This example creates an alarm on a cluster.

Creating an Alarm

1. From the ServerWORKS Manager Console menu, choose Tools→Alarm Configuration.
2. Select an object for alarming from the list of network objects.
3. Click on Add New Alarm.
4. Define the alarm in the Add New Component Status Alarms dialog box. You have several areas to define.
   - Category tab: The alarm category lists the elements you can alarm based on the object type. In turn, the subelements that can be alarmed change with the category. Select an Alarm Category (for example, Cluster Group Status) and Items to be Monitored (Cluster Group). The Alarm at a Glance pane displays a summary of the alarm.
   - States tab: From the list of Possible States to be monitored, select the states you want in the alarm definition (for example Not Functional) and click the right arrow button to add the state to the Alarm States list.
   - Severity tab: Choose the importance of the alarm being set. Because you are setting a notification action, High is a reasonable severity level. Typically, you do not need notification of informational or low importance alarms.
   - Polling tab: Select the polling interval for the object. A high severity alarm should have frequent polling, for example, one minute.
   - Actions: If you are specifying an action, click on Add New. The Add New Actions dialog box opens to define the action.

5. Refer to the section "Adding the Notification Action on an Alarm" and the subsection that describes the action you want:

Notification action	Described in subsection
Pager notification	Setting up a Pager Notification Action
Email notification	Setting up an Email Notification Action
Application launch notification	Setting up an Application Launch

Adding the Notification Action on an Alarm

You can choose between several actions—pager notification, email notification, and an application launch—when an alarm condition occurs. For any action, you also set the frequency of the action from the following choices on the Policy property page:

- Always, for any alarm, for any action, whenever the alarm condition is met
- Once for the first alarm only
- At specified intervals for all alarms, regardless of how often the alarm occurs
- At specified intervals for some individual alarms, up to a maximum number of times regardless of how often the alarm occurs

For high severity alarms, you might choose always. For less severe alarms, choose an interval to avoid overloading your email or pager with repeat messages. For minor alarms, once is sufficient (assuming you act on the notification before the problem becomes severe).

Setting Up a Pager Notification Action

ServerWORKS Manager V3.2 supports only numeric paging using TAPI. Alphanumeric paging is not supported. Before you can use the pager for notification, you must check that you have a properly configured modem and com port specified for the telephone number that will contact the pager. Refer to the section "Configuring a Modem and Com Port for Paging" if you are not sure that you have a working modem.

1. In the Add New Actions dialog box, choose the Pager tab and click New.

2. In the New User dialog box, enter the user information. The Pager number is the telephone number. (Refer to the section “Changing the Default Pager Wait Time for details about using commas.) The Pager Message is a numeric code that you devise to interpret messages. For example, the message "111" might mean a severe server environmental condition. More elaborate schemes are available with some pagers. See your pager documentation for specific information.
3. Click OK. The user name appears in the All Users list. Click Add to also place the name in the Pager User list. Then click OK.
4. Enter the action name, for example Page Me. Click OK. The new action Page Me appears in the Action Directory Contents list. Click OK.
5. Click on the Policy tab and choose the interval (as described previously in this section) if you want to specify an interval for the pager notification only. Then click OK.

When an alarm condition is detected, the modem calls the pager and sends the message to the pager.

Changing the Default Pager Wait Time

Pagers allow you to include a wait time to adjust for timing between dialing a phone number and sending the numeric message. The standard symbol is a comma. ServerWORKS Manager Console paging alarm has a default wait time of five commas. You can change the wait time if you need more or less wait time between dialing the phone number and sending the numeric message.

To change the wait time:

1. Open the swmgr.ini file and find the section [Setup].
2. Add the following statement to the section:

   ```
   PagerWaitTime=
   ```

3. Enter a number for the page wait time. The page wait time is the number of commas. You may have to try several numbers until you find the right wait interval for your paging system.

Configuring a Modem and Com Port for Paging

If you have not already done so, install the modem hardware and software according to the manufacturer's instructions.

Attempt to dial from the modem using any dialup software. If you cannot connect and reach the phone number of the test location, recheck the computer-to-modem and modem-to-phone physical connections and make sure the modem is turned on. Also check that the phone number, area codes, and country codes are correct. Refer to the dialup software manufacturer’s directions for details about the dialup software.

Settting Up an Email Notification Action

Before you can use email for notification, you must check that you have a valid profile for Microsoft Exchange mail so the recipient gets the notification. First check that the profile for your mail is ‘MS Exchange Settings.’ If not, you must specify this profile. Refer to the section "Setting Up the ‘MS Exchange Settings’ Default Profile." Then set up the email notification action with the following instructions:

1. On the Add New Actions dialog box, choose the Email tab and click New.
2. On the New User dialog box, enter the user information. The email address is the Internet mail address for the recipient (for example support@company.com). The message to the recipient contains the date and time, node name of the object that triggered the alarm, and a description of the triggering effect. SNMP traps may include additional information.
3. Click OK. The user name appears in the All Users list. Click Add to also place the name in the Email User list. Then click OK.
4. Enter the action name, for example Email Me. Click OK. The new action Email Me appears in the Action Directory Contents list. Click OK.
5. Click on the Policy tab and choose the interval (as described previously in this chapter) if you want to specify an interval for the email notification only. Then click OK.

When an alarm condition is detected, the mail protocol sends a message to the named recipient.

Setting Up the ‘MS Exchange Settings’ Default Profile

To configure Exchange for email notifications, first install your favorite mail protocol on the same system where ServerWORKS Manager console in installed. (Refer to the mail protocol installation documentation for details. Instructions for specific mail applications are beyond the scope of this manual). When you run ServerWORKS Manager, also run Microsoft Exchange to receive the notification at the console.

The ‘MS Exchange Settings’ default profile contains your mail protocol and logon information. The profile is required for the email notification action.

1. From the Windows desktop, right click on the Exchange Inbox icon and choose Properties.
2. Choose the Show Profiles button. If ‘MS Exchange Settings’ appears in the list of profiles and in the "When starting MS Exchange, use this profile" field, choose Close. If the profile is not listed, create the profile.
   - Before you proceed, consult your system administrator for the mail protocol name and logon information (such as the user name or mailbox and whether you are using Exchange Server, Internet mail, or other information services).
3. Click the Add button. On the Inbox Setup Wizard dialog box, select the option "Use the following information services" and choose your protocol from the list of information services.
4. Click the Next button. In the Profile Name dialog box, select ‘MS Exchange Settings’ (or enter the name ‘MS Exchange Settings’ exactly, if it does not appear. You must use this name). Then click Next again.
5. Continue to follow the prompts on the remaining dialog boxes. These vary according to the information service you selected but will include protocol and user information.
6. Continue to follow the prompts and choose Finish on the last Wizard dialog box.

The ‘MS Exchange Settings’ profile is added to the list of profiles. Select the profile and choose Close.

Setting Up an Application Launch Action

The application launch action can be as simple or complex as you want. You will have to determine the command line for any procedure. The following is a simple example.

1. On the Add New Actions dialog box, choose the Application Launch tab.
2. Enter the file name. You need the full path name and the file extension (for example, c:\netscape.exe to open a browser window).
3. Select the alarm information (parameters) that you want passed to the application to be launched. Your application must be programmed to use the parameters (for example, to display an animated alert and the passed parameters on an html page). Click OK.
4. On the Action Name dialog box, enter a name for the action (for example, Alert Me.) The name appears in the Actions Directory list.
5. Click on the Policy tab and choose the interval (as described previously in this chapter) if you want to specify an interval only for the application launch notification. Then click OK.

When an alarm condition is detected, the application opens and performs the specified activity.

Forwarding Traps

The ServerWORKS Manager console that receives traps can in turn *forward* those traps to other systems. This allows workgroup-level managers to run ServerWORKS Manager, while enterprise-level managers run manager programs such as HP OpenView or Tivoli TME 10. Forwarded traps are redirected by the ServerWORKS Manager Event Dispatcher and Event Logger, not by the agent.

To forward traps in ServerWORKS Manager, define the forwarding destinations from the ServerWORKS console Trap Forwarding utility.

Trap forwarding takes place only when the Event Dispatcher and Event Logger are running and only if no other application has opened trap port 162. By default, no forwarding takes place. Agent-based traps are always forwarded to the management console. Data Collector alarms can be forwarded as traps if you specify this in the Trap Forwarding utility.

Specify a unique address and a port for each destination. If a port number is not specified, then port 162 is assumed to avoid problems with systems that have multiple SNMP trap listeners on them.

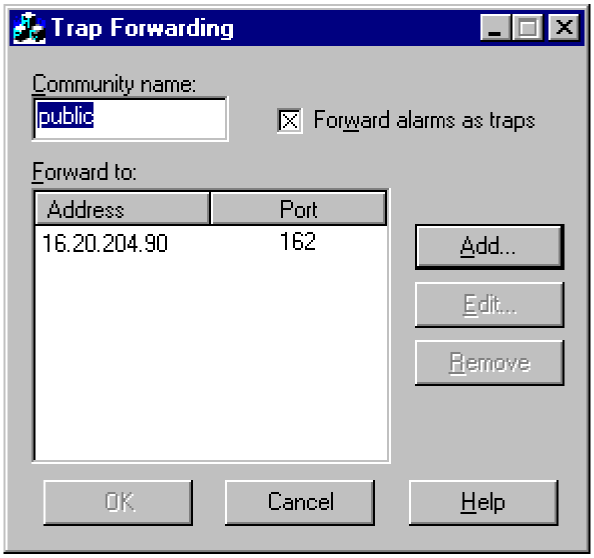
All traps will be forwarded to each destination you define. ServerWORKS Manager allows up to ten forwarding destination addresses.

To specify a trap forwarding destination:

1. From the ServerWORKS Manager Console menu, choose Tools→Trap Forwarding
2. Perform the following tasks:
   - Change the community name, if necessary. Public is the NT default community. You can change the community name, but the name you use applies to all forwarding destinations in the list.
   - Select ‘Forward alarms as traps’.
   - Click Add. On the Add dialog box, enter the Address and Port number. For example, to forward all traps received at a management console to another IP address of 16.20.204.90 using the TCP/IP port number 162, you would complete the dialog box as shown in Figure 5-6. Then click OK.

You can also delete or modify a forwarding address. To delete, select an address and click Remove. To modify, select an address and click Edit. Then change the Address and Port information on the Edit dialog box.

3. On the Trap Forwarding dialog box, click OK again to close.



Community name: public

☒ Forward alarms as traps

Forward to:

Address	Port
16.20.204.90	162

Figure 5-6 Trap Forwarding Dialog Box

Using NT Server Management for Windows NT Domains

To manage an NT domain on your network, you can use ServerWORKS Manager NT Server Management instead of using the NT administration utilities. The following procedure explains how to create a Local group and assign rights to the group. (For more information about NT Server installation and administration, refer to the MSDN CD-ROM Windows NT Books Online volume *Basics and Installation: Microsoft Windows NT Server, Version 4.0.*)

To create a group in ServerWORKS Manager NT Server Management

1. From the Explorer, choose NT Server Management.
2. Select the NT domain. The list expands to display the Groups, Servers, and Users objects for the domain.
3. Select Servers. The list expands to display the servers in the domain.
4. Select the server or workstation where you want to create the group.
5. Select Groups.
6. From the Actions menu, choose Create. The Create Group dialog box appears.
7. Enter the group name and a brief comment identifying the group. Then select Global or Local.
8. Click Apply to create the group and remain in the Create Group dialog box to create more new groups, or click OK to create the group and close the dialog box.
9. You are prompted to set other attributes for the new group. Do one of the following:
   - Select No to accept the default attributes.
   - Select Yes to open the Properties of Groups dialog box to change other attributes.

To modify the rights

1. From the NT Server Management, select the domain and machine where you are assigning group rights.
2. Select Groups.
3. Choose Actions→Properties.
4. On the Properties of Server dialog box, click on the User Rights tab.
5. On the User Rights page, select a right from the Right drop-down list. For example, to allow the group members to log on locally to the selected machine, click Log on Locally.
6. Click Add.
7. On the Add Groups and Users to… dialog box, select the group and click Add to include this right for this group. Then click OK.
8. Repeat steps 1 to 7 for each right you are assigning until you are satisfied that the group has the appropriate rights.

Assigning Rights to Multiple Groups at Once

Simply select several groups in the Groups list. Press and hold CTRL and click on the groups you are including. All rights assigned or deleted are applied to all groups selected.

Reference Information A

Bibliography

This chapter provides additional sources of information on topics covered in the manual.

Topic	Additional Source of Information
DIGITAL UNIX	Network Administration and Network Programmer’s Guide
Discovering objects on your network	Online help, Chapter 3 of this manual.
KCRCM	KCRCM AlphaServer Remote Console Module Installation and User's Guide (EK-KCRCM-IN) included with the KCRCM product
Monitoring Systems	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994
	SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993

Topic	Additional Source of Information
Monitoring Systems (continued)	Internetworking with TCP/IP, Volume 2, Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991
	Internetworking with TCP/IP, Volume 1, Principles, Protocols, and Architecture by Douglas E. Comer published by Prentice Hall 1991, Second Edition
Mylex GAM	Mylex Global Array Manager 2 Installation and User's Guide (ER-MYL02-IA) found on the ServerWORKS Manager CD-ROM in the documentation section
Novell NetWare	Novell's Guide to Multiprotocol Internetworking, by Laura A. Chappell and Roger L. Spicer published by the Novell Press
	NetWare, The Professional Reference, Third Edition, published by News Rider Publishing 1994
OpenVMS	TCP/IP Networking on OpenVMS Systems and OpenVMS System Manager's Manual
RSM	RSM Installation Guide (ER-PCDSC-IA) and RSM Station Software User's Guide (ER-PCDSM-UA) included with the RSM product
SCO UNIX	SCO OpenServer Handbook How to install, configure, and start using an SCO OpenServer system, published by The Santa Cruz Operation 1995

Topic	Additional Source of Information
Sending SNMP Traps	Online help, Chapter 4 of this manual
	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994
	SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993
Setting and Receiving Alarms	Online help, Chapter 3 of this manual
SNMP	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994
	SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993
	Internetworking with TCP/IP Volume 2 Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991
SWCC	StorageWORKS Command Console Installation Guide (AA-R0HJB-TE) found on the ServerWORKS Manager CD-ROM in the documentation section

Topic	Additional Source of Information
Windows 95	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995
Windows 95 SNMP	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995
Windows NT	Windows NT Networking Guide - Windows NT Resource Kit by and published by Microsoft Press
Windows NT SNMP Service	Windows NT Networking Guide - Windows NT Resource Kit published by Microsoft Press

The following web site may also provide additional information on ServerWORKS:

http://www.digital.com/info/alphaserver/sworks.html

Glossary

The following terms are used frequently in any discussion of SNMP and network management.

Term	Definition
Alarm	An SNMP trap generated by an agent or an event and triggered by the results of polling an agent.
Allocation Units	The size in bytes for a particular storage device. For example, the allocation units for a disk are typically 512, 1024, or 2048 bytes and are sometimes referred to as 'block size.'
CPU Utilization	Average percentage of time that this processor was not idle.
Data Collector	Process that runs on the management console and polls objects for SNMP data. The collector analyzes the data and either generates alarms or passes the data on to registered applications such as the System Browser.
DMI	Desktop Management Interface.
FAT	File Allocation Table (listed on the System Browser File System property page).
File System Utilization	The percentage of the file system being used (local file systems).

Term	Definition
IP	Internet Protocol (see also TCP/IP).
IP Address	An address of an object on a network. The standard address is composed of four numbers each of which is less than 255.
Management Information Base (MIB)	Data Specification for passing information using the SNMP protocol.
MIF	Management Information File - This is a database file that defines a given host's configuration, hardware inventory, storage devices, processors, and memory.
Mount Point	The top level name for a mounted file system.
MTU	Maximum Transmission Unit.
Network Interface	Communication between the management console machine and the network. Usually completed through Network Interface cards.
Network Interface Inbound Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Network Interface Inbound Packet Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Network Interface Inbound Packets	The number of packets delivered to a higher-layer protocol.

Term	Definition
Network Interface Outbound Errors	The number of outbound packets that could not be transmitted because of errors.
Network Interface Unknown Protocol Errors	The number of packets received through the interface which were discarded because of an unknown or unsupported protocol.
NOS	Network Operating System. The operating system and protocol used to communicate between objects on a network.
NTFS	NT File system. File system used on NT.
Polling Interval	The time between polling queries of a device.
Re-Enable Value	Value that can be set in the Threshold screen to automatically enable an alarm that has previously triggered.
SNMP	Simple Network Management Protocol - The application protocol offering network management service in the Internet.
SNMP Trap	An asynchronous event generated by the agent and sent to the SNMP manager.
Status Alarm	Alarm set on server processors or disks to indicate the status of the device (options are running, non-functional, and warning).
System Name	The name of the object on the IP network as returned by the Naming server or found in the Hosts file on the management console machine.
System Up Time	The time the system has been up since it was booted.

Term	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol. A widely used set of software communications protocols. TCP delivers data over a connection between applications on different computers on a network: IP controls how packets (units of data) are transferred between computers on a network.
Threshold Alarm	Alarm triggered when a value entered on the Threshold Alarm screen meets a specified condition.
Threshold Value	Value at which an alarm is triggered (e.g., 10000 packets per second).

Registry Keys

Warning: Do not edit the Registry unless you are familiar with Windows NT or Windows 95 operating systems. Do not remove the full tree path.

If you cannot install successfully, you can edit the Registry keys for ServerWORKS Manager Console, ClientWORKS, and the agents.

Before you edit the Registry, review the following guidelines:

- Always use the ServerWORKS Manager Console→unInstallShield menu item or the Control Panel→Add/Remove Programs applet first to remove previous versions of ServerWORKS Manager Console, ClientWORKS, and the agents.
- Always back up the Registry before you edit it in case you must restore a damaged Registry. From the Registry editor, use the Registry→Export Registry File menu item to save the file as a .reg file. The Registry online help describes how to complete this procedure and restore the backed up Registry.
- Keys and values may be different for Windows NT and Windows 95 systems.
- Not all keys and values appear on all systems. Keys entered with earlier versions may be obsolete although they remain on your system.
- If your system does not contain a value for a key as listed in the following tables, do not remove the key.
- Keys and values are subject to change between releases.

Table A-1 ServerWORKS Manager Console Registry Keys and Values

Registry Tree	Remove keys or values
HKEY_CURRENT_USER\\ Software\\ ODBC\\ ODBC.INI\\ ODBC Data Sources\\	SWMgrDB SWMgrDBEmpty
HKEY_CURRENT_USER\\ Software\\ ODBC\\ ODBC.INI\\ SWMgrDB\\	SWMgrDB
HKEY_CURRENT_USER\\ Software\\ ODBC\\ ODBC.INI\\ SWMgrDBEmpty\\	SWMgrDBEmpty
HKEY_CURRENT_USER\\ System\\ CurrentControlSet\\ Services\\ EventLog\\ Application\\	SWMgr
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ DigitalEquipmentCorporation\\	ServerWORKS Manager Console ServerWORKS Manager Console Browser
HKEY_LOCAL_MACHINE\\ Software\\ Microsoft\\ Windows\\ CurrentVersion\\ Uninstall\\	ServerWORKSv3.2 SWMgrTME10
HKEY_LOCAL_MACHINE\\ Software\\ Microsoft\\ Windows\\ CurrentVersion\\ AppPaths\\	pwMgmt.EXE smb.exe

Table A-2 ClientWORKS Registry Keys and Values

Registry Tree	Remove keys or values
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ DigitalEquipmentCorporation\\	AssetWORKS LiveLINK ClientWORKS ClientWORKS DMIBrowser ClientWORKS Init ClientWORKS SMART DMI
HKEY_CURRENT_USER \\Software \\Microsoft \\Windows \\CurrentVersion \\Uninstall	CWInstallInit CWSNMP1.0 LiveLINK1.0 SMART1.0 DMIPATH
HKEY_CURRENT_USER \\Software \\Microsoft \\Windows \\CurrentVersion \\Run	Digital SmartMonitor
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ Microsoft\\ Windows\\ CurrentVersion\\ Run	Digital SmartServer
HKEY_LOCAL_MACHINE\\ Software\\ Microsoft\\ Windows\\ CurrentVersion\\ RunOnce\\	SNMP TrapSeed

Table A-2 ClientWORKS Registry Keys and Values (cont’d)

Registry Tree	Remove keys or values
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ Microsoft\\ Windows\\ CurrentVersion\\ RunService	Read BIOS
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ Microsoft\\ Windows\\ CurrentVersion\\ RunServicesOnce	SecureOnClient DMI Remoting Layer

Table A-3 Registry Keys and Values for Shared Agents

Registry Tree	Remove keys or values
HKEY_CURRENT_USER\\ System\\ CurrentControlSet\\ Services\\ SNMP\\ Parameters\\ ExtensionAgents\\	DIGHRAG DIGPVAG DIGSMAG CWDIGHRAG CWDIGPVAG
HKEY_LOCAL_MACHINE\\ SOFTWARE\\ DigitalEquipmentCorporation\\	HostResourcesAgent ServerManagementAgent ServerSystemAgent