[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise™ 2.5

NetWare Management Agent™ 2.1
Installation and Configuration Guide

ManageWise™
MANAGEMENT SOFTWARE

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries.

The Novell Network Symbol, Internet Packet Exchange, IPX, IPX/SPX, ManageWise, NDS, NetWare 3, NetWare 4, NetWare Directory Services, NetWare DOS Requester, NetWare Loadable Module, NetWare MHS, NetWare Message Handling System, NLM, Novell Directory Services, Sequenced Packet Exchange, SMS, SPX, Virtual Loadable Module, and VLM are trademarks of Novell, Inc.

Apple, AppleLink, AppleTalk, LocalTalk, Macintosh, and Power Macintosh are registered trademarks and Apple Desktop Bus is a trademark of Apple Computer, Inc. CompuServe is a registered trademark of CompuServe Incorporated. NetPort and SatisFAXtion are registered trademarks and

Novell, Inc.
2180 Fortune Drive
San Jose, CA 95131

ManageWise™ 2.5
NetWare Management Agent™ 2.1 Installation and Configuration Guide
October 1997
100-002799-002

Contents

Index

chapter 1

Overview of NetWare Management Agent 2.1

The NetWare® Management Agent™ 2.1 software provides real-time server performance data and information about server alarms to network management consoles. NetWare Management Agent 2.1 completely replaces NetWare Management Agent 1.*x*.

This chapter describes the main features and the major improvements offered by NetWare Management Agent 2.1. This chapter contains the following sections:

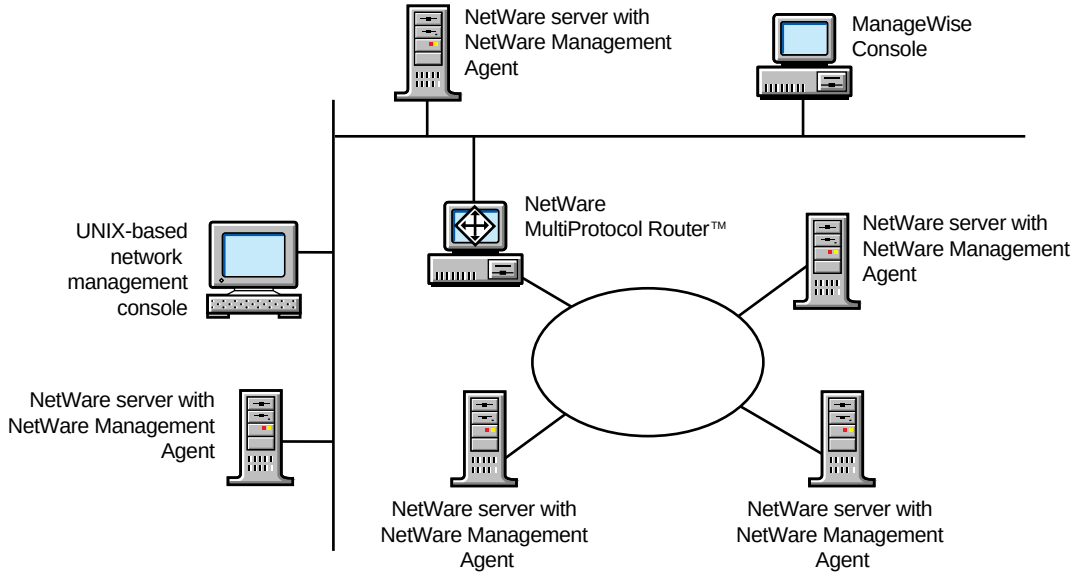
- About SNMP-Based Management
- Gathering Local Trend Information at the Server
- Support for Secure SNMP Transactions
- About NetWare Management Agent 2.1 NLM Files

About SNMP-Based Management

The main advantage of NetWare Management Agent 2.1 is that it is based entirely on the Simple Network Management Protocol (SNMP). This makes NetWare Management Agent 2.1 easily managed by third-party management consoles as well as the ManageWise™ Console. This expands the management options for using SNMP-based management consoles other than ManageWise Consoles or in conjunction with ManageWise. To facilitate this, all MIBs used with NetWare Management Agent enable you to compile at your console using any standard MIB compiler.

Figure 1-1 illustrates an internetwork using NetWare Management Agent 2.1 and two network management consoles: ManageWise and a console based on UNIX* software.

Figure 1-1
NetWare Management Agent Configuration



Gathering Local Trend Information at the Server

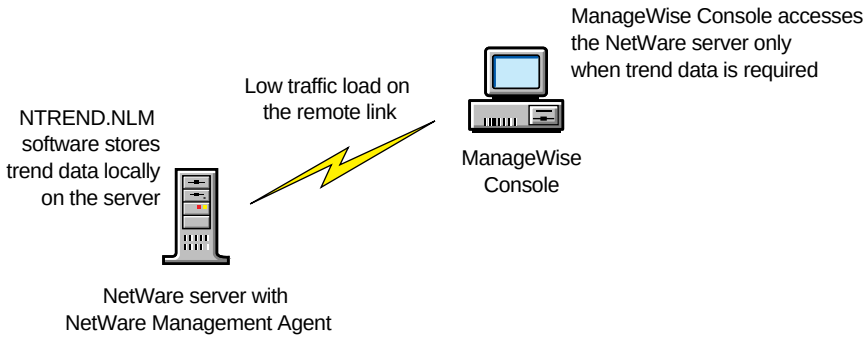
Collecting trend data about devices creates a large amount of traffic on the network. This is because the management console must query the

device continually to develop data. This can be particularly expensive and burdensome when you are monitoring remote devices. NetWare Management Agent 2.1 provides a solution to this problem.

The NTREND.NLM software supplied with NetWare Management Agent 2.1 enables you to collect trend data at the server. Because the trend data is stored at the server, the management console does not have to poll the server constantly to maintain an internal trend data file. The management console can save on network traffic by collecting the trend data only as needed. Figure 1-2 illustrates this process using NetWare Management Agent 2.1.

Figure 1-2

Server-Based Trend Data Collection



Refer to “Setting Default Trends and Thresholds” on page 44 for details about how to configure NTREND.NLM.

Support for Secure SNMP Transactions

You can limit the access of management consoles performing GET and SET requests. You can accomplish this by either of the methods described in the following sections:

- "Using SNMP Over a NetWare Core Protocol Connection" on page 28
- "Setting Security for SNMP Management" on page 29

With these two methods, NetWare Management Agent 2.1 provides traditional SNMP Agent security and also much enhanced security by requiring NetWare SUPERVISOR or OPERATOR login before granting access to SNMP functionality.

For details about these security features and instructions about their configurations, see Chapter 3, "Setting Up Secure SNMP Transactions."

About NetWare Management Agent 2.1 NLM Files

The NetWare Management Agent 2.1 software consists of the following NetWare Loadable Module™ (NLM™) files that are installed on a NetWare server.

SERVINST.NLM

Implements the NetWare Server MIB (NWSERVER.MIB).

HOSTMIB.NLM

Implements the standard Host Resources MIB [RFC 1514] and Novell's extensions to that MIB (NWHOSTX.MIB).

NTREND.NLM

Implements the Threshold and Trend MIB (NWTREND.MIB). When loaded, NTREND.NLM sets up trends and thresholds for each monitored attribute according to the server's configuration. The NTREND.INI file contains configuration parameters for NTREND.NLM.

NWTRAP.NLM

Implements the NetWare Server Trap MIB (NWALARM.MIB). The NWTRAP.CFG file contains configuration parameters for NWTRAP.NLM.

FINDNMS.NLM

Used by NetWare servers running NetWare Management Agent 2.1. Employ FINDNMS.NLM to listen for ManageWise Consoles advertising themselves using the Service Advertising Protocol (SAP) number 0x026a. FINDNMS.NLM then adds the Internetwork Packet Exchange™ (IPX™) address of each ManageWise Console discovered to the list of stations that receive traps.

chapter 2

Installing NetWare Management Agent 2.1

This chapter describes the NetWare® server hardware, version, and system configuration requirements for installing NetWare Management Agent™ 2.1 software. The chapter also provides information about how to get NetWare Management Agent 2.1 up and running on NetWare 3.1*x* and NetWare 4.1x servers.

Skip this chapter, if you installed ManageWise 2.5 on the server. ManageWise2.5 automatically installs NetWare Management Agent 2.1 on the server.

This chapter contains the following sections

- NetWare Server Hardware Requirements
- Versions of NetWare Supported
- Installing the NetWare Management Agent 2.1 Software
- Loading and Unloading NetWare Management Agent 2.1

NetWare Server Hardware Requirements

The NetWare Management Agent files must be installed on a server that meets these hardware requirements:

- An additional 2 MB RAM on NetWare 3.11 servers, NetWare 3.12 servers, and NetWare 4.1x servers. For NetWare SFT III™ servers, the additional 2 MB RAM must be installed on the IOEngines and MSEngine.

  At least 1 MB of memory (cache nonmovable) is required to load the NLM™ files, and at least 1 MB (alloc short term) is recommended for memory allocations.

  Allocation memory requirements vary depending on the server configuration (disks, volumes, NLM files, and so forth). After you load NetWare Management Agent, verify that you have at least 40 percent of available memory resources for file caching. Unpredictable results occur when there is insufficient server memory.

- 3.5-inch floppy disk drive

- At least 2 MB of free disk space on the SYS: volume

Versions of NetWare Supported

Use NetWare Management Agent 2.1 only with the following versions of NetWare:

- NetWare 3.1x and NetWare 4.1x. All released versions except NetWare SFT III.

- NetWare 4.1 for OS/2*. All released versions.

This product should *not* be used with the following versions:

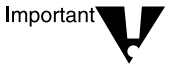
- NetWare versions prior to NetWare 3.11.

- NetWare 4™ servers prior to NetWare 4.1.

- NetWare servers running SMP.

Installing the NetWare Management Agent 2.1 Software

If you are installing NetWare Management Agent 2.1 over NetWare Management Agent 1.*x*, make sure that you unload all the 1.*x* NLM files before you proceed with the installation.



Before installing NetWare Management Agent 2.1 on a NetWare 3.1*x* server, you must update the NetWare SNMP Services.

Installation of the NetWare Management Agent software can be performed both locally or remotely. Before installing, make sure to check the following items:

- ❑ Make sure you have the following diskettes:
  - NetWare Management Agent *Agent* diskette (NMA_DISK)
  - *NetWare SNMP Services Update* diskette (SNMP_1 DISK) *(for NetWare 3.1x only)*
  - NetWare Management Agent *License* diskette
- ❑ To install on the current server, start the server if it's not already running.
- ❑ To install remotely, follow the procedure described in "Preparing for Remote Installation" on page 10.

The installation procedures are described in the following sections:

Preparing for Remote Installation

To perform a remote installation of the NetWare Management Agent 2.1 software, complete the following steps first:

At the server:

1. ***For NetWare 3.1x only:*** **Edit the AUTOEXEC.BAT file on the server's DOS partition to load SERVER.EXE when the system is restarted.**

2. **Edit the AUTOEXEC.NCF file to configure the remote password.**

At the workstation:

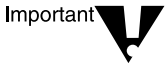
1. **Install the latest version of NetWare Client™ 1.2 software on your workstation.**

   You can find it on the NetWare Management System CD-ROM.

   Novell does not recommend running RCONSOLE on a version of NetWare Client prior to 1.2.

2. **Map a drive to a volume on the server where you want to install NetWare Management Agent 2.1.**

3. **On the mapped volume on the server, create directories to hold the files from each diskette required for installation.**



   The directory where the SNMP Agent Update installation files will reside *must* be named SNMP_1.

4. **Copy all diskettes required for installation into the appropriate directories.**

   - For NetWare 3.1*x*, you must copy the *SNMP Agent Update* diskette (SNMP_1) and the NetWare Management *Agent* diskette (NMA_DISK).
   - For NetWare 4.1x, youmust copy only the NetWare Management *Agent* diskette (NMA_DISK).

5. **Remotely, start either DOS RCONSOLE or Windows* RCONSOLE from within NMS 2.1.**

   For information about using Windows RCONSOLE, refer to the *NetWare 4.0 Utilities Reference*.

6. **Choose the server where you want to install NetWare Management Agent 2.1.**

Updating the NetWare SNMP Services

The Simple Network Management Protocol (SNMP) is required only on NetWare 3.1*x* servers.

To update the NetWare SNMP Services on a NetWare 3.1*x* server, complete the following steps:

1. **At the server console or RCONSOLE prompt, enter**

   `LOAD INSTALL`

   The Installation Options menu appears.

2. **To install locally, insert the *NetWare SNMP Agent Update* diskette into the server disk drive.**

3. **Select *Product Options*.**

   The Currently Installed Products list appears, displaying the NetWare products currently installed on your server.

4. **Press** <Insert>**.**

   The following message appears:

   ```
   Enter drive and/or path to new product source
   media.
   ```

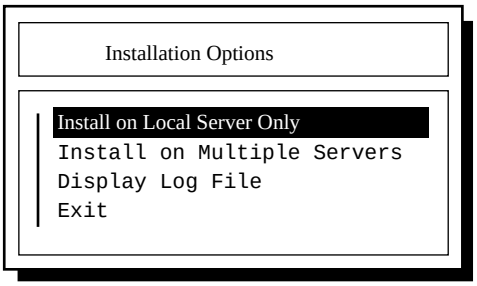
   Drive A: is the default.

   - To install from the server's A: drive, press <Enter>. If you are installing from a different drive, type the drive name, then press <Enter>.
   - To install remotely, type the server path to the location of the SNMP_1 directory, then press <Enter>.

For example, if you placed the files in the SNMP_1 directory in the SYS: volume, the path would be SYS:\SNMP_1.

The NetWare SNMP Services S2_1 Installation Options menu appears.

Figure 2-1
NetWare SNMP Services S2_1 Installation Options Menu



5. **Select *Install on Local Server Only*.**

   The Installation utility copies the files to a local temporary directory.

   The following message appears when all files have been installed:

   ```
   Installation was successful. Bring down and
   restart each server on which you installed the
   software to ensure that it uses the newest NLM
   files. <Press ENTER to continue>
   ```

Note

The SNMP update installation is complete. The SYS:\SYSTEM\INSTALL.LOG file contains a log of all files that were modified or copied during installation.

6. **Press** <Enter>**.**

   You return to the NetWare SNMP Services S2_1 Installation Options menu.

7. **Press** <Esc> **or select *Exit*.**

   The Exit product installation confirmation panel appears.

8. **Select *Yes*.**

You return to the Currently Installed Products list. *NetWare SNMP Services S2_1* is displayed in the list of installed products.

9. **Press** <Esc> **and select *Yes* at the Exit Install confirmation panel to exit the Installation utility.**

10. **Remove the *NetWare SNMP Agent Update* diskette from the drive.**

11. **To load SNMP, bring down the server and restart it.**

    Restarting from the Server

    To restart the server from the server console prompt, issue the following commands:

    `DOWN`

    The server is brought down safely.

    `EXIT`

    You return to the DOS prompt.

    `SERVER`

    The server starts up.

    Restarting the Server Remotely

    To restart the server remotely through RCONSOLE, issue the following commands:

    `REMOVE DOS`

    The DOS partition is removed.

    `DOWN`

    `EXIT`

    The server restarts and automatically loads SERVER.EXE from the AUTOEXEC.BAT file.

Installing NetWare Management Agent 2.1 on a NetWare 3.1*x* Server

To install the NetWare Management Agent 2.1 software on a NetWare 3.1*x* server, complete the following steps:

1. **To install on the current server, insert the NetWare Management Agent *Agent* diskette into the disk drive.**

2. **At the server console or RCONSOLE prompt, enter the following command:**

   `LOAD INSTALL`

   The *Installation Options* menu appears.

3. **Select *Product Options*, then press** <Enter>**.**

   The Currently Installed Products list displays the NetWare products currently installed on your server.

If a previous version of NetWare Management Agent 2.*x* is already installed, deinstall it by pressing <Delete>.

4. **Press** <Insert>**.**

   The following message appears:

   ```
   Enter drive and/or path to new product source
   media.
   ```

   Drive A: is the default.

   - To install from the server's A: drive, press <Enter>. If you are installing from a different drive, type the drive name, then press <Enter>.
   - To install remotely, type the server path to the location of the NMA_DISK directory, then press <Enter>.

     For example, if you placed the files in the NMA2.1 directory in the SYS: volume, the path would be SYS:\NMA_DISK.

   The Installation utility displays this message:

   ```
   The installation process will modify the server's
   AUTOEXEC.NCF file, copy NetWare Management Agent
   ```

```
and the associated Patch files. Old files will be
backed up under the SYS:\BACKUP directory.
```

The Options menu appears.

5. **Select *Continue to Install*.**

   You are prompted to insert the *License* diskette.

6. **Remove the *Agent* diskette and insert the *License* diskette, then press** <Esc>**.**

   When the licenses are installed, you are prompted to insert the *Agent* diskette.

7. **Remove the *License* diskette and insert the *Agent* diskette, then press** <Esc>**.**

   When all the agent files have been installed in their respective destination directories on the server, the following message appears:

```
The Installation process is complete. Older files
have been backed up to the \backup\nma21\
backup.nnn directory. Refer to this directory if
you need to restore the old files. Please exit and
restart your server. <Press ESCAPE to continue>
```

If NetWare Management Agent 1.5 or 1.6 was installed previously on this server, the NetWare Management Agent 2.1 installation program backs it up under the NMA.SAV directory and then overwrites it.

8. **Press** <Esc>**.**

   You return to the Currently Installed Products list. *NetWare Management Agent* is displayed in the list of installed products.

9. **Press** <Esc> **and select *Yes* at the Exit Install confirmation panel to exit the Installation utility.**

10. **Remove the *Agent* diskette.**

11. **To launch NetWare Management Agent 2.1, bring down the server and restart it.**

Restarting from the Server

To restart the NetWare 3.1*x* server from the server console prompt, issue the following commands:

DOWN

The server is brought down safely.

EXIT

You return to the DOS prompt.

SERVER

The server starts up.

Restarting the Server Remotely

To restart the NetWare 3.1*x* server remotely through RCONSOLE, issue the following commands:

REMOVE DOS

The DOS partition is removed.

DOWN

EXIT

When you bring up the server, the NetWare Management Agent software is launched.

Installing NetWare Management Agent 2.1 on a NetWare 4.1x Server

To install the NetWare Management Agent 2.1 software on a NetWare 4.1x server, complete the following steps:

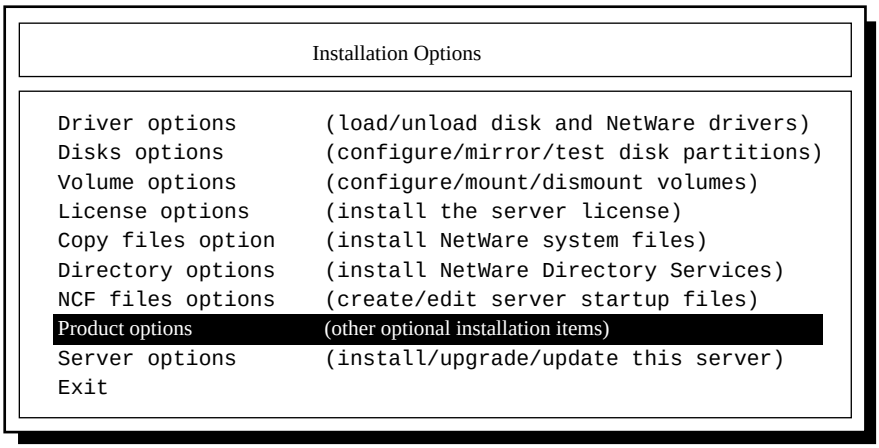
1. **To install on the current server, insert the NetWare Management Agent *Agent* diskette into the disk drive.**

2. **At the server console or RCONSOLE prompt, enter the following command:**

   LOAD INSTALL

   The Installation Options menu appears.

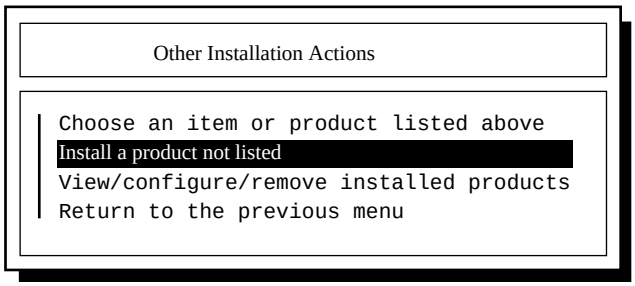
Figure 2-2
Installation Options Menu Under NetWare 4.1x



3. **Select *Product options*, then press** <Enter>**.**

   Two menus appear: the Other Installation Actions menu and the Other Installation Items / Products menu.

Figure 2-3
Other Installation Actions Menu



4. **From the Other Installation Actions menu, select *Install a product not LIsted*.**

Note

If a previous version of NetWare Management Agent 2.*x* is already installed, select *View/configure/remove installed products*, and deinstall it by selecting it and pressing <Delete>. Then press <Insert>.

The following message is displayed:

```
Product will be installed from A:\. If you are installing from
floppy, insert the first diskette of the product you want to
install into the drive and verify that the path above is correct.
 Press <F3> to specify a different path;
 Press <Enter> to continue.
```

5. **Press** <Enter>**.**

   To specify a different path, press <F3>, type the path or drive name, then press <Enter>.

   For example, if you placed the installation files in the NMA_DISK directory in the SYS: volume, the path would be SYS:\NMA_DISK.

   The Installation utility displays this message:

   ```
   The installation process will modify the server's
   AUTOEXEC.NCF file, copy NetWare Management Agent
   and the associated Patch files. Old files will be
   backed up under the SYS:\BACKUP directory.
   ```

   The Options menu is also displayed.

6. **Select *Continue to Install*.**

   You are prompted to insert the NetWare Management Agent *License* diskette.

7. **Remove the *Agent* diskette and insert the *License* diskette, then press** <Esc>**.**

   When the licenses are installed, you are prompted to insert the *Agent* diskette.

8. **Remove the *License* diskette and insert the *Agent* diskette, then press** <Esc>**.**

   When all the agent files have been installed in their respective destination directories on the server, the following message appears:

```
The Installation process is complete. Older files
have been backed up to the \backup\nma21\
backup.nnn directory. Refer to this directory if
you need to restore the old files. Please exit and
restart your server. <Press ESCAPE to continue>
```

If NetWare Management Agent 1.5 or 1.6 was installed previously on this server, the NetWare Management Agent 2.1 installation program backs it up under the NMA.SAV directory and then overwrites it.

9. **Press** <Esc>**.**

   You return to the Other Installation Actions menu.

10. **Press** <Esc> **and select *Yes* at the Exit Install confirmation panel to exit the Installation utility.**

11. **Remove the *Agent* diskette.**

    You must now restart your server.

12. **To launch NetWare Management Agent 2.1, bring down the server and restart it.**

    To restart the NetWare 4.1x server from either the server console prompt or remotely through RCONSOLE, issue the following commands:

    `DOWN`

    The server is safely brought down in orderly fashion.

    `RESTART SERVER`

    The server starts up. When the server is up, the NetWare Management Agent software is launched.

Installing NetWare Management Agent on SFT III Servers

To install NetWare Management Agent 2.1 on SFT III™ servers, follow the same procedure described in “Installing NetWare Management Agent 2.1 on a NetWare 4.1x Server” on page 16.

When you start the installation, be sure to insert the NetWare Management Agent *Agent* diskette into the drive on the primary server.

The installation procedure installs the NetWare Management Agent 2.1 software on the MSEngine and both IOEngines. The installation program also modifies the MSAUTO.NCF file and the IOAUTO.NCF file on both IOEngines.

You might receive the following message during the installation:

```
The Install process could not access the SFT III
Engine's IOAUTO.NCF file. Please manually add the
line "NMA2.NCF" to the IOAUTO.NCF file on both the IO
Engines.
```

If you receive this message, follow its instructions and add the **NMA2.NCF** statement to both the IOAUTO.NCF files. Then restart the server.

Restarting the SFT III Servers

The procedure for restarting SFT III servers after you install NetWare Management Agent 2.1 differs slightly from the procedure for a standard NetWare 4.1x server.

Issue the following commands *on both engines*:

DOWN

The server is safely brought down in orderly fashion.

EXIT

You return to the DOS prompt.

MSERVER

The server starts up. When both servers are back up, issue the following command at the server console prompt of the *primary server*.

ACTIVATE SERVER

The two SFT III servers are synchronized.

Installing NetWare Management Agent 2.1 from Windows

Complete the following procedure to install NetWare Management Agent 2.1 from Microsoft* Windows on one or more selected NetWare 4.1x or NetWare 3.1*x* servers.

If you want to install NetWare Management Agent 2.1 on SFT III servers, do not use the Windows installation procedure. Instead, use the installation procedures described in "Installing NetWare Management Agent 2.1 on a NetWare 4.1x Server" on page 16 and "Installing NetWare Management Agent on SFT III Servers" on page 19.

All the files replaced on the server by the Agent Setup for Windows are backed up in the SYS:\NMA.SAV directory. However, Agent Setup for Windows does not archive files from multiple installations. Agent Setup for Windows overwrites the NWTRAP.NLM and NWTRAP.CFG files. All the rest of the files are newly installed.

Bindery emulation for NetWare 4.1x servers. To install NetWare Management Agent 2.1 on a NetWare 4.1x server, the server requires bindery emulation.

Before you start, do the following:

- Make sure you have access to the server (or servers) you intend to install NetWare Management Agent on.
- Make sure you have the SERVER.EXE statement in the server's AUTOEXEC.BAT file on the DOS partition.

To install NetWare Management Agent 2.1, complete these steps:

1. **Start Windows.**
2. **Insert the *Agent Setup for Windows* diskette into your workstation's disk drive.**
3. **From the Windows Program Manager, select *File > Run*.**

   The Run dialog box appears.
4. **Type** *drive*:**\SETUP, then click *OK*.**

   Agent Setup for Windows checks for free disk space in the NMS directory and, if necessary, the Windows directory. If at least 3 MB

of free disk space is available in either directory, Agent Setup for Windows temporarily copies the NetWare Management Agent 2.1 files to the hard disk. This makes it fast and easy for you to do subsequent installations of the software without having to use the installation diskettes.

The EnterDisk dialog box appears, displaying this prompt:

```
Insert Agent Diskette
```

The source path *A:* or *B:* is displayed in the entry box, depending in which drive you inserted the *Agent Setup for Windows* diskette.

5. **Remove the *Agent Setup for Windows* diskette and insert the *Agent* diskette.**

6. **Enter the correct source drive if necessary, then click *OK*.**

   The EnterDisk dialog box appears, displaying this prompt:

   ```
   Insert NetWare SNMP Services Update Diskette
   ```

7. **Remove the *Agent* diskette and insert the *NetWare SNMP Services Update* diskette, then click *OK*.**

   The EnterDisk dialog box appears, displaying this prompt:

   ```
   Insert License Diskette
   ```

8. **Remove the *NetWare SNMP Services Update* diskette and insert your *License* diskette, then click *OK*.**

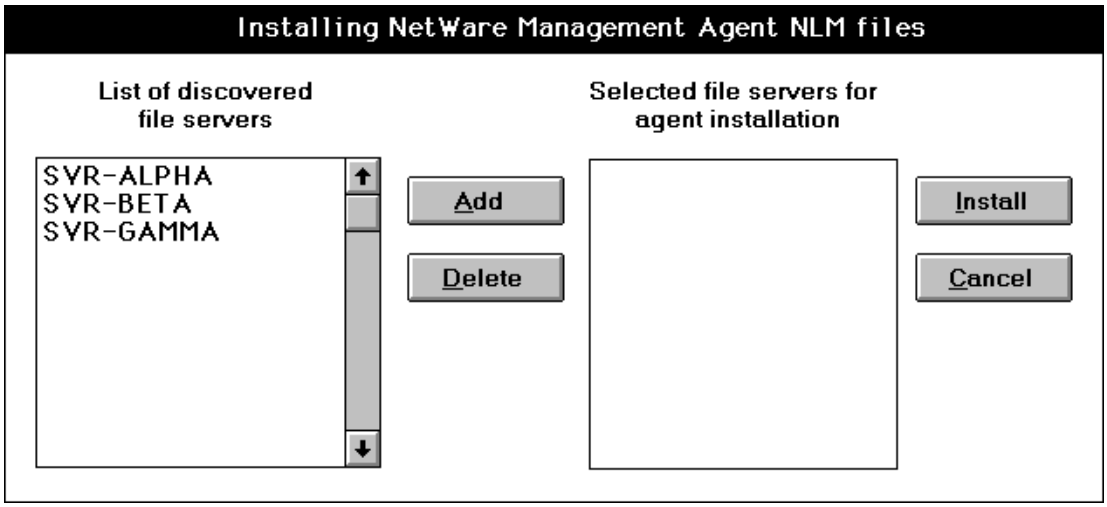
   The EnterDisk dialog box appears, displaying this prompt:

   ```
   Insert Agent Setup for Windows Diskette
   ```

9. **Remove the license diskette and insert the *Agent Setup for Windows* diskette, then click *OK*.**

   Agent Setup for Windows displays the Installing NetWare Management Agent NLM Files dialog box.

Figure 2-4
Installing NetWare Management Agent NLM Files Dialog Box



You can choose one or more servers to install the agent on.

10. **To select one or more servers, select each server you want to select from the list of discovered file servers, then click *Add*.**

    The servers you selected are displayed in the "Selected file servers for agent installation" list box.

    - If you select a server mistakenly, select the server's name in the "Selected file servers for agent installation" list box, then click *Delete*.

Note

If you have a *Master License Agreement* diskette, you need to install licenses only once, regardless of how many servers you install the agent on. If you have a single-server license, you are prompted to insert the *License* diskette for each server you select.

11. **When you have finished selecting servers, click *Install*.**

    The NetWare Management NLM File Installation dialog box appears, and displays the following prompt:

```
Enter the user name with supervisor rights and
password for the [server_name] NetWare server.
```

12. Enter the appropriate username and password, then click *Install*.

Agent Setup for Windows automatically replaces older files. During the installation process, Agent Setup for Windows may discover that some files already installed are newer versions than the corresponding files on the installation diskette. If so, you can choose to replace any of the newer files with the older versions of those files that reside on the installation diskette. Under most circumstances, this is not recommended.

When the NetWare Management Agents are installed on the selected servers, the following prompt is displayed:

```
Would you like to install NetWare Management
Agents on additional NetWare servers?
```

13. Click *Yes* to install agents on additional servers. Click *No* to proceed with the installation procedure.

- If you click *Yes*, you return to the Installing NetWare Management Agent NLM Files dialog box (see Figure 2-4 on page 23).

13a. To install agents on additional servers, repeat Steps 10 through 12.

- If you click *No*, you are prompted as follows:

```
Do you want to keep the cache directory for future
installations from the hard disk?
```

14. Click *Yes* to keep the installation files in the cache directory. Click *No* to remove the cache directory from your hard disk.

Keeping Agent Setup for Windows and its associated files in a cache directory makes subsequent installation procedures for NetWare Management Agent 2.1 notably faster and easier.

- If you click *Yes*, Agent Setup for Windows first creates the NetWare Management Agent 2.1 program group in your Windows Program Manager, and then opens the README file.

- If you click *No*, Agent Setup for Windows deletes the cache directory and its files and opens the README file.

  If Agent Setup for Windows and its associated files are not in a cache directory on your hard disk, you must perform subsequent installations of Netware Management Agent 2.1 from the installation diskettes.

15. **Read or print the README file and exit the file.**

    The installation of NetWare Management Agent 2.1 is complete.

    To launch NetWare Management Agent 2.1, you must bring down the server (or servers) the agent is installed on and restart them.

16. **To launch NetWare Management Agent 2.1, bring down the server and restart it.**

Loading and Unloading NetWare Management Agent 2.1

To load NetWare Management Agent 2.1 from the server prompt, enter this command:

```
NMA2
```

To unload all the NetWare Management Agent 2.1 NLM files from the server, run the following command from the SYS:SYSTEM directory:

```
UNNMA2.NCF
```

This concludes Chapter 2. The next chapter discusses how to set up SNMP transactions.

chapter 3

Setting Up Secure SNMP Transactions

Because NetWare Management Agent 2.1 software is based on SNMP, all actions that are directed from network management consoles to a server involve SNMP SET and GET commands. Any console action that gets data from the server does so by issuing an SNMP GET command. An SNMP SET command is required to set server alarm thresholds or configuration parameters. In most cases, you are unaware of the underlying SNMP commands required to carry out requests you make from a management console.

Conducting these management operations from a remote management console, such as the ManageWise Console, raises the problem of ensuring security. In particular, if unchecked, unauthorized users setting configuration parameters on a server could cause severe performance problems or even sabotage network operations.

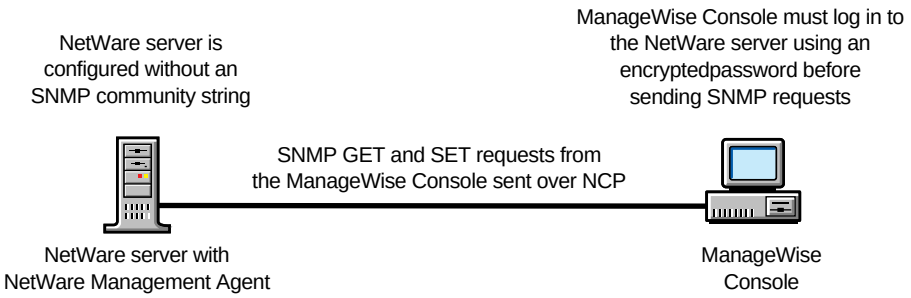
For these reasons, NetWare Management Agent 2.1 provides security for SNMP commands through mechanisms described later in this chapter.

Using SNMP Over a NetWare Core Protocol Connection

NetWare Management Agent 2.1 provides maximum security using the NetWare Core Protocol™ (NCP™) option. When configured this way, a NetWare server accepts only SNMP SET or GET commands from management consoles that log in to the NetWare server with SUPERVISOR or OPERATOR privileges.

In this configuration, the NetWare server accepts SET and GET commands from appropriately logged-in consoles and ignores whatever SNMP community string might be used in the command. Because the login password is encrypted, this password is secure from anyone using a network protocol analyzer to decode packets on the network. Figure 3-1 illustrates this configuration.

Figure 3-1
Server Configuration with SNMP Over NCP



You can configure the SNMP SET and SNMP GET commands separately. For example, you might want to allow open access to configuration information on your server, but allow only limited access for changing configuration parameters. In this situation, you would configure the server to allow only SNMP SET transactions over NCP.

You set this option at the NetWare server using either LOAD SNMP command, as described in “Configuring Community Name Options Using SNMP LOAD Commands” on page 32. You can also set this option using the Internetworking Configuration utility (INETCFG) on NetWare 4.1 servers or servers running NetWare MultiProtocol Router software, as described in “Configuring Community Name Options Using INETCFG” on page 33.

To configure a ManageWise Console to operate with a NetWare server using this configuration, see “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 36.

Note NCP cannot be used on SFT III™ server IOEngines. Therefore, you must set the ControlCommunity string on the IOEngine to the community name the MSEngine uses.

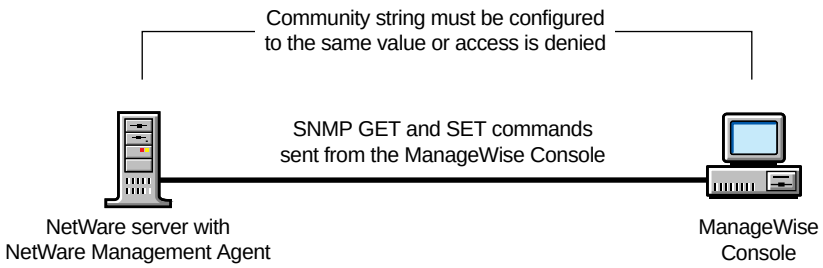
Setting Security for SNMP Management

Security for SNMP management is often provided through use of the SNMP community name. NetWare Management Agent 2.1 provides this mechanism that enables you to limit the access of management consoles performing GET and SET commands.

To accomplish this, set a unique community name at the NetWare server where NetWare Management Agent 2.1 is installed. Any console requesting access to that server must use the same community name or access is denied.

Figure 3-2 illustrates the concept of community name–based security using the ManageWise Console.

Figure 3-2
Secure SNMP Commands Using the Community Name



This security mechanism is limited and insufficient for networks where security is highly valued. This is because the community name is not encrypted and can be read easily using a network protocol analyzer.

See “Configuring Security Options on a NetWare Server” on page 31 for configuration instructions. To configure a ManageWise Console to

operate with a NetWare server in this configuration, see “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 36.

Allowing Access to a ManageWise Console and a Third-Party Management Console

In some networks, you might want to allow access to both a ManageWise Console and a third-party network management console. In this case, only management consoles using NCP, of which the ManageWise Console is one, can operate with SNMP over an NCP connection. In this situation, more security than is typically provided by community name access can be made available.

You can accomplish this by setting the community name at the ManageWise Console to a different value than the value that is set at the server and by setting up the ManageWise Console to provide SNMP over NCP connectivity.

In this configuration, the ManageWise Console always logs in to the NetWare server with SUPERVISOR or OPERATOR privileges when conducting an SNMP command. Although the ManageWise Console uses an incorrect or null community name, it succeeds in logging in because the NetWare server ignores the community name for consoles that have logged in with SUPERVISOR or OPERATOR privileges. If someone monitors any of these commands using a network protocol analyzer, they obtain an incorrect community name.

Because the NetWare server has not been configured for exclusive SNMP access to users with SUPERVISOR or OPERATOR privileges, any SNMP command that contains the correct community name is accepted. A third-party console can perform SNMP commands on this server by using the correct community name in the command.

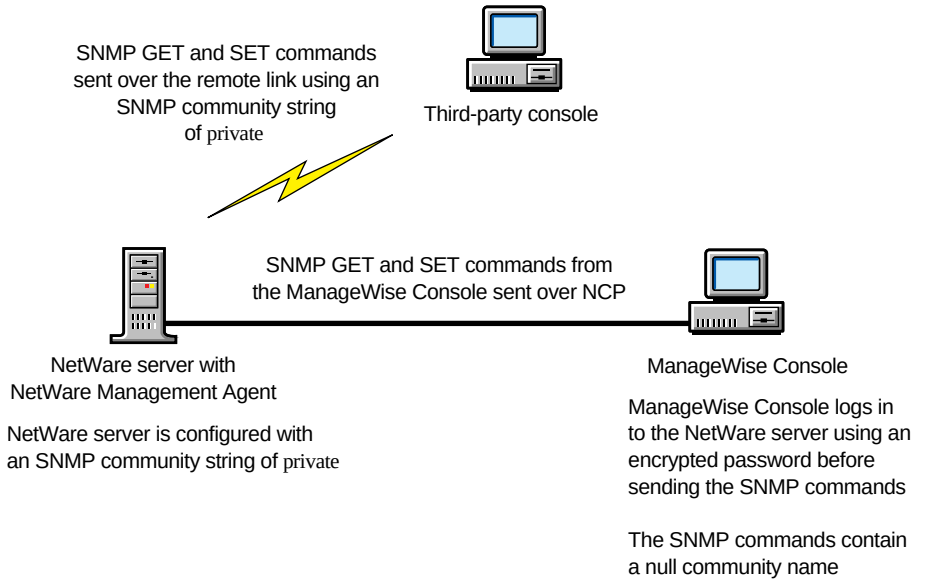
These commands can be monitored and decoded using a network protocol analyzer. From this decoding, the correct community name can be deciphered and used to breach the security of the server. Additional security is provided, however, because only the commands conducted by the third-party console can be deciphered.

This configuration is most useful for network management configurations that use ManageWise for local management of a

NetWare server but also allow occasional management from a third-party management console at a remote site.

Figure 3-3 illustrates this type of NetWare Management Agent 2.1 configuration.

Figure 3-3
Secure SNMP Transaction Using a False Community Name



Refer to the next section for configuration instructions. To configure a ManageWise Console to operate with a NetWare server in this configuration, refer to “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 36.

Configuring Security Options on a NetWare Server

Configuring security on a NetWare Management Agent 2.1 server involves setting the *SNMP community name*. You configure security access for SNMP transactions using either SNMP LOAD command-line parameters (NetWare 3™ servers or NetWare 4™ servers) or through

INETCFG (NetWare 4 servers or servers with NetWare MultiProtocol Router™ software installed).

Community names are used to authenticate SNMP commands received at the NetWare Management Agent 2.1 server. The community name in a message requesting a given access type must match the name defined by that access type by one of the SNMP community options.

Community names are arbitrary ASCII strings of up to 64 characters. They can include any character except space, tab, open square bracket ([), equal sign (=), colon (:), semicolon (;), and number sign (#).

The community name can be set to any of the following options:

- Read access or read / write access by anyone
- Read access or read / write access by consoles specifying the correct community name
- Read access or read / write access by users with SUPERVISOR or OPERATOR privileges only

Configuring Community Name Options Using SNMP LOAD Commands

The LOAD command accepts the following SNMP option parameters:

- *MonitorCommunity*—Sets the community name for read-only (GET) access. The default value is *public*. The syntax is as follows:

  ```
  LOAD SNMP MonitorCommunity=community name
  ```

- *ControlCommunity*—Sets the community name for read and write (GET and SET) access. By default, this community name is disabled.

  When *ControlCommunity* is disabled, write access is available only to users who log in with SUPERVISOR or OPERATOR privileges.

  The syntax is as follows:

  ```
  LOAD SNMP ControlCommunity=community name
  ```

These options set the community name for the indicated community. Community names are case-sensitive.

Table 3-1 shows examples of available settings.

Table 3-1
SNMP Example Settings

Access available to requester with	Read Only	Read/Write
Any community name	LOAD SNMP MonitorCommunity= or LOAD SNMP ControlCommunity=	LOAD SNMP ControlCommunity=
Community name: "secret"	LOAD SNMP MonitorCommunity=*secret* or LOAD SNMP ControlCommunity=*secret*	LOAD SNMP ControlCommunity=*secret*
Community name: "str1" or "str2"	LOAD SNMP MonitorCommunity=*str1* and LOAD SNMP ControlCommunity=*str2*	
SUPERVISOR or OPERATOR	LOAD SNMP MonitorCommunity and LOAD SNMP ControlCommunity	LOAD SNMP ControlCommunity

Configuring Community Name Options Using INETCFG

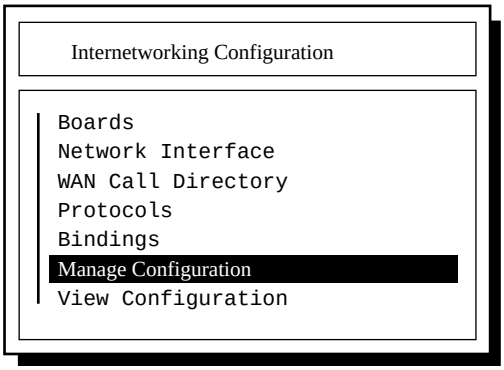
To configure the community name options using INETCFG, follow these steps:

1. **At the server prompt, enter the following command:**

   `LOAD INETCFG`

   The Internetworking Configuration menu is displayed.

Figure 3-4
Internetworking Configuration Menu



2. **From the Internetworking Configuration menu, select *Manage Configuration*.**

   The Manage Configuration menu is displayed.

3. **Select *Configure SNMP Parameters*.**

   The SNMP Parameters menu is displayed.

4. **Select *Monitor State*.**

5. **Select one of the following options, and then press** Enter**.**

   These options let you indicate how SNMP handles SNMP read operations coming from outside this server.

Option	Description
Any Community May Read	Allows all GET (read) commands no matter what community name is provided in the incoming read request.
Leave as Default Setting	Avoids changing the Monitor Community name from its default (which is usually *public*). The default Monitor Community can still be changed manually through SNMP command-line options, as described in “Configuring Community Name Options Using SNMP LOAD Commands” on page 32.
No Community May Read	Allows GET (read) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming read request is ignored.

Option	Description
Specified Community May Read	Allows only GET (read) commands for requests that contain the name specified in the Monitor Community field. If you selected this option, enter a name in the Monitor Community field, and then press Enter. Enter the name of the community that is allowed to read management information. SNMP management stations that belong to this community can read the network management database.

6. **Select *Control State*.**

7. **Select one of the following options, and then press** Enter**.**

   These options allow you to indicate how SNMP handles SNMP write operations coming from outside this server:

Option	Description
Any Community May Write	Allows all SET (write) commands, no matter what community name is provided in the incoming write request.
Leave as Default Setting	Avoids changing the Control Community from its default, which is usually to allow write requests only for management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. You can change the default manually through SNMP command-line options, as described in “Configuring Community Name Options Using SNMP LOAD Commands” on page 32.
No Community May Write	Allows SET (write) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming write request is ignored.
Specified Community May Write	Allows SET (write) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming write request is ignored.

8. **When you are finished, press** Esc**. If prompted, select *Yes* to save changes to the SNMP parameters, and then press** Enter**.**

   The Manage Configuration menu is displayed.

9. **To return to the Internetworking Configuration menu, press** Esc**.**

10. **To exit INTECFG, press** Esc**.**

Note

Changes made in INETCFG are not active immediately. To put these changes into effect, bring down the server and restart it.

Setting Up the ManageWise Console for Secure SNMP Transactions

Configuring secure SNMP transactions involves setting parameters at both the console and the server being managed. This section describes how to configure a ManageWise Console for each of the following SNMP security options:

- Configuring the SNMP community string for SET and GET commands
- Directing the ManageWise Console to log in with SUPERVISOR or OPERATOR privileges for SNMP SET and GET commands

To configure the ManageWise Console SNMP security options, follow these steps:

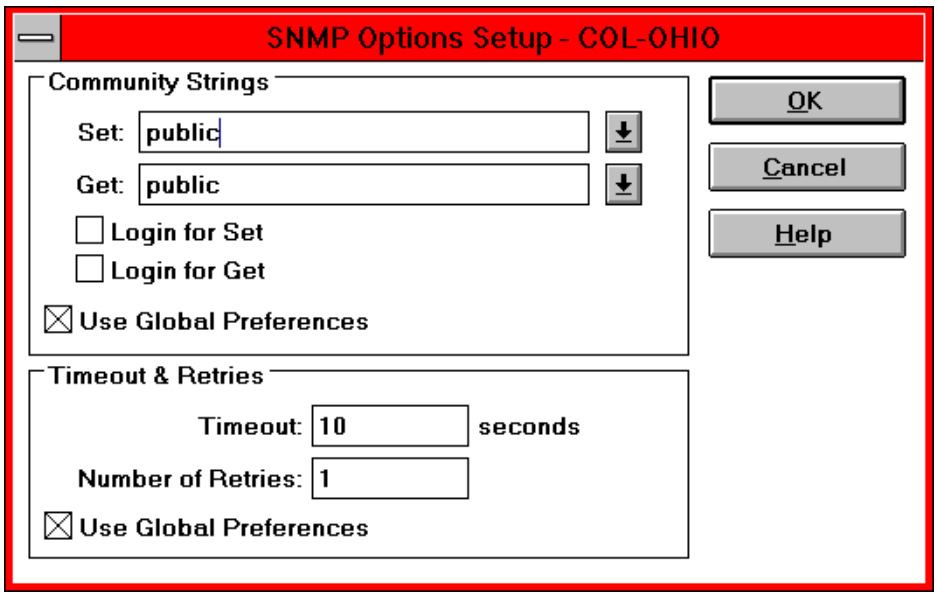
Procedure

1. **Select a ManageWise Server.**

2. **Select *Configure > SNMP Options*.**

   The SNMP Options Setup dialog box is displayed as shown in Figure 3-5.

Figure 3-5
SNMP Setup Options



3. **If you want the ManageWise Console to log in with SUPERVISOR or OPERATOR privileges, select the following options:**

   - For SET (write) commands, select the Login for SET check box. The server ignores SET community name in this case.
   - For GET (read) commands, select the Login for GET check box. The server ignores GET community name in this case.

4. **Otherwise, select the following options:**

   - Select a community string for SNMP SET commands.

     You can either accept the default value of *public*, type a unique value for the server you are managing, or select *null* for no community string value.

   - Select a community string for SNMP GET commands.

     You can either accept the default value of *public*, type a unique value for the server you are managing, or select *null* for no community string value.

5. **When you are finished, click OK to exit the SNMP Options Setup dialog box and set the new values.**

chapter 4

Configuring NetWare Management Agent 2.1

Once NetWare Management Agent 2.1 software has been installed on your system, it is ready to operate in its default state. In most cases, this configuration is sufficient; however, you can customize NetWare Management Agent 2.1.

Examine each of the configuration options in the sections that follow to determine whether you require any of the functionality provided.

Configuring NLM Load Parameters

The NetWare Management Agent 2.1 installation process creates the NMA2.NCF file in the SYS:\SYSTEM directory. When the NetWare server is started, this file automatically loads all the NLM files required for NetWare Management Agent 2.1 in a default configuration state. There are, however, several LOAD parameters that you can configure for each of the NLM files used with the agent.

You can configure your server to use these options by editing the NMA2.NCF file on your server. Also, if your server is already running, you can unload any of these NLM files and then load them at the NetWare server console using any of the configuration parameters. You can configure these parameters at the NetWare server console or by using one of the NetWare remote consoles: RCONSOLE or XCONSOLE. RCONSOLE for DOS workstations is available at the NetWare server.

XCONSOLE is available with the following Novell® products:

- NetWare Flex/IP™ software
- NetWare/IP™ software
- NetWare NFS*

- NetWare NFS Gateway

The sections that follow describe each of the command-line parameters that you can configure for NetWare Management Agent 2.1.

Load Parameters for SERVINST.NLM

SERVINST.NLM implements the NetWare Server MIB (NWSERVER.MIB). You can load SERVINST.NLM at the command line with any or all of the following parameters:

LOAD SERVINST D U=*n* V B=*n* H

Parameter	Description
D	DisableSets—If this parameter is present, SERVINST.NLM does not allow SNMP SET commands for objects in NWSERVER.MIB. Default: SETS enabled (subject to SNMP security)
U=*n*	UpdateInterval=*n*—Sets the list update interval to *n* (*n* is a value in seconds). This determines how often certain internal lists kept by SERVINST.NLM (such as volumes and queues) are updated. Set this parameter higher, to minimize the number of CPU cycles used by SERVINST.NLM, or lower, to guarantee immediate reporting of server status changes that affect the lists. Default: 300 seconds.
V	Verbose—Displays informational messages. Default: Off.
B=*n*	BuildUserListHour=*n*—The local time each day on a 24-hour clock (0 to 23) at which the SERVINST.NLM software builds a list of users that have access to the server. Default: 2 (2:00 AM).
H	Help—Displays help on command-line parameters. If you use the H parameter, SERVINST.NLM displays the help messages and then exits. It does not remain loaded even if other parameters are entered on the command line.

Load Parameters for HOSTMIB.NLM

HOSTMIB.NLM implements both the standard Host Resources MIB [RFC 1514] and Novell's extensions to the Host Resources MIB (NWHOSTX.MIB). You can load HOSTMIB.NLM at the command line with any or all of the following parameters:

LOAD HOSTMIB.NLM D U=*n* V H

Parameter	Description
D	DisableSets—If this parameter is present, HOSTMIB does not allow SNMP SET commands for objects in RFC1514.MIB or NWHOSTX.MIB. Default: SETS enabled (subject to SNMP security).
U=*n*	UpdateInterval=*n*—Sets the list update interval to *n* (*n* is a value in seconds). This determines how often certain internal lists kept by HOSTMIB.NLM are updated. Set this parameter higher, to minimize the number of CPU cycles used by HOSTMIB.NLM, or lower, to guarantee immediate reporting of server status changes that affect the lists. Default: 60 seconds.
V	Verbose—Displays informational messages. Default: Off.
H	Help—Displays help on command-line parameters. Default: Off.

Load Parameters for NTREND.NLM

NTREND.NLM implements the Threshold and Trend MIB (NWTREND.MIB).

When first loaded, NTREND.NLM automatically sets up trends and thresholds for each monitored attribute according to the server's configuration from values stored in the NTREND.INI file (located in the SYS:\ETC directory). You can edit this file as described in "Setting Default Trends and Thresholds" on page 44.

Thereafter, as configuration changes occur over time, NTREND.NLM adjusts to changes in the number and type of physical network interfaces, queues, volumes, and disks. Default thresholds are set only for important parameters. The user can later use SNMP SET commands to set thresholds for parameters like files read and packets in.

A trend file is created for each monitored attribute instance, even if trending is disabled for that object. The file header contains all the information from nwtControlTableEntry, and the rest of the file stores the sample history (if any). Once a trend file is created, it exists until deleted explicitly by the operator, even if the monitored object (queue, for example) no longer exists. When a monitored object no longer exists, the associated nwtControlStatus is recorded as invalid.

You can load NTREND.NLM at the command line with any or all of the following parameters:

LOAD NTREND D=<*dir*> R V H

Parameter	Description
D= <*dir*>	Directory=<*dir*>—Enables you to specify the volume and directory where NTREND.NLM stores the history data files. Example: To use VOL1: \TEST as the directory for trending files, enter the following command: **LOAD NTREND D=VOL1:\TEST** Default: SYS:\NTREND.
R	Reset—Causes NTREND.NLM to discard all the old trending history data and restart the sampling.
V	Verbose—Displays informational messages. Default: Off.
H	Help—Displays help on command-line parameters. Default: Off.

Load Parameters for FINDNMS.NLM

FINDNMS.NLM discovers workstations running the ManageWise Console by reading its server's bindery and looking for SAP 0x026a, which is broadcast periodically by ManageWise. FINDNMS.NLM then adds the IPX address of the console to the list of stations that want to receive traps. Entries that cease to send SAP packets are removed from the list at an interval set by the aging-period parameter.

Third-party management stations using SNMP over IPX can share this mechanism by broadcasting SAP 0x026a periodically, or they can use the TRAPTARG.CFG method described in "Defining Recipients for SNMP Alarms" on page 55. You can load FINDNMS.NLM at the command line with any or all of the following parameters.

LOAD FINDNMS U=*n* **A=***n* **H**

Parameter	Description
U=*n*	UpdateInterval=*n*—Interval, in seconds, between reads by FINDNMS.NLM of the server's bindery. Default: 300 (5 minutes).
A=*n*	AgingPeriod=*n*—Period, in seconds, to wait before removing stations that have ceased to send SAP packets from the table created by FINDNMS.NLM. Default: 600 (10 minutes).
H	Help—Displays help on command-line parameters. Default: Off.

Setting Default Trends and Thresholds

When NTREND.NLM is first loaded, it obtains the initial (default) values for trends and thresholds from the NTREND.INI file. This file is stored in the NetWare server's SYS:\ETC directory. The initial values in the NTREND.INI file are also used whenever a new trend file is created. A new trend file is created when an instance of a monitored object (volume, disk, interface, and so on) is discovered on the server. Example 4-1 presents a portion of a sample NTREND.INI file.

Example 4-1

Sample NTREND.INI File

```
#-------------------------------------------------------------------------
#               | Sample   | Trend        |         Threshold             |
# Parameter     | Interval | Buckets Enbl | Rising Falling Enbl Type      |
#-------------------------------------------------------------------------
NUMBER_LOGGED_IN_USERS    5          60  1       100     90    1  rising
NUMBER_LOGGED_IN_USERS    7        8928  1        90     81    1  rising

NUMBER_CONNECTIONS        5          60  1         0      0    0  rising
NUMBER_CONNECTIONS        7        8928  1         0      0    0  rising

FILE_READS                5          60  1         0      0    0  rising
FILE_READS                7        8928  1         0      0    0  rising

FILE_WRITES               5          60  1         0      0    0  rising
FILE_WRITES               7        8928  1         0      0    0  rising

FILE_READ_KBYTES          5          60  1         0      0    0  rising
FILE_READ_KBYTES          7        8928  1         0      0    0  rising

FILE_WRITE_KBYTES         5          60  1         0      0    0  rising
FILE_WRITE_KBYTES         7        8928  1         0      0    0  rising

LSL_IN_PACKETS            5          60  1         0      0    0  rising
LSL_IN_PACKETS            7        8928  1         0      0    0  rising

LSL_OUT_PACKETS           5          60  1         0      0    0  rising
LSL_OUT_PACKETS           7        8928  1         0      0    0  rising

NCP_REQUESTS              5          60  1         0      0    0  rising
NCP_REQUESTS              7        8928  1         0      0    0  rising

CPU_UTILIZATION           5          60  1        90     81    1  rising
CPU_UTILIZATION           7        8928  1        80     72    1  rising

CACHE_BUFFERS             5          60  1        45     40    1  falling
CACHE_BUFFERS             7        8928  1         0      0    1  falling

CODE_DATA_MEMORY          5          60  1         0      0    0  rising
CODE_DATA_MEMORY          7        8928  1         0      0    0  rising
```

Once the NTREND.NLM software is running, trend and threshold values can be changed (using the ManageWise Console) by making use of the threshold-setting features of ManageWise. If the server is brought down, it retains the last trend and threshold settings that were set. A NetWare server with NetWare Management Agent 2.1 installed only returns to the initial values of the NTREND.INI file when any of the following situations occurs:

- NTREND.NLM is loaded for the first time.
- NTREND.NLM is loaded with the Reset argument.
- NTREND.NLM is loaded with the Directory argument and the specified directory does not already contain the trend files.
- Trend files have been deleted manually.
- If a system administrator changes the server configuration by adding a new volume, disk, interface, and so on, the trend value of the new device is set to the default value.

Trends are not maintained for CD-ROM volumes. Therefore, changing trend parameters for CD-ROM volumes has no effect.

You can edit the NTREND.INI file to change the initial trend and threshold values of the NTREND.NLM software, as described in the sections that follow.

Changing the Initial Trend Values

The trend values in the NTREND.INI file specify the time interval (Sample Interval) at which a particular trend parameter is sampled, the duration of time for which those samples are kept (Trend Buckets), and whether this sampling parameter is enabled (Enbl). For each value specified by a line in the NTREND.INI file, a trend record is stored in a separate file in the SYS:\NTREND directory by default.

Example 4-2 is an example of a line in the NTREND.INI file for the NUMBER_LOGGED_IN_USERS trend parameter with a Sample Interval of 5, Trend Buckets specified at 60, and the enable parameter specified at 1 (enabled).

Example 4-2
Sample Trend Values

```
#-------------------------------------------------------------------
#                 | Sample   | Trend        |         Threshold         |
# Parameter       | Interval | Buckets Enbl | Rising Falling Enbl  Type |
#-------------------------------------------------------------------
NUMBER_LOGGED_IN_USERS    5        60      1    100     90    1   rising
```

The sections that follow describe how to set or alter each of the parameters required for a trend file.

You can specify more than one sampling interval or duration for any trend parameter by creating another line in the NTREND.INI file. In the sample file in Example 4-1, two time intervals and durations are sampled for each parameter.

Setting the Sample Interval

The NTREND.NLM software enables you to collect samples of a specified parameter at any of 12 possible time intervals (Sample Interval), from 5 seconds to 1 day.

Each of these Sample Intervals is specified by a code number in the NTREND.INI file. Table 4-1 specifies the code used in the NTREND.INI file for each of the Sample Intervals permitted. For example, if you want to sample a particular trend parameter once every hour, you would use the code 9.

Table 4-1
Time Interval Code

Sample Interval	Code
5 seconds	1
10 seconds	2
15 seconds	3

Table 4-1 *continued*
Time Interval Code

Sample Interval	Code
30 seconds	4
1 minute	5
5 minutes	6
15 minutes	7
30 minutes	8
1 hour	9
4 hours	10
8 hours	11
1 day	12

Setting the Trend Buckets

Once you have determined a Sample Interval for collecting samples, you must set a duration of time for which you want to collect samples. For example, if you selected a Sample Interval of one hour for a particular parameter, you might decide that you want to be able to review the state of that parameter for every hour over the duration of a day.

You determine the duration of time for which a parameter is collected by the number of Trend Buckets you specify. You must specify a Trend Bucket for each sample that is collected over a specific period of time. For example, to review the state every hour for 1 day, 24 Trend Buckets (1 per hour x 24 hours in a day) are required.

The number of Trend Buckets required for any particular Time Duration and Sample Interval is calculated easily. However, for your convenience, Table 4-2 shows the number of Trend Buckets required for each Sample Interval allowed, for each of seven possible time durations of from 1 hour to 1 year.

Once the Sample Interval and the Time Duration for trend collection is set, you can compute the size of trend files. The number of Trend Buckets possible, and the approximate size in kilobytes (in

parentheses), for a given Sample Interval and Time Duration are given in Table 4-2. The size of each Trend Bucket is 4 bytes plus 512 bytes for the header file. For example, if the sampling interval is 5 seconds for a period of 1 hour, the file size would be 720 Trend Buckets x 4 bytes long (rounded to the closest 4 KB boundary) plus 512 bytes for a total of 4.5 KB. There are always as many trend files (.NT) as there are enabled trends.

Table 4-2
Trend Buckets Required for Several Possible Durations

Sample Interval	1-Hour Duration	1-Day Duration	1-Week Duration	1-Month Duration	3-Month Duration	6-Month Duration	1-Year Duration
5 seconds	720	17280	120960	535680	1607040	3214080	63076400
(KB)	(4)	(72)	(488)	(2144)	(6432)	(12860)	(252308)
10 seconds	360	8640	60480	267840	803520	1607040	3153600
(KB)	(4)	(36)	(244)	(1072)	(3216)	(6432)	(12616)
15 seconds	240	5760	40320	178560	535680	1071360	2102400
(KB)	(4)	(24)	(164)	(716)	(2144)	(4284)	(8412)
30 seconds	120	2880	20160	89280	267840	535680	1051200
(KB)	(4)	(16)	(84)	(360)	(1072)	(2144)	(4208)
1 minute	60	1440	10080	44640	133920	267840	525600
(KB)	(4)	(8)	(44)	(180)	(540)	(1072)	(2104)
5 minutes	12	288	2016	8928	26784	53568	105120
(KB)	(4)	(4)	(12)	(40)	(108)	(216)	(424)
15 minutes	4	96	672	2976	8928	17856	35040
(KB)	(4)	(4)	(4)	(16)	(40)	(72)	(144)
30 minutes	2	48	336	1488	4464	8928	17520
(KB)	(4)	(4)	(4)	(8)	(20)	(40)	(72)
1 hour	1	24	168	744	2232	4464	8760
(KB)	(4)	(4)	(4)	(4)	(12)	(20)	(36)
4 hours		6	42	186	558	1116	2190
(KB)		(4)	(4)	(4)	(4)	(8)	(12)
8 hours		3	21	93	279	558	1095
(KB)		(4)	(4)	(4)	(4)	(4)	(8)

Table 4-2 *continued*

Trend Buckets Required for Several Possible Durations

Sample Interval	1-Hour Duration	1-Day Duration	1-Week Duration	1-Month Duration	3-Month Duration	6-Month Duration	1-Year Duration
1 day		1	7	31	93	186	365
(KB)		(4)	(4)	(4)	(4)	(4)	(4)

Once a particular time duration is exceeded for a file (all the Trend Buckets have been filled), NTREND.NLM keeps adding the most recent sample by overwriting the oldest. This means that the file contains the most recent duration recorded. For example, if you select a Sample Interval of 1 hour for a duration of 24 hours (using 24 Trend Buckets), the associated file contains the trend data for the last 24 hours.

Enabling or Disabling a Trend File

Each line in the NTREND.INI file contains a parameter that either enables or disables the NTREND.NLM software to begin creating a trend file at startup. The total number of trend files is equal to the number of lines in the NTREND.INI file. To enable the collection of data for a trend file, set this parameter to 1. To disable the collection of data for a trend file at startup, set this parameter to 0.

Backing Up Trend Data

Trend data is not automatically backed up. If you feel the need to back up this data, please do so manually.

Changing the Initial Threshold Values

The default threshold values in the NTREND.INI file specify when a trap is generated. User-defined values are stored in the trend file (.NT) header. If the parameter rises above or falls below the set threshold value, a rising or falling trap type is sent. Example 4-3 is an example of a line in the NTREND.INI file for the NUMBER_LOGGED_IN_USERS Trend Parameter with a Threshold Range of 90 percent to 100 percent. This implies that the threshold is 100 percent, while the lower marker is

90 percent. In Example 4-3, the falling threshold indicates the lower marker.

Example 4-3
Sample Trend Values

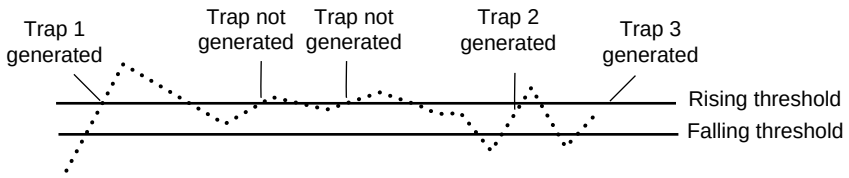
```
#-------------------------------------------------------------------------
#                  | Sample   | Trend        |         Threshold          |
# Parameter        | Interval | Buckets Enbl | Rising Falling Enbl  Type |
#-------------------------------------------------------------------------
NUMBER_LOGGED_IN_USERS    5        60      1    100     90    1   rising
```

The sections that follow describe how to set or alter each of the parameters required for a threshold value.

Setting Rising and Falling Thresholds

Each line in the NTREND.INI file contains a parameter for the Rising Threshold and the Falling Threshold. For each Sample Interval, a rising or falling trap can be generated as specified. After a trap is generated, another such trap is not generated until the sampled value falls below this threshold and reaches the falling threshold. Figure 4-1 provides an example of this process for a Rising Threshold trap.

Figure 4-1
Rising Threshold



In this example, Trap 1 is generated because it is the first time that the parameter value rises above the Rising Threshold. The next two times the parameter value rises above the Rising Threshold, a trap is not generated because the parameter did not fall below the Falling Threshold. Trap 2 and Trap 3 are generated because the parameter value dropped below the Falling Threshold before exceeding the Rising Threshold.

In Example 4-3, a Rising Trap is generated the first time that the NUMBER_LOGGED_IN_USERS parameter exceeds the Rising Threshold value of 100. For a second Rising Trap to be generated, the parameter must fall below the Falling-Threshold of 90, and then exceed the Rising Threshold of 100 again.

Enabling or Disabling a Threshold Trap

Each line in the NTREND.INI file contains a parameter that enables or disables the NTREND.NLM software to send traps as determined by the Rising and Falling Thresholds. This parameter is set to 1 to enable the software to send a trap for the values given, or to 0 to disable the software from sending a trap for this parameter.

Controlling Alarm Generation

The NWTRAP.NLM configuration file is NWTRAP.CFG, which is stored in the SYS:\ETC directory. The configuration file is read only when NWTRAP.NLM is loaded; therefore, any changes made to the file do not take effect until the next time you load NWTRAP.NLM.

On a NetWare 3.1*x* server, EDIT.NLM does not have a large enough buffer to edit the NWTRAP.CFG file. To edit the NWTRAP.CFG file, map a drive to the server SYS: volume and proceed from there.

You can use the NWTRAP.NLM configuration file to configure or change any of the following:

- Types of alarms NWTRAP.NLM forwards to management stations, including ManageWise.
- Community strings NWTRAP.NLM uses.
- Time interval during which NWTRAP.NLM ignores duplicate alarms.
- List of traps to be disabled, using the *mask* keyword.
- Minimum severity of alarms NWTRAP.NLM forwards to the management station.
- Specific alarms that you want to prevent NWTRAP.NLM from forwarding.

The configuration file consists of keywords and their associated data (case is ignored). Each keyword must be on a line by itself (except for mask values, where they might span several lines), and must be followed by one or more lines of associated data. Keywords are *community*, *time interval*, *mask*, and *severity*.

You can place comments anywhere in the file, even between a keyword and its associated information. A comment starts with a number sign (#), and continues to the end of the line.

Example 4-4 is an example of an NWTRAP.CFG file.

Example 4-4

Sample NWTRAP.CFG File

```
#
#################################################################
# NWTRAP.CFG
#
# NWTRAP Configuration File
#
# This file specifies information to be used by NWTRAP.NLM
# The file is read and the parameters set when NWTRAP is loaded.It must
# reside on volume SYS: in the directory SYS:\ETC and must be named
# NWTRAP.CFG to be found by NWTRAP. To change the parameters, first edit
# this file, then unload NWTRAP and load it again. Any changes to this file
# will not take effect until NWTRAP is next loaded. The parameters
# are specified by using a parameter keyword followed by the desired
# parameter value.
#
#################################################################################

Community
        Public
Time Interval
        10
Severity
        Warning

mask
#        "Memory: Short term alloc failed"
#         1


#        "FileSys: Directory write err (no vol)"
#         2

#        "FileSys: File write err, by server (no path)"
#         3

#        "FileSys: File write err, by user (no path)"
#         4
```

Defining the Community String

Use the *community* keyword to define the community string to be used in the traps generated. The length of the community string is restricted to 32 bytes and cannot contain space (except between quotes), tab, square bracket, equal sign, colon, semicolon, or number sign (#) characters.

The default string is *public*.

Setting the Time Interval

Sometimes an alarm repeats rapidly (several times per second or per minute) with identical or nearly identical parameters. When this occurs, the second and later alarms *within a time interval* are *usually* not as interesting as the first alarm.

To prevent the network and the management station from being inundated with identical alarms, you can specify a time interval to be applied to every alarm generated by ManageWise. During this interval, alarms that are identical to an initial alarm are discarded.

You can define the time interval in the configuration file as follows:

```
Time Interval
n
```

where *n* can take any value between 0 and 232, inclusive, to indicate the number of seconds that must elapse before a later alarm is not discarded.

The default time interval is 10 seconds.

Using Masks

Use the *mask* keyword to provide a list of traps to be disabled. NWTRAP.NLM never forwards these traps to the management stations. You can use a comma (,), a space, or a return (Enter) as a delimiter between trap numbers.

The NWTRAP.CFG file lists each of the traps that can be sent from NetWare Management Agent 2.1 and its trap number. The trap name is

on one line and the trap number is on the following line. The following example shows the first three entries of the mask section in the NWTRAP.CFG file:

```
mask
#    "Memory: Short term alloc failed"
#    1
#    "FileSys: Directory write err (no vol)"
#    2
#    "FileSys: File write err, by server (no path)"
#    3
```

The default state of the file is for these statements to be disabled by placing a number sign (#) before the statement. In addition, the *mask* keyword is not disabled initially because trap 46, *Router configuration error # 1*, is masked out by default.

- To disable a particular trap, locate it in the NWTRAP.CFG file and remove the number sign preceding the trap number.
- If you do not want to mask any traps, be sure that the *mask* keyword is disabled to avoid generating an NWTRAP.CFG parse error.

The default is to not disable any specific trap. All traps are sent, except those filtered by the severity level configured.

Configuring Alarm Severity Levels

Use the *severity* keyword to set a minimum alarm severity level so that traps for lesser severity alarms are not sent.

The severity levels you can set in the NWTRAP.CFG file are *informational*, *warning*, *recoverable*, *critical*, and *fatal*.

When you set a severity level of *informational*, all traps are forwarded. When you set a severity level of *fatal*, no traps are forwarded because there are no fatal traps in the NWTRAP.CFG file.

NetWare defines seven severity levels (adding *operation aborted* and *unrecoverable*). NWTRAP.NLM translates them to the SNMP severity levels shown in Table 4-3. The table also shows the corresponding ManageWise Console severity levels.

Table 4-3
Comparison of NetWare, SNMP, and ManageWise Severity Levels

NetWare Severity Level	SNMP Severity Level	ManageWise Console Severity Level
0 - Informational	Informational	Informational
1 - Warning	Minor	Minor
2 - Recoverable	Major	Major
3 - Critical	Critical	Critical
4 - Fatal	Fatal	Critical
5 - Operation Aborted	Fatal	Critical
6 - Unrecoverable	Fatal	Critical

The default is *warning*. Under the default, all alarms with a severity level of *warning* or greater are forwarded.

Defining Recipients for SNMP Alarms

You can configure NetWare Management Agent 2.1 to send SNMP traps (alarms) to your ManageWise Console or to other management nodes. The NetWare Management Agent software has two ways to determine where to send alarms, which are described in the following sections.

Automatic Discovery Using FINDNMS.NLM

ManageWise Consoles use the SAP value to identify themselves to NetWare Management Agent 2.1 software installed on NetWare servers. NetWare Management Agent 2.1 uses FINDNMS.NLM on the NetWare server to identify SAP packets being sent by a ManageWise Console and directs traps to that console.

The list of trap-recipient consoles is dynamic. Consoles that do not send SAP packets regularly are removed from the list. The list of trap recipients is available in the FINDNMS.ADR file in the server's SYS:\ETC directory.

Third-party management consoles that use SNMP over IPX can also use this feature. To do this, they must broadcast the SAP ID number 0x026a periodically. NetWare Management Agent 2.1 then adds their IPX addresses to the list of recipient stations.

Editing the TRAPTARG.CFG File Manually

In addition to the automatic discovery feature, trap recipients can be added manually to a NetWare server using NetWare Management Agent 2.1. This is useful for having traps sent to network management consoles other than ManageWise, for working with networks where SAP filtering makes automatic discovery impossible, and for receiving traps on networks other than IPX networks.

You must add trap recipients manually by specifying their addresses in the TRAPTARG.CFG file, which is located in the SYS:\ETC directory of all NetWare servers.

The TRAPTARG.CFG file defines the recipients of SNMP traps. You can use this file to define recipients of SNMP traps over IPX and over UDP/IP. The file is fully disabled to show you how to divide the file into IPX and UDP/IP sections and how to write the IPX and IP addresses of recipients.

The TRAPTARG.CFG file is read only when SNMP is loaded. In most cases, this means bringing the server down and restarting it because a variety of modules must be unloaded and reloaded as well. Thus, any changes made to the TRAPTARG.CFG file do not take effect until the next time you load NWTRAP.NLM.

If you are sending traps to third-party management stations, you might need to integrate the NetWare Server trap MIB into those management stations. The MIB can be found in the NWALARM.MIB file on the NetWare Management Agent *Agent Diskette*.

Note The NWALARM.MIB file imports symbols from the Host Resources MIB (RFC1514.MIB), which is also on the NetWare Management Agent *Agent Diskette.*

Consult your management station documentation for further information about integrating the trap MIB.

Configuring the ManageWise Console to Not Send SAP Packets

Each ManageWise Console sends a SAP packet with the ID number 0x026a. FINDNMS.NLM uses this packet to identify consoles that it should send traps to. This procedure can create excessive traffic on remote links. This is a particular problem for on-demand, dial-up connections, which can be kept up almost constantly by this process.

To configure the ManageWise Console to not send SAP packets, follow these steps:

Procedure

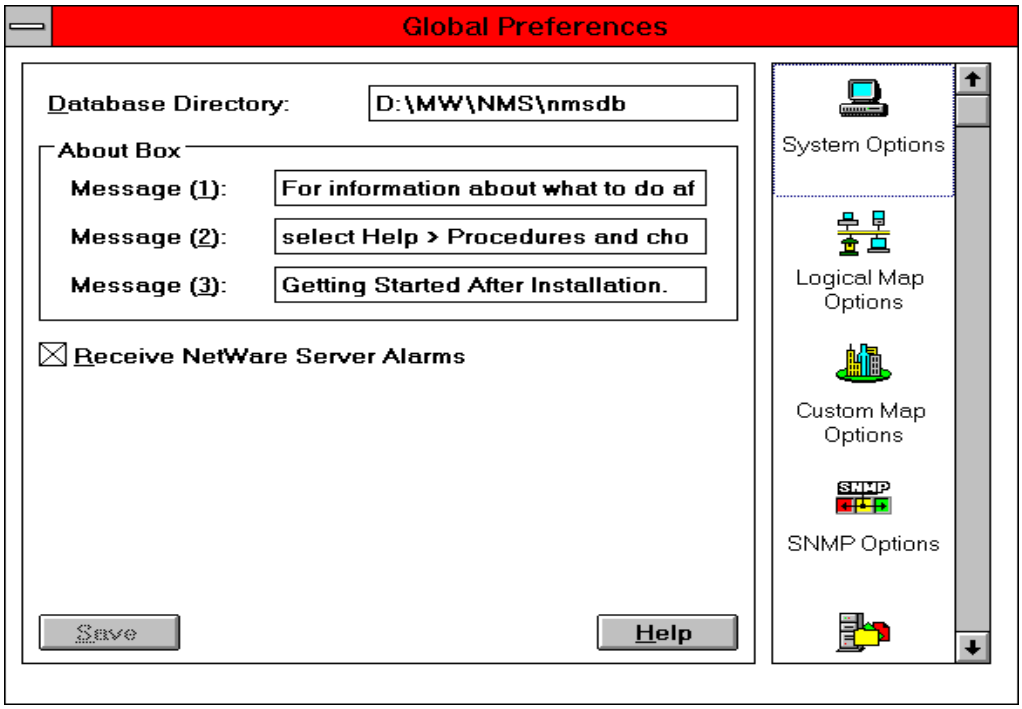
1. **To define the recipients of SNMP traps, follow the instructions in “Editing the TRAPTARG.CFG File Manually” on page 56.**

2. **From the ManageWise Console window, select *Configure* > *Global Preferences*.**

   The System Options Global Preferences dialog page is displayed.

   It is identified by the highlighted icon on the right side of the dialog box.

Figure 4-2
Global Preferences



3. **Deselect the Receive NetWare Server Alarms check box.**

   The ManageWise Console no longer sends SAP packets. However, ManageWise might have already sent a SAP packet. In this case, the address of the console is in the server's memory and remains so until it is removed. The default value for removing the console's address is 10 minutes. This value can be altered as described in "Load Parameters for FINDNMS.NLM" on page 43.

Index

A

B

C

F

G

H

I

L

M

N

O

R

S

T

U

X