Solstice NFS Client User's Guide for Microsoft Windows 95 and Windows NT

Sun Microsystems, Inc.
901 N. San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part No: 805-6572–10
June 1998, Revision A

Contents

Preface xix

1. Installing Solstice NFS Client 1

System Requirements 1

Questions Asked During Installation 2

Serial Number 2

Installation Directory 2

Setup Type 3

PC-CacheFS Preferences 4

License Server 4

Name Service 5

Installing Solstice NFS Client 6

▼ To Install Solstice NFS Client 6

Creating a Silent Installation 6

▼ To Create a Silent Installation 7

▼ To Run a Silent Installation 7

Automating Installation 8

▼ To Create an Installation Script 8

Uninstalling Solstice NFS Client 9

▼ To Uninstall Solstice NFS Client 9

2. Setting Up Serial Connections 11

Gathering Information 11

Installing Dial-Up Networking on Windows 95 12

▼ To Install Dial-Up Networking 12

Setting Up a Serial Connection to a PPP Server on Windows 95 13

▼ To Create a Dial-Up Connection 13

▼ To Set Up TCP/IP Properties 14

▼ To Configure the Authentication Server 14

▼ To Log In and Connect to a PPP Server 15

Adding and Removing an NFS Server 16

▼ To Add an NFS Server 16

▼ To Remove an NFS Server 17

Setting Up a Serial Connection to a PPP Server on Windows NT 17

▼ To Add Remote Access Service 17

▼ To Create a Dial-Up Connection 18

▼ To Configure an Authentication Server 18

▼ To Grant Dialin Permission to a User 19

▼ To Log In and Connect to a PPP Server 19

▼ To Log In to the Solstice Network 21

Troubleshooting 22

3. NFS File Services 27

Accessing NFS File Systems 27

Accessing NFS Servers 28

How UNC and NFS Names Differ 28

Aliasing Multilevel Directories on Windows 95 29

Aliasing Multilevel Directories on Windows NT 30

Mapping Network Drives 31

Browsing NFS Servers 35

▼ To Browse for NFS Servers on Windows 95 35
▼ To Browse for NFS Servers on Windows NT 36
▼ To Add an NFS Server Outside the Local Subnet on Windows 95 37
▼ To Add an NFS Server Outside the Local Subnet on Windows NT 37
▼ To Remove an NFS Server Outside the Local Subnet on Windows 95 38
▼ To Remove an NFS Server Outside the Local Subnet on Windows NT 38
Browsing NFS Automount Maps 39
Configuring NIS or NIS+ 40
▼ To Configure NIS or NIS+ 41
▼ To Browse NFS Automount Maps on Windows 95 41
▼ To Browse NFS Automount Maps on Windows NT 42
User Profiles and Connected Drives 43
▼ To Set Up Custom User Profiles on Windows 43
Accessing WebNFS Servers 44
About the WebNFS Protocol 44
About the WebNFS Client 44
Mapping a WebNFS Drive 45
▼ To Map a Network Drive Using WebNFS 46
Browsing WebNFS Servers 46
Customizing Solstice NFS Client 46
Setting General Preferences 47
Setting Security Preferences 47
Setting Caching Preferences 48
Setting Tuning Preferences 49
Setting Files and Folders Preferences 49
Setting Advanced Preferences 51
▼ To Change Default Settings for Solstice NFS Client Properties 52
Changing Mount Options for Specific Connections 53

Troubleshooting 55

Checklist for TCP/IP Settings on Windows 95 57

Checklist for TCP/IP Settings on Windows NT 58

4. NFS Server 61

About NFS Server 61

Enabling NFS File Services 62

▼ To Enable File Sharing on Windows NT 62

▼ To Enable File and Printer Sharing on Windows 95 63

NFS Server on Windows NT 64

Running NFS Server 65

▼ To Start NFS Server from the Local System Account 65

▼ To Start NFS Server from a Specific User Account 65

▼ To Stop NFS Server 66

Granting Access to Shared Resources on Windows NT 66

▼ To Share Folders and Drives 66

▼ To Remove Access to Shared Resources on Windows NT 67

Viewing Exported Folders and Drives on Windows NT 68

▼ To View a List of Exported Folders and Drives 68

How NFS Server Handles Access Requests from Remote Hosts 68

Security Control When Sharing Folders and Drives 69

Logging NFS Server Events on Windows NT 70

▼ To Enable NFS Server Event Logging Using Solstice Network Event Log 70

▼ To Configure Network Event Log for NFS Server Events 71

▼ To View NFS Server Events Using Event Viewer 71

NFS Server on Windows 95 72

Sharing Directories and Devices 72

Running NFS Server 72

Sharing Properties 73

▼ To Start NFS Server 73

▼ To Suspend NFS Server 73

▼ To Resume NFS Server 73

Granting Access to Shared Resources on Windows 95 73

▼ To Grant Access to Shared Resources 73

▼ To Revoke Access to Shared Resources 74

Logging NFS Server Events on Windows 95 75

▼ To Enable NFS Server Logging 75

▼ To Configure Network Event Logging 76

▼ To Disable NFS Server Logging 76

5. Printing 77

Setting Up Printing 77

Road Map for Printer Setup 78

Setup Requirements for Print Servers 78

Setup Requirements for Print Clients 79

Browsing for Network Printers 81

▼ To Browse for PCNFSD Printers on Windows 95 81

▼ To Browse for Printers on Windows NT 82

Mounting Network Printers on Print Clients 83

Specifying Which Print Protocols to Use 83

▼ To Mount a Network Printer on Windows 95 83

▼ To Mount Network Printers on Windows NT 84

▼ To Delete Printer Ports on Windows NT 85

Mounting Shared PC Printers in a UNIX Environment 86

▼ To Mount a Shared PC Printer from a UNIX Workstation 86

Enabling DOS Printing 87

Enabling DOS Printing on Windows 95 87

Enabling DOS Printing on Windows NT 88

Viewing Print Jobs 88

▼ To View Print Jobs on Windows 95 and Windows NT 89

▼ To View Print Jobs on UNIX Systems 89

Sharing Local Printers on Windows NT 90

▼ To Add the TCP/IP Print Server Service 90

▼ To Configure a Local NT Printer as a Shared Network Printer 91

Logging Print Events on Windows NT 92

▼ To Enable Auditing 92

▼ To Set Up Logging for Print Events 92

▼ To View Logged Print Events 93

Providing LPD Print Services on Windows 95 93

Setting Up an LPD Shared Network Printer 94

▼ To Set Up the LPD Server 94

▼ To Enable Print Requests From Network Users 95

Starting LPD Print Server 96

▼ To Start LPD Print Server Automatically 96

▼ To Start LPD Print Server Manually 96

Stopping LPD Print Server 97

▼ To Stop (or Disable) LPD Print Server 97

Adding a Shared Printer to a Users' Work Environment 97

▼ To Add a Shared Printer to a PC Environment 97

▼ To Add a Shared Printer to a UNIX Environment 98

Managing LPD Printing 99

▼ To View Print Jobs in a PC Windows Environment 99

▼ To View Print Jobs in a UNIX Environment 99

Working with the LPD Print Server Log File 100

▼ To View and Print the LPD Print Server Log File 100

▼ To Purge the LPD Print Server Log File 100

Turning Off a PC With a Shared Printer 100

Turning Off a Shared PC Printer 101

Interpreting Carriage Returns and Line Feeds 101

Troubleshooting LPD Print Servers 102

Troubleshooting Printing Problems 102

6. Managing Work Environments 105

User Work Environments 105

Management Tools 106

Setting Up the Authentication Server 107

▼ To Set Up an Authentication Server 107

User Profiles 108

Using User Profiles on Windows NT 108

Using User Profiles on Windows 95 108

Updating User Profiles 109

Setting Up Roaming User Profiles 110

▼ To Set Up Roaming User Profiles on Windows NT 110

▼ To Set Up Roaming User Profiles on Windows 95 112

Setting Up Mandatory User Profiles 113

▼ To Set Up Mandatory User Profiles on Windows NT 113

▼ To Set Up Mandatory User Profiles on Windows 95 113

System Policies 114

Creating System Policy Files 115

How System Policies Work 115

How System Policies Differ From Mandatory User Profiles 116

▼ To Set Up System Policy Files 116

▼ To Create a System Policy File on Windows NT 117

▼ To Install System Policy Editor on Windows 95 117

▼ To Create System Policies for Users or Computers on Windows 95 118

▼ To Create Group Policies on Windows 95 119

Logon Scripts 119

When a User Logs In 119

▼ To Create a Logon Script for Windows 95 Clients 120

▼ To Create a Logon Script for Windows NT Clients 120

Example Logon Scripts 120

SNC Scripts 122

Scripting on PC-Admin and Solstice Network Client Computers 122

Running SNC Scripts 123

▼ To Adapt PC-Admin SNC Scripts 124

Running the Script Interpreter 124

SNC Scripts on PC-Admin Clients and Solstice NFS Clients 125

Environment Variables Local to SNC Scripts 127

System Policies, User Profiles, and Scripts in an NT Domain 127

Troubleshooting 128

7. Logging In to Windows NT and Windows 95 Clients 131

Logging In and Changing Passwords on Windows NT 131

▼ To Log In to a Solstice network from Windows NT 131

▼ To Change the UNIX Password in Windows NT 132

Synchronizing Windows NT and UNIX Passwords 133

▼ To Enable Password Synchronization in Windows NT 133

▼ To Change Both UNIX and NT Passwords in Windows NT 134

Logging In and Changing Passwords on Windows 95 135

▼ To Log In to a Solstice network from Windows 95 135

▼ To Synchronize a UNIX and Windows 95 Login Password 136

▼ To Change the UNIX Password on Windows 95 138

Troubleshooting 140

8. PC-CacheFS 143

About PC-CacheFS 143

What You Need to Know About Cache Security 144

Starting PC-CacheFS 144

▼ To Start the PC-CacheFS Monitor 144

Managing the Cache 145

▼ To Set Up the Cache 145

Flushing the Cache 146

▼ To Flush the Cache 146

Deleting and Restoring the Cache 146

▼ To Delete the Cache 146

▼ To Restore the Cache 147

Customizing PC-CacheFS 147

Directory Caching 147

Directory Time-out 148

File Time-out 148

Read or Write Size 149

▼ To Change Advanced Settings 149

Using Cache Statistics 150

Cache-Hit Rate 150

Capacity 151

Relative Performance 151

Resetting Cache Statistics 152

A. Frequently Asked Questions 153

NFS Client 153

NFS Server 155

LPD Printing 156

PC-CacheFS 157

B. Setting Up PCNFSD 159

UNIX Server Requirements 159

PCNFSD Daemon Overview 160

Services Provided by rpc.pcnfsd 160

Authentication and System Security 160

Shared Printer Support 161

Support for User Views and Site Policies 161

Determining if rpc.pcnfsd Is Already Installed 162

▼ To See if rpc.pcnfsd Is Installed 162

▼ To See if rpc.pcnfsd Is Running 162

Deciding Where to Install rpc.pcnfsd 163

Installing rpc.pcnfsd 163

▼ To Install rpc.pcnfsd on a Server Running the SunOS 5.4 Operating System or compatible Verstions 163

▼ To Install rpc.pcnfd on a Server Running the SunOS 4.0 Operating System or Compatible Versions 165

Upgrading the PCNFSD Daemon 167

▼ To Determine if Version 2 Is Running 167

▼ To Upgrade rpc.pcnfsd on a Server Running the SunOS 4.0 Operating System or Compatible Version 168

Configuring the PCNFSD Daemon 169

Non-SunOS Platforms Installation 169

C. SNC Script Directives 171

Script Interpreter Command 171

SNC Script Directives 172

COPY *source_file destination_file* 172

DELETE *file1 dir1 file2 file3* ... 172

ECHO [ON | OFF] ECHO *text_string* 173

EXIT *exit_value* 173

EXPORT *varname* 173

GOTO *label* 173

IF [NOT] *condition statement* 174

INCLUDE *snc_filename* 174

INI *ini_file_pathname section* [*entry*=[*value*]] 174

LAUNCH *filename* [*options*] 175

LOGIN 175

LOGOUT 175

MKDIR *dirname1 dirname2* 175

MOUNT [-o *option*,*option*,...] DRIVE *server*:/*dir1*/*dir2 drive* 176

MOUNT PRINTER 179

PAUSE *number* 179

REG DELKEY *keypath* 179

REG DELVAL *keypath value_name* 179

REG NEWKEY *keypath* 179

REG *type keypath value_name value* 180

REM *comment text* 181

RESERVE 181

SET [*value_source*] *varname*=*value_specifier* 181

STOP 184

UMASK *octal_tuple* 184

UNMOUNT [DRIVE *drive*: | PRINTER *lpt_device*:] 185

Environment Variables Local to SNC Scripts 185

Index 187

Tables

TABLE 2–1 Troubleshooting 22

TABLE 2–2 Solutions to Problems Logging In 23

TABLE 2–3 Solutions to Common Problems Connecting to the Network 24

TABLE 3–1 Problems Using Network File Services 55

TABLE 5–1 Tasks Needed to Configure and Set up Print Servers for PCNFSD-based Jobs 78

TABLE 5–2 Tasks Needed To Configure and Set Up Print Servers for LPD-based Jobs 79

TABLE 5–3 Tasks Needed to Send PCNFSD-based Jobs 79

TABLE 5–4 Tasks Needed to Send LPD-based Jobs 80

TABLE 5–5 Print Commands for the Solaris 2.6 Operating Environment or Compatible Version 89

TABLE 5–6 Printer Driver Interpretation of Carriage Returns and Line Feeds 101

TABLE 5–7 Frequent Printing Problems 102

TABLE 6–1 Comparison of Features on PC-Admin Client and Solstice Network Client 122

TABLE 6–2 Troubleshooting on Windows NT 128

TABLE 6–3 Troubleshooting on Windows 95 129

TABLE 7–1 Common Error Messages 140

TABLE 7–2 Possible Solutions 141

Figures

Figure 2–1 Changing the Default Authentication Server 15

Figure 2–2 NFS Servers Dialog Box 16

Figure 2–3 Solstice NFS Client Dialog Box 20

Figure 2–4 Solstice NFS Client Login Dialog Box 20

Figure 2–5 Solstice NFS Client Dialog Box 21

Figure 2–6 Solstice NFS Client Login Dialog Box 21

Figure 3–1 Mapping a Network Drive on Windows 95 32

Figure 3–2 Mapping a Network Drive on Windows NT 33

Figure 3–3 Browsing NFS Servers in Network Neighborhood 35

Figure 3–4 NFS Servers Listed in Network Neighborhood 35

Figure 3–5 Selecting Solstice_NFS_Client Workgroup 36

Figure 3–6 NFS Servers in Network Neighborhood on Windows NT 36

Figure 3–7 Add/Remove NFS Servers Dialog Box 37

Figure 3–8 A Home Automount Map 40

Figure 3–9 A Master Automount Map 40

Figure 3–10 NFS Automount Maps Listed in Network Neighborhood 42

Figure 3–11 Solstice NFS Client Properties Dialog Box 53

Figure 4–1 Select Network Service Dialog Box 63

Figure 4–2 Selecting Solstice File and Printer Sharing 63

Figure 5–1 Browsing for Printers 82

Figure 5–2 Add Printer Wizard Dialog Box 84

Figure 8–1 PC-CacheFS Monitor – Expanded 145

Preface

This *Solstice NFS Client User's Guide* explains how to install, use, and manage Solstice™ NFS™ Client™ software on your network.

Who Should Use This Book

This guide contains instructions for users of Solstice NFS Client installed on a Windows 95 or Windows NT system, or anyone helping users to manage this software on a network.

How This Book Is Organized

This manual is organized as follows:

Chapter 1, describes how to install the software components that make up the Solstice NFS Client product.

Chapter 2, describes how to set up a serial connection to a PPP server from a computer running Solstice NFS Client software.

Chapter 3, explains how to access files and devices across the network using NFS file services.

Chapter 4, describes how to set up, use, and manage NFS Server software on your computer. NFS Server enables you to share files and directories with other computers on the network.

Chapter 5, describes how to set up and manage printing and how to share a printer from your computer.

Chapter 6, provides information about how to use system policy files, user profiles, and SNC scripts to manage clients from a UNIX® server.

Chapter 7, describes how to log in to a client and change your UNIX password.

Chapter 8, describes the PC-CacheFS™ program and explains how to use it to improve the performance of your CD-ROM and network drives.

Appendix A, lists some typical questions users would ask about the product components and provides answers.

Appendix B, describes how to set up the PCNFSD software on a Solaris server.

Appendix C,“ lists and describes the commands used in SNC scripts. SNC scripts can be used to manage clients on the network.

Related Books

Solstice Network Client Installation and Licensing Guide—Refer to this book for complete information on installing, setting up, and licensing Solstice NFS Client software.

Solstice Network Client Administration and Maintenance Guide—Refer to this book for information on how to set up and administer your Solstice network. This book also contains information about managing clients using system policy files, user profiles, and SNC scripts.

Consult your Solaris documentation, or books such as *Managing NFS and NIS* (O’Reilly & Associates, 1991), for specific information about NFS performance.

Other Sources of Information

The Solstice Network Client Web page at `www.sun.com/netclient/` includes the following links which you may find useful:

- News and Updates, providing updates to the release notes, tips and workarounds, and similar technical information
- Solstice FAQ, containing frequently asked questions about using Solstice Network Client
- White papers, listing technical backgrounders for Sun software products; look in the Client Solutions section for the Solstice Network Client white paper

- *Solstice Network Client Today*, a news magazine presenting articles of interest to users of Solstice Network Client.

What Typographic Changes Mean

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

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

Shell Prompts in Command Examples

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

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`

Shell	Prompt
Bourne shell and Korn shell prompt	$
Bourne shell and Korn shell superuser prompt	#

CHAPTER 1

Installing Solstice NFS Client

This chapter describes how to install and configure the Solstice NFS Client software on Windows 95 and Windows NT systems, how to create a silent installation, how to create custom installation scripts for batch installations, and how to uninstall the product.

The installation instructions assume you are installing Solstice NFS Client from a Web site. If you are installing over a network connection or from a CD-ROM, follow the instructions in *Solstice Network Client QuickStart* or *Solstice Network Client Installation and Licensing Guide.*

You can read the background information, or consult the references below to go directly to the specific topic.

- "System Requirements" on page 1
- "Questions Asked During Installation" on page 2
- "Installing Solstice NFS Client" on page 6
- "Creating a Silent Installation" on page 6
- "Automating Installation" on page 8
- "Uninstalling Solstice NFS Client" on page 9

System Requirements

Be sure your computer meets these requirements before installing Solstice NFS Client.

- IBM-compatible computer with 80486 or Pentium CPU
- 16 Mbytes RAM

- VGA / MVGA (640x480) or higher resolution graphics capability
- 2 Mbytes free disk space (or less depending on components installed)
- Microsoft Windows 95 or Windows NT
- Microsoft TCP / IP network protocol stack

Questions Asked During Installation

During installation, you are asked to provide the following information. Some installation screens only appear if you choose to install using Custom setup.

- Your name and your company name
- Serial number
- Installation directory
- Setup type
- Authentication server (Custom setup)
- Enable file locking / sharing (Custom setup)
- Enable user work environment (Custom setup)
- PC-CacheFS preferences (Custom setup)
- License Server (Custom setup)
- NIS / NIS+ name server

Serial Number

Enter a valid serial number from your license certificate or click the Evaluation button. An evaluation license allows you to use the software for a period of 30 days. This license must be replaced by a permanent license before the expiration date if you want to continue using the software.

Installation Directory

The default is to install the Solstice NFS Client software into the directory `C:\Program Files\Solstice`. If this directory does not exist, you can choose to create it during installation. You can also choose to install NFS Client into an alternate directory.

Setup Type

Choose the setup type to determine which components are installed on your computer.

- Typical – Installs the full Solstice NFS Client product: NFS and Printing support, NFS Server, Printer Server, and PC-CacheFS.
- Compact – Installs a portion of Solstice NFS Client: NFS and Printing support, and PC-CacheFS.
- Custom – Allows you to choose which components and subcomponents to install. Select the component and click Change to see the list of subcomponents for that component.

Authentication Server

If you choose Custom as the setup type, you can specify an authentication server or select Broadcast (the default). The authentication server is the server running the `rpc.pcnfsd` daemon.

If you specify an authentication server, your client will use only the specified server to check user permissions.

If you select Broadcast, the client will broadcast for an authentication server. Solstice Network Client uses the first server that responds to the broadcast.

Enable or Disable File Locking/Sharing

If you choose Custom as the setup type, you can enable or disable file locking/sharing. Some applications (MS Office, for example) use file locking to request exclusive access to data files. If you are working in a network environment that allows other users to access files you are working on, enabling the file locking/sharing option will safeguard the data in your files.

Some servers do not support file locking (Solstice NFS Server, for example). If you enable file locking/sharing and then attempt to mount drives from an NFS server that does not support file locking, you will not be able to map drives, browse exports, or read and write files on that server.

The default is to disable file locking/sharing.

Enable User Work Environments

If you choose Custom as the setup type, you can select whether or not to mount the `/opt/MSPolicy` directory from the PCNFSD server. Support for user views, site policies, and script interpreter requires the administrator to create a directory named `/opt/MSpolicy` on the PCNFSD server. By default, this directory is mounted by the client during login.

If you disable this option, the client will not mount the `/opt/MSPolicy` directory. However, with this option disabled, you will not be able to run the script interpreter or download user profiles directly from the selected PCNFSD server.

If you enable this option (the default), the client will attempt to mount the `/opt/MSPolicy` directory. This will increase login time slightly.

For more information about managing Windows 95 and NT clients see the *Solstice Network Client Administration and Maintenance Guide.*

PC-CacheFS Preferences

PC-CacheFS uses a location on your hard drive to cache or store data. When you open a file on a network drive, the file is written to the cache. This may improve network performance, especially over a serial connection. If you select Typical setup during installation, PC-CacheFS uses default settings. If you select Custom setup, you can customize the following settings:

- Cache on Drive – Designate a drive that PC-CacheFS will use to hold the cached information. Be sure you have enough space on this drive to accommodate the cache.
- Size – You can limit the size of the cache buffer. The default limit for the size of the cache is determined from the amount of available disk space.
- Drives to Cache – By default, PC-CacheFS caches files that you access from any network drives currently mapped and all new drives as they are added. You can choose to:
  - Select which currently mapped network drives to cache
  - Cache files read from the CD-ROM
  - Cache all currently mapped network drives
  - Cache all new drives when they are mapped

License Server

If you choose Custom as the setup type, you are asked to designate a license server. Click Next if you are not using a license server.

The license server manages concurrent licenses. Fill in the host name or IP address of the license server and the port number that this server will use to receive license requests. See the *Solstice Network Client Installation and Licensing Guide* for more information on how to choose a license server and install licenses.

The port number identifies the port used by this server to monitor license requests. To get the port number of your license server, log in to the license server and type

```
more /etc/opt/licenses/licenses_combined |grep SERVER
```

The port number is the last number in this line. In the following example, the port number is 1726.

```
SERVER bigserver 7220b150 1726
```

Name Service

Solstice NFS Client uses a name service, such as NIS or NIS+, to locate other machines on the network. Some applications also use either DNS or a local `HOSTS` file to resolve names and IP addresses.

If your site uses either NIS or NIS+ as a name service, you can configure the service during installation. Enter the domain name and the IP address of the NIS or NIS+ name server. The domain name is case-sensitive; be sure to enter it correctly. The client cannot broadcast for a NIS or NIS+ server.

After installation, you can use the Solstice NIS / NIS+ Services Configuration page to add or change your name service and set up a search order. Access the NIS / NIS+ page from the Services tab in the Network dialog box.

NIS

NIS is Sun's network information service. It is a name service that provides access to a set of network databases that contain information such as server names, IP addresses, and host IDs (Ethernet addresses).

NIS+

NIS+ is a successor to NIS. It is a hierarchical name service that provides read / write access to a set of distributed network databases. NIS+ provides scalability, which makes it suitable for very large networks. It also provides authentication services, which provide security and improved updating capability.

Windows Default

The Microsoft network uses the domain name service (DNS) or a local file named `HOSTS` as a name service. If you enable DNS, it will be used as the default name service. If DNS is not enabled, the `HOSTS` file becomes the default.

On Windows 95, a sample `HOSTS` file is in the `C:\WINDOWS` directory, called `HOSTS.SAM`.

On Windows NT, a sample `HOSTS` file has the path name `C:\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS`. If you edit this file using a text editor, save it without a `.TXT` or `.DOC` extension.

Installing Solstice NFS Client

Solstice NFS Client relies on the Microsoft TCP/IP network protocol stack to provide the network connection. The Microsoft TCP/IP stack must be set up before you can install the Solstice software. When you start the Solstice NFS Client installation, the installation detects your current network configuration. If the required TCP/IP network is not configured, the installation stops and an online Help program guides you to set up and configure the Microsoft TCP/IP stack.

▼ To Install Solstice NFS Client

1. **Start the installation by double clicking on the self-extracting executable file** `sunwlite.exe`**.**

   The installation program expands the program files and starts the setup program.

2. **Click Next to step through the installation screens, answering the questions.**

3. **Restart your computer.**

   When you finish installing the software, restart your system to include the new configuration information. Restarting Windows is not enough.

Creating a Silent Installation

A silent installation uses a setup file to provide installation and configuration information, eliminating the need for a user to enter information during the installation process.

Running the installation program in administration mode creates a setup file containing information recorded during the installation. The setup file must end with a `.SIS` extension.

A silent installation proceeds as specified by the `.SIS` file and can be completed without user interaction. (The user will see any screen that contains a field with no value assigned to it in the `.SIS` file.)

▼ To Create a Silent Installation

To create a silent installation, run the installation program in administration mode, on the installation platform. Because you must supply an argument to the `setup` command, you must start this program from the Run prompt.

1. **Click Start, click Run, and then start Setup in administration mode. Type the full path name of the setup command:** <*pathname*>`\setup /a`**.**

   The installation program starts in administration mode.

2. **Enter the name of the silent install file.**

   Enter the full path name of the file you are creating. The file name must end in `.SIS`. If you do not enter a full path name, the default is to place the file in the current directory.

Note - If the setup file is named `setup.sis` and it resides in the same directory as the `setup.exe`, then this file is called automatically whenever you enter the `setup` command.

---

3. **Progress through the installation screens, entering information as requested.**

   Fill in all fields that contain information common to the type of installation you are designing. If any fields are left blank on a screen, the screen that contains the blank field will appear to the user during installation.

Caution - The `.SIS` file contains coded text. Do not edit this file.

▼ To Run a Silent Installation

Because you supply the path name of the `.SIS` file as an argument to the `setup` command, you must execute the `setup` command from the Run prompt.

- **Click Start, click Run, and then type the full path name of the installation** `setup` **command followed by the full path name of the** `.SIS` **file. For example, if you are installing from a CD-ROM in drive E, type:**

```
E:pcpro3\setup C:\install\setupfile.sis
```

The installation proceeds according to the contents of the `.SIS` file.

Automating Installation

If you are supporting users with various system configurations, you may want to automate installations. You could, for example, copy the installation software to a network area that is available to the computers at your site, create a separate setup file for each type of installation, and place the `.SIS` files in the installation directory. You can then write a separate batch file (or installation script) for each type of installation.

▼ To Create an Installation Script

You can create a batch file that will run the installation program and call the setup file for installation and configuration settings.

1. **Create a network installation area on your computer.**

   Create an area that can be accessed by other computers at your site.

2. **Copy the installation software to the network installation directory on your computer.**

3. **Run Setup in administration mode, creating one or more silent installation files. (See "To Create a Silent Installation" on page 7.)**

4. **Create a batch file that starts a silent installation from your network directory. For example, for a Windows 95 installation:**

   a. **Create a directory called** `C:\install` **on the computer** `admin`**.**

   b. **Run** `setup /a` **from this directory, creating a Windows 95 silent installation file called** `C:\install\sunw95.sis`**.**

   c. **Create a file called** `sunw95.bat` **containing the command:**
   `\\admin\install\pcpro3\setup.exe sunw95.sis`

   Users can run the batch file from a mounted directory, using the Microsoft Run command.

Uninstalling Solstice NFS Client

You can use the Add/Remove capability in Windows 95 or Windows NT to uninstall the Solstice NFS Client components from your system.

Uninstalling is a four-step procedure.

▼ To Uninstall Solstice NFS Client

1. **Remove NFS Printer and Drive Connections.**
   a. **Click the Start button, click Settings, and then click Printers.**
      The Printers dialog box opens.
   b. **Select the NFS printer icons, click File, and then click Delete.**
   c. **Double-click the My Computer icon.**
   d. **Select any NFS-mounted drives, click File, and then click Disconnect.**
2. **Shut down and restart your computer.**
3. **Uninstall Solstice NFS Client.**
   a. **Click the Start button, click Settings, and then click Control Panel.**
   b. **Double-click Add/Remove Programs.**
   c. **From the Install/Uninstall tab, select Solstice, and then click Add/Remove.**
      A confirmation box opens.
   d. **Click Yes to confirm removal of the Solstice NFS Client software.**
      The uninstall program removes all files and folders that are not being shared by another program. If a shared file is empty, the uninstall program notifies you and gives you the option to keep or remove it.
      If you are certain that the shared file is not used by another application, then you may remove it. If there is any doubt, the safest course is to retain it.
   e. **Click OK in the Add/Remove Programs Properties dialog box.**
4. **Delete the Installation Directory.**

The last step is to delete the directory in which Solstice NFS Client was installed. After the uninstall program has finished, you can remove the folders the Solstice NFS Client installation created.

CHAPTER 2

Setting Up Serial Connections

You can set up network connections on a Windows 95 or Windows NT computer running the Solstice Network Client software by configuring the Microsoft TCP/IP protocol. Configuring a serial connection from a client to a point-to-point (PPP) server requires changing the default authentication method from broadcast to using a specific authentication server. This chapter describes how to set up a serial connection to a PPP server from a client running Windows NT or Windows 95.

Refer to your Microsoft Windows documentation for information on setting up a LAN connection and for switching between LAN and serial connections.

You can read background and procedural information throughout this chapter, or you can use the following references to go directly to a specific topic.

- "Gathering Information" on page 11
- "Installing Dial-Up Networking on Windows 95" on page 12
- "Setting Up a Serial Connection to a PPP Server on Windows 95" on page 13
- "Adding and Removing an NFS Server" on page 16
- "Setting Up a Serial Connection to a PPP Server on Windows NT" on page 17
- "Troubleshooting" on page 22

Gathering Information

For a serial connection, your Internet service provider determines the information you need. Your provider may require all or only some of the following information:

- Your login user name
- Telephone number of the service provider

- PC COM port number
- Name service (DNS)
- IP address for your PC
- Name and IP address of name server
- Modem speed and parity setting

Installing Dial-Up Networking on Windows 95

This section explains how to install dial-up networking on a Windows 95 computer running Solstice Network Client software with the NFS Client component installed. If you have not yet installed and set up the Solstice Network Client software, refer to the “Installing Solstice NFS Client” on page 6 for instructions.

▼ To Install Dial-Up Networking

1. **Double-click My Computer on the Windows 95 desktop.**

   If you do not see a Dial-Up Networking folder in the My Computer program group, then either dial-up networking software or a modem is not installed in the computer. If dial-up networking software is not installed, follow these steps to install it.

2. **Make sure you have the Windows 95 CD-ROM. You will be asked to insert it in the CD-ROM drive during this procedure.**

3. **Click the Windows 95 Start button, point to Settings, and then click Control Panel.**

4. **Double-click Add/Remove Programs.**

   The Add/Remove Programs Properties dialog box opens.

5. **Click the Windows Setup tab.**

6. **Select Communications.**

7. **Click Details.**

   The Communications page lists communications software components.

8. **Select Dial-Up Networking and click OK.**

9. **Click OK to close the Windows Setup dialog box.**

Note - If you are asked to insert the Windows 95 CD-ROM, insert the CD-ROM in the CD-ROM drive and then click OK.

---

10. **Click Yes when asked to restart the computer.**

Setting Up a Serial Connection to a PPP Server on Windows 95

Setting up a serial connection to a PPP server on a Windows 95 computer includes four steps.

▼ To Create a Dial-Up Connection

1. **Double-click the My Computer icon, and then double-click Dial-Up Networking.**

   If you do not see a Dial-Up Networking folder in My Computer, then either dial-up networking software or a modem is not installed in the computer. If dial-up networking software is not installed, see “To Install Dial-Up Networking” on page 12.

2. **Double-click Make New Connection.**

   The Make New Connection Wizard starts.

3. **(Optional) Click Configure to customize the modem properties.**

   Click one or more of the tabs and make any desired changes. For example, select the Options tab and choose to open a terminal window before or after dialing the number. You can use this window to enter modem AT commands or dynamic passwords.

4. **Type a name for the dial-up connection.**

5. **Type the telephone number of the service provider, and then click Next.**

6. **Click Finish.**
   The name of the new connection is listed in the Dial-Up Networking dialog box.

▼ To Set Up TCP/IP Properties

1. **Select the New Connection icon, click the right mouse button, and then select Properties.**
2. **Click Server Type.**
3. **In Type Of Dial-Up Server, select PPP: Windows 95, Windows NT 3.5, Internet.**
4. **Under Advanced Options, select Log On To Network.**
   Windows 95 prompts you to log in just after the connection is made.
5. **Under Allowed Network Protocols, select TCP/IP.**
6. **Click TCP/IP Settings.**
7. **Type the IP address for the domain name service (DNS) server to use for this serial connection.**
   To use the same DNS server for all PPP connections, specify the DNS server in the TCP/IP property page in the Network dialog box.
8. **Click OK to close the TCP/IP Settings dialog box.**
9. **Click OK to close the Server Types dialog box, and then click OK again.**

▼ To Configure the Authentication Server

1. **Select Network Neighborhood and click the right mouse button.**
   The Network dialog box opens.
2. **Select the Microsoft TCP/IP protocol and click Properties.**
   Make sure the TCP/IP protocol is selected next to the Dial-Up Adapter.
3. **Select Solstice NFS Client and click Properties.**
4. **Click the Security tab (Figure 2–1).**

Figure 2–1 Changing the Default Authentication Server

5. **Type the name or IP address of your authentication server.**

   When you connect to a PPP server, only the client and the PPP server are considered hosts on the local subnet. You must specify the IP address of the authentication server if it is outside the local subnet.

▼ To Log In and Connect to a PPP Server

1. **Start Windows 95.**

   If you selected Solstice Network Client as the primary network logon, the Solstice Network Client login dialog box opens. If you selected Microsoft Windows as the primary network login, the Windows 95 login dialog box opens.

2. **Click Cancel in the login dialog box.**

   You cannot successfully log in to the network and be authenticated until you establish a connection to the Solaris server. The Windows 95 desktop opens.

3. **Select the Serial Connection icon and type your network user name and password.**

4. **Click Connect.**

5. **Log in to the PPP server.**

   You might need to type a string such as `ppp` to start the PPP server. The message, `Verifying Username and Password`, means that the PCNFSD server is

authenticating your user name and password. The message, `Logging on to Network` is displayed, and then either the Solstice Network Client or Windows 95 network login dialog box opens.

6. **In the login dialog box, type your user name and password.**
   If the login is successful, the message, "`Connected at` *baud rate* `is shown`." You can now run TCP/IP applications.

Adding and Removing an NFS Server

In a PPP configuration, the local subnet includes only your Windows computer and the PPP server. You cannot browse files on an NFS server that is outside the local subnet. To access files on an NFS server in a PPP configuration, you must add the NFS server.

▼ To Add an NFS Server

1. **Open Network Neighborhood and double-click Entire Network.**
   Network Neighborhood displays a list of NFS Servers and NFS Automount Maps.

2. **Select NFS Servers and click the right mouse button.**

3. **Click Add/Remove NFS Servers.**
   The NFS Servers dialog box opens (Figure 2–2).

Figure 2–2 NFS Servers Dialog Box

4. **Type the name of an NFS server and then click Add.**

5. **Click OK to close the NFS Servers dialog box.**

▼ To Remove an NFS Server

1. **Open Network Neighborhood and double-click Entire Network.**
   Network Neighborhood displays a list of NFS Servers and NFS Automount Maps.

2. **Select NFS Servers and click the right mouse button.**

3. **Click Add/Remove NFS Servers.**
   The NFS Servers dialog box opens (Figure 2–2).

4. **Select an NFS server to remove and then click Remove.**

5. **Click OK to close the NFS Servers dialog box.**

Setting Up a Serial Connection to a PPP Server on Windows NT

If your computer has a network adapter card installed *and* you plan to use the computer to make both serial and LAN connections, create a separate Windows NT hardware profile for each configuration. Refer to Windows NT on-line Help for instructions on setting up hardware profiles.

Setting up a serial connection to a PPP server on a Windows NT computer includes five steps.

▼ To Add Remote Access Service

1. **Right-click Network Neighborhood icon, then click Properties.**
   The Network properties dialog box opens.

2. **Click the Services tab, click Add, select Remote Access Service, and then click OK.**
   The Remote Access Setup program opens the Add RAS Device dialog box.

3. **Follow the instructions on the screens to install your modem.**

   When you have installed your modem, it is listed in the Remote Access Setup dialog box.

4. **Click Continue.**

   Remote Access Service is added to the list of services.

5. **Click Close to close the Network dialog box.**

6. **Click Yes when asked if you want to restart your computer.**

▼ To Create a Dial-Up Connection

1. **Double-click the My Computer icon, and then double-click Dial-Up Networking.**

2. **Click New.**

   The New Phonebook Entry Wizard starts. Fill in the information asked for on each screen with information provided by your Internet Service Provider.

3. **Type a name for the connection and then click Next.**

   Answer questions about how you dial the Internet and then click Next.

4. **Type the telephone number of the service provider, and then click Next.**

5. **Click Finish.**

6. **(Optional) Click More and choose from the menu to customize modem properties and dialing preferences.**

7. **Click Close.**

▼ To Configure an Authentication Server

1. **Right-click Network Neighborhood and then click Properties.**

   The Network dialog box opens.

2. **Click the Services tab, select Solstice NFS Client, and then click Properties.**

   The Solstice NFS Client Configuration page opens.

3. **Click the Security tab.**

4. **In the Authentication field, select Use A Specific Authentication Server, type the IP address of your authentication server, and then click OK.**

   When you connect to a PPP server, only the client and the PPP server are considered hosts on the local subnet. You must specify the IP address of the authentication server if it is outside the local subnet.

5. **Click Close to close the Network dialog box.**

6. **Click Yes when asked if you want to restart your computer.**

▼ To Grant Dialin Permission to a User

A Windows NT user must have dialin permission to log in to a network over a serial connection.

1. **From the Start menu, select Programs, select Administrative Tools, and then click User Manager.**

2. **Double-click the user's name to open the User Properties dialog box.**

3. **Click Dialin.**

4. **Select Grant Dialin Permission To User, choose a Call Back option, and then click OK.**

5. **Click OK to close the User Properties dialog box.**

▼ To Log In and Connect to a PPP Server

1. **Press Ctrl+Alt+Delete to log in to Windows NT.**

2. **Type your Windows NT user name and password, and then click OK.**

   You will see a message stating that the Solstice NFS Client was not started because a local network was not detected. You cannot successfully log in to the network and be authenticated until you establish a connection to the Solaris server.

3. **Click OK.**

   The Windows NT desktop opens.

4. **Double-click the Network Neighborhood icon, double-click Entire Network, and then double-click Solstice_NFS_Client.**

   The Solstice NFS Client dialog box (Figure 2–3) opens.

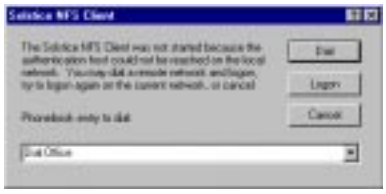


Figure 2–3 Solstice NFS Client Dialog Box

5. **Select a number to dial from the phonebook entries listed and click Dial to dial a network connection.**

6. **Log in to the PPP server.**

   You might need to type a string such as `ppp` to start the PPP server. The message, `Registering Your Computer on the Network`, means your computer has successfully connected to the PPP server. The message, `Authenticated`, means the PPP server has verified your user name and password.

   The Solstice NFS Client Login dialog box (Figure 2–4) opens.

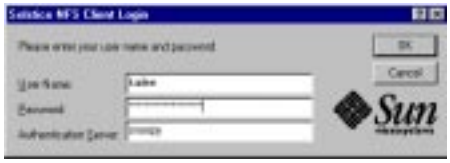


Figure 2–4 Solstice NFS Client Login Dialog Box

7. **Type your Solstice user name and password, type the name of an authentication server, and then click OK.**

   You are now logged in to the network and can use NFS to connect to network files.

▼ To Log In to the Solstice Network

If you have set up an automatic dial-in connection, your computer might start dialing the remote server before you click Dial on the Solstice NFS Client dialog box. You are connected to the remote PPP server, but not yet logged in to the network. Logging in to the Network Provider allows you to access NFS files and printers.

1. **Double-click the Network Neighborhood icon, double-click Entire Network, and then double-click Solstice_NFS_Client.**

   The Solstice NFS Client dialog box (Figure 2–5) opens.

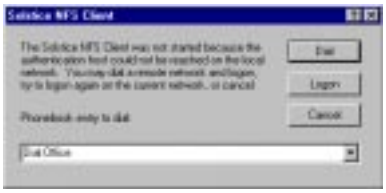


Figure 2–5 Solstice NFS Client Dialog Box

2. **Select a number to dial from the phonebook entries listed and click Dial to dial a network connection.**

   Your computer dials the number you selected.

3. **Log in to the PPP server.**

   You might need to type a string such as ppp to start the PPP server. The message, Registering Your Computer on the Network, means your computer has successfully connected to the PPP server. The message, Authenticated, means the PPP server has verified your user name and password.

   The Solstice NFS Client Login dialog box (Figure 2–6) opens.

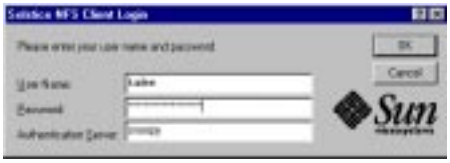


Figure 2–6 Solstice NFS Client Login Dialog Box

4. **Type your Solstice user name and password, type the name of an authentication server, and then click OK.**

   You are now logged in to the network and can use NFS to connect to network files.

Troubleshooting

Table 2–1 lists solutions to common problems connecting to the network from a Windows 95 computer running the Solstice Network Client software using a serial connection.

TABLE 2–1 Troubleshooting

Problem	Possible Cause	Solution
PC hangs on starting Windows 95 before any login dialog box appears. Pressing Ctrl+Alt+Del shows nothing running.	DNS server address is configured incorrectly on the TCP/IP property page (e.g., `123.345.6.7` instead of `123.345.6.15`).	Boot in safe mode and fix the DNS server address. Click Start, point to Settings, click Control Panel, and then double-click Network. Double-click TCP/IP. After you correct the problem, restart your computer.
Logging in fails after a few minutes with the message `Unable to contact authentication server.`	When you make a serial connection, you must first connect to the Solstice network so that a PCNFSD server can authenticate your username and password. Then you can log in to the network provider.	Click OK to close the message. Click Cancel in the Solstice or Windows 95 network login dialog box. When the Windows 95 desktop appears, double-click the icon for the dial-up connection you configured. When the network login dialog box again appears, type your user name and password for the Solstice network. You will see the message `Logging on to network` when the login succeeds.
You can use TCP/IP applications, such as Netscape, but browsing or mapping NFS servers fails with the message `You are not logged in to the network`.	You have a TCP/IP connection to the server, but were not authenticated by a PCNFSD server and are, therefore, not logged in to the network.	Select the icon for the dial-up connection you are making. Select Properties, click Server Type, and then make sure Log On To Network is selected. Select Start, select Shutdown, and then click Close All Programs and Log On As A Different User. Then follow the procedure in "To Log In and Connect to a PPP Server" on page 15.

Table 2–2 lists possible solutions to problems logging in to a Windows 95 or Windows NT computer running the Solstice Network Client software using a serial connection.

TABLE 2–2 Solutions to Problems Logging In

Possible Causes	Solutions
You entered the authentication server incorrectly or the authentication server is not working.	Use the Windows `ping` command to reach the machine running the authentication server. Ask a network administrator for the correct IP address of the authentication server to use. Retype the correct authentication server address in the login dialog box and click OK.
One or more TCP/IP settings are incorrect.	On Windows 95, follow the steps in the "Checklist for TCP/IP Settings on Windows 95" on page 57. On Windows NT, follow the steps in the "Checklist for TCP/IP Settings on Windows NT" on page 58.
You have not yet configured a serial connection.	Click Cancel on the Solstice NFS Client login dialog box to log in without networking enabled. Follow the instructions in "To Create a Dial-Up Connection" on page 13.
You are trying to connect to a PPP server, and Solstice NFS Client is set up with an asterisk (*) for the authentication server. When you connect to a PPP server, the local network consists of only the client and the PPP server. Solstice NFS Client cannot broadcast beyond the local subnet.	Select NFS Client, click Properties, and then click the Security tab. Type the IP address for an authentication server on the network.
The name server cannot find an IP address for the remote computer.	Verify that you typed the name for the remote computer correctly. Ping the remote computer's IP address.
The remote computer, the network, or part of the network is down.	Check your modem or network cables. Ping your computer to verify it can connect to itself (which verifies that your local interface is running). Ping your name server (by name or by IP address) and your local gateway.

Table 2–3 lists solutions to common problems connecting to the network from a Windows NT computer running the Solstice Network Client software using a serial connection.

TABLE 2–3 Solutions to Common Problems Connecting to the Network

Problem	Possible Cause	Solution
You log in to NT and see the message `The Solstice NFS Client was not started because a local network was not detected and the authentication server could not be reached.`	You cannot successfully log in to the network and be authenticated until you establish a connection to the Solaris server.	Click OK to complete the NT login. Follow the procedure "To Log In and Connect to a PPP Server" on page 15.
You see the message `Unable to browse the network. The network is not present or is not started.`	You cannot browse NFS servers until you connect to a PPP server and log in to the Solstice network.	Follow the procedure "To Log In and Connect to a PPP Server" on page 15.
After you log in to NT, network drives fail to automatically reconnect and are marked with a red x in My Computer.	You are not logged in to the network.	Make sure you are logged in to the network. Follow the procedure "To Log In and Connect to a PPP Server" on page 15. Double-click the drive to re-establish the connection.

CHAPTER 3

NFS File Services

This chapter describes how to use and manage Solstice NFS Client file services on Microsoft Windows 95 and Windows NT 4.0.

You can read background and procedural information or use the following references to go directly to the specific topic.

- "Accessing NFS File Systems" on page 27
- "Accessing WebNFS Servers" on page 44
- "Customizing Solstice NFS Client" on page 46
- "Troubleshooting" on page 55

Accessing NFS File Systems

You can access files on NFS servers using Network Neighborhood or Windows Explorer similar to the way you access Microsoft or Netware file services. You access an NFS file system in the following ways.

- Using NFS Servers – You can find an icon for NFS Servers on the Entire Network screen from Network Neighborhood. When you access it, you see a list of all the NFS servers on your local subnet. If the NFS server you need is part of your local subnet, you can browse its file system and map its folders to network drives. If the NFS server exists outside your subnet, you can easily add the server to the subnet. If you know the name of the folder you want to access, you can also map it to a network drive using the Tools menu of Windows Explorer or Windows NT Explorer.
- Using NFS Automount Maps – These maps provide a means of accessing file systems, independent of their actual network location. You do not need to browse for servers or know the name of the server and its directories. Instead, you browse

for the automount map that points to the file system. You can access the server's folders the same way you would those of an NFS server, browsing files or mapping drives.

Accessing NFS Servers

On a Windows 95 or Windows NT system, you can access NFS servers using Network Neighborhood. You can browse for NFS servers on your local subnet, or add NFS servers from outside your local subnet. You can also map a drive letter to an NFS server.

The multiple provider router (MPR) component of Microsoft Windows uses the universal naming convention (UNC) for specifying network resource names, and Solstice NFS Client uses two NFS conventions. Because of this use of multiple conventions, Solstice NFS Client's file-name mapping feature differs in detail from the file-name mapping used by Windows 95 and NT.

Windows 95 and Windows NT use this naming convention:

- Universal Naming Convention (UNC), which uses the syntax *server**share*

The Solstice NFS Client conventions include:

- NFS, which uses the syntax *server*:*/dir1/dir2/dir3*...
- Automount, which uses the syntax */automap/autokey/dir1/dir2/dir3*...

Solstice NFS Client must convert the NFS and automount formats to UNC format to enable processing by Windows 95 and Windows NT.

You can use UNC everywhere (that is, from the Map Network Drive dialog box, a Windows application, or a DOS box). NFS and automount formats can be used only when mapping a drive from a Map Network Drive dialog box.

On Windows NT, NFS format can also be used when mapping a drive from DOS with the `net use` command. See "Mapping Network Drives" on page 31 for more information.

How UNC and NFS Names Differ

UNC resource names use the format `\\server\share`. The *server* is the computer on which the shared component is located. The share is the network resource name, usually an exported file system or a printer, that is being shared.

NFS file-name conventions use the format `server:/directory1/directory2`. An important function of the Solstice NFS Network Provider is to translate the NFS network resource names into the UNC format that is recognized by Windows 95 and Windows NT. This translation creates an alias for an NFS resource name.

Aliases are created when you map a drive or browse a file system.

How an Alias is Created

An alias is actually a combination of two aliases: a server alias and a share alias. The server alias is usually identical to the NFS server name minus the domain name. The exception occurs when you access two servers with the same name in different domains. For example, if the server `sarge.bread.com` is on your subnet and you add the server `sarge.roses.com`, the first `sarge` would be assigned the alias `sarge`, and the second might be assigned `sarge~1`. Network Provider stores both the NFS server name and its corresponding server alias.

Network Provider creates a share alias to match the name of the last subdirectory in a network path that you browsed or to which you mapped a drive.

Aliases Created When You Browse

If you browse servers in Network Neighborhood, the Solstice NFS Client Network Provider creates server aliases for all active NFS servers on your subnet. Network Provider first broadcasts to the NFS network servers on the local subnet, and any servers you have added. For each network server that responds, Network Provider translates the NFS name into a server alias. After server aliases are created, the list of responding servers is displayed in Network Neighborhood.

When you browse a particular server, Network Provider creates share aliases for the server's exported file systems. At this point, you can connect to those exports using the UNC format. When you browse a subdirectory within an export, a share alias is created only if you map a drive to the subdirectory. The share alias corresponds to the name of the last subdirectory in the path.

Aliases for Automount Maps

When you browse NFS automount maps or map a drive to an automount point, Network Provider creates a server alias for the automap and share aliases for the autokeys and subdirectories. For example, if you browsed the automount map for `/home/joeuser`, a server alias for `/home` and a share alias for `/joeuser` would be created. You could then use UNC format to access the directory.

Once Solstice NFS Client has created a UNC alias, you can connect to the network resource using either a UNC or NFS resource name format. When you enter the NFS name for a network resource, the Network Provider checks the entry for that name and uses the UNC name to connect the network resource on Windows 95 or NT. If no alias is found, Network Provider generates one automatically from the NFS name.

Aliasing Multilevel Directories on Windows 95

On a Windows 95 system, the multiple provider router (MPR) recognizes only UNC format (`\\server\mount_point`), and will not allow the mapping of path names

consisting of more than two components. If you try to map more than two components, for example, `\\server\mount_point\directory`, to a drive letter, you will get an error.

If you want to map a drive to a subdirectory beneath the exported mount point, you must use NFS format. Windows does not recognize NFS formatted network resource names, but the MPR passes those names along to other network providers running on the computer. The NFS syntax, `server:/mount_point/directory/subdirectory`, lets you connect to a server using a multiple-level directory path. Windows MPR knows multiple-level NFS path names are not valid UNC names and just passes them on to the Solstice NFS Client Network Provider.

Solstice NFS Client handles the two-component limitation on path names by creating an alias for the full UNIX path of a network resource in the correct format. For example, the NFS resource name:

server:*/mount_point/directory/subdirectory1/subdirectory2*

is aliased as:

*server**subdirectory2*.

In summary, alias creation is the key to successful network resource connection. Aliases are created in one of two ways:

- Browsing NFS resources with Network Neighborhood
- Using the NFS resource name convention when making connections

Aliasing Multilevel Directories on Windows NT

In contrast to Windows 95, Windows NT allows you to use multiple-level UNC path names when mapping a drive. Solstice Network Provider creates an alias when you map a drive using either the NFS or UNC path formats. You do not need to browse a file system in order to create an alias.

If you map a drive to the file system `/usr/doctools/dp` on the server `bluebird`, using either the NFS path `bluebird:/usr/doctools/dp` or the UNC path `\\bluebird\usr\doctools\dp`, the resulting server alias would be `\\bluebird` and the share alias would be `\dp`.

You could then use the UNC format name in a Windows application or from DOS, using either the alias `\\bluebird\dp` or the full path `\\bluebird\usr\doctools\dp`.

If you look at your network drive connections through Windows NT's My Computer, or use the `net use` command in DOS, you see the full paths rather than the aliases of your network drives.

Mapping Network Drives

You can map an NFS network drive from:

- Network Neighborhood
- Windows Explorer
- Other parts of the Windows 95 or Windows NT user interface, such as My Computer (using a toolbar icon)
- Microsoft's `net use` command from a DOS prompt

Any time Windows 95 and Windows NT give you access to a drive, you can map it. Some applications may also provide drive mapping capability from the Open and Save As dialog boxes.

The following procedures describe several ways to map a network drive.

To Map a Network Drive from Network Neighborhood on Windows 95

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays a list of workgroups, including workgroups labeled NFS Automount Maps and NFS Servers.

2. **Double-click NFS Servers.**

   Network Neighborhood displays a list of all active NFS servers on your local subnet.

3. **Double-click any NFS server.**

   Network Neighborhood displays a list of shared directories on that server.

4. **Select the folder to map to a network drive. Right click on the directory, select Map Network Drive (Figure 3–1), and then click OK.**

Figure 3–1 Mapping a Network Drive on Windows 95

To Map a Network Drive from Network Neighborhood on Windows NT

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays two icons labeled Microsoft Windows Network and Solstice_NFS_Client.

2. **Double-click the Solstice_NFS_Client icon.**

   Network Neighborhood displays workgroups labeled NFS Automount Maps and NFS Servers.

3. **Double-click the NFS Servers workgroup.**

   Network Neighborhood displays a list of all active NFS servers on your local subnet.

4. **Double-click any NFS server.**

   Network Neighborhood displays a list of exported folders on that server.

5. **Select the folder to map to a network drive. Right-click on the folder, then select Map Network Drive (Figure 3–2).**

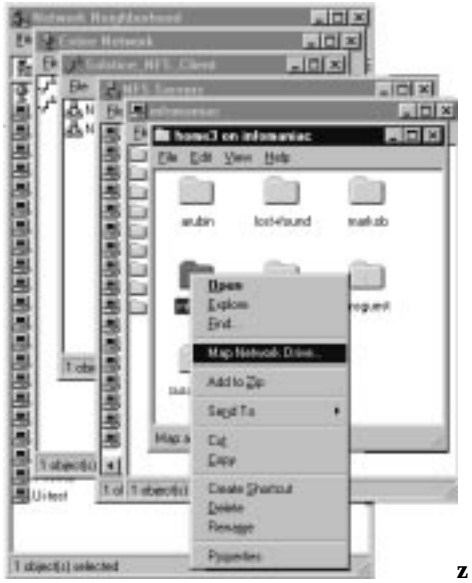


Figure 3–2 Mapping a Network Drive on Windows NT

To Map a Network Drive from Windows Explorer

1. **Click the Start button, point to Programs, and then click Windows Explorer or Windows NT Explorer.**

2. **From the Tools menu, click Map Network Drive.**

   The Map Network Drive dialog box opens.

3. **In the Path text entry box, type the NFS name of the network resource to which you want to connect.**

   Be sure to use the correct case (upper, lower, or mixed) for the server and directory names as they appear in the UNIX file system.

   If you enter the NFS name `spooky:/fun/house`, for example, Network Provider creates an alias for the NFS resource and stores it. The next time you connect to this network resource, you can specify either its NFS file name (`spooky:/fun/house`) or its alias (`\\~spooky\house`).

   You can also use automount syntax here, using the format */automap/autokey/dir1/dir2*

   For example, if your home directory is an automount point, you could enter a path similar to `/home/joeuser`. See “Browsing NFS Automount Maps” on page 39 for more information about automounting.

Note - Solstice NFS Client does not support the Connect As feature of drive mapping on Windows NT. To connect a drive, you must use your login name.

To Map a Network Drive Using a UNC Name on Windows 95

On Windows 95, you can specify the alias for a network resource only if it already exists. If you have connected to this resource before, the Solstice network has created and stored an alias for it. If you are not sure whether the alias exists, use Explorer or My Computer to browse the network.

1. **Click the Start button, point to Programs, and then click Windows Explorer.**

2. **From the Tools menu, click Map Network Drive.**

   The Map Network Drive dialog box opens.

3. **In the Path text entry box, type the tilde (~) character followed by the alias. For example:**

```
\\~spooky\house
```

To Map a Network Drive Using a UNC Name on Windows NT

On Windows NT, you can specify the full path to a network resource in UNC format. If you have not connected to this resource before, the Solstice network creates and stores an alias for it as it makes the connection. You do not need to browse the network before using a UNC name.

1. **Click the Start button, point to Programs, and then click Windows NT Explorer.**

2. **From the Tools menu, click Map Network Drive.**

   The Map Network Drive dialog box opens.

3. **In the Path text entry box, type the tilde (~) character followed by the alias. For example:**

```
\\~spooky\house
```

Browsing NFS Servers

The Solstice NFS Client software uses the implicit drive mapping capability of Windows 95 and Windows NT to mount servers transparently when you browse for NFS servers. This implicit mapping process lets you look at and access files on NFS servers without mapping a network drive first.

▼ To Browse for NFS Servers on Windows 95

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays a list of Microsoft network workgroups, including workgroups labeled NFS Servers and NFS Automount Maps (Figure 3–3).

Figure 3–3 Browsing NFS Servers in Network Neighborhood

2. **Double-click on the NFS Servers workgroup.**

   Network Neighborhood displays a list of all active NFS servers on the local subnet to which your machine is attached (Figure 3–4).

Figure 3–4 NFS Servers Listed in Network Neighborhood

3. **Double-click any NFS server.**

   Network Neighborhood displays a list of exported folders on that server.

Note - You will see the alias for the network resources you browse. To see the NFS names, click Details from the View menu. The aliases are listed under Name, and the corresponding NFS names are listed under Comment.

4. **Access these folders as you would folders on your local computer.**

▼ To Browse for NFS Servers on Windows NT

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays workgroups labeled Microsoft Windows Network and Solstice_NFS_Client (Figure 3–5).

Figure 3–5 Selecting Solstice_NFS_Client Workgroup

2. **Double-click Solstice_NFS_Client.**

   Network Neighborhood displays workgroups labeled NFS Servers and NFS Automount Maps.

3. **Double-click the NFS Servers workgroup.**

   Network Neighborhood displays a list of all active NFS servers on your local subnet (Figure 3–6).

Figure 3–6 NFS Servers in Network Neighborhood on Windows NT

▼ To Add an NFS Server Outside the Local Subnet on Windows 95

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays a list of Microsoft network workgroups, including workgroups labeled NFS Servers and NFS Automount Maps.

2. **Right-click NFS Servers and then select Add/Remove NFS Servers.**

   The Add/Remove NFS Servers dialog box opens (Figure 3–7).

Figure 3–7 Add/Remove NFS Servers Dialog Box

3. **Type the name of an NFS server that is not on the local network and then click Add.**

   Repeat this step for each server you want to add.

4. **Click OK to close the Add/Remove NFS Servers dialog box.**

▼ To Add an NFS Server Outside the Local Subnet on Windows NT

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays workgroups labeled Microsoft Windows Network and Solstice_NFS_Client.

2. **Double-click Solstice_NFS_Client.**

   Network Neighborhood displays workgroups labeled NFS Servers and NFS Automount Maps.

3. **Right-click NFS Servers and then select Add/Remove NFS Servers.**
   The Add/Remove NFS Servers dialog box opens (Figure 3–7).

4. **Type the name of an NFS server that is not on the local network and then click Add.**

5. **Click OK to close the Add/Remove NFS Servers dialog box.**

▼ To Remove an NFS Server Outside the Local Subnet on Windows 95

1. **Open Network Neighborhood and double-click Entire Network.**
   Network Neighborhood displays a list of Microsoft network workgroups, including workgroups labeled NFS Servers and NFS Automount Maps.

2. **Right-click NFS Servers and then select Add/Remove NFS Servers.**
   The Add/Remove NFS Servers dialog box opens (Figure 3–7).

3. **Select an NFS server to remove and then click Remove.**

4. **Click OK to close the Add/Remove NFS Servers dialog box.**

▼ To Remove an NFS Server Outside the Local Subnet on Windows NT

1. **Open Network Neighborhood and double-click Entire Network.**
   Network Neighborhood displays workgroups labeled Microsoft Windows Network and Solstice_NFS_Client.

2. **Double-click Solstice_NFS_Client.**
   Network Neighborhood displays workgroups labeled NFS Servers and NFS Automount Maps.

3. **Right-click NFS Servers and then select Add/Remove NFS Servers.**
   The Add/Remove NFS Servers dialog box opens (Figure 3–7).

4. **Select an NFS server to remove and then click Remove.**

5. **Click OK to close the Add/Remove NFS Servers dialog box.**

Browsing NFS Automount Maps

In addition to browsing NFS servers, Solstice NFS Client lets you browse NFS automount maps. The maps can be either NIS/NIS+ automount maps, or local automount maps. These maps contain information about other computers on your network.

The Solstice NFS Client Automounter is an NFS automounter. It enables administrators to define mount points without regard to their actual location on a network. Automount maps provide the links between file system names and their actual locations. For example, a file system name of `/dat/pcapps` could map to a network location of `appserver:/export/pcapps`. This location could change with a simple update to the automount maps.

The Solstice NFS Client automount maps use the same format as the NIS/NIS+ automount maps in Solaris. The Solstice NFS Client installation program installs two required automount maps in the `C:\Program Files\Solstice\Etc` directory, `auto_home` and `auto_master`. These files must reside in this directory whether you use a local name service or NIS/NIS+. Figure 3–9 and Figure 3–8 show slightly modified versions of these two files. For more information on the format of these files, see the UNIX man page for automount (enter `man automount` on a Solaris workstation command line), and consult the Solaris system administration documentation.

You can view NIS/NIS+ maps on a Solaris machine by entering:

```
ypcat --k auto.home
```

or

```
niscat auto_home
```

If your network does not use NIS or NIS+, your computer will use the locally installed automount maps. These files must reside in your `C:\Program Files\Solstice\Etc directory`.

Home Automount Map

The `auto_home` file requires an entry for each user. To edit the automount maps, use a 32-bit editor (like WordPad) to prevent Windows from converting the file names to 8.3 DOS names.

```
#
# The auto_home map
#
# use +auto_home for NIS+
# use +auto.home for NIS

+auto_home
#
# sample lines in auto_home
#
edwards tandoori:/os_eng/edwards
jenifer topfuel:/top3/jenifer
```

Figure 3–8 A Home Automount Map

Master Automount Map

The `auto_master` file is read only at startup so you must reboot after editing it. However, the `auto_home` file is read as "needed" so it does not require a reboot after editing.

```
# Master map for automounter
#
# use +auto_master for NIS+
# use +auto.master for NIS
+auto_master
/net            -hosts          -nosuid
/home           auto_home
/xfn            -xfn
#
# next line is a sample: use auto_sac for all entries
# for directory /sac
#
/sac auto_sac -intr,nosuid
```

Figure 3–9 A Master Automount Map

Configuring NIS or NIS+

To browse NIS or NIS+ maps, you must configure either NIS or NIS+ as your Solstice naming service. Configure the naming service by entering the domain and IP address of your NIS or NIS+ server, following the directions in "To Configure NIS or NIS+" on page 41.

To see the host name of your NIS server, use the following command on a Solaris system:

```
ypwhich
```

To see the IP address of your NIS server, use the following command:

```
ypcat hosts | grep hostname
```

To see the domain name and IP address of your NIS+ server, use the following command:

```
niscat -o org_dir
```

▼ To Configure NIS or NIS+

1. **In Control Panel, double-click the Network icon.**
   - For Windows 95, click the Configuration tab.
   - For Windows NT, click the Services tab.
2. **Double-click Solstice NIS/NIS+ Naming Services, or select Solstice NIS/NIS+ Naming Services and click Properties.**

   The Solstice NIS/NIS+ Naming Services Properties dialog opens.
3. **Click Enable NIS or Enable NIS+ to enable the appropriate name service for your network.**
4. **Enter the name service domain.**

   The name service domain is the complete name of your domain, usually ending in `.COM`, `.EDU`, `.NET`, `.ORG` and so on. To find out the domain name, enter the command below on a Solaris system on your subnet.

   ```
   /bin/domainname
   ```
5. **Specify a name server search order.**

   Select a name service and click Up or Down until the service you want is at the top of the list. The NIS or NIS+ service does not need to be at the top of the list for you to browse automount maps.

▼ To Browse NFS Automount Maps on Windows 95

1. **Open Network Neighborhood and double-click Entire Network.**

Network Neighborhood displays a list of Microsoft network workgroups, including workgroups labeled NFS Servers and NFS Automount Maps.

2. **Double-click the NFS Automount Maps workgroup.**

   Network Neighborhood displays a list of the local NFS automount maps on your machine, or a list of NIS / NIS+ automount maps (Figure 3–10).

Note - If your network uses NIS / NIS+ but you do not see NIS / NIS+ automount maps, you may need to configure NIS or NIS+, as explained in "Configuring NIS or NIS+" on page 40.

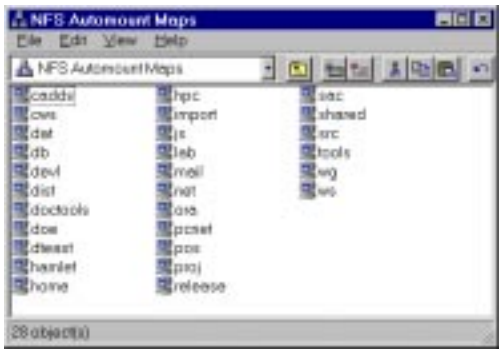


Figure 3–10 NFS Automount Maps Listed in Network Neighborhood

3. **Double-click any NFS automount map.**

   Network Neighborhood displays a list of all NFS mount points defined in the automount maps.

4. **Access these automount points as you would folders on your local computer.**

   Note that you can open an automount point and map a network drive to a folder within it by right-clicking the folder, selecting Map Network Drive, and clicking OK in the Map Network Drive dialog box.

▼ To Browse NFS Automount Maps on Windows NT

1. **Open Network Neighborhood and double-click Entire Network.**

   Network Neighborhood displays workgroups labeled Microsoft Windows Network and Solstice_NFS_Client.

2. **Double-click Solstice_NFS_Client.**

   Network Neighborhood displays workgroups labeled NFS Servers and NFS Automount Maps.

3. **Double-click the NFS Automount Maps workgroup.**

   Network Neighborhood displays a list of the local NFS automount maps on your machine, or a list of NIS/NIS+ automount maps (Figure 3–10).

4. **Double-click any NFS automount map.**

   Network Neighborhood displays a list of all NFS mount points defined in the automount maps.

5. **Access these automount points as you would folders on your local computer.**

User Profiles and Connected Drives

Windows 95 and Windows NT differ in the way persistent drive mappings are treated when different users log in to a system.

Due to the default behavior of Windows 95, a network drive specified to be reconnected on login is mapped whenever a user logs in to Windows 95 on that computer. You can, however, set up Windows 95 so that drive mappings are associated with specific users. See the *Solstice Network Client Administration Guide* for information about user profiles.

In Windows NT 4.0, each user account has a unique user profile by default. As a result, drive mappings are associated with specific users. However, if you want all users to be reconnected to the same network drives when they log in, you can take advantage of the mandatory user profile ability of Windows NT Server 4.0 to give users identical environments. See the Windows NT documentation for more information about mandatory user profiles.

▼ To Set Up Custom User Profiles on Windows

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Passwords.**

   The Passwords Properties dialog box opens.

2. **Click the User Profiles tab.**

3. **Click the option button labeled "Users can customize their preferences and desktop settings."**

   The previously grayed-out User Profile Settings become active.

4. **Click the options to turn settings on and off.**

Use What's This help to determine what settings you need.

Accessing WebNFS Servers

The WebNFS™ protocol is an extension of the NFS protocol. The WebNFS protocol enables clients to access a WebNFS server anywhere on the Internet. It makes information on NFS servers available to Web browsers and Java™ applets. WebNFS also makes it easy to connect to Internet NFS servers through corporate firewalls.

About the WebNFS Protocol

The WebNFS protocol was designed to overcome some of the drawbacks to using NFS over an Internet connection. A WebNFS server implements the following features:

- Supports TCP transport – Firewalls can be easily configured for protocols that use TCP on well-known ports.
- Supports NFS v3 – NFS version 3 overcomes a number of limitations in version 2. It allows users to access larger files and larger transfer sizes. This results in much faster file access operations across a network.
- Supports the use of a well-known port – Clients can skip the Portmapper protocol and communicate directly with the server on port 2049.
- Exports files using a public file handle – A WebNFS server makes files available to clients with a public file handle. A WebNFS client uses this as an initial file handle to access files and directories, bypassing the Mount protocol.
- Supports multicomponent lookup – A WebNFS server can evaluate an entire path name with a single request when the path name is relative to the public file handle.

The Solaris 2.6 server is a WebNFS server.

About the WebNFS Client

The Solstice NFS Client can connect to a WebNFS server by mounting or by connecting with an NFS URL of the format `nfs://`*`host/path`*. The NFS URL can be used when mapping a drive using `net use` (Windows NT only), in the Map Network Drive dialog box, or with the script interpreter. Automount maps containing NFS URLs are also supported.

Using an NFS URL

When an NFS URL is used, the connection will be made using TCP transport, NFS version 3, port number 2049, and a public file handle. If any of these requirements cannot be met, the client uses a secondary option.

The WebNFS client connects to the server, following these rules:

- Use TCP protocol first. If the connection is refused, use UDP.
- Use NFS version 3. If rejected, use NFS version 2.
- Use port number 2049 on the server.
- Use a public file handle as an initial file handle with a lookup request. If the request is rejected, use the Mount protocol.

Note - If the public file handle is used, locking/sharing will be disabled.

Using WebNFS Mount Option

You can select WebNFS as an option on the Advanced screen of the NFS Client Properties page or on a network server Properties page. If this option is selected, the client will connect to the NFS server using only the WebNFS protocol. No secondary options will be attempted. For example, if a public file handle request is refused, the mount will fail. Use this option to avoid delays when using WebNFS through a firewall.

Mapping a WebNFS Drive

You can map a drive on a WebNFS server using any of the methods already described for mapping drives. This includes mapping a drive from Network Neighborhood, from Windows Explorer, using the toolbar icon, and with the `net use` command (on Windows NT only).

When you are required to enter a path name, use the following syntax:

`nfs://`*`server:port/path`*

The *port* is optional. If not specified, port number 2049 is assumed.

The *path* is evaluated by the server relative to the public file handle. Note that if the path begins with a slash, it is evaluated relative to the root directory on the server.

For example, if the public file handle is associated with the directory `/home`, then the URL

`nfs://`*`server`*`/charlie/dir1/dir2`

refers to the path `/home/charlie/dir1/dir2`, and the URL

```
nfs://server//home/charlie/dir1/dir2
```

refers to the same path relative to the root directory on the server.

▼ To Map a Network Drive Using WebNFS

1. **Click the Start button, point to Programs, and then click Windows Explorer.**

2. **From the Tools menu, click Map Network Drive.**
   The Map Network Drive dialog box opens.

3. **In the Path text entry box, type the WebNFS path. For example**:

```
nfs://spooky/fun/house
```

Browsing WebNFS Servers

You can browse for a WebNFS server using the browsing mechanism described in “Browsing NFS Servers” on page 35. WebNFS servers will be listed along with the servers running `pcnfsd`.

If you select a server on the list and click File ->Explore, the system will display all exported directories, those exported by `mountd` as well as a directory exported with a public file handle (the WebNFS directory).

If you have set the WebNFS option for this server, then you will see only the WebNFS directory, displayed with the export alias name `webnfs`.

Customizing Solstice NFS Client

The Solstice NFS Client software provides a Properties dialog box for adjusting the global default values for the connection (mount) options that it uses when it connects to an NFS file system or creates files on an NFS server. See “To Change Default Settings for Solstice NFS Client Properties” on page 52 for the steps to open the Solstice NFS Client dialog box.

All NFS Client mount option settings have default values, which you can change using the Solstice NFS Client Properties dialog box. The settings in this dialog box are used initially for all connections and will be suitable in most situations. When you change any of the settings here, the values are applied to all connections (including existing persistent connections), except those values that have been changed for specific connections. You can change many mount option settings for

specific connections and mapped drives, which is explained in “Changing Mount Options for Specific Connections” on page 53.

For more information about NFS options, consult your Solaris documentation.

Setting General Preferences

Use the NFS General tab to select mount options, the file name mapping character, and the data transfer size.

Mount Options

You can choose to connect drives with read-only permissions, and set file-locking so that others will not be able to access a file that you have opened. You should be aware that some servers do not support file locking (Solstice NFS Server, for example). If you enable File Locking / Sharing and then attempt to mount drives from an NFS server that does not support file locking, you will be unable to map drives, browse exports, or read and write files on that server.

File Name Mapping

Select which character Solstice NFS Client uses as a replacement character when it maps long file names to the DOS 8.3 file name convention.

Data Transfer

Select the read / write size of NFS transfers.

- Read size (in bytes) is the number of bytes per data block read from a file during a data transfer across the network. A larger size increases NFS performance if the network hardware can handle the larger size. Default is 32768 bytes for TCP and 8 kilobytes for UDP.
- Write size (in bytes) is the number of bytes per data block written to a file or sent to a printer during a data transfer across the network. A larger size increases NFS performance if the network hardware can handle the larger size. Default is 32768 bytes for TCP and 8 kilobytes for UDP.

Setting Security Preferences

Use the Security tab to set file permissions and to specify whether to broadcast for an authentication server.

Default File Creation Permissions

Use this option to set the default UNIX permissions for each file created across the network through NFS. This performs a function similar to that of the UNIX `umask` command.

Authentication

Specify whether Solstice NFS Client will broadcast for an authentication server.

- Broadcast For An Authentication Server tells Solstice NFS Client to broadcast across the subnet to find a server running the `rpc.pcnfsd` daemon when the user logs in to verify the user's login name and password. Locating an authentication server in this way may take a little longer, but eliminates problems accessing a specific server that is down.
- Use A Specific Authentication Server tells NFS Client to contact a specific server (by name or IP address) to verify the user's login and password. This method is faster, but only if the server is up and running. If it is not, Solstice NFS Client prompts you to specify a different server.

You should select Use A Specific Authentication Server if you are using a serial connection.

Setting Caching Preferences

Use the Caching tab to set preferences for caching:

Attribute Cache

You can enable caching of file attributes (such as file size and modification time) which do not change often. Caching these attributes improves NFS performance. Use the drop-down lists to adjust the rates at which the attributes are updated. A smaller interval assures earlier detection that a file or folder has been modified by someone else. A larger interval improves performance by decreasing the frequency of NFS reads.

Data Cache

You can enable caching of previously read files in memory. Data caching can improve NFS Client file access time if your computer has free memory available. Read-write cache size (in Kbytes) determines how much memory the cache can use. The default setting, Automatic, allows NFS Client to select a value based on the free memory available.

File Name Cache

Specify how many mappings of long file names to DOS 8.3 file names can be stored in the file name cache. This cache is necessary for applications that do not support long file names.

Note - Another cache setting can be changed through the Registry only. If you see slow performance when accessing files in a directory with a large number of files (more than 256), you may want to increase the number of entries in the Directory Name Lookup Cache. For information about registry entries, see the *Solstice Network Client Administration and Maintenance Guide.*

Setting Tuning Preferences

Use the Tuning tab to adjust performance settings:

NFS Retransmissions

This setting determines the number of times NFS Client tries to reach an NFS server.

Asynchronous Transmissions

This setting turns on an NFS v3 performance enhancement. This enhancement detects when NFS is reading a file sequentially rather than randomly as in a database file, and prompts NFS to retrieve into the data cache several data blocks ahead of the data you are currently reading. If you notice poor performance when using a database or other random-access file, turn off asynchronous readaheads.

Automounter

You can specify the number of seconds an automounted file system remains connected after all files on it have been closed.

Setting Files and Folders Preferences

Use the Files and Folders tab to set preferences for case handling and how folders are created.

Archive Attribute

Showing NFS files with archive attribute checked specifies that you want to see when a file has the DOS archive attribute set, although it has no meaning in NFS.

Preferred Case

You can determine which case NFS should use when creating new files and doing file lookups. The preferred case is used only if the next option (Create File Names In Preferred Case) is selected.

Case Handling

The default selections for the two Case Handling options are intended to replicate the case-handling behavior of Windows 95 and Windows NT. Windows will allow you to create file names using mixed case. However, unlike UNIX, Windows cannot differentiate between two files with the same name but different cases in the same directory.

For this reason, you should not create files or directories on your NFS server whose names are the same except for case. For example, you should not create one directory named `STATUS` and another named `status` within the same parent directory.

- Create File Names In Preferred Case causes NFS to create and save files using the case specified in the previous field, Preferred Case.

  For example, if you select Uppercase as the preferred case and then select Create File Names In Preferred Case, all file names you enter will be converted to uppercase.

- Use Case Sensitive File Name Lookup specifies that NFS should look up file names using the preferred case. This option is available only when you first select Create File Names In Preferred Case.

  For example, if you select Uppercase as the preferred case, select Create File Names In Preferred Case, and then select Use Case Sensitive File Name Lookup, all file names will be created in uppercase, and a file lookup will look for the uppercase version of the file name searched for. If this feature is selected and you use Explorer to enter the directory on your NFS server called `status`, NFS looks for the directory `STATUS`. You will see an error such as `D:\Status is not accessible. The folder was moved or removed.` The folder is still there, but NFS cannot find it because it is looking for a different name.

  If Use Case Sensitive File Name Lookup option is not selected, a file name lookup will first look for the file in the case in which it was created. If that instance of the file is not found, then file name lookup will search the entire directory. It uses the first instance of the case-insensitive version of the file that it finds.

For example, if you select Uppercase as the preferred case, then select Create File Names In Preferred Case, and then do not select Use Case Sensitive File Name Lookup, all file names will be created in uppercase, and a file name lookup will first look for the uppercase version of the file name searched for. If the file name is not found, then NFS will continue to search the entire directory in a case-insensitive manner.

Case-insensitive lookups are slower than case-sensitive lookups, but are more compatible with the way Microsoft Windows looks for file names.

Folder Creation Semantics

Determine how NFS handles the group identification (GID) assigned to files it creates. UNIX System V normally assigns to a file the GID of the process that creates it. However, if the parent folder was set up to pass its GID to all files created within it, System V assigns the GID of the parent folder to the new file. Berkeley Software Distribution (BSD) UNIX always assigns the GID of the creating process to a new file.

Setting Advanced Preferences

Use the Advanced tab to select the transport mechanism, the NFS version, and determine how to specify the NFS port.

Transport

Select which transport to use. Automatic tries TCP first and then UDP. Using the UDP transport speeds up network traffic by reducing packet overhead on LANs and high-speed reliable networks. TCP works better when high reliability of packet transmission is a requirement, as on WANs where transmission speed is slower and more errors are encountered. TCP is able to recover one bad packet without requiring the whole frame to be resent. TCP waits for acknowledgment that a packet arrived, and if it does not receive one, it retransmits the packet.

NFS Version

You can speed up connections to the network by specifying what version of NFS to use. If the servers to which you most often connect support only one version, configure that version as a default. Automatic tries v3 first and then tries v2.

If a server is running Solaris 2.5 or later, its default NFS version is v3, but it can use v2 if the client needs to use v2. If a server is running Solaris 2.4 or earlier, it can only run NFS v2.

For any UNIX server, including one running a brand of UNIX other than Solaris, you can find out which NFS version it supports using the `rpcinfo` command, as follows:

```
rpcinfo -p hostname | grep 100003
```

(NFS is RPC program #100003.)

Running this command on a Solaris 2.5 system would return the following, which means that v2 and v3 are supported over UDP and TCP.

```
100003    3    udp    2049    nfs
100003    2    tcp    2049     nfs
100003    3    tcp    2049    nfs
100003    2    udp     2049    nfs
```

Running this command on a Solaris 2.4 system would return the following, which means that only v2 is supported over UDP.

```
100003    2    udp    2049    nfs
```

Compare the output for a non-Solaris system to determine which NFS version it supports.

NFS Port

Determine how to specify a port.

- Use Portmapper tells NFS to use the Portmapper program to determine which port to use. Using Portmapper is less efficient than using a specific port, but frees you from having to know the NFS server's listening port number.
- Use A Specific Port tells NFS to use the port you specify instead of using Portmapper. Using a specific port speeds up NFS operations. The NFS specification suggests port number 2049 as the standard NFS server port. Your network may choose to use another port number.

WebNFS

Select this option if you are using WebNFS through a firewall. If this option is selected, the client will try to use the public file handle to locate files and directories on the server. If the server does not support the public file handle, the mount will fail.

▼ To Change Default Settings for Solstice NFS Client Properties

1. **In the Control Panel, double-click the Network icon.**

2. **Open the Solstice NFS Client Properties dialog box.**

- In Windows 95, click the Configuration tab, then double-click Solstice NFS Client.
- In Windows NT, click the Services tab, then double-click Solstice NFS Client.

The Solstice NFS Client Properties dialog box opens (Figure 3–11).

Figure 3–11 Solstice NFS Client Properties Dialog Box

Use the property pages to change the default settings for NFS Client properties. Use What's This? help to jog your memory about various NFS options.

3. Click OK when finished.

Changing Mount Options for Specific Connections

The Solstice NFS Client Properties are global mount options, meaning they are the initial settings used for all network connections made, either implicitly by browsing in Network Neighborhood, or explicitly by mapping a drive. The global properties are applied to persistent connections as well.

The Solstice NFS Client software also lets users change mount options for connections to a server and for implicit mounts and mapped drives. This capability allows users to access servers or exported file systems using options that are different from the default options.

NFS Client allows two kinds of per-connection options:

- Server-level options, which affect all connections to that server
- Connection-point options, which affect only that connection

Not all the NFS properties are available at all levels. For example, the Data Cache and File Name Cache options are available as global properties, but are not available as properties of server-level connections.

Changing Mount Options for Connections to a Server

Users can set mount options for all connections made from a client computer to a particular server. Once this is done, each connection (implicit, or explicit drive map) will use the same mount options set for the server. Change mount options by first browsing NFS servers, and then selecting a specific server or file system. Once selected, display a server's or file system's properties to see its current connection options. Use these property sheets to modify these options.

When Changes to Connection Options Take Effect

Changes to connection options will take effect the next time a network resource is *connected*, not *mapped*. There is a reason for this distinction. When you browse into an exported file system on a network through Network Neighborhood, that resource gets temporarily connected. If you then change a connection option and map that same resource to a local drive letter, the new option will not be used because the resource is already connected.

Resources that are connected through Network Neighborhood, but not mapped, will be disconnected:

- After the 5-minute time-out has been reached
- When the user logs out

Once the resource has been disconnected, browsing or mapping that resource will use the new connection options.

The surest way, however, to make sure the changed connection options are used when you connect to a server or other resource is to restart Windows 95.

Order Used in Applying Mount Options to a Connection

Mount options are applied to a connection in the order of global, server, mount point. This means that when NFS makes a connection and decides which mount options to use, it looks at the global NFS Client Properties first, the server properties second, and the mount point properties last. To illustrate this, consider one particular mount option, the Mapping Character feature. Suppose you set this feature as

follows for the global NFS Client properties, for server `woody`, and the connection to `/files on woody`.

Which Properties dialog box?	Mapping character	Connection that would use this setting
Solstice NFS Client Properties	`~`	`buzz:/files2`
woody Properties	`@`	`woody:/opt`
files on woody Properties	`#`	`woody:/files`

If Mapping Character were the only property set at the server level and mount point level, each connection would use the Solstice NFS Client Properties for the values of all other mount options besides Mapping Character.

Troubleshooting

Table 3–1 lists problems that might occur using network file services on a computer running Solstice NFS Client.

TABLE 3–1 Problems Using Network File Services

Problem	Possible Cause	Solution
Cannot log in to Solstice NFS Client Login dialog box.	One or more TCP/IP settings are incorrect.	Click Cancel on the Solstice NFS Client Login dialog box to log in without networking enabled. Click Start, point to Settings, click Control Panel, and then double-click Network. In Windows 95, double-click TCP/IP. Refer to "Checklist for TCP/IP Settings on Windows 95" on page 57. In Windows NT, click the Protocols tab, then double-click TCP/IP Protocol. Refer to "Checklist for TCP/IP Settings on Windows NT" on page 58.
On Windows 95, you tried to enter a UNC file name in the Map Network Drive dialog box and received the error message, "`The following error occurred while trying to connect drive to server. Resource not found.`"	The UNC name for the network resource you tried to access does not exist.	Use NFS format in the Map Network Drive dialog box, or browse the network resources listed in Network Neighborhood. As you select each network resource, the Network Provider creates a UNC name for it.
You tried to map a drive on Windows NT using the Connect As feature and received the error message: `The credentials supplied conflict with an existing set of credentials.`	You tried to connect as a different user.	The Connect As feature is not supported by Solstice NFS Client, so you should leave this field blank.

TABLE 3–1 Problems Using Network File Services *(continued)*

Problem	Possible Cause	Solution
You logged in to Solstice NFS Client, but when you browse NFS Servers, no servers are listed.	No NFS servers are running on the same subnet as Solstice NFS Client.	Open Network Neighborhood and double-click Entire Network. In Windows NT, double-click Solstice_NFS_Client. In both environments, select NFS Servers and click the right mouse button. Click Add/Remove NFS Servers. Type the name of an NFS Server outside the local subnet, and then click Add. Click OK to close the dialog box.
Attempting to copy a directory on which you only have read permission from one NFS server to another using Explorer, Windows 95, or Windows NT fails with the message, `Cannot create or replace directory_name. Access is denied.`	The directory was copied read-only and then none of the contents could be copied into it.	Open a DOS prompt window and use the `xcopy` command to copy the directory.

Checklist for TCP/IP Settings on Windows 95

If you cannot log in to Solstice NFS Client, follow these steps to troubleshoot the problem:

1. **Right-click on the Network Neighborhood icon and click Properties to open the Network dialog box.**

2. **Click the Configuration tab and double-click TCP/IP.**

3. **If your site uses DNS:**
   a. **Click the DNS Configuration tab and make sure Enable DNS is selected.**

   b. **Make sure the DNS domain name is correct.**

c. **Make sure the number listed in DNS Server Search Order is the correct address of your DNS server.**

4. **If your site uses DHCP to automatically generate IP addresses for clients, click the IP Address tab and make sure Obtain An IP Address Automatically is selected.**

5. **If your site does not use DHCP:**
   a. **Click the IP Address tab and make sure Specify An IP Address is selected and the number typed in the IP Address box is correct.**

   b. **Click the Gateway tab and make sure the number listed in Installed Gateways is the correct address of a gateway on your local subnet.**

6. **Check the authentication server:**
   a. **In the Network dialog box, double-click the Solstice NFS Client.**

   b. **Click the Security tab and check the authentication server.**
   If Broadcast For An Authentication Server is selected, make sure there is a server running the `pcnfsd` daemon on the same local subnet as the computer running Solstice NFS Client. Do this by entering the following command from a Solaris system on the subnet:

```
rpcinfo -b 150001 2
```

   c. **If no server on the subnet is running the `pcnfsd` daemon, select Use A Specific Authentication Server and type the IP address of an authentication server outside the local subnet.**

Checklist for TCP/IP Settings on Windows NT

If you cannot log in to Solstice NFS Client, follow these steps to troubleshoot the problem:

1. **Right-click on the Network Neighborhood icon and click Properties to open the Network dialog box.**

2. **Click the Protocols tab and double-click TCP/IP Protocol.**

3. **In the IP address tab, check the following:**

a. **If you use DHCP for dynamic configuration, verify that the Obtain An IP Address From A DHCP Server option is selected.**

b. **If you don't use DHCP, verify that the Specify An IP Address option is selected. Make sure correct values are entered for the IP Address of your computer, the subnet mask used in your subnetwork, and the IP address of the default gateway server.**

4. **If your site uses DNS, click the DNS tab and check that:**
   a. **The name of your system appearing in the Host Name field is correct.**

   b. **The name listed in the Domain field is correct.**

   c. **The IP addresses of DNS servers are correct in the DNS Service Search Order.**

5. **Click OK to close TCP/IP Properties.**

6. **Click Services, and double-click Solstice NIS/NIS+ Naming Service.**
   a. **If you have selected NIS or NIS+, the name service you selected should be enabled. Be sure you have entered an IP address and domain name for the NIS or NIS+ name server. If there is an asterisk (*) in the IP address field, you must replace it with a real address.**

   b. **The name service domain name is case-sensitive. Be sure you have entered the name correctly.**

7. **Verify the authentication server:**
   a. **In the Services tab of the Network dialog box, double-click Solstice NFS Client.**

   b. **Click the Security tab and verify the authentication server.**
   If Broadcast For An Authentication Server is selected, make sure there is a server running the `pcnfsd` daemon on the same local subnet as Solstice NFS Client. Do this by entering the following command from a Solaris system on the subnet:

```
rpcinfo -b 150001 2
```

c. If no server on the subnet is running the `pcnfsd` daemon, select Use A Specific Authentication Server and type the IP address of an authentication server outside the local subnet.

CHAPTER 4

NFS Server

This chapter describes how to set up and manage NFS Server on Windows 95 or Windows NT.

You can read background and procedural information throughout this chapter, or you can use the following references to go directly to a specific topic.

- "About NFS Server" on page 61
- "Enabling NFS File Services" on page 62
- "NFS Server on Windows NT" on page 64
- "Logging NFS Server Events on Windows NT" on page 70
- "NFS Server on Windows 95" on page 72
- "Logging NFS Server Events on Windows 95" on page 75

About NFS Server

NFS Server enables an NFS client to share directories, files, and devices with other Microsoft Windows and UNIX users connected to the network. The NFS Server runs as a daemon on a Windows 95 system and as a service on a Windows NT system.

The computer running the NFS Server program shares computer resources with other users on the network by "exporting" a folder or a device, such as a CD-ROM drive. Once the resource is exported, a coworker can mount that folder or device and access it from another Windows computer or from a UNIX workstation.

Enabling NFS File Services

The installation program automatically adds the Solstice NFS File Sharing as a network service for Windows NT systems and Solstice File and Printer Sharing for Windows 95 systems. The following instructions are provided in the event this component is removed and you need to add it again.

▼ To Enable File Sharing on Windows NT

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Network.**

   The Network dialog box opens.

2. **Click the Services tab and click Add.**

3. **Select Solstice File Sharing and click OK.**

   You return to the Network dialog box. Solstice File Sharing is added to the list of network services.

4. **Select Solstice File Sharing, and then click Properties.**

   The Solstice File Sharing Configuration window opens.

5. **On the NFS Server tab, do the following**:

   a. **Verify that Enable Solstice NFS Server is selected.**

      If not, click the option to select it.

   b. **(Optional) Keep the Log NFS Server Activity option selected so that you have continuing access to the log of NFS Server activity and problems.**

6. **Click OK.**

   You may be prompted to insert the Windows NT CD-ROM.

7. **Click OK again.**

8. **Click Yes when asked if you want to restart your computer.**

▼ To Enable File and Printer Sharing on Windows 95

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Network.**

   The Network dialog box opens.

2. **Click Add.**

   The Select Network Component Type dialog box opens.

3. **Select Service and then click Add.**

   The Select Network Service dialog box (Figure 4–1) opens.

Figure 4–1 Select Network Service Dialog Box

4. **In the Manufacturers list, select SunSoft, and in the Network Services list, select Solstice File and Printer Sharing (Figure 4–2).**

Figure 4–2 Selecting Solstice File and Printer Sharing

5. **Click OK.**

   You return to the Network dialog box. The Solstice network services you installed appear in the list of installed network components.

6. **In the list of installed network components, select Solstice File and Printer Sharing and click Properties.**

7. **On the NFS Server tab, do the following:**

   a. **Verify that Enable Solstice NFS Server is selected. If not, select the option to ensure that NFS Server starts when Windows starts.**

   b. **(Optional) Keep the Log NFS Server Activity option selected (recommended) to get access to the log of NFS Server events.**

8. **Click OK.**

   You return to the Network dialog box.

9. **Click OK again.**

   Windows 95 will inform you that you must restart Windows for your changes to take effect.

10. **Click Yes when offered to restart Windows.**

NFS Server on Windows NT

On Windows NT, NFS Server runs as a service. This allows NFS Server to run in the background without requiring that the user who provides the service be logged in.

By default, NFS Server is set to be started manually under the system Administrator's account (Local System Account.) You can change the setting to have NFS Server start automatically.

The NFS Sharing property sheet is accessible only to NT Power Users and above and is not displayed in accounts of ordinary users. The Sharing property sheet is accessible by means of two commands:

- The Properties command in the File menu in Windows Explorer
- The Sharing command after right-clicking a selected folder on a local drive

NFS Server supports only Version 2 of NFS over UDP.

NFS Server does not support file locking/sharing.

Running NFS Server

By default, the local system account is the Administrator's account. You must be logged in as an Administrator or as an NT Power User with Full Control access rights to carry out the following procedures.

▼ To Start NFS Server from the Local System Account

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Services.**

2. **Select Solstice NFS Server and proceed as follows:**
   - To start the service manually, click Start.
   - To start the service automatically, click Startup, select Automatic, click OK and then click Start.

3. **Click Close.**

   NFS Server will start the next time you start Windows NT.

▼ To Start NFS Server from a Specific User Account

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Services.**

2. **Select Solstice NFS Server and click Startup.**

3. **In Log On As, click the option This Account.**

4. **Either type the account name manually, or click the More (...) button to select the account name from the Names list.**

5. **Type the password, confirm it, and then click OK.**

▼ To Stop NFS Server

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Services.**

2. **Select Solstice NFS Server and click Stop.**

   An informational message indicates that the NFS Server service is stopped.

3. **Click Close.**

Granting Access to Shared Resources on Windows NT

You can grant access to a file or directory by selecting it in Explorer and designating it as an NFS shared folder or device. You can restrict access by system rather than by user, and by specifying Read-Only or Full access rights.

▼ To Share Folders and Drives

1. **If necessary, start NFS Server.**

   Note that you can export folders and local drives without NFS Server running. However, the exported shares will not become available until you start NFS Server.

2. **Start Explorer or My Computer.**

3. **In My Computer or in the Explorer folders pane, select the device or the folder that contains the files you want to share.**

4. **Right-click to open the pop-up menu and then click Properties.**

   The property sheet for the selected device or folder opens.

5. **Click the NFS Sharing tab.**

6. **Click the Shared As option.**

   The name of the selected device or folder appears in the Share Name field. Optionally, replace the name with a name that is meaningful to users when they browse the PC as an NFS Server.

7. **Specify the type of access.**

   - Read-Only: Users of remote systems can display the contents of the shared folder or drive, or execute any executable therein. They cannot modify or delete any files or folders in the shared folder or drive.

- Full: Users of remote systems can read, write, execute, and delete the shared folder or drive. These permissions are subject to restrictions that may apply on a folder or file-by-file basis on an NTFS file system.

8. **Specify which access restrictions apply.**
   - Click Unrestricted if you want to allow all network systems to access the shared folder or device with the type of access specified in Step 7 on page 66.
   - Click Restricted and then click Access Restrictions. The Access List dialog box opens.

9. **Complete the Access List dialog box as follows.**
   a. **Enter the name of the system whose users may access the shared folder or device, or select from the list of systems.**

   b. **Click Add.**
      The system name appears in the Clients Granted Access field.

   c. **Click OK.**
      The Access List dialog box closes.

10. **Click OK.**
    The property sheet closes.

▼ To Remove Access to Shared Resources on Windows NT

1. **Start Explorer.**

2. **In the Explorer folders pane, select the device or the folder for which you want to revoke access.**

3. **Right-click to open the pop-up menu and then click Properties.**
   The property sheet for the selected folder opens.

4. **Click the NFS Sharing tab.**

5. **(Optional) Change the access type.**

6. **In Access Restrictions, select the Restricted option, and then click the Access List button.**
   The Access List dialog box opens.

7. **In Clients Granted Access, select the name of the system whose users may no longer access the shared folder or device, and then click Delete.**

   If necessary, repeat the previous step for additional systems.

8. **When you are finished, click OK to return to the property sheet.**

9. **Click OK.**

   The property sheet closes.

   Users on the systems that were removed immediately lose access to the device or folders.

Viewing Exported Folders and Drives on Windows NT

Folders or local drives that are shared using Windows NT sharing options are recognized by the “folder with hand” icon in the Explorer window. Solstice NFS Server uses a different mechanism for identifying folders or local drives that are shared using NFS Server.

▼ To View a List of Exported Folders and Drives

1. **Double-click Network Neighborhood.**

2. **Double-click Entire Network and then double-click NFS Servers.**

3. **Browse for your Windows NT system.**

4. **Double-click the name of your system to display a list of your exported folders and drives.**

5. **(Optional) To view the share details, right-click an export and click Properties.**

   If the export has been shared using NFS Server, then the same NFS Sharing Properties page that was used to specify the sharing attributes, opens.

How NFS Server Handles Access Requests from Remote Hosts

When NFS Server receives an access request from a remote host, it verifies the following.

- The requesting host is allowed access as defined in the NFS Sharing Access Restriction option.

- The access operation is allowed as specified in the NFS Sharing Access Type option (read only or full).
- The account under which NFS Server is running has the permission to perform the operation.

If the answer to any of these verifications is no, access to the exported share is denied. If the answer to all verifications is yes, access to the exported share is granted.

In order to share folders or drives, the user exporting the folder or drive must be an NT Power User or above. The NFS sharing property sheet is not visible to ordinary users. Once shared, the resource remains shared regardless of the current user logged in. Note that folders and drives can be shared using the Microsoft Sharing tab independently of using Solstice NFS Sharing.

Security Control When Sharing Folders and Drives

By default, NFS Server runs as a LocalSystem service from the system account. Usually, this is the Administrator's account which, also by default, has Full Control access rights. NFS Server does not change existing NT permissions on directories and files. If the remote system has Full access rights to the exported share, NFS Server exports the file system privileges of the local user (that is, the user account under which NFS Server is started) to the remote system. This is important in the case of Windows NT with an NTFS file system where files have been marked with additional security attributes.

In effect, a remote user on an NFS Client who accesses files on a Windows NT machine, has the privileges of the account under which the NFS Server service is started.

Limiting Remote System Access

You can limit the access privileges of users on remote systems as follows.

- Create a user account with limited access rights and permissions and configure NFS Server to run from that account. NFS Server will take on the security attributes specified for that account and export those privileges to the remote system. Refer to the Microsoft Windows NT Workstation or Server documentation for creating user accounts.
- For shared folders and drives that contain important files, restrict access to read-only or restrict access to well-known and trusted hosts.

Logging NFS Server Events on Windows NT

With NFS Server logging enabled, any interaction between the NFS clients and server is written in the Network Event's log file, which by default is named `C:\LOGGING.TXT`.

Enabling the logging of NFS Server events helps you isolate the problem when:

- A client fails to mount a PC folder or device from a server, and gets no response from that server.
- A client can mount a folder or device from a server, but cannot do anything with that folder or device while getting no error message.
- The error message does not clearly indicate whether the problem exists on the server, on the client, or on both.

You can view NFS Server events in two places:

- In the Solstice Network Event Log window and its associated `C:\LOGGING.TXT` log file.
- In the Windows NT Event Viewer window.

▼ To Enable NFS Server Event Logging Using Solstice Network Event Log

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Network.**
2. **Click the Services tab.**
3. **Select Solstice File Sharing and click Properties.**
4. **Click the Logging tab.**
5. **Select the options Enable Network Event Log and Save Log Messages To File.**
   The default file name is `C:\LOGGING.TXT`.
6. **Click OK and then click Close.**
7. **Restart Windows NT when prompted.**
8. **Start the Network Event Log utility by double-clicking its icon in the Solstice Utilities program group.**

The Network Event Log window opens. You can configure event logging by clicking Display and then clicking Configure (see the following directions).

9. **Minimize the Network Event Log.**

   NFS Server events are recorded and displayed in the Network Event Log window but are not written out to the `log` file. Only after you exit Network Event Log will `C:\LOGGING.TXT` be updated with the current status of NFS Server events.

▼ To Configure Network Event Log for NFS Server Events

1. **If necessary, start Network Event Log from the Solstice Utilities program group.**

2. **From the Display menu, click Configure.**

3. **Complete the Network Event dialog box as follows.**
   - (Optional) Adjust the time frame when events should be logged. The default is every 20 minutes.
   - To log the messages locally, click the option Log Messages To File and type the name of the log file (the default is `C:\LOGGING.TXT`).
   - To log the message on a remote host, click the option Log Messages To Host and type the name of a remote server that runs the `syslogd` program.
   - Select the severity level of the messages to be logged. Click the Help button to display the Network Event online Help, click the Index tab and type **`severity`** to display online information about available severity levels.

4. **Click Save.**

5. **If you will start monitoring NFS Server events now, minimize (do not exit) Network Event Log.**

   Messages will appear in the Network Event Log window as they occur. Only after you exit Network Event Log are these messages written into the `C:\LOGGING.TXT` log file.

▼ To View NFS Server Events Using Event Viewer

1. **From the Start menu, point to Programs, point to Administrative Tools, and then click Event Viewer.**

2. **Choose the Log menu and click Applications.**

3. **Isolate the events pertaining to NFS Server by choosing the View menu and clicking Filter Events.**

4. **Scroll through the Source list to view event generators, select Solstice NFS Server, and then click OK.**

   NFS Server messages are displayed.

   Double-click an NFS Server message to display more details.

NFS Server on Windows 95

The NFS Server runs as a daemon on Windows 95, and enables the PC client to share folders and local files. The NFS Server supports version 2 of NFS over UDP. NFS Server does not support file locking.

Sharing Directories and Devices

To share PC folders and local drives with other users using NFS Server, the PC user must be running NFS Server and “export” one or more folders or drives, such as a CD-ROM drive. Once the PC user has exported the folders or drives, users from trusted hosts can mount that folder or drive and access it.

The PC user restricts access to the folders or drives by system, rather than by user, and by giving either Read Only or Full access rights.

Running NFS Server

When NFS Server is running, the NFS Server icon appears in the status area.

Right-click on the icon to open the NFS Server menu from which you can:

- Display a list of shared directories and devices
- Suspend the NFS Server temporarily
- Enable or disable NFS Server logging
- Access the NFS Server Help
- Exit NFS Server

Sharing Properties

Use the NFS Server and Logging property sheets for adjusting the default values used by the NFS Server.

Before you can modify these property sheet settings, you must first add Solstice File and Printer Sharing as a network component, if this was not done during the installation process. See “Enabling NFS File Services” on page 62.

▼ To Start NFS Server

- **From the taskbar, click the Start button, point to Programs, point to Solstice Utilities, and then click NFS Server.**

NFS Server starts and its icon appears in the status area.

▼ To Suspend NFS Server

1. **Right-click the NFS Server icon in the status area.**
2. **Click Suspend.**

   Users temporarily lose access to the shared folders and devices.

▼ To Resume NFS Server

1. **Right-click the NFS Server icon in the status area.**
2. **Click Resume.**

   Users regain access to the shared folders and devices.

Granting Access to Shared Resources on Windows 95

You can grant access to a file or directory by selecting it in Windows Explorer and designating it as an NFS shared folder or device. You can restrict access to the folder or device by system, rather than by user, and by specifying read and write access rights.

▼ To Grant Access to Shared Resources

1. **Start Explorer.**

2. **In the Explorer folders pane, select the folder that contains the files you want to share, or select a device such as your CD-ROM drive.**

3. **Right-click and then click Properties in the pop-up menu.**

4. **On the NFS Sharing tab, select Shared As.**

5. **(Optional) Replace the name of the folder or the device with a new name.**

6. **(Optional) Specify the access type.**
   - Click Full if you want to grant read, write, execute, and delete rights.
   - Click Read Only to limit the access to reading.

7. **(Optional) Specify which access restrictions apply.**
   - Click Unrestricted if you want to allow all network hosts to access the shared folder or device with the type of access specified in step 6.
   - Click Restricted and then click the Access List button to limit access to specific hosts.

8. **Complete the Access List dialog box as follows:**
   - Enter the name of the host whose users may access the shared folder or device, or select it from the list of host names.
   - Click Add. The host name appears in the Clients Granted Access field.

9. **Repeat the previous step for additional systems.**

10. **When you are finished, click OK to return to the Properties sheet.**

11. **Click OK.**

    Users on the selected systems gain immediate access to the shared resources.

▼ To Revoke Access to Shared Resources

1. **Start Explorer.**

2. **In the Explorer folders pane, select the folder (or the device) for which you want to revoke access.**

3. **Right-click and then click Properties in the pop-up menu.**

4. **On the NFS Sharing tab, do one of the following:**

- Select Not Shared to revoke access to all users of all hosts specified in the Access List.
- Click the Access List button to open the Access List dialog box.

5. **Select the host whose users should no longer have access to the folder or device, and then click Delete.**

6. **When you are finished, click OK to return to the Properties sheet.**

7. **Click OK.**

   The Properties sheet closes.

   The selected folder or device is no longer shared and network users immediately lose access.

Logging NFS Server Events on Windows 95

With NFS Server logging enabled, any interaction between the NFS clients and server is written in the NFS log file `c:\LOGGING.TXT`.

To start NFS Server logging, you must enable both NFS Server logging and Network Event logging.

▼ To Enable NFS Server Logging

If logging of NFS Server events has not been enabled in the Network control panel, you can start the logging manually.

1. **Right-click on the NFS Server icon in the status area.**

   The NFS Server menu opens.

2. **Select NFS Logging if it is not already selected.**

3. **Start the Network Event Log from the Solstice Utilities program group.**

   The Network Event Log window opens.

4. **Configure Network Event Log.**

5. **Minimize the Network Event Log.**

NFS Server events will initially be recorded and displayed in the Network Event Log window and not in the `C:\LOGGING.TXT` file. Only after you exit Network Event Log will `C:\LOGGING.TXT` be updated with the current status of NFS Server events.

▼ To Configure Network Event Logging

1. **Click the Start button, point to Programs, point to Solstice Utilities, and then click Network Event Log.**
   The Network Event Log window opens.

2. **On the Display menu, click Configure.**
   The Network Event Log dialog box opens.

3. **Set the desired options, such as how frequently network events are to be written, the name of the log file, the severity levels of the messages you want to record, and so on.**
   Click Help for detailed information on each option.

4. **Click Save.**

5. **Minimize the Network Event Log.**
   Activities can be logged as they occur.

▼ To Disable NFS Server Logging

1. **Right-click the NFS Server icon in the status area.**
   The NFS Server menu opens.

2. **Click NFS Logging.**
   The check box is no longer selected.

CHAPTER 5

Printing

This chapter describes how to set up print servers and mount network printers on Microsoft Windows computers running the Solstice Network Client software.

You can read background and procedural information throughout this chapter, or you can use the following references to go directly to a specific topic.

- "Setting Up Printing" on page 77
- "Road Map for Printer Setup" on page 78
- "Browsing for Network Printers" on page 81
- "Mounting Network Printers on Print Clients" on page 83
- "Enabling DOS Printing " on page 87
- "Viewing Print Jobs" on page 88
- "Sharing Local Printers on Windows NT" on page 90
- "Providing LPD Print Services on Windows 95" on page 93
- "Managing LPD Printing" on page 99

Setting Up Printing

Setting up the print environment for Solstice Network Client is accomplished in two stages:

- First, print servers must be configured correctly so they can process print requests from print clients.
- Then, print clients must mount printers and specify which print protocol to use.

The next section provides high-level guidelines to the tasks that must be done on the print servers and print clients before you can print successfully.

Road Map for Printer Setup

The four tables in this section constitute a road map of the requirements for setting up print servers and print clients in a Solstice Network Client environment.

Print Servers

- Table 5–1 covers setting up print servers to provide PCNFSD print services.
- Table 5–2 covers setting up print servers to provide LPD print services.

Print Clients

- Table 5–3 covers setting up print clients to send PCNFSD print jobs.
- Table 5–4 covers setting up print clients to send LPD print jobs.

Setup Requirements for Print Servers

Print servers provide either PCNFSD or LPD print services, or both, to print clients.

Table 5–1 identifies the tasks necessary to configure and set up print servers to handle PCNFSD-based print jobs from print clients.

TABLE 5–1 Tasks Needed to Configure and Set up Print Servers for PCNFSD-based Jobs

UNIX Server	Windows 95 Server	Windows NT Server
Install and configure the `rpc.pcnfsd` daemon. Then, export the print spool directory with no access restrictions. See *Installation and Licensing Guide -> Setting Up Server Programs -> The PCNFSD Daemon* for detailed instructions.	No PCNFSD print services are provided.	No PCNFSD print services are provided.

Table 5–2 identifies the tasks necessary to configure and set up print servers to handle LPD-based print jobs from print clients.

TABLE 5–2 Tasks Needed To Configure and Set Up Print Servers for LPD-based Jobs

UNIX Server	Windows 95 Server	Windows NT Server
Install and configure the LPD daemon. Refer to the man page or documentation set for the operating system for detailed instructions.	Install and configure the Solstice NFS Client LPD Print Server Utility, and enable it to accept incoming print jobs. See "Setting Up an LPD Shared Network Printer" on page 94 for details.	Add the Microsoft TCP/IP Print service to the Services environment in the Control panel to support UNIX print jobs. Then, using the Add Printer Wizard, select the sharing option to set up the printer as a shared network printer. See "Setting Up an LPD Shared Network Printer" on page 94.

Setup Requirements for Print Clients

Table 5–3 highlights the tasks necessary to send PCNFSD-based print jobs to network printers.

TABLE 5–3 Tasks Needed to Send PCNFSD-based Jobs

UNIX Client	Windows 95 Client	Windows NT Client
No PCNFSD print jobs can be sent from a UNIX workstation to Windows computers running Solstice Network Client.	Add Solstice NFS Client service to the print client's network environment. Then, using the Add Printer Wizard, mount the network printer and specify the PCNFSD print protocol using the following syntax: `pcnfs://`*servername/ queuename*. See "To Mount a Network Printer on Windows 95" on page 83 for details.	Add the Solstice NFS Client service to the print client's network environment. Mount a PCNFSD network printer using the Add Printer Wizard or Network Neighborhood. See "To Mount Network Printers on Windows NT" on page 84for details.

Table 5–4 highlights the tasks necessary to send LPD-based print jobs to network printers.

TABLE 5–4 Tasks Needed to Send LPD-based Jobs

UNIX Client	Windows 95 Client	Windows NT Client
Use Admin Tool, or an equivalent printer administration tool, to add the network printer from a Windows 95 or Windows NT print server. See "To Mount a Shared PC Printer from a UNIX Workstation" on page 86 for the details.	Add the Solstice File and Print Sharing service and the Solstice NFS Client service to the print client's network environment. Using the Add Printer Wizard, mount the network printer and specify the LPR print protocol using the following syntax: `lpr://` *servername/ queuename*. See "To Mount a Network Printer on Windows 95" on page 83 for details.	Add the Microsoft TCP/IP printing service and the Solstice NFS Client service to the print client's network environment. Using the Add Printer Wizard, mount an LPR network printer. See "To Mount Network Printers on Windows NT" on page 84for step-by-step instructions.

Browsing for Network Printers

You can browse for printers only on servers running the `pcnfsd` daemon. You cannot browse for LPR printers.

You can start browsing from the Add Printer Wizard or from Network Neighborhood. In either case, the Solstice printer name takes a different form than when you enter a printer name manually.

When browsing, the name takes the form: `\~`*hostalias*`\`*queuename*. Here, *hostalias* is an internal name and may not be an actual server name.

Browsing makes printer resources on servers running the `pcnfsd` daemon visible to users. But users cannot connect to these printers unless the print spool directory on the server is exported. The system administrator can decide to make a PCNFSD printer available to users by exporting the print spool directory on the print server. For detailed instructions on installing the `pcnfsd` daemon and exporting the print spool directory, see Appendix B.

▼ To Browse for PCNFSD Printers on Windows 95

1. **From Network Neighborhood, click the Entire Network icon.**

2. **Double-click NFS Servers.**

   The list of NFS servers appears.

3. **Open each server icon to see which printers it offers.**

   Note - When you find a printer you want to mount, look for a `usr`, `var`, `spool`, or `pcnfs` folder in the list of resources. If you do not see one of these folders, you cannot connect to the printer either because the print spool directory is not exported or has been changed to some other location on the server.

   ---

4. **Double-click the printer or drag the printer icon to the Printer control window.**

5. **When you are asked "Do you want Windows to set up the printer and continue this operation?", click Yes.**

   The Add Printer Wizard starts.

Figure 5–1 Browsing for Printers

6. **Complete the remaining questions as required.**

▼ To Browse for Printers on Windows NT

1. **Double-click Network Neighborhood.**

2. **Double-click Entire Network, double-click Solstice_NFS_Client, and then double-click NFS Servers.**

3. **Double-click a server name to reveal its resources.**

   You will recognize PCNFSD printers by the `pcnfs` or `var` folder listed under the printer icon. LPR printers do not display such folders. If you see printer icons but no `pcnfs` or `var` folders, you will not be able to mount the printer.

4. **Right-click the icon of the printer to be mounted and click Open or Install on the pop-up menu.**

   The Add Printer Wizard starts. Alternatively, drag the selected printer icon and drop it in the Printers Window.

   See “To Mount Network Printers on Windows NT” on page 84for step-by-step instructions.

Mounting Network Printers on Print Clients

On Windows 95, Solstice NFS Client supports both the PCNFSD and LPR print protocols. Mount network printers using the Add Printer Wizard and specifying the print protocol in the printer's path name.

On Windows NT, Solstice NFS Client provides support for the PCNFSD print protocol; Microsoft Windows NT provides support for the LPR print protocol. In both cases, you need to add a local printer port for mounting the network printer using the Add Printer Wizard.

Specifying Which Print Protocols to Use

You can add a printer to the Solstice network environment using the Add Printer Wizard. When you start the process from the wizard, you can specify which print protocol to use as in the following example:

`lpr://`*`servername/queuename`*

Here, `lpr` is the print protocol, *servername* is the server name, and *queuename* is the printer name. For the PCNFSD protocol, use this syntax:

`pcnfs://`*`servername/queuename`*

▼ To Mount a Network Printer on Windows 95

1. **Click the Start button, point to Settings, and then click Printers.**

2. **Double-click Add Printer to start the Windows 95 Add Printer Wizard.**

3. **When prompted, select To Add A Network Printer.**

4. **In the path name of the network printer, add the print protocol to the beginning of the printer name, using the following syntax:**
   - LPR print protocol: `lpr://`*`servername/queuename`*. For example, to add a network printer with a queue name `dopey_laser` connected to a print server named `dopey`, enter this path name: `lpr://dopey/dopey_laser`.

- PCNFSD print protocol: `pcnfs://`*servername/queuename*. For example, to add a network printer with a queue name `dopey_laser` connected to a print server named `dopey`, enter this path name: `pcnfs://dopey/dopey_laser`.

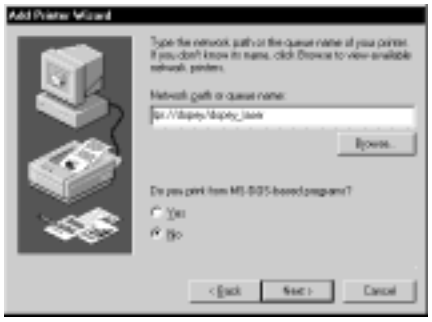


Figure 5–2 Add Printer Wizard Dialog Box

5. **Complete the remaining Wizard questions as required.**

▼ To Mount Network Printers on Windows NT

Before you begin this procedure, you must know the names of the server and the printer queue. If you need to find a PCNFSD printer, see "To Browse for Printers on Windows NT" on page 82. Also, you must have added the Solstice NFS Client service to your network environment.

1. **Click the Start button, point to Settings, and then click Printers.**

2. **Double-click the Add Printer icon.**

3. **Click Network Printer and click Next.**

   The Connect to Printer dialog box opens. If the option Expand By Default is checked, a list of available NFS print servers that run the `rpc.pcnfsd` daemon is displayed. If the option Expand By Default is not checked, double-click Solstice NFS Client, and then double-click NFS Servers to reveal the NFS print servers.

4. **Double-click an NFS print server to reveal its available printers.**

5. **Continue as follows**:

   a. **To mount a PCNFSD printer.**

Click the printer you want to mount and click OK. The software automatically completes the printer's path name in the Printers field, using the syntax `pcnfsd://`*server_name/printer_queue_name*.

b. To mount an LPR printer.

Do NOT select a printer from the list, but type its path name in the Printers field, using the syntax `lpr://`*server_name/printer_queue_name*.

6. **Click OK to dismiss the informational message that appears.**
7. **Select the manufacturer and printer model from the lists and click OK.**
8. **(Optional) Set the printer as the default printer and click Next.**
9. **Click Finish.**

Alternative Syntax for Specifying the Printer's Path Name

You can specify the printer path name in a number of ways. For example, to add a printer that has the queue name `hornbeam` and is attached to a server called `melody`, you can specify the port as follows:

- `melody:hornbeam`
- `pcnfsd:\\melody\hornbeam`
- `pcnfs:\\melody\hornbeam`
- `pcnfsd://melody/hornbeam`
- `pcnfs://melody/hornbeam`
- `\\melody\hornbeam`
- `//melody/hornbeam`
- `123.456.78.90:hornbeam` (where `123.456.78.90` is the IP address of the server `melody`)

▼ To Delete Printer Ports on Windows NT

1. **Click the Start button, point to Settings, and then click Printers.**
2. **On the File menu, click Server Properties.**
3. **Select the PCNFSD or LPR port to be deleted and then click Delete Port.**
4. **Click OK in the warning message box.**

5. **Click OK again.**

Mounting Shared PC Printers in a UNIX Environment

Individual UNIX users with superuser privileges can mount PC printers that are shared on Windows 95 computers running LPD Print Server, or are shared using the sharing capabilities of the Add Printer Wizard on Windows NT.

▼ To Mount a Shared PC Printer from a UNIX Workstation

1. **From a command window, enter the command** `su` **to become superuser.**

2. **At the superuser system prompt, enter** `admintool&`**.**
   The Administration Manager starts.

3. **Click Host Manager, and then click the appropriate name service to verify that the Windows computer is listed in the hosts list.**

4. **Close the Host Manager dialog when finished.**

5. **Click Printer Manager to open the Printer Manager dialog.**

6. **Click Edit, click Add Printer, and then click Add Access To Remote Printer.**

7. **Complete the Add Access To Remote Printer dialog as follows:**
   a. **In Printer Name, enter the queue name of the shared PC printer, for example,** `dopey1_laser`**.**

   b. **In Printer Server, enter the name of the Windows computer to which the printer is connected, for example,** `dopey1`**.**

   c. **In Comment, add some text that identifies the printer to the users, for example,** `Laser in Jackie's office`**.**

   d. **For Printer OS Server, click BSD.**

   e. **(Optional) Set the printer as the system default printer.**

   f. **Click Add and close the Access to Remote Printer dialog.**

8. **Quit the Administration tool, press Ctrl+D to exit superuser.**

Enabling DOS Printing

A DOS print redirector enables you to print from a DOS application to a network printer. To enable DOS printing, you must first add the printer using the Windows 95 or Windows NT Printer Wizard.

Once the printer has been added, enable DOS printing by associating the network printer with an LPT port on your computer (referred to as capturing a port). Print requests that are sent to that port are then redirected to the network printer.

Enabling DOS Printing on Windows 95

On a Windows 95 system, you can enable DOS printing by capturing a printer port with Print Wizard or with the `net use` command:

`net use LPT# \\`*`server_name`*`\`*`printer_queue_name`*

where # is number 1-4.

To Enable DOS Printing on Windows 95 Using Print Wizard

1. **Click the Start button, point to Settings, and then click Printers.**
2. **Right-click a printer icon and then click Properties.**
3. **Click Details.**
   The printer Properties window opens.
4. **Click Capture Printer Port.**
   The Capture Printer Port window opens.
5. **Select an LPT port: LPT1, LPT2, LPT3, or LPT4.**
6. **Type the path of the selected printer. For example,**

`pcnfsd://`*`server_name/printer_queue_name`*

or

`lpr://`*server_name/printer_queue_name*

7. **Click OK on the Capture Printer Port window.**

8. **Click OK in the printer Properties window.**

Enabling DOS Printing on Windows NT

On a Windows NT system, you can use the print pooling option to pool a network printer with an unused LPT port. When you send a print request to that LPT port, the document will be redirected to the network printer.

To Enable DOS Printing on Windows NT

1. **Click the Start button, point to Settings, and then click Printers.**

2. **Right-click a printer icon and then click Properties.**
   The printer Properties page opens.

3. **Click Ports.**

4. **Select Enable Printer Pooling.**

5. **Select a port— LPT1, LPT2, or LPT3—that does not have a local printer attached to it.**
   You should now be able to print to the LPT port from a 16-bit DOS application.

Viewing Print Jobs

You can monitor the status of your print jobs using the Print utility on a Windows 95 or NT system or using the `lp` commands on a UNIX system.

▼ To View Print Jobs on Windows 95 and Windows NT

1. **Click the Start button, point to Settings, and then click Printers.**

   The Printers window opens.

2. **Double-click the shared printer's queue name.**

   A window opens that shows details such as the document name, the status, the owner, the progress, and the start time.

▼ To View Print Jobs on UNIX Systems

Use the print commands of your UNIX operating system to view the available printers, the status of print requests, and to cancel print requests.

For example, assuming the queue name of a shared PC printer is `dopey1_laser`, you would enter the commands shown in Table 5–5 in the Solaris 2.6 operating environment or compatible versions.

TABLE 5–5 Print Commands for the Solaris 2.6 Operating Environment or Compatible Version

To do the following...	Enter this command in Solaris 2.6 or compatible versions
Display status information about print jobs on the PC printer	`lpstat dopey1_laser` *filename*
Print to the shared PC printer when it is not the default printer	`lp -d dopey1_laser` *filename*
View print jobs sent to the shared PC printer	`lpstat -p dopey1_laser`
Cancel print jobs sent to the shared PC printer	*cancel job-ID*

Sharing Local Printers on Windows NT

On Windows 95, a Solstice Network Client can act as a print server by using the LPD Print Server utility.

The Solstice Network Client software on Windows NT does not provide an LPD Print Server utility. Instead, you share local printers using the printer sharing option available in the Add Printer Wizard on Windows NT.

This section provides basic procedures for sharing local printers. For full details, refer to the Microsoft documentation for Windows NT Workstation or Windows NT Server.

The procedures provided in this section assume that you have already mounted the printer locally. You be logged in as Administrator or as an NT Power User with Full Control access rights to configure a shared printer.

Use the printer's Properties dialog box to configure the settings for the shared printer. See "To Configure a Local NT Printer as a Shared Network Printer" on page 91.

If the printer will be servicing print jobs coming from UNIX print clients, you will have to add the TCP/IP Print Server service to the system's Services environment. For instructions, see "To Add the TCP/IP Print Server Service" on page 90.

Your printer may be shared with users from different platforms. You will need to prepare a list of the operating systems, version numbers, and CPU platforms of the print clients that will access the NT print server. Windows NT Workstation 4.0 supports computers running Windows 95 as well as Alpha, MIPS, and PowerPC systems running Windows NT. You may need to have the Windows NT CD-ROM available and those of the other platforms.

▼ To Add the TCP/IP Print Server Service

To service print jobs from UNIX print clients, the Windows NT print server must be running the LPDSVC service. Start the TCP/IP Print Server in the Services environment.

1. **Click the Start button, point to Settings, and then click Control Panel.**

2. **Click Services.**
   The Services dialog box opens.

3. **Select TCP/IP Print Server from the list of Services and then click Startup.**

4. **Click Automatic and click OK.**
   This starts the LPDSVC service on the Windows NT computer.

5. **Click Close and reboot the system when prompted.**

▼ To Configure a Local NT Printer as a Shared Network Printer

1. **Click the Start button, point to Settings, and then click Printers.**

   The Printers window opens.

2. **Right-click the icon of the printer you want to share and then click Properties on the pop-up menu.**

   The printer's Properties dialog box opens. You can set all configuration options in this dialog box.

3. **Click the Scheduling tab.**

   When sharing a local printer, you may find that applications run sluggishly while documents are spooled and printed. You can overcome this by specifying when the printer is available.

   a. **Select the From option and type the start and end times.**

   b. **Keep the option Spool Print Document selected.**

   c. **Select the option Start Printing After Last Page Is Spooled.**

      This ensures that the whole document has been spooled before printing starts.

4. **Click the Sharing tab.**

   You must specify a share name for the printer, and specify which printer drivers must be loaded on the Windows NT system to service the print requests from various clients.

   a. **Click Shared.**

      Windows NT automatically populates the share name with an eight-character queue name. You can replace the share name with a more meaningful name.

   b. **From the Alternative Drivers list, select all the Windows platforms that may send print jobs to the printer.**

      For example, if some users use an Alpha machine running Windows NT 4.0, select Windows NT 4.0 Alpha. Click each platform that you want to include. You may need to install drivers from your Windows NT CD-ROM, or from those of other systems.

5. **Click the Security tab.**

   You must specify who can access the printer. While not required, you may also wish to specify which print events to monitor and log.

   a. **Click Permissions.**

The Printer Permissions dialog box opens.

b. Click Add.
The Add Users And Groups dialog box opens.

c. In the Names list, select Network, and then click Add.

d. In the Type of Access list, select Print.
This setting enables the network users to pause, resume, restart and delete print jobs.

e. Click OK to close the Add Users And Groups dialog box.
You return to the Printer Permissions dialog box.

f. Click OK to close the Printer Permissions dialog box.

Logging Print Events on Windows NT

You can monitor print events and problems. Before you begin, verify that Auditing is turned on. Then set up print logging.

▼ To Enable Auditing

1. **Click the Start button, point to Programs, point to Administrative Tools, and then click User Manager.**

2. **Select Audit from the Policies Menu.**

3. **Click Audit These Events and select File and Object Access.**

▼ To Set Up Logging for Print Events

1. **Click the Start button, point to Settings, and then click Printers.**
   The Printers window opens.

2. **Right-click the icon of the printer you want to share and then click Properties on the pop-up menu.**
   The printer's Properties dialog box opens.

3. **Click Auditing.**
   The Printer Auditing dialog box opens.

4. **Click Add, select Network from the Names list, and then click OK.**

5. **For each of the listed Events to Audit, select if you want to log the events if they are carried out successfully, or if they failed, or both.**

6. **Click OK.**
   The Printer Auditing dialog box closes.

7. **Click OK again.**
   The Properties dialog box closes.

At this point, if you have configured drivers that are not loaded into your computer, you will be prompted to insert one or more CD-ROMs.

▼ To View Logged Print Events

1. **Click the Start button, point to Programs, point to Administrative Tools, and then click Event Viewer.**
   The Event Viewer window opens.

2. **Filter out non-print-related events.**
   a. **From the View menu, click Filter Events.**

   b. **Choose LPDSVC to view events pertaining to the TCP/IP Print Server service.**

   c. **Choose Print to view events pertaining to print jobs.**

   d. **Click OK.**

Providing LPD Print Services on Windows 95

The Solstice NFS Client includes a UNIX-like LPD Print Server that runs on Windows 95. Using this software, you can share a printer connected to your PC with other users on the network. When your PC is running the LPD print daemon, a

coworker can send a job to your local printer from a UNIX system or from a computer running Microsoft Windows.

When active, the LPD Print Server runs minimized, and its icon appears in the taskbar status area. Start LPD Print Server by double-clicking its icon, or enable the LPD server to start up automatically each time Windows starts.

LPD Print Server relies on the Windows Print Manager to spool print requests and display information. The print server processes print requests on a first-come first-served basis. When the print request has been processed, LPD Print Server directs the processed requests to the LPD spool directory.

Windows Print Manager starts automatically when you start LPD Print Server. When you exit Print Manager, LPD Print Server stops running.

In most situations, you would set up LPD Print Server to start automatically when Windows starts. You can also start LPD Print Server manually.

Note - The LPD Print Server only supports the LPR print protocol.

Setting Up an LPD Shared Network Printer

The LPD Server lets you share a PC printer with any PC or UNIX user with network access to that PC. To set up an LPD Shared Network Printer:

- Set up the LPD Server on the PC with the shared printer
- Start up the LPD Print Server so it can accept print requests from network users.

You can access LPD settings for the LPD Print Server control menu. Click the LPD icon to open this menu.

▼ To Set Up the LPD Server

Note - The Solstice File and Printer Sharing service should be added automatically as part of your installation. However, if it does not appear in the Network Properties page of the Control Panel, you must add it manually. See “To Enable File and Printer Sharing on Windows 95” on page 63.

---

1. **From the taskbar, click the Start button, point to Settings, click Control Panel, and then double-click Network.**

   The Network Properties dialog box opens.

2. **Select Solstice File And Printer Sharing and click Properties.**

3. **Click the Printer Sharing tab.**

4. **Select Enable Solstice LPD Server.**

   This starts the LPD Print Server daemon on the PC. The option is enabled by default.

5. **If you want to log the print activities in a log file:**

   a. **Select Log LPD Server Activity.**

   b. **(Optional) Select a different font and point size for the LPD Print Server messages that are written in the log file.**

      The fonts listed are those installed on the PC.

6. **Select the PC printer from the list in the Add Printer dialog box and click OK. Remain in the Properties dialog box.**

7. **In Queue Name, enter a printer queue name. For example:** `dopey_laser`**.**

   The printer's queue name must follow the naming rules and conventions of UNIX printer queues. The first character cannot be a number, and the length of the queue name cannot exceed fourteen characters.

8. **Accept Detect Automatically (default) as the file type checking option.**

9. **Decide how the printer driver should interpret carriage returns and line feeds when formatting binary files to be printed.**

   Choosing Assume Binary as the file type affects how the printer driver interprets carriage returns and line feeds. See "Interpreting Carriage Returns and Line Feeds" on page 101 for more information about your choices.

10. **(Optional) Replace the default spool directory** `c:\tmp` **with a directory of your choice. For example:** `pc_spool`**.**

    The directory will be created if it does not exist.

11. **Click OK.**

    The LPD Print Server daemon starts and the LPD Print Server icon appears in the taskbar status area.

▼ To Enable Print Requests From Network Users

Before users can print documents on the shared PC printer, you must enable LPD Print Server to accept incoming print requests.

If you see the LPD Print Server icon in the taskbar status area, and when you move your mouse pointer over it, the message `LPD: Accept Files` appears, the setup is complete.

If you see the LPD Print Server icon with the red stop sign in the taskbar status area, then continue as follows:

- **Click the right mouse button on the LPD icon in the status area.**

The LPD Print Server menu opens. The appearance of the LPD Print Server icon in the status area changes.

Starting LPD Print Server

When the Enable Solstice LPD Server option is checked (the default), the LPD Print Server daemon starts automatically. You can also start it manually. The daemon runs in the background until you disable it.

▼ To Start LPD Print Server Automatically

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Network.**

   The Network Properties dialog box opens.

2. **Select Solstice File And Printer Sharing and click Properties.**

3. **Select Enable Solstice LPD Server and click OK.**

   The LPD Print Server icon appears in the taskbar status area.

   If you do not see the LPD Print Server icon with the red stop sign in the taskbar status area, continue, with the steps in “To Enable Print Requests From Network Users” on page 95.

▼ To Start LPD Print Server Manually

1. **Click the Start button, point to Programs, and then point to Solstice Utilities.**

2. **Click the LPD Print Server icon.**

   LPD Print Server starts minimized and its icon appears in the status area of the taskbar.

   Print Manager starts running if it was not already running.

Stopping LPD Print Server

If you want to stop sharing a PC printer, you need to disable LPD Print Server daemon. Use the following procedure on the PC with the shared printer.

▼ To Stop (or Disable) LPD Print Server

1. **Click the Start button, point to Settings, click Control Panel, and then double-click Network.**

   The Network Properties dialog box opens.

2. **Select Solstice File And Printer Sharing and click Properties.**

3. **Click the File and Printer Sharing tab.**

   Remove the checkmark from the Enable Solstice LPD Server option. Disabling this option stops the LPD Print Server daemon.

4. **Click OK.**

   Both LPD Print Server and Print Manager stop running. Print requests that were already processed and placed in the LPD Print Server spool directory print when you restart LPD Print Server.

Adding a Shared Printer to a Users' Work Environment

Users who want to access the shared LPD printer need to add the printer to their work environment. These users must have network access to the PC with the shared printer.

▼ To Add a Shared Printer to a PC Environment

Note - You do not need to perform the following procedure on the PC with the shared printer.

---

1. **Click the Start button, point to Settings, and then click Printers.**

2. **Double-click Add Printer to start the Microsoft Add Printer Wizard.**

3. **When prompted, select To add a Network Printer.**

4. **Add the path name for the printer using the following syntax:**

   `lpr://`*hostname*`/`*queuename* or `lpr:\\~`*hostalias*`\`*queuename*

For example, to add a shared PC printer with a queue name `dopey_laser` connected to a PC with a hostname `dopey`, enter this path name: `lpr://dopey/dopey_laser`.

5. **If you want to print from MS-DOS based applications, click Yes.**

6. **(Optional) Set the shared PC printer as the default printer.**

▼ To Add a Shared Printer to a UNIX Environment

Individual UNIX users with superuser privileges can add a shared PC printer by following these steps:

1. **From a command window, enter the command `su` to become superuser.**

2. **At the superuser system prompt, enter `admintool&`.**
   The Administration Manager starts.

3. **Click Host Manager, and then click the appropriate name service to verify that the PC is listed in the hosts list.**

4. **Close the Host Manager dialog when finished.**

5. **Click Printer Manager to open the Printer Manager dialog.**

6. **Click Edit, click Add Printer, and then click Add Access to Remote Printer.**

7. **Complete the Add Access To Remote Printer dialog as follows:**
   a. **In Printer Name, enter the queue name of the shared PC printer, for example, `dopey1_laser`.**

   b. **In Printer Server, enter the name of the PC to which the printer is connected, for example, `dopey1`.**

   c. **In Comment, add some text that identifies the printer to the users, for example, `Laser in Jackie's office`.**

   d. **As Printer OS Server, click BSD.**

   e. **(Optional) Set the printer as the system default printer.**

   f. **Click Add and close the Access to Remote Printer dialog.**

8. **Quit the Administration tool and press Ctrl-D to exit superuser.**

Managing LPD Printing

You can view your print jobs, cancel print jobs, log messages, and set printing options for your LPD printer.

▼ To View Print Jobs in a PC Windows Environment

1. **Click the Start button, point to Settings, and then click Printers.**

   The Printers window opens.

2. **Double-click the shared PC printer's queue name.**

   A window opens that shows details such as the document name, the status, the owner, the progress, and the start time.

▼ To View Print Jobs in a UNIX Environment

Use the default UNIX `lpstat` commands to view the available printers, the status of print requests, and to cancel print requests. For example, assuming the queue name of the shared PC printer is `dopey1_laser`,

- To print to a shared printer when it is not the default, enter:

```
lp -d dopey1_laser
```

- To view print requests sent to the shared PC printer, enter:

```
lpstat -p dopey1_laser
```

- To cancel a print request sent to the shared PC printer, enter:

```
cancel job-ID
```

The *job-ID* is the first field in the response from the `lpstat -p` command.

Working with the LPD Print Server Log File

Messages related to printing documents under the control of the Solstice LPD Print Server are written in the LPD Print Server log file. The default path and file name of the LPD Print Server log file is `c:\spool\logfile.txt`.

While there is no physical limit to the size of the LPD Print Server log file other than the available disk space, it is a good idea to purge the log file regularly.

▼ To View and Print the LPD Print Server Log File

1. **Click the right mouse button on the LPD Print Server icon in the taskbar status area to open the LPD Print Server menu.**

2. **Click View Log File.**

   Solstice opens the file `logfile.txt` in Notepad.

3. **(Optional) On the File menu, click Print.**

4. **Close Notepad when you are finished.**

▼ To Purge the LPD Print Server Log File

1. **Click the right mouse button on the LPD Print Server icon in the taskbar status area to open the LPD Print Server menu.**

2. **Click Purge Log File.**

   A message appears asking if you really want to purge the contents of the log file.

3. **Click Yes to purge the contents of the log file, or click No to retain the log file contents.**

Turning Off a PC With a Shared Printer

When you turn off your PC, the LPD Print Server stops. When you turn the PC on again, the LPD Print Server automatically prints any files that are in the spool directory.

Users who sent documents to the shared PC printer may have to wait until you turn on the PC to get their printed documents. Alternatively, users can print their documents on another available printer, and cancel their print requests on the shared PC printer.

As a convenience to all users who access the shared printer, consider keeping the PC turned on at all times.

Turning Off a Shared PC Printer

When users send files to a shared PC printer which is not available (but is turned on) LPD Print Server processes the files for printing and places them in the spool directory. When the shared PC printer becomes available again, it prints the files in the spool directory.

When you turn off a shared PC printer, processed files are stored in the LPD Print Server spool directory. These files print when you turn on the PC printer again.

Unprocessed files are lost when you turn off the shared PC printer. Users have to resend those files to the shared PC printer.

Interpreting Carriage Returns and Line Feeds

The options Assume Binary and Map Newline to CR+LF For Binary Files in the Solstice File And Printer Sharing Properties dialog box work together.

If you select both options, the printer driver interprets the carriage returns and line feeds as shown in Table 5–6.

TABLE 5–6 Printer Driver Interpretation of Carriage Returns and Line Feeds

If the binary file contains...	The printer does the following...
Carriage returns followed by line feeds.	Starts a new line and adds a blank line. XXXXXXX. XXXXXXXXXXX
Carriage returns only	Starts a new line and starts printing from the left margin. XXXXXXX. XXXXXXXXXXX
Linefeeds only	Adds a blank line and continues printing. XXXXXX. XXXXXX

Troubleshooting LPD Print Servers

Refer to the Troubleshooting section in the LPD Print Server online Help for solutions to problems related to LPD Print Server.

When LPD Print Server is running, Print Manager must also be running. LPD Print Server starts Print Manager automatically. When you exit Print Manager, LPD Print Server also stops.

Troubleshooting Printing Problems

Table 5–7 discusses frequent printing problems on Windows NT and Windows 95 and their solutions. Refer to the online Help for additional troubleshooting information on printing.

TABLE 5–7 Frequent Printing Problems

Problem	Possible Cause	Solution
When attempting to mount network printers on Windows NT, My Computer is grayed out.	Default settings on Windows NT.	By default, only users with Administrator privileges can load and unload device drivers. Either change the policies to give the access right to users in the "User" group, or log in as a user with Administrator privileges.
You can browse a PCNFSD printer, but cannot connect to it. You might see the error message, `Problem printing Printer Test Page on host` *unixhost* `in queue` *lp*. `Unable to write to the remote filesystem` \\~*unixhost**pc.domain*.	The print spool directory is not exported.	Export the print spool directory on the server. For example, on a SunOS 5.*x*, enter `share -F nfs /var/spool echo share -F nfs /var/spool >> /etc/dfs/dfstab`. See the *Solstice Network Client Installation and Licensing Guide* for details.
When you try to print on a PCNFSD printer, you see an error message about a problem writing to the remote file system.	The print spool directory is mounted with read-only permissions.	Select Network Neighborhood. Click the right mouse button, and click Properties. On Windows 95, double-click Solstice NFS Client. On Windows NT, select the Services tab and double-click Solstice NFS Client. In both environments, on the NFS General page, under Mount Options, clear Connect Drives Read-Only. Make sure that on the UNIX system, the spool directory is shared read-write. On a Solaris system, enter the `share` command. You should see output similar to the following: `/var/spool/pcnfs rw " "`

CHAPTER 6

Managing Work Environments

This chapter describes how to manage clients in a 32-bit Solstice network. If you have a PC-Admin network, you can manage clients in a 16-bit Solstice network from a PC-Admin server.

Management tools, such as user profiles, system policies, and SNC scripts, enable you to manage clients running Windows 95 and Windows NT from an authentication server (a server running the `pcnfsd` daemon).

You can read background and procedural information throughout this chapter, or you can use the following references to go directly to a specific topic.

- "User Work Environments" on page 105
- "User Profiles" on page 108
- "System Policies" on page 114
- "Logon Scripts" on page 119
- "SNC Scripts" on page 122
- "System Policies, User Profiles, and Scripts in an NT Domain " on page 127
- "Troubleshooting" on page 128

User Work Environments

User work environments include desktop items and settings such as screen colors, mouse settings, window size and position, and network and printer connections. Using the Solstice Network Client management tools allows a user to have an identity independent of their PC. With this independent identity, a user can maintain a home directory on a file server and have user-based privileges to access other file systems.

Using management tools available in Solstice Network Client, you can set up individual work environments for each user in the network as well as common work environments for groups of users.

Management Tools

Windows 95 and Windows NT systems include mechanisms that are used to set up and configure the user's work environment. These include user profiles and system policies.

Solstice Network Client provides a way to use these management tools from a central location. It also provides a script interpreter that allows you to write or convert SNC scripts, which mount drives and directories, create Registry entries, access shared applications, and manage user views.

System policy files, user profiles, and scripts can be stored on the authentication server (the server running the `pcnfsd` daemon) and made available to a user logging into a client computer anywhere on the network. The files are stored in the directory `/opt/MSPolicy` on the authentication server.

- User profiles

  A user profile defines the desktop environment that is loaded by the system when a user logs in. A user profile contains configuration preferences and options for each user, such as:

  - Control Panel settings and preferences for the user interface
  - Settings for persistent network connections
  - Settings for applications that can write directly to the Registry

  Use the user profiles to enforce a consistent desktop for users. A user can log into the network from any computer and work with the same desktop settings. Multiple users on a computer will retain their personal settings.

- System policies

  System policies enable the system administrator to control user-definable settings in Windows NT and Windows 95 user profiles, as well as system configuration settings.

  Use the System Policy Editor to change desktop settings and restrict what users can configure, such as network settings and network client configuration options.

- Logon scripts

  Logon scripts are batch files (`*.bat`) that run each time a user logs in to a computer on the network. logon scripts contain system commands, such as commands to start applications. They can also call user-specific batch and executable files stored anywhere on the network.

Use the logon scripts to manage part of the user environment (such as network connections) without managing or dictating the entire environment. Use the scripts to create common network connections for multiple users.

- SNC scripts

  SNC scripts are script files (`*.snc`) that can be run in the 32-bit Solstice Network Client environment. SNC scripts previously written for a PC-Admin network can be adapted to run on Windows 95 and Windows NT clients.

  Use SNC scripts to securely manage SNC features, mount user network drives, create Registry entries, and set environment variables.

Setting Up the Authentication Server

Solstice Network Client provides a mechanism for central management of clients from a server in the network. System policy files, user profiles, logon scripts, and SNC scripts can be stored on the authentication server (the server running the `pcnfsd` daemon) and made available to a user logging into a client computer anywhere on the network. The files are stored in the directory `/opt/MSPolicy` on the authentication server.

If you have more than one authentication server, you must ensure that the appropriate files and scripts are available to clients on the network. You can do this by:

- Setting up duplicate scripts and files on each authentication server. If a client broadcasts for an authentication server, it will get the same scripts no matter which server responds.
- Setting up a specific authentication server for each user's network configuration. You can then maintain the appropriate files and scripts on the authentication server assigned to a user or to groups of users.

▼ To Set Up an Authentication Server

1. **Log in as `root` on a server running the `pcnfsd` daemon.**

   To check that the `pcnfsd` daemon is running, type:

   ```
   # ps --ef | grep pcnfsd
   root 1206 1 80 Feb 05? 0:30 /opt/SUNWpcnfs/sbin/rpc.pcnfsd
   root 24452 24450  5 14:49:15 pts/2 0:00 grep pcnfsd
   #
   ```

2. **Create the directory `/opt/MSPolicy`.**

```
# mkdir /opt/MSPolicy
```

3. **Make sure the** `/opt/MSPolicy` **directory is world readable and writable by** `root`**. For example:**

```
# cd /
   # chmod 755 /opt/MSPolicy
   # ls -l /opt
   drwxr-xr-x   2 root     other        512 May 21 16:38 MSPolicy
```

4. **Export the** `/opt` **file system. For example:**

```
# share -F nfs /opt/MSPolicy
```

User Profiles

Use user profiles to set up personal settings, such as desktop colors, fonts, and program groups that appear on the desktop. User profiles are available on both Windows 95 and Windows NT systems.

Using User Profiles on Windows NT

Windows NT 4.0 security requires a user profile for each user account. When a user logs in for the first time, Windows NT automatically creates a user profile. You can also create and modify user profiles on a computer running Windows NT Server. On Windows NT, all user-specific settings are automatically saved into the Profiles folder within the system root folder (typically `C:\winnt\profiles`).

You can create user profiles on the client running Windows NT and store them on an NFS server. You must specify the path name of the user profile in the NT user's account information. For users with only local NT user accounts, you must specify the user profile path name in each user account on each client.

If you have an NT domain set up with domain user accounts, you can specify the user profile path in the user's account on the domain controller. Then, whenever the user logs in, the user profile is downloaded and run.

Using User Profiles on Windows 95

In Windows 95, user profiles are not created by default. The system administrator must enable user profiles.

Each time the user logs in, the client running Windows 95 passes to Windows the location of the user's home directory (\\home*username*) on an NFS server. The *username* is the name the user types when logging in to the client machine. The \\home directory is the entry in the auto_home file in the NIS or NIS+ tables on the server, or in the local auto_home file.

For user profiles to work on Windows 95, you must configure the Solstice NFS Client as the Primary Network Logon, and you must configure either NIS or NIS+ as the name service on the client. When NIS or NIS+ is configured, the Automounter automatically mounts the user's home directory. If you configure the DNS or Files-based name service but not NIS or NIS+, the Automounter does not automatically mount user's home directories and user profiles stored in those directories are not downloaded to the client.

Updating User Profiles

The Windows NT and Windows 95 networks follow these rules for updating user profiles.

1. Each time a user logs in to a computer, Microsoft Windows searches the Registry to determine whether the user has a local profile. On Windows NT, the local profile path is stored in the Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Windows NT\Current Version\ProfileList
```

   On Windows 95, the local profile path is stored in the Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Windows\Current Version\ProfileList
```

2. Windows NT checks for the user profile in the User Profile Path specified in User Manager, User Profiles. If the user profile on the server is the most current, Windows NT copies it to the local computer for use during the current session. Windows NT then loads the settings in this local copy into the Registry. Windows 95 checks for the user profile in the user's home directory on the server. If the user profile on the server is the most current, Windows 95 copies it to the client computer for use during the current session. Windows 95 then loads the settings in the client copy into the Registry.
3. If no user profile exists on the client, Windows copies the server version to the client computer. If no profile is found on the server, Windows creates a new user profile on the client computer using default settings. If the user does not log in, then Windows automatically uses the default user profile.
4. Both the client and network copies of the user profile are automatically updated with the current settings when the user logs out.
5. If the user is logged in to more than one computer at the same time, any changes made to the profile on the computer where the user first logs out will be overwritten when the user logs out of the other computer. In other words, the last logout is saved, and no merging of changes occurs.

Setting Up Roaming User Profiles

A roaming user profile is a server-based user profile that is downloaded to the local computer when a user logs in and is updated both on the client and on the server when the user logs out. A roaming profile is available from the server when logging in to any computer running the Solstice Network Client software on Windows NT Workstation, Windows NT Server, or Windows 95. A roaming user profile enables a user to log in to the network from any computer and work with the same desktop settings.

You can store roaming user profiles created on computers running Windows NT Workstation, Windows NT Server, or Windows 95 on an NFS server.

To use a roaming user profile, a user must have a user account on that computer. On Windows 95, each user can create a user account by specifying a user name and password when logging in.

You can create user accounts in Windows NT in one of the following ways:

- If you have an NT domain set up, log in to the domain controller as administrator and create a domain user account for each user. Set the profile path in each user account on the domain controller to the location of the profile on the NFS server.
- If you do not have an NT domain set up, log in to each NT workstation as Administrator and create a local user account for each user. You must also set the profile path in each user account on each NT workstation to the location of the profile on the NFS server.

▼ To Set Up Roaming User Profiles on Windows NT

Note - To assign the same preconfigured roaming user profile to multiple user accounts, enter a separate user profile path for each user account, and use System in Control Panel (User Profiles tab) to copy the preconfigured user profile to the server location for each user.

---

1. **Log in to an NFS server as root and make sure each user is properly set up and has an assigned home directory.**

   Store each user's profile in the user's home directory on the server. You can store user profiles in another location on the server, but it is not recommended.

2. **Make sure the directory is world readable. For example:**

```
# cd /
# chmod 755 /home/users
```

3. **Share the top level directory of the file system. For example:**

```
# share -F nfs /home
```

4. **On a computer running Windows NT Workstation 4.0 or Server 4.0, log in as an Administrative user and customize the desktop as you want it to be for the user profile.**

5. **Click Start, point to Programs, then point to Administrative Tools (Common), and select User Manager.**

6. **Double-click a user from the listed user names.**

   The User Properties dialog box opens.

7. **Click Profile.**

   The User Environment Profile dialog box opens.

8. **In the User Profile Path box, type the complete path to the profile on an NFS server in the form: *server**mount_point**directory 1**directory 2*\...**

   The mount point is the directory you shared in Step 3 on page 111. Specify the complete path name to the profile on the server. For example:
   `\\saturn\home\users`

9. **Click OK to close the User Environment Profile dialog box. Click OK again to close the User Properties dialog box.**

10. **Select Exit from the User menu to close the User Manager dialog box.**

11. **(Optional) Copy a preconfigured user profile to the user profile path location.**
    a. **Click Start, point to Settings, and then select Control Panel.**

    b. **Double-click System and then click User Profiles.**

    c. **Under Profiles Stored On This Computer, select the profile to copy to the Solaris server and click Copy To.**

    d. **Type the location of the user profile on the server.**
       This should be the same location you typed in Step 8 on page 111.

    e. **Click OK to close the Copy To dialog box. Then click OK to close the User Profiles tab.**

When the user logs out, the client automatically places an updated copy of the user profile in the user profile path on the server. In the following example, the server is named `saturn`: `\\saturn\home\users\mary\ntuser.dat`

▼ To Set Up Roaming User Profiles on Windows 95

Make sure user profiles are enabled for each computer.

Note - You can facilitate this step by creating a system policy that enables user profiles on all PCs running Windows 95. When the user logs in, Windows 95 downloads the policies from the server and copies the information to the Registry on the client.

---

1. **Make sure either NIS or NIS+ is configured as the name service on the client.**

   When NIS or NIS+ is configured, the Automounter automatically mounts the user's home directory. If you configure the DNS or Files-based name service but not NIS or NIS+, the Automounter does not automatically mount user's home directories and user profiles stored in those directories are not downloaded to the client. "To Configure NIS or NIS+" on page 41

2. **In the Passwords option in Control Panel, click the User Profiles tab.**

3. **Select Users Can Customize Their Preferences And Desktop Settings.**

4. **Select the options you want under User Profile Settings and click OK.**

   These options describe what should be included as part of the user profile.

   Note - If you include desktop icons in the user profile, only the shortcuts (icons that represent links) will be available when the user logs in to the network from another computer. Actual files on the desktop are part of the local user profile only.

   ---

5. **Click Yes when asked to restart the computer.**

6. **In the Network option in Control Panel, make sure Solstice NFS Client is listed as the Primary Network Logon.**

7. **On an NFS server, make sure each user is properly set up and has an assigned home directory.**

When the user logs out, Solstice Network Client automatically places an updated copy of the user profile in the user's assigned home directory on the server, in the path: *server**user_home_directory*

Setting Up Mandatory User Profiles

In Windows NT and Windows 95, a mandatory user profile creates a standard user profile that is implemented at every login. You can create mandatory user profiles on an NT workstation and store them on an NFS server.

If you have an NT domain set up, set the profile path in each user account on the domain controller to the location of the profile on the NFS server. If you do not have an NT domain set up, log in to each NT workstation as Administrator and set the profile path in each user account to the location of the profile on the NFS server.

▼ To Set Up Mandatory User Profiles on Windows NT

1. **Create a user profile using the instructions in "To Set Up Roaming User Profiles on Windows NT" on page 110.**

2. **Rename `NTUSER.DAT` to `NTUSER.MAN` in the user's profile path.**

   Windows NT recognizes the `.MAN` file extension as a mandatory user profile.

▼ To Set Up Mandatory User Profiles on Windows 95

Make sure user profiles are enabled for each computer.

Note - You can avoid enabling user profiles on each computer by creating a system policy that enables user profiles on all clients. When the user logs in, Windows downloads the policies from the server and copies the information to the Registry on the client.

---

1. **Make sure either NIS or NIS+ is configured as the name service on the client.**

   When NIS or NIS+ is configured, the Automounter automatically mounts the user's home directory. If you configure the DNS or Files-based name service but not NIS or NIS+, the Automounter does not automatically mount user's home directories and user profiles stored in those directories are not downloaded to the client. "To Configure NIS or NIS+" on page 41

2. **In the Passwords option in Control Panel, click the User Profiles tab.**

3. **Select Users Can Customize Their Preferences And Desktop Settings.**

4. **Select the options you want under User Profile Settings.**
   These options describe what should be included as part of the user profile.

5. **Shut down and restart the computer.**

6. **In the Network option in Control Panel, make sure Solstice NFS Client is listed as the Primary Network Logon.**

7. **On any computer running Windows 95, customize the desktop as you want it to be for the mandatory user profile.**

8. **Copy the** `USER.DAT` **file to the user's home directory on the server.**

9. **Rename** `USER.DAT` **to** `USER.MAN` **in the user's home directory.**
   Windows 95 recognizes the `.MAN` file extension as a mandatory user profile.

System Policies

The Windows NT or Windows 95 client computer can download and set Windows system policies from the authentication server. The authentication server is one that is running the `pcnfsd` daemon, which verifies that users are authorized to log in to the network.

System administrators can use system policies to manage clients by:

- Restricting access to Control Panel options
- Restricting what users can do from the desktop
- Customizing parts of the desktop
- Configuring network settings

On Windows 95, you can download system policies for specific users, groups, specific computers, or for all users. On Windows NT, you can download system policies for specific users, specific computers, or for all users. But you cannot download group policies from an NFS server.

Creating System Policy Files

To create a system policy file on Windows NT, use the System Policy Editor on a computer running Windows NT Workstation or Windows NT Server. The System Policy Editor is available only on Windows NT server, but you can copy the editor from a Windows NT Server to a workstation and then run the editor on the workstation.

The system policy entries you set are stored in a binary file with the `.POL` extension. You should save this file with the name `ntconfig.POL`. The Windows NT Workstation software reads and interprets the `ntconfig.POL` policy file by overriding any conflicting information in that workstation's Registry.

To create a system policy file on Windows 95, use the Windows 95 System Policy Editor. The system policy entries you set are stored in a binary file with the `.POL` extension. You should save this file with the name `config.POL` on a server running the `pcnfsd` daemon. When the user logs in, Windows 95 overwrites the default `USER.DAT` and `SYSTEM.DAT` settings in the Registry with the policy settings in the `config.POL` file.

To apply system policies to a network that uses both Windows 95 and Windows NT, run the System Policy Editor once from each platform to produce two different system policy files.

How System Policies Work

When the user logs in to a client, the client passes the location of the system policy file to Microsoft Windows:

- *authentication_server*`:/opt/MSPolicy/ntconfig.pol` on Windows NT
- *authentication_server*`:/opt/MSPolicy/config.pol` on Windows 95

Microsoft Windows then downloads system policies for computers and users from the `/opt/MSPolicy` directory on the authentication server. Windows NT and Windows 95 follow these rules for updating user information with system policy files:

1. If user profiles are enabled, Windows checks for a user policy file that matches the user name. If it finds one, it applies the user-specific policy. If it does not find a user policy file, it applies the default user policy file. On Windows NT, user profiles are always enabled.
2. Group policies are not applied if there is a policy file for a specific user. If Windows support for group policies is installed on a client running Windows 95, Windows checks whether the user is registered as a member of any secondary UNIX groups. If so, group policies are downloaded, starting with the lowest priority group and ending with the highest priority group. Group policies are processed for all groups to which the user belongs. The group with the highest priority is processed last so the settings in that group's policy file supersede those

in lower priority groups. The client on Windows NT does not download or process group policies.

3. All settings are then copied into the `USER.DAT` portion of the Registry.
4. Microsoft Windows checks for a computer policy file to match the computer name. If one exists, Microsoft Windows applies the computer-specific policies to the user's desktop environment. If a policy file for that computer name does not exist, Microsoft Windows applies the default computer policy.
5. This data is then copied into the `SYSTEM.DAT` portion of the Registry.

How System Policies Differ From Mandatory User Profiles

System policies and mandatory user profiles differ in the following ways.

System Policies	Mandatory User Profiles
Settings can be user-specific or computer-specific.	Settings can only be user-specific.
You can selectively determine a subset of user settings to control. Users may control the remaining settings.	You always control every user-specific setting.

▼ To Set Up System Policy Files

Set up system policy files on each authentication server on the network.

1. **Set up the authentication server.**

   See the instructions in "To Set Up an Authentication Server" on page 107.

2. **(Optional) On a client running Windows NT, create a Windows NT policy file and copy it to the `/opt/MSPolicy` directory on the authentication server.**

   See the instructions in "To Create a System Policy File on Windows NT" on page 117.

3. **(Optional) On a client running Microsoft Windows 95, create a Microsoft Windows 95 policy file and copy it to the `/opt/MSPolicy` directory on the authentication server.**

   See the instructions in "To Create System Policies for Users or Computers on Windows 95" on page 118.

▼ To Create a System Policy File on Windows NT

The NT version of the System Policy Editor (`poledit.exe`) is included with the NT Server software, but not with the NT Workstation software. You can use the System Policy Editor on an NT workstation by copying the editor (`poledit.exe`) on an NT server to the `\winnt\system32` folder on an NT workstation, and copying the files `common.adm`, `windows.adm`, and `winnt.adm` to the `\winnt\inf` folder on the NT Workstation.

For detailed information on installing the System Policy Editor and creating system policy files in Windows NT, refer to the *Microsoft Windows NT Server Resource Kit*, published by Microsoft Press.

1. **On an NT server, click Start, point to Programs, point to Administrative Tools (Common), and then select System Policy Editor.**

   The System Policy Editor dialog box opens.

2. **Click File and then select New Policy.**

3. **Depending on which policies you are creating:**
   - Double-click the Default User icon to define the default settings for user-specific policies.
   - Double-click the Default Computer icon to define the settings for computer-specific policies.

4. **In the Policies tab, select the policies you want to put in place and then click OK.**

5. **Click File and then select Save.**

6. **Type `ntconfig` for the name of the policy and then click Save.**

   The system policy file is saved with the `.POL` extension.

7. **Copy the system policy file you created from the workstation to the `/opt/MSPolicy` directory on an authentication server.**

   You can use the Network Neighborhood to browse for the server, and then drag the system policy files from the workstation (usually in `\winnt\system32\`)to the `/opt/MSPolicy` directory on the authentication server.

▼ To Install System Policy Editor on Windows 95

1. **Click Start, point to Settings, and then click Control Panel.**

2. **Double-click Add/Remove Programs.**

3. **Click the Windows Setup tab, and then click Have Disk.**

4. **In the Install From Disk dialog box, click Browse and specify the** `admin\apptools\poledit` **folder on the Microsoft Windows 95 compact disk. Click OK, and then click OK again.**

5. **Make sure System Policy Editor is checked.**

6. **To use group policies, make sure Group Policies is checked.**
   Windows 95 Setup will copy `GROUP.DLL` in the Microsoft Windows `SYSTEM` directory on the client computer and make the required Registry changes.

7. **Click Install.**

▼ To Create System Policies for Users or Computers on Windows 95

To use System Policy Editor, you must install the following files from the `admin\apptools\poledit` folder on the Windows 95 distribution media: `admin.adm`, `poledit.exe`, and `poledit.inf`. For instructions on installing System Policy Editor, see "To Install System Policy Editor on Windows 95" on page 117.

1. **In System Policy Editor, click the File menu, and then click New File.**

2. **Depending on which policies you are creating:**
   - Double-click the Default User icon to define the default settings for user-specific policies.
   - Double-click the Default Computer icon to define the settings for computer-specific policies.

3. **Select the policies you want to put in place.**

4. **Click File and then select Save.**

5. **Type** `config` **for the name of the policy and then click Save.**
   The system policy file is saved with the `.POL` extension.

6. **Copy the system policy file you created from the workstation to the** `/opt/MSPolicy` **directory on an authentication server. You can use the Network Neighborhood to browse for the server, and then drag the system policy files from the PC (usually in** `\WINDOWS\Profiles\`***username***`\Desktop\`**)to the** `/opt/MSPolicy` **directory on the server.**

▼ To Create Group Policies on Windows 95

1. **In System Policy Editor, click the Edit menu, and then click Add Group.**

2. **Type the UNIX group ID number for the group you want to add, and click OK.**

   For example, if the group named `staff` has the UNIX ID 10, then you must type 10 when asked for the name of the group.

3. **Click or clear policies by clicking the policy name.**

Logon Scripts

Clients running Windows NT and Windows 95 can download and execute logon scripts from an authentication server. Logon scripts are batch files that run automatically when a user logs in. You are required to create logon scripts to configure the network connections and start applications in users' environments. A logon script can call other scripts and executable files that reside in any local or NFS directory.

On Windows NT, you create the logon script, ntlogon.bat, to provide users with the appropriate environment when they log in. On Windows 95, the corresponding file is `winlogon.bat`.

Note - If the client computer is running over a PPP connection, you will not be able to run the logon scripts (`winlogon.bat` and `ntlogon.bat`). If it is necessary to run these batch files, you should run them from within the SNC scripts using the `LAUNCH` directive. See "SNC Scripts" on page 122 and "`LAUNCH` *filename* [*options*]" on page 175.

When a User Logs In

When a user logs in to a client machine, the client broadcasts to the authentication servers on the network. The authentication servers respond to the broadcast, and the client uses the first server that responds as its authentication server. The client reads the logon script from the server and runs it. The same logon script can be shared by all network users.

Clients can either broadcast for or choose a specific authentication server. Choosing a specific authentication server is recommended because it is the most secure method.

If you create a logon script to be used by all users, store the logon script files on every authentication server on your network.

You can create specialized logon scripts for one or more users. When run, the logon scripts determine the user or group and customize the start up of the Solstice Network Client environment for the specific user or group. In a typical implementation, you would have a *group*.snc script for each group in your domain and supplemental *user*.snc scripts for specific users.

Note - Windows NT clients can run logon scripts that contain the Windows NT built-in environment variables. For an example, see Code Example 6–1.

▼ To Create a Logon Script for Windows 95 Clients

1. **Use any text editor to create the logon script.**
2. **Save the script as** `winlogon.bat`**.**
3. **Copy** `winlogon.bat` **to the** `/opt/MSPolicy` **directory on the authentication server.**

▼ To Create a Logon Script for Windows NT Clients

1. **Use any text editor to create the logon script.**
2. **Save the script as** `ntlogon.bat`**.**
3. **Copy** `ntlogon.bat` **to the** `/opt/MSPolicy` **directory on the authentication server.**

Note - The `winlogon.bat` and `ntlogon.bat` files support the same commands as any `.bat` file.

Example Logon Scripts

Code Example 6–1 is a sample `ntlogon.bat` logon script that is executed when the user logs in to the client running Windows NT.

CODE EXAMPLE 6–1 Sample nt.logon.bat logon script

```
REM Sample ntlogon.bat script
net use
```

```
REM
REM Set Policy path environment variable
set PCNFSDSERVER=space
set POLICYPATH=\\%PCNFSDSERVER%\opt\MSPolicy
REM
REM Invoke globalboot.bat
cmd /C %POLICYPATH%\globalboot.bat
```

The `globalboot.bat` script in Code Example 6–2 is called by the `ntlogon.bat` script.

CODE EXAMPLE 6–2 globalboot.bat script

```
REM Sample script to set other environment variables
set VARIABLE1=test
set VARIABLE2=dir
mkdir c:\%VARIABLE1%.%VARIABLE2%
REM
REM Invoke globallogon.bat
cmd /C %POLICYPATH%\globallogon.bat
```

The `globallogon.bat` script in Code Example 6–3copies files from `saturn` to the `\tmp\planets` directory on the client. The following lines in the `globallogon.bat` script run user Pat's `.bat` file in the directory `\\home\pat` on the server named jupiter.

```
set USER=pat
 set HOME=\\jupiter\home\%USER%
 cmd /C %HOME%\globallogon.bat
```

To call a logon script for many users, you would need to repeat these lines for each user. If users have identical user names and passwords on UNIX and NT, you can set the built-in NT variable `USER` to the user's username, and set the variable `HOME` to the path to the user's home directory on the server, for example, `\\jupiter\home\%USER%`. The variables `%USER%` and `%USERNAME%` are Windows NT variables that dynamically refer to any user.

CODE EXAMPLE 6–3 Calling a logon Script

```
REM Sample script to do a copy operation
copy \\saturn\\Dir1\Dir2\*.* c:\tmp\planets
REM
REM Now invoke individual user's logon script
set USER=pat
set HOME=\\jupiter\home\%USER%
cmd /C %HOME%\%USER%.bat
```

The script in Code Example 6–4 runs an executable over NFS.

CODE EXAMPLE 6–4 Running an Executable over NFS

```
REM
REM Use predefined NT environment variable
dir %SystemRoot%
```

```
REM Remotely run residing executable.
%HOME%\regmon.exe
```

SNC Scripts

SNC scripts are read from an NFS server in the Solstice Network Client network. Using SNC scripts, clients can access system policies, user profiles, logon scripts, and other SNC scripts stored on an NFS server.

In a PC-Admin network, SNC scripts are used to manage and control the environment of PC-Admin clients. These scripts can be adapted to manage Windows 95 and Windows NT client in a Solstice network. The SNC scripts and the script interpreter should be copied to the `/opt/MSPolicy` directory on the authentication server.

This section:

- Compares PC-Admin SNC scripts on PC-Admin and Solstice Network Client computers
- Describes how to run existing SNC scripts on Windows 95 and Windows NT systems running Solstice Network Client software
- Describes how to run the script interpreter, using the `sunwrun` command.

For detailed information on SNC script directives, turn to Appendix C.

Scripting on PC-Admin and Solstice Network Client Computers

Table 6–1 compares scripting features on PC-Admin client and Solstice Network Client computers.

TABLE 6–1 Comparison of Features on PC-Admin Client and Solstice Network Client

Script Feature	PC-Admin Clients	Solstice Network Clients
Script server	Any NFS server designated by DHCP	A server running the `rpc.pcnfsd` software.
Location of scripts on the server	Stored in the DHCP databases.	`\opt\MSPolicy`, which is created on the authentication server.

TABLE 6–1 Comparison of Features on PC-Admin Client and Solstice Network Client *(continued)*

Script Feature	PC-Admin Clients	Solstice Network Clients
Centralized script management	Yes	Yes
Preemptive logon scripts	Yes	Yes
Supported events	Login, Logout, Boot, Shutdown	Login on Windows 95 and Windows NT Logout on Windows 95
Script hierarchy (Site, Group, User)	Yes	Yes
Scripts controlled by environment variables	Yes	Yes
Modification of environment variables	Local and Global	Local
Command to remotely set drive mounts	`MOUNT`	`MOUNT`
Directives (script commands)	20 script commands for 16-bit client	20 script commands for 32-bit client
Global environment variables	Yes	Environment can be passed to `LAUNCH`ed applications only.
Support for NIS/NIS+ environment variables	Current User, Current Group, Secondary Group	Current User, Current Group, Secondary Group

Running SNC Scripts

If you have created SNC scripts that run in your PC-Admin network, you can run these scripts from any authentication server to manage the 32-bit clients in the Solstice network. The Solstice Network Client software includes a script interpreter (`sunwrun.exe`) that interprets new SNC scripts or existing PC-Admin SNC scripts. Although there may be minor differences, you should be able to run your existing PC-Admin SNC scripts with no changes. Differences are described in “SNC Scripts on PC-Admin Clients and Solstice NFS Clients” on page 125.

During installation, the script interpreter is installed on the Solstice Network Client in the directory `C:\Program Files\Solstice\Bin\sunwrun.exe`. Copy this file to the `/opt/MSPolicy` directory on the authentication server. The SNC scripts are read from the server and run on the client.

Using SNC scripts, clients can access system policies, user profiles, logon scripts, and other SNC scripts. If you have created scripts for your PC-Admin clients, you can adapt those scripts to run on the client in a Solstice network. To reuse the SNC scripts, use the following procedure.

▼ To Adapt PC-Admin SNC Scripts

1. **Copy the SNC scripts to the `/opt/MSPolicy` directory on the authentication server.**

2. **Rename or copy `login.snc` to either `ntlogon.snc` (on Windows NT) or `winlogon.snc` (on Windows 95).**

3. **Rename or copy `logout.snc` to either `ntlogout.snc` (on Windows NT) or `winlogout.snc` (on Windows 95).**

Running the Script Interpreter

You can run the script interpreter to develop and debug new scripts. The `sunwrun` command invokes the script interpreter, which automatically runs the appropriate SNC scripts when the user logs in.

To run the command, type:

`sunwrun.exe [-ripn]` *filename*`.snc`

You can specify multiple file script file names on the command line. Each file name must end with the `.snc` extension. The interpreter will execute each file in order until a script exits with a non-zero exit code or all files are processed.

Available options include:

`-r`	Causes the script interpreter to reset the shared environment before interpreting the first file.
`-i`	Causes the script interpreter to reset the shared environment after interpreting the last file.
`-p`	Causes the script interpreter to execute only files from the location specified in the `SNDRIVE` variable.
`-n`	Causes the script interpreter to exit immediately after executing the last script file, rather than waiting the default 5 seconds provided to enable the user to view the output.

SNC Scripts on PC-Admin Clients and Solstice NFS Clients

While, for the most part, you can run existing PC-Admin SNC scripts unchanged, there are some differences that you should be aware of.

- Some commands that were run on PC-Admin clients are ignored by the script interpreter (see "Ignored Script Directives" on page 125).
- New directives read and write to the system Registry (see "New Script Directives for Windows 95 and Windows NT Clients" on page 126).
- Environment variables are handled differently (see "Environment Variables Local to SNC Scripts" on page 127).
- With the addition of NIS+ support, the NIS and NIS+ values are handled differently (see "NIS and NIS+ Changes" on page 126).

Ignored Script Directives

The following directives are ignored by the script interpreter.

Command	**Function in PC-Admin**
`LOGIN`	Starts the Microsoft Windows Login dialog box
`LOGOUT`	Logs out current user and set current user ID to `nobody`
`RESERVE`	Prevents users from mounting drives
`EXPORT`	Copies local to global variables
`STOP`	Shuts down client's connection to network

Command	Function in PC-Admin
`MOUNT –o preserve`	Prevents user from unmounting a drive or printer
`MOUNT –o type`	Media type (`cdrom` or `std`)

New Script Directives for Windows 95 and Windows NT Clients

New commands are available that enable you to read and write to the system Registry.

Read Values from the Current Registry

The `SET REG` command enables you to read values from the system Registry into a variable. This is analogous to the `SET NIS` command. The keys `HKEY_LOCAL_MACHINE` may be abbreviated to `HKLM` and `HKEY_CURENT_USER` may be abbreviated to `HKCU`.

Write Values to the Registry

The `REG` directive command enables you to write to the system Registry. This command should be used with great caution.

For example, the command `REG NEWKEY` *keypath* creates a new key, and the command `REG DELKEY` *keypath* deletes the named key.

NIS and NIS+ Changes

Solstice Network Client supports both NIS and NIS+ on Windows 95 and Windows NT clients. The `SET NIS` directive looks up values in either or both NIS and NIS+, depending on the configuration of the local machine.

To facilitate backward compatibility, you should use NIS table names, unless you KNOW that you are using NIS+ in native (non-yp) mode. If you are using NIS+, do NOT add the trailing `org_dir` to the table name.

If NIS+ is enabled, table names are converted according to these rules:

- The first period in a name is converted to an underscore.
- The string `org_dir` is appended to the name.

For example,

- `auto.home` becomes `auto_home.org_dir`

- `passwd` becomes `passwd.org_dir`

If you are adapting PC-Admin scripts, note that the return value from NIS+ can be different from NIS, so you may need to use the `SET STR` command to alter the result.

The `SET STR VAR=# %OTHERVAR` and `SET STR VAR=* %VAR%` directives are useful for this purpose. See the description of SNC directives in “SNC Script Directives” on page 172.

Environment Variables Local to SNC Scripts

Environment variables are handled as in PC-Admin, but are preserved across invocations in the Registry. Exported variables (using the `EXPORT` directive) are not placed in the Windows global environment. However, any application that is started will have the exported variables set in its environment.

In addition to variables explicitly set in the `SNC` script, the PC-Admin server sets local variables on clients each time a user logs in. For a list of SNC script variables, see “Environment Variables Local to SNC Scripts” on page 185.

In general, 32-bit applications should use the system Registry for application-specific data and not rely on the environment.

System Policies, User Profiles, and Scripts in an NT Domain

If you have an NT domain, you can set up roaming and mandatory user profiles on an NFS server. When a user logs in to a client running Solstice Network Client software, the user profile is downloaded from the NFS server. This allows you to take advantage of the speed and power of a Solaris server.

However, before setting up system policies, user profiles, and logon scripts you should be aware of the following restrictions in the way these features work on Solstice Network Client computers that are part of an NT domain.

- System policies – Users cannot download system policies from an NFS server. This is true whether the user has a local or domain NT user account on the client.
- Logon scripts – Users cannot download the `ntlogon.bat` script from an NFS server to a client running Windows NT Workstation. Users can download the `ntlogon.bat` script from an NFS server to a client running Windows NT Server.
- User profiles – Users can download user profiles from an NFS server to all clients running the Solstice Network Client software. If you include any files, for example

a bitmap file as a background, in user profiles for NT domain users, those files must be stored on the client. If they are not stored on the client, the user profile will not be downloaded.

Troubleshooting

Table 6–2 presents possible solutions to common problems that can occur in setting up and managing a user's work environment on clients running Windows NT.

TABLE 6–2 Troubleshooting on Windows NT

Problem	Possible Cause	Solution
A user logs in and sees the message, `Cannot create user's profile in \\server_name\profile_path\.pds`	The client cannot mount the directory specified in the profile path. This might happen if you log in to the client with a different user name than your NT user name.	Make sure you typed correct UNC format for the `\\server_name\profile_path` and that the top-level directory exists and is shared from the server. Press Ctrl+Alt+Delete and log in using a user name that exists on both NT and Solaris.
The user profile cannot be downloaded from the server. The local copy is used instead.	The client is part of an NT domain, served by an NT domain controller and the user profile includes a file (for example, a bitmap for a background) that is not stored on the client.	Copy the included file to the client or remove it from the profile.

TABLE 6–2 Troubleshooting on Windows NT *(continued)*

Problem	Possible Cause	Solution
System policies are not downloaded from the server.	1. The system policy file (`ntconfig.pol`) is not in the `/opt/MSPolicy` directory on the user's authentication server. If you have more than one `authentication` server on a network and have not copied the `ntconfig.pol` file to *all* servers, the user might be authenticated by a server that does not store the system policy files.	Copy the `ntconfig.POL` file from an NT workstation or server to each Solaris server running the `pcnfsd` daemon on the network. Log in to the server and verify it is running a `pcnfsd` daemon. If you have more than one authentication server on a network, copy the `ntconfig.POL` file to each authentication server. Or, specify the authentication server that contains the `ntconfig.POL` file by Selecting Solstice NFS Client->Properties->Security->Use a Specific Authentication Server.
	2. The client is part of an NT domain, served by an NT domain controller. Users cannot download system policies from a Solaris server to a Solstice Network Client machine that is part of an NT domain. This is true whether the user has a local or domain NT user account on the client.	Store the system policy file on the domain controller

Table 6–3 presents possible solutions to common problems that can occur in setting up and managing user profiles, system policies, and login scripts on clients running Windows 95.

TABLE 6–3 Troubleshooting on Windows 95

Problem	Possible Cause	Solution
System policies are not downloaded from the server.	The system policy file (`config.pol`) is not in the `/opt/MSPolicy` directory on the user's authentication server. If you have more than one authentication server on a network and have not copied the `config.pol` file to *all* servers, the user might be authenticated by a server that does not store the system policy files.	Copy the `config.POL` file from a Microsoft Windows 95 client to each server running the `pcnfsd` daemon on the network. 2. Log in to the server and check to see if it is running a `pcnfsd` daemon. 3. If you have more than one authentication server on a network, copy the `config.POL` file to each authentication server. Or, specify the authentication server that contains the `config.POL` file by selecting Solstice NFS Client->Properties->Security->Use a Specific Authentication Server. 4. Make sure the Solstice NFS Client is selected as the primary network logon in the Network dialog box.
User profiles are not downloaded from the server.	The Solstice NFS Client is not selected as the primary network logon.	In the Network option in Control Panel, select Solstice NFS Client as the primary network logon.
	NIS or NIS+ is not configured as the name service on the client. If you configure the DNS or Files-based name service but not NIS or NIS+, the Automounter does not automatically mount user's home directories, and user profiles stored in those directories are not downloaded to the client.	Make sure NIS or NIS+ is set up on the server and then select NIS or NIS+ as the name service on the client.

CHAPTER 7

Logging In to Windows NT and Windows 95 Clients

On Windows NT and Windows 95, you can log in to the Microsoft network and the Solstice network at the same time. If your Windows and UNIX user names and passwords are identical, you will see only one network login dialog box.

You can read background and procedural information throughout this chapter, or you can use the following references to go directly to a specific topic.

- "Logging In and Changing Passwords on Windows NT" on page 131
- "Logging In and Changing Passwords on Windows 95" on page 135
- "Troubleshooting" on page 140

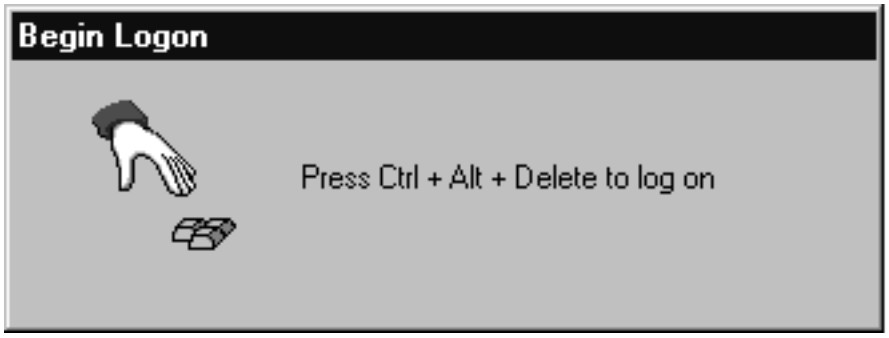
Logging In and Changing Passwords on Windows NT

On Windows NT, you can change your UNIX password without changing your NT password. You can also change your NT password without changing your UNIX password.

You can enable synchronized passwords which means that if you use the same password for both domains, changing your Windows NT password automatically changes your UNIX password as well.

▼ To Log In to a Solstice network from Windows NT

1. **Press Ctrl+Alt+Delete to log in to Windows NT.**



2. **Type your Windows NT user name and password, and then click OK.**

   If your UNIX user name and password are the same as for Windows, logging in to the Windows NT login dialog box logs you in to both the Microsoft and Solstice networks. If your Windows NT user name and password differ from your UNIX user name and password, the Solstice NFS Client Login dialog box opens.

3. **In the Solstice NFS Client Login dialog box, type your user name and password, type the name of an authentication server, and then click OK.**

   You are now logged in to the network and can use NFS to browse network files.

▼ To Change the UNIX Password in Windows NT

Note - Your user name must match the user name of the user whose password is being changed.

---

1. **Make sure that the NIS or NIS+ name service is enabled:**
   a. **Select Network Neighborhood.**
   b. **Click the Right Mouse button and click Properties.**
   c. **Double-click Solstice NIS/NIS+ Naming Services.**
   d. **Make sure either Enable NIS or Enable NIS+ is checked.**

2. **Press Ctrl+Alt+Delete and then click Change Password.**

3. **In the Change Password dialog box, type your UNIX user name in the User Name box.**

4. **In the Domain box, click the arrow to show available domains.**

5. **Select Solstice_NFS_Client.**

6. **Type your old UNIX password.**

7. **Type your new UNIX password, and then type it again in the Confirm New Password box.**

   Your UNIX password is updated in the NIS or NIS+ database.

Synchronizing Windows NT and UNIX Passwords

If you enable synchronized passwords, changing your Windows NT password will automatically change your UNIX password. Enable synchronized passwords by selecting the Enable Password Synchronization option in the Security tab of the Solstice NFS Client Configuration menu.

If synchronized passwords are enabled:

- Changing your Windows NT password by selecting the NT domain will automatically change your UNIX password.
- Changing your UNIX password by selecting the Solstice NFS Client domain will not automatically change your Windows NT password.

Be sure that your passwords are the same before you change passwords with synchronization enabled. If the passwords are not the same, these problems can result:

- When changing passwords by entering the UNIX password, the NT password change fails (since the NT password is not the same) and the UNIX password change will not be attempted. As a result, neither password will change.
- When changing passwords by entering the NT password, the NT password succeeds, but the UNIX password change will fail (since the UNIX password is not the same).

Note - You must be using NIS/NIS+ as your name service In order to change your UNIX password from your Windows NT computer. If NIS/NIS+ is not enabled, then changing your Windows NT password will not affect your password on the UNIX system. To maintain synchronized passwords, you will have to enter the new password manually, on the UNIX computer.

▼ To Enable Password Synchronization in Windows NT

1. **Right-click Network Neighborhood and then click Properties.**

2. **Click the Services tab, select Solstice NFS Client, and then click Properties.**
   The Solstice NFS Client Configuration window opens.

3. **Click the Security tab.**
   The Security window opens.

4. **Select Enable Password Synchronization and then click OK.**

5. **Click Close to close the Network Configuration window.**
   You must shut down and restart your computer for password synchronization to become enabled.

▼ To Change Both UNIX and NT Passwords in Windows NT

Be sure you fulfill the following requirements before attempting to change synchronized passwords:

- Both the UNIX password and NT password are identical.
- You are logged in as the user whose password is being changed.
- NIS / NIS+ is enabled.

1. **Press Ctrl+Alt+Delete and then click Change Password.**

2. **In the Change Password dialog box, type your user name in the User Name box.**

3. **In the Domain box, select the NT domain.**
   The NT Domain displays your PC name.

4. **Type your old password.**

5. **Type your new password, and then type it again in the Confirm New Password box.**
   You will see two confirmation boxes, one from Windows NT and one from Solstice NFS Client.

Logging In and Changing Passwords on Windows 95

You can log in to all networks and Windows 95 at the same time. If your password for Windows 95 or for another network is the same as the password for the primary network login, Windows 95 automatically logs you in to Windows 95 and the networks using that password.

When you log in to other networks with different passwords and choose to save them, the passwords are stored in the password list file. The Windows 95 password unlocks the password list file and uses the passwords to log you in to other networks, so no additional passwords need to be typed.

On Windows 95, you can:

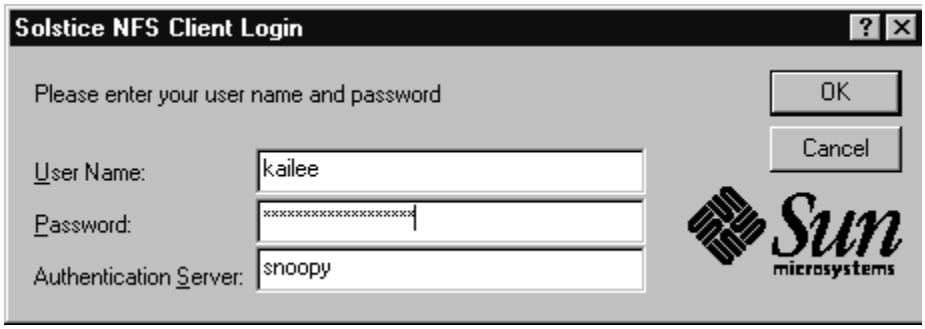
- Change your UNIX password without changing your Windows password
- Change your Windows password without changing your UNIX password
- Synchronize your UNIX and Windows passwords, which means that changing your Windows password automatically changes your UNIX password as well

▼ To Log In to a Solstice network from Windows 95

1. **Start Windows 95.**

2. **In the Welcome to Windows dialog box, type your user name and password and then click OK.**

If your UNIX user name and password are the same as for Windows 95, logging in to the Windows login dialog box logs you in to both the Microsoft and Solstice networks. If your Windows user name and password differ from your UNIX user name and password, the Solstice NFS Client Login dialog box opens.



3. **Type your UNIX user name, UNIX password, and authentication server, and then click OK.**

   You can type an asterisk in the Authentication Server box to broadcast for the first available authentication server.

▼ To Synchronize a UNIX and Windows 95 Login Password

1. **Click Start, point to Settings, and then click Control Panel.**

2. **Double-click the Passwords icon.**

   The Passwords Properties dialog box opens.

3. **In the Change Passwords property sheet, click Change Windows Password.**

   The Change Windows Password dialog box opens.

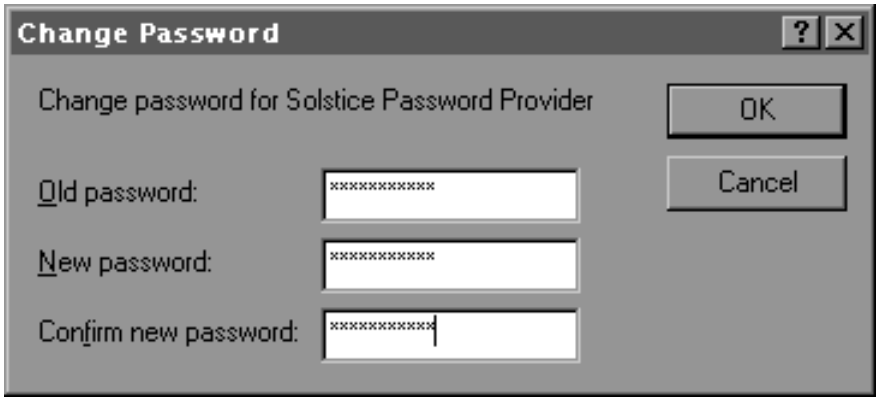
Note - The Windows Screen Saver passwords option will be listed here only if the Windows screen saver has been turned on and the password-protected option has been selected.

---

4. **In the Change Windows Password dialog box, select Solstice Password Provider and then click OK.**

   This tells Windows 95 to change the password for Windows 95 and for the Solstice network. The Change Password dialog box opens.

5. **In the Change Password dialog box, type your old Windows password, type your new Windows password, and then, in the Confirm New Password box, type the new password again. Click OK.**



The Windows and UNIX passwords are both changed to the same new password at the same time.

▼ To Change the UNIX Password on Windows 95

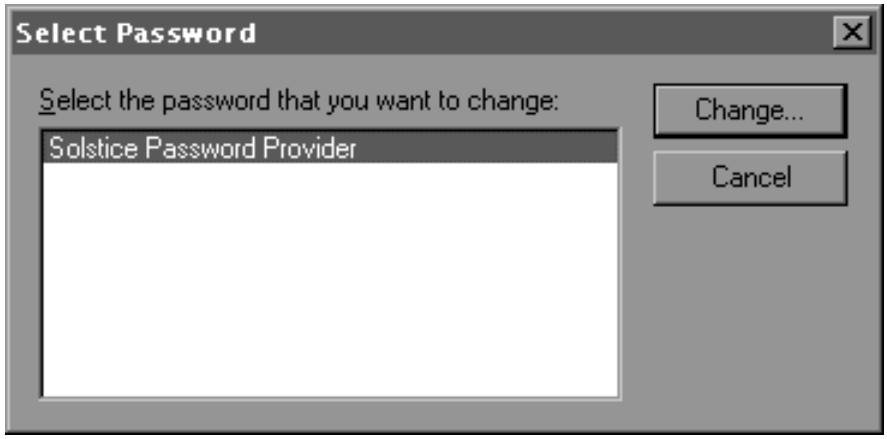
Note - Your username must match the username of the user whose password is being changed.

---

1. **Click Start, point to Settings, and then select Control Panel.**

2. **Double-click the Passwords icon.**
   The Passwords Properties dialog box opens.

3. **In the Change Passwords property sheet, click Change Other Passwords.**
   The Select Password dialog box opens.



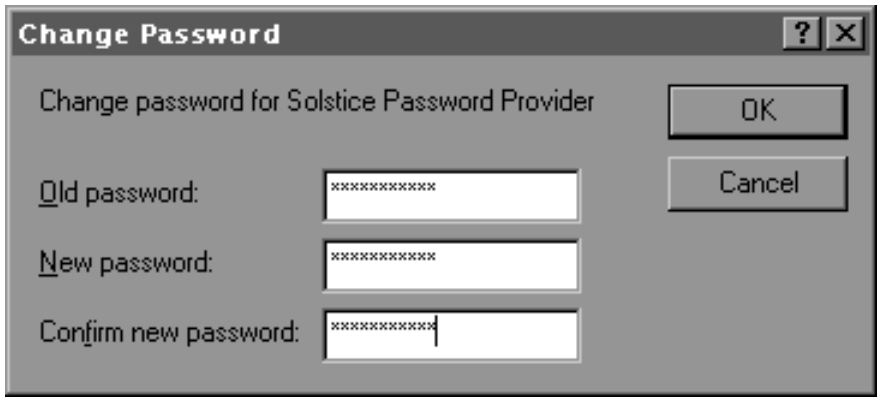
4. **In the Select Password dialog box, select Solstice Password Provider and then click Change.**

   The Change Password dialog box opens.

5. **In the Change Password dialog box, type your old UNIX password and type your new UNIX password.**

6. **In the Confirm New Password box, type the new password again, and then click OK.**

   You now must type a separate password to access the Solstice network.



Your UNIX password is changed, without changing your Windows password.

Troubleshooting

Table 7–1 presents common error messages you might see when changing a UNIX password on Windows NT and Windows 95.

TABLE 7–1 Common Error Messages

Message	Solution
`The NIS/NIS+ name service is not enabled. Please configure NIS/NIS+ before attempting to change the password.`	1. Select the Network Neighborhood icon and click with the right mouse button. 2. Double-click Properties. 3. Click Solstice NIS / NIS+ Naming Services. 4. Select either the NIS or NIS+ naming service. 5. Click OK to close the Naming Services properties tab. 6. Click OK again to the close the Network dialog box. 7. Click Yes to restart your computer.
`The username provided is invalid. The user name you typed is not stored in the NIS passwd map.`	If you are using NIS+, either the `passwd` or `cred` entry for user name cannot be found in the NIS+ tables. Make sure you type the name correctly. Check with your network administrator to make sure the entries for your user name are correct in the NIS / NIS+ name service.
`Username of the user attempting to change the password must match the username of the user whose password is being changed. Please be sure that a single username is used to log in to every network.`	You tried to change the password of a user other than the user you are logged in as. 1. Click Start, then click Shut Down, and select Close All Programs And Log On As A Different User. 2. Log in and type a user name that is the same for Windows and UNIX.
`The password provided is invalid.`	The new password must have at least 6 characters (at least 2 alphabetic and 1 numeric), must differ from the old password by at least 3 characters, and may not be a circular shift of the username.

TABLE 7–1 Common Error Messages *(continued)*

Message	Solution
`The old password contains invalid characters`	The old password you typed contains characters that are not allowed on a UNIX server. You probably mistyped the password. Retype the password correctly.
`The old password provided does not match actual old password stored on the network. A valid old password must be provided in order to change it to a new password.`	You probably mistyped your old UNIX password. Retype the password correctly.
`The old password you typed does not match your current UNIX password.`	Type your current UNIX password.
`Failed to contact or communicate with NIS/NIS+ server to change the password. Please try again.`	The NIS / NIS+ server might not be running. To check, log in to the server and type the command: `ps -ax | grep yppasswd` Contact your system administrator.
`Failed to change the password. Please try again.`	You do not have secure RPC credentials to change the NIS+ password on the server. Contact your system administrator.
`You don't have permission to change the password.`	You do not have permission (in the NIS+ `cred` table) to change the UNIX password. Contact your system administrator.

Table 7–2 lists possible solutions to problems logging in to a Windows 95 or Windows NT client connected to a LAN.

TABLE 7–2 Possible Solutions

Possible Causes	Solutions
You entered the authentication server incorrectly or the authentication server is not working.	Use the Windows `ping` command to reach the machine running the authentication server. Ask a network administrator for the correct IP address of the authentication server to use. Retype the correct authentication server address in the login dialog box and click OK.
One or more TCP/IP settings are incorrect.	On Windows 95, follow the steps in the "Checklist for TCP/IP Settings on Windows 95" on page 57. On Windows NT, follow the steps in the "Checklist for TCP/IP Settings on Windows NT" on page 58.
The name server cannot find an IP address for the remote computer.	Verify that you typed the name for the remote computer correctly. Ping the remote computer's IP address.
The remote computer, the network, or part of the network is down.	Check your modem or network cables. Ping your computer to verify it can connect to itself (which verifies that your local interface is running). Ping your name server (by name or by IP address) and your local gateway.

CHAPTER 8

PC-CacheFS

This chapter describes the PC-CacheFS program and explains how to use it to improve system performance.

You can read background and procedural information throughout this chapter, or use the following references to go directly to a specific topic.

- "About PC-CacheFS" on page 143
- "What You Need to Know About Cache Security" on page 144
- "Starting PC-CacheFS" on page 144
- "Managing the Cache" on page 145
- "Customizing PC-CacheFS" on page 147
- "Using Cache Statistics" on page 150

About PC-CacheFS

PC-CacheFS is a software application that reduces network traffic and improves system performance by copying the files you work with most frequently across the network to your local hard drive. The network files are written to a designated location called a cache. Cached data can be accessed more quickly because you access it from your local hard drive instead of across the network.

What You Need to Know About Cache Security

During setup, PC-CacheFS creates a directory called `CFS.SYS`, which is located in the root directory of the selected cache drive. As you access information from the network and CD-ROM drives, PC-CacheFS retains this information in the `CFS.SYS` directory.

Users who are either permitted to use your personal computer, or who are granted network access, can look in the `CFS.SYS` directory and access any files and directories that you have cached there. These files may contain information to which they should not have access. For this reason, you should be cautious about the kinds of information you cache. Be sure you have cached only work-related, non-confidential information that can be viewed, without consequences, by users who share your computer or network.

To remove data from the cache directory, flush the cache. See “To Flush the Cache” on page 146.

Caution - Do not to remove the `CFS.SYS` directory or modify any of the information it contains, as doing so may cause the removal or malfunction of the cache.

Starting PC-CacheFS

PC-CacheFS works transparently and automatically. Even when the PC-CacheFS Monitor is not running or displayed, PC-CacheFS continues to cache your network drives. You can view the PC-CacheFS Monitor when you want to view cache statistics or change cache settings.

▼ To Start the PC-CacheFS Monitor

1. **Click Start in the Windows control bar.**
2. **Point to Programs, point to Solstice Utilities, and then click PC-CacheFS Monitor.**
3. **Click the View Statistics button to expand the monitor.**

   The expanded PC-CacheFS monitor screen opens (Figure 8–1).

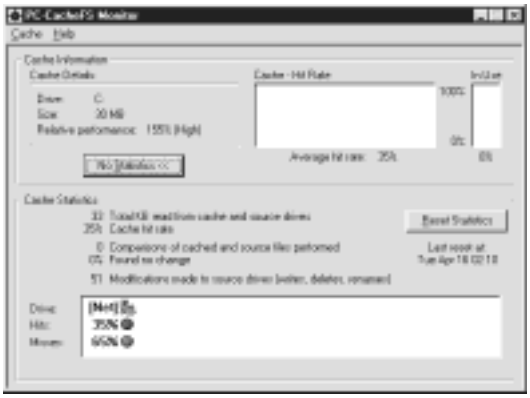


Figure 8–1 PC-CacheFS Monitor – Expanded

Managing the Cache

When starting PC-CacheFS for the first time after installation, you can set up and customize the cache. If you ever delete the cache, for example, to free disk space, you can restore it by setting it up again.

▼ To Set Up the Cache

1. **In the PC-CacheFS Monitor, click Cache, and then click Configuration.**

2. **In the PC-CacheFS Configuration dialog box, click Let Me Specify My Own Cache Settings.**

3. **Change the following settings as needed.**
   - Cache On Drive – Selects the location for the cache. The default is to locate the cache on drive C.
   - Size of Current Disk Cache – Represents the size of the cache in megabytes. The recommended size is calculated as a percentage of the available space on the disk.
   - Drives to Cache – Connects new network drive letters to the cache. You can also cache CD-ROMs and removable media. You can cache all network drives

as you connect to them, or select and deselect drives that are already connected.

4. **Click OK.**

Flushing the Cache

If you need more disk space than is currently available on your computer, you can either change the size of your cache or flush the cache.

Making your cache smaller is a preferable solution if you are not using all the cache space. Determine the amount of cache space currently in use by looking at the In Use graph on the PC-CacheFS Monitor.

Flushing the cache is a preferable solution if you temporarily need to make space available on your computer. Flushing the cache causes the information contained in the cache to be temporarily removed from your hard disk until you access the information again.

▼ To Flush the Cache

1. **In the PC-CacheFS Monitor, click the Cache menu.**
2. **Click Flush Cache.**
3. **Click Yes.**

Deleting and Restoring the Cache

Deleting the cache causes the cache and the information contained in it to be completely removed from your computer. This is a more permanent operation than flushing the cache, as you have to set up the cache when you want to use it again. Delete the cache if you need to free the disk space and no longer wish to cache data.

▼ To Delete the Cache

1. **In the PC-CacheFS Monitor, click the Cache menu.**
2. **Click Configuration.**
3. **In the PC-CacheFS Configuration dialog box, click Delete Cache.**
4. **In the confirmation box, click Yes.**
5. **Click OK.**

The cache is deleted.

▼ To Restore the Cache

1. **In the PC-CacheFS Monitor, click Cache, and then click Configuration.**
2. **Select Let Me Specify My Own Cache Settings.**
3. **Select a drive letter in the Cache On Drive field.**
4. **Click Change.**

Customizing PC-CacheFS

You can customize PC-CacheFS to make your cache perform according to your needs by changing advanced settings. You can change settings for each drive, or configure settings that apply to all drives available to be cached. Use PC-CacheFS advanced settings to configure the following properties:

- *Directory Caching* – Caches the attributes of a directory.
- *Directory Time-out* – Determines how long PC-CacheFS will retain a cached copy of directory information.
- *File Time-out* – Determines how often PC-CacheFS compares the modification time of the file on the source drive with the cached copy.
- *Read Size* – The number of bytes of information used during a read function.
- *Write Size* – The number of bytes of information used during a write function.

Directory Caching

PC-CacheFS provides the ability to move information about characteristics of and changes to directory structures in your cache. Moving this information into the cache saves the time it takes to search for directory information on your server.

Directory Time-out

The directory time-out determines how long PC-CacheFS will retain a copy of the directory information. The minimum and maximum time-out values establish a range. (The default range is between a 30-second directory time-out minimum and a 120-second maximum.) PC-CacheFS selects a value within the range based on the amount of time that has passed since the directory was last modified. Recently modified directories are read again more quickly than less-recently modified directories.

If a file is copied to the source drive from a computer other than yours, you will not see the changes until the time-out expires and PC-CacheFS updates the cache. Setting low time-out values increases directory consistency at the expense of network traffic. Use higher time-out values for directories that are modified only from your computer, or if you are accessing information using a slow network connection, such as a PPP dial-up connection.

File Time-out

The file time-out determines how often PC-CacheFS compares the modification time of the file on the source drive with the cached copy. The minimum and maximum time-out values establish a range. (The default range is between a 3-second minimum and a 60-second maximum.) PC-CacheFS selects a value within the range based on the amount of time that has passed since the file was modified. Recently modified files are checked for consistency more frequently than less-recently modified files.

Setting low time-out values increases file consistency at the expense of network traffic. Use higher time-out values for files that change infrequently or if you are accessing information using a slow network connection, such as a PPP dial-up connection.

If the file on the source drive changes infrequently, you can increase the file time-out to allow more time to pass between consistency checks. For example, you can increase the default file time-out maximum from 60 seconds to 75 seconds, and increase the minimum from 3 seconds to 5 seconds. An amount of time greater than 5 seconds but not more than 75 seconds will pass before PC-CacheFS makes a consistency check of the cache and the source drive. The additional time between consistency checks results in less network traffic and improved network performance.

If the file on the source drive changes frequently, you can ensure greater consistency between the file on the source drive and the copy in your cache by decreasing the default file time-out maximum from 60 seconds to 45 seconds and minimum from 3 seconds to 2 seconds. An amount of time greater than 2 seconds but not more than 45 seconds will pass before PC-CacheFS makes a file comparison between the source drive and your cache. Because comparisons and updates of cache and server information are more frequent, greater load is added to your network and you may notice more of a delay in retrieving information. In most situations, you do not need to decrease the file time-out minimum below the 3-second default.

Read or Write Size

The read size is the number of bytes of information used during a read function. A read function is any task that retrieves information from a file, such as opening a file for editing. In the PC-CacheFS Monitor, the effects of the read function are displayed in the field, Total Kbytes Read From Cache And Source Drives.

The write size is the number of bytes of information used during a write function. A write function is any task that causes information in your cache to be changed, such as saving a file, deleting a file, or renaming a file. The effects of the write function are displayed in the field, Modifications Made To Source Drives (Writes, Deletes, Renames).

PC-CacheFS breaks down large read and write requests into smaller blocks of the specified read or write size to help your computer perform other tasks in a timely manner. You can select a read or write size from 512 to 8192 bytes.

The default value of 8192 bytes is suitable for most LAN connections. Selecting a smaller read or write size may provide improved response times when accessing information using a slow network connection, such as a PPP dial-up connection.

▼ To Change Advanced Settings

1. **In the PC-CacheFS Monitor, click Cache, and then click Configuration.**
   The PC-CacheFS Configuration dialog box opens.

2. **Click Let Me Specify My Own Cache Settings.**

3. **Click the Advanced button.**

4. **In the PC-CacheFS Advanced Configuration dialog box:**
   a. **To configure a single drive, click Configure Drives Independently, then click the tab showing the drive letter of the drive for which you want to change settings.**

   b. **To configure options for all drives, click Use One Setting For All Drives.**

5. **Change the required settings, and then click OK.**

Using Cache Statistics

The PC-CacheFS Monitor displays statistics that allow you to monitor performance. Click on the View Statistics button to expand the monitor. The monitor displays the cache-hit rate, the capacity, and the relative performance.

Cache-Hit Rate

PC-CacheFS retrieves file or directory information from a network drive and moves the information into the cache, stored on your local hard drive. Also, PC-CacheFS makes consistency checks between the cache and the remote location, and updates the cache.

A hit occurs when the information in the source network drive is current with the information in the cache. A miss occurs when the information on the source network is more recent than the information in the cache.

The average of the number of hits to the total number of hits and misses is referred to as the cache-hit rate, and is displayed in the Cache-hit Rate graph.

Factors Affecting the Cache-hit Rate

The cache-hit rate is affected by the type of access, the size of the cache, and the frequency of the consistency checks.

Type of Access

The way you access your files affects the cache-hit rate. If you access many files and you have a large cache, you will have a larger cache-hit rate because older information still remains in the cache during consistency checks. However, if you have a small cache, there is less room for information to remain. As the cache fills, older information is automatically removed from the cache. You will experience more misses and a lower cache-hit rate.

Cache Size

The cache size implies cache capacity. The larger the cache, the better the chances are that least recently accessed information remains in the cache and has not been automatically removed. The smaller the cache, the more likely that least recently accessed information will be removed from the cache.

Frequency of Consistency Checks

The file and directory time-out values affect the frequency with which PC-CacheFS performs consistency checks. When information on the network drive changes, PC-CacheFS updates the cache. These instances are misses and result in a lower cache-hit rate.

Capacity

The In Use graph monitors the capacity of the cache. The In Use statistic fluctuates as you access new files from a network drive and the information is added to your cache. When your cache is full, capacity reaches 100% on the In Use graph. As the cache becomes updated with new information from the source network drive, the least recently accessed information is automatically removed from the cache to make space available for the new information.

Relative Performance

Your most precise indicator of cache effectiveness is the relative performance value displayed in the PC-CacheFS Monitor. After you restart your computer, relative performance displays at 100 percent, which indicates that the system performance is the same as without PC-CacheFS. As you retrieve information from a remote location, the relative performance increases or decreases to indicate the overall gain or loss of performance for your particular mix of applications. A low relative performance may indicate that while your network is fast, your local disk, where your cache is located, may be slow.

A relative performance under 100 percent can occur when PC-CacheFS automatically updates information in the cache, slowing the speed of your system below your regular system speed. A continued relative performance below 100% indicates you are not using the information on the current drive enough times to necessitate caching that particular network drive. Select a different drive to cache; one on which you use information more frequently.

Since PC-CacheFS has the benefit of reducing network traffic and server load, a slightly lower relative performance may indicate increased productivity across multiple clients at your site. A high relative performance indicates that your cache is performing well in relation to the network, thereby enhancing your personal productivity. Other indicators of cache effectiveness include an average cache-hit rate greater than 50 percent, and green lights in the Hits field more often than yellow lights in the Misses field.

Resetting Cache Statistics

Over time, PC-CacheFS accumulates statistics about your cache, such as the cache-hit rate and total kilobytes (KB) read. If you want the fields in the PC-CacheFS Monitor to display the statistics for a particular drive, you can reset the statistics. By resetting the statistics, you can determine the changes of statistics for a particular drive over time. You can also find out how one particular drive contributes to cache performance overall.

Reset cache statistics by expanding the PC-CacheFS Monitor and clicking Reset Statistics.

APPENDIX **A**

Frequently Asked Questions

NFS Client

Can I use other network clients at the same time as Solstice NFS Client?

Yes. For example, if you are using both Solstice NFS Client and Client for Microsoft Network, when you go into Network Neighborhood you will see both your local network and also icons for NFS Servers and Automount Maps.

Do I need to be authenticated by a `pcnfsd` server?

Yes. If you want to access NFS file servers, you must have user and group IDs as credentials. The only way to get them is from an authentication server. An exception to this rule is accessing files on a computer running the NFS Server which grants or rejects access based on machine name rather than user/group IDs.

If you just want to use NFS Server, LPR Server, or PC-CacheFS, then you do not need to be authenticated.

How do I specify the Authentication server to use?

From the Properties screen of the Solstice Network Client, you select the Security tab and select either to broadcast on your local subnet for a server or enter the IP address of a server if there is not one on your local subnet or you are making a serial connection.

Does the Solstice NFS Client have to be the Primary Network Logon?

The answer depends on how your computer is set up. Windows 95 uses the Primary Network Logon to determine which network client will present its logon screen first, and from where user and system policies are downloaded.

- If you have both Microsoft Client networking and Solstice NFS Client networking installed and you are using the same username/password for both clients, you can use either network as the Primary Network Logon and you will only have to login once to reach both networks. If you use different username/passwords for each network, it also doesn't matter which is the primary logon since you will have to enter your username and password for each client's logon screen.

- Only one Network Provider governs where user and system policies are downloaded from. So if you want to be sure that your Windows client downloads any Solstice related policy files, you must set the Solstice NFS Client to be the Primary Network Logon. If you don't care, then it doesn't matter.

- Some applications communicate only with the primary network provider. If you want to perform an operation over the NFS network, you may need to ensure that Solstice NFS Client is the Primary Network Logon.

How do I access NFS files?

The Solstice NFS Client mounts servers transparently when you browse for NFS servers. This implicit mapping process lets you look at and access files on NFS servers without having first to map a network drive. You can also explicitly map a network drive, using the Tools menu of Windows Explorer.

What is the difference between mapping a network drive and accessing an NFS server through Network Neigh

The convenience of browsing Network Neighborhood does come with a small price—when you close Network Neighborhood or one of the windows that is viewing an NFS file system, the files on that file system are no longer accessible until you browse that file system again. In addition, the files on an implicitly mapped file system cannot be accessed from an MS-DOS box, or by an application that uses only mapped drives to access files. When you explicitly map network drives you have access to them all the time.

What is an Automount map?

The Solstice NFS Client automounter provides administrators with the capability to define mount points without regard to their actual location on a network. Automount maps provide the links between file system names and their actual locations. For example, a file system name of `/pcapps` could map to a network location of `appserver:/export/pcapps`. This location could change with a simple update to the automount map.

Can I access NFS files on UNIX servers other than Solaris?

Solstice NFS Client is an NFS V2 and V3 implementation. It should interoperate with NFS servers that support those standards.

NFS Server

What is NFS Server?

The NFS Server is a daemon (Windows 95) or a service (Windows NT) that runs on your Windows computer and lets you share files and directories with other Windows computers and UNIX workstations connected to your network. The NFS Server is a Winsock application and it supports NFS version 2 functionality. The NFS Server will not turn your computer into a full-fledged file server. Rather, NFS Server provides a simple mechanism for the casual sharing of PC-based files among a limited number of users.

Using NFS, what can I share with coworkers?

With NFS Server, you can share files and folders located on your computer or devices, such as a CD-ROM drive.

How do I share files, folders and devices?

To share files, folders and devices you configure the NFS Server program and then start it. From then on, any coworker who has network access to your computer and who has the right to access your shared devices, can mount a drive pointing to the shared device.

Who can access my shared devices?

When configuring the NFS Server, you specify which remote computer may access your shared devices. These remote computers are either Microsoft Windows computers running Solstice Network Client, or UNIX workstations. Remote computers that have access to shared devices are referred to as NFS Server clients.

Can I restrict access to my shared devices?

NFS Server lets you restrict access based on a list of names of remote NFS Server clients rather than on the basis of individual users. For example, restricting access to a remote computer called `galaxy` means that no user working on `galaxy` has access to your shared devices. You cannot specify that certain users on `galaxy` can access your shared devices while others cannot.

What other type of restrictions can I specify?

In addition to specifying which NFS Server client can access your shared devices, you can restrict access based on the following:

- By type of access: Read Only or Read / Write
- By prompting NFS Server clients to enter a password

Where does NFS Server store access rights data?

NFS Server maintains the list of shared devices in the Windows 95 or Windows NT Registry. The only way to modify this information is though the NFS Sharing property sheet that you access through the Windows Explorer program.

Must the NFS Server program be running to enable coworkers to access shared devices?

Yes, without NFS Server running on your computer, coworkers will not be able to see your shared devices. As a courtesy to your coworkers, we suggest you add NFS Server in the Start Programs menu so that it is started automatically when you start Microsoft Windows.

Where can I find out about problems with NFS Server?

You can enable the logging of NFS Server and Port Map activities using the Logging command in the NFS Server and Port Map menus. Once you have enabled logging, you must make sure that the Network Event Log program is running. Start Network Event Log by clicking its icon in the Solstice program group, or by entering `sunwsyslogd` at the Run prompt. Also refer to the Troubleshooting section in the NFS Server online help.

LPD Printing

Can I share my PC printer with my coworkers and what must I do?

To make your printer available to coworkers, you must define a printer queue for the printer on your computer, start LPD Print Server, and enable your computer to receive print requests.

Who can access my printer?

When you share your printer using LPD Print Server, your printer becomes a network printer. Coworkers within your networked environment who use software

that can interpret the LPD protocol, can print documents on your PC printer. This includes coworkers using a Windows computer or a UNIX workstation.

What happens to my coworkers' print requests when I turn off my printer or my computer?

Print requests that were processed and placed in the LPD Print Server spool directory are saved before you turn off either your computer or your printer. Those print requests will be printed when you restart your computer, the LPD Print Server, and your PC printer.

How can I find out which print requests belong to me and which belong to coworkers?

To find out which print requests belongs to you or your coworkers, display the Printers window from the Settings menu, and double-click the printer's queue name. A window appears listing such details as document name, status and owner.

Where are printer problems logged?

All operations related to print requests sent to your LPD printer are written in a log file. You can open, print, or purge the log file. The default path and file name of the log file is `C:\spool\logfile.txt`. The Troubleshooting section of the Solstice LPD Print Server utility provides solutions pertaining to LPD Print Server setup and error messages.

What must I do to access a coworker's printer?

To print documents on a coworker's printer, you add that printer to your list of available printers using the Microsoft Add Printer Wizard. If you will use that printer frequently, you may want to specify it as your default printer.

PC-CacheFS

What Is PC-CacheFS?

PC-CacheFS is a software application that reduces network traffic and improves system performance by copying the files you work with most frequently on the server to your local hard drive. This technique is referred to as caching. The location on your hard drive is referred to as a cache. Caching helps you to use your files more quickly because you access them from your local hard drive instead of across the network.

Does PC-CacheFS only work with NFS file systems?

Solstice PC-CacheFS operates with any file system that is compliant with Microsoft's Windows Installable File System (IFS), allowing you to use the same product throughout your heterogeneous network environment.

Can I install and use just the PC-CacheFS part of the Solstice NFS Client product?

Yes, during installation, select Custom as the setup type, then click Change to list the subcomponents. From the list of subcomponents, make sure that only PC-CacheFS is checked.

How can I tell if PC-CacheFS is working?

The PC-CacheFS Monitor shows cache statistics. A high Relative Performance indicates that your cache is performing well in relation to the network, thereby enhancing your personal productivity. Other indicators of cache effectiveness include:

- Average cache-hit rate greater than 50%
- Green lights in the Hits field more often than yellow lights in the Misses field

APPENDIX **B**

Setting Up PCNFSD

This chapter provides background information and instructions for installing the authentication server daemon on a UNIX server.

You can read background and procedural information throughout this appendix, or use these references to go directly to a specific topic.

- "UNIX Server Requirements" on page 159
- "`PCNFSD` Daemon Overview" on page 160
- "Services Provided by `rpc.pcnfsd`" on page 160
- "Deciding Where to Install `rpc.pcnfsd`" on page 163
- "Determining if `rpc.pcnfsd` Is Already Installed" on page 162
- "Installing `rpc.pcnfsd`" on page 163
- "Upgrading the PCNFSD Daemon" on page 167
- "Configuring the PCNFSD Daemon" on page 169
- "Non-SunOS Platforms Installation" on page 169

UNIX Server Requirements

You can install the `pcnfsd` server software on one of the following:

- Sun-3™, Sun-4™, or SPARCstation™ servers running SunOS™ operating system version 5.4 or compatible versions
- Sun-3, Sun-4, or SPARCstation servers running SunOS operating system version 4.0 or compatible versions for `rpc.pcnfs` daemon installation only
- Intel-based PCs running the SunOS 5.4 operating system or compatible versions

- Other NFS servers such as a Digital Equipment Corporation system running the Ultrix operating system. (Contact your local Solstice NFS Client distributor or service provider for more information.)

PCNFSD Daemon Overview

The PCNFSD daemon, `rpc.pcnfsd`, provides user authentication services that allow the Solstice Network Client to access files on any NFS server in the network. The daemon also provides access to PCNFSD-based printing. Using these services requires you to install `rpc.pcnfsd` on at least one server in your network.

The PCNFSD daemon runs continuously on a UNIX server to service requests for user authentication and for printing to network printers. The `rpc.pcnfsd` daemon is based on Sun's remote procedure call (RPC) services. Programs running on the PC make remote procedure calls to the `rpc.pcnfsd` program running on a UNIX server.

Although not part of the PCNFSD services, Solstice Network Client provides support for user views and client management using the PCNFSD server.

Services Provided by `rpc.pcnfsd`

The `rpc.pcnfsd` daemon provides the following services:

- *Authentication* – PC users can identify themselves to the network and be granted appropriate privileges for file access and program execution.
- *Access to printer spooling services* – PC users can send printing requests to printers attached to servers on the network.

Authentication and System Security

A Solstice Network Client user can log in to the Solstice network in much the same way as the user can log in to a UNIX system. The Login program takes the user name and password, encrypts them, and calls the authentication procedure in `rpc.pcnfsd` on the authentication server. If this procedure succeeds, it returns a user ID and a group ID to be used when constructing the credentials for the user. These credentials are used for subsequent NFS file access. If the user name and password are not found, then authentication fails and the user is denied access.

The authentication server may also return secondary group membership, `umask`, and home directory information (such as server name and home directory path name).

Solstice NFS Client users who do not log in to the network have no access to the Solstice network.

Shared Printer Support

The `rpc.pcnfsd` daemon provides users with the following printing services:

- Connecting to a network printer and starting a print job
- Browsing for network printers
- Viewing network print queues
- Canceling or removing print jobs in network print queues

In order to support NFS print services, you must export the spool directory on the pcnfsd server. The spool directory has the default name of `/var/spool` on a SunOS 5.4 operating system or compatible versions and `/usr/spool` on a SunOS 4.0 operating system or compatible versions.

By exporting `/var` or `/var/spool` or `/usr/spool`, printing should work correctly. You cannot simply export the root directory ("`/`").

Support for User Views and Site Policies

For Windows 95 and Windows NT users, a system administrator can create a directory on the PCNFSD server that contains user profiles and system policy files. Storing user profiles on the PCNFSD server allows users to have an identity separate from the machine on which they are working. Users can carry their preferences with them whenever they log in to any PC in the network.

The system administrator can use centrally located policy files to manage clients by customizing the desktops, configuring network settings, and restricting access to applications and options.

Support for user views and site policies requires the administrator to create a directory on the PCNFSD server called `/opt/MSPolicy`. For more information about managing Windows 95 and NT clients see Chapter 6.

Determining if rpc.pcnfsd Is Already Installed

If rpc.pcnfsd is already installed, you do not need to reinstall it. However, the SUNWpcnfd package includes a multi-threaded version of rpc.pcnfsd that allows greater numbers of simultaneous logins than earlier versions (in Solstice Network Client 3.1 Plus and earlier).

To see if rpc.pcnfsd is installed on a server, use one of the following methods:

- Use the ps command to list all processes by name, and check if rpc.pcnfsd is among them.
- Use the ls command to see if rpc.pcnfsd is present in any of the following directories: /opt/SUNWpcnfs/sbin (SunOS 5.4 operating systems and compatible versions only), /etc, /usr/etc, /usr/lib, /bin, or /usr/bin.

▼ To See if rpc.pcnfsd Is Installed

- **On the server with a SunOS 4.0 operating system or compatible version, enter** ls /usr/etc/rpc.pcnfsd**.**

See if the output shows that the rpc.pcnfsd daemon is already installed. You may also list other directories such as /etc/usr/bin, /bin, and /usr/lib, in case it is not in the expected directory.

- **On a server with a SunOS 5.4 operating system or compatible version, enter** ls /opt/SUNWpcnfs/sbin/rpc.pcnfsd**. See if the output shows that the** rpc.pcnfsd **daemon is already installed.**

▼ To See if rpc.pcnfsd Is Running

- **On a server with a SunOS 4.0 operating system or compatible version, enter** ps -ax | grep rpc.pcnfsd**.**

See if the output shows that the daemon is already running.

- **On a server with a SunOS 5.4 operating system or compatible version, enter** ps -ef | grep rpc.pcnfsd**.**

See if the output shows that the daemon is already running.

Deciding Where to Install rpc.pcnfsd

You can install and run rpc.pcnfsd on a single server, on several servers, or on all servers on the network.

If you run rpc.pcnfsd on a single server, this machine will be used for all PCNFSD authentication and printing. In this case, make sure this server is always available and is accessible to all client computers. When the PC user configures Solstice Network Client software, the user can identify this server by name, and the software will always try to use this server for authentication.

This method has disadvantages, however, particularly in a large network. For example, if there is only one PCNFSD server and it fails, users will not be able to log in or print from their computer to a network printer. Also, a client may not be able to access the PCNFSD server if a router in the network fails.

It is better to run rpc.pcnfsd on several servers on the network. Users can enter the server's name or IP address when they set up Solstice Network Client software, or they can broadcast for a PCNFSD server on the local subnetwork by entering an asterisk (*) rather than a server name or IP address.

Note - You do not need to reinstall the SUNWpcnfd package if your server is already running the PCNFSD daemon.

Installing rpc.pcnfsd

The Solstice Network Client CD-ROM contains software to install the rpc.pcnfsd version 2 daemon on a Sun server running the SunOS 4.0 operating system or compatible versions or the SunOS 5.4 operating system or compatible versions. For non-SunOS platforms, the CD-ROM contains the source files that allow you to build and install binaries on other UNIX servers.

▼ To Install rpc.pcnfsd on a Server Running the SunOS 5.4 Operating System or compatible Verstions

1. **Move to the product installation page, to the section marked Server Components, and click SPARC or x86 to download the correct version of the server software to your machine.**

The compressed tar file is copied to your system (`pkgs.sparc.tar.Z` or `pkgs.i386.tar.Z`, depending on your operating system).

2. Uncompress the file. For example, on a SPARC system, type

```
uncompress pkgs.sparc.tar.Z
```

3. Extract the files. For example, for a SPARC system, type

```
tar xvf pkgs.sparc.tar
```

This creates four packages: `SUNWipop`, `SUNWlit`, `SUNWlicsw`, and `SUNWpcnfsd`. You can then run the `pkgadd` utility in this directory to install the software on your system.

4. Become superuser.

5. Enter the following command:

```
pkgadd -d ‘pwd‘
```

Note - If you change to the directory where you installed the packages, you can type: `pkgadd -d`.

When you press Return, the `pkgadd` program displays information for the SPARC architecture and similar information for Intel, as in the following example.

```
The following packages are available:
  1  SUNWipop      Solstice Internet Mail POP3 server
                   (sparc) 1.0

  2  SUNWlicsw     FlexLM License System
                   (sparc) 5.12a

  3  SUNWlit       STE License Installation Tool
                   (sparc) 4.0

  4  SUNWpcnfd     PC-NFSpro Daemons
                   (sparc) 1.2

Select package(s) you wish to process (or ’all’ to process
all packages). (default: all) [?,??,q]:
```

6. Enter the number 4 to select the PCNFSD daemon package.

During the installation, you are prompted for permission to execute with superuser privileges. Answer yes to each request.

When the package has been installed, the original `pkgadd` screen is displayed.

The `pkgadd` program stops related server daemons already running, starts the server components, and copies a script to the `init.d` directory to start these components each time you reboot the machine.

7. **Set the man page path or add the man pages to your man page directory.**

   Find out where the man pages are located.

   Enter `env` and look at `MANPATH`. For example:

```
# env | grep MANPATH
  MANPATH=/usr/share/man:/usr/man
```

8. **Copy the man page for `pcnfsd.1m` into section 1M. For example:**

```
# cp /opt/SUNWpcnfs/man/pcnfsd.1m /usr/share/man/man1m
```

9. **If necessary, create a `pcnfsd` configuration file, `/etc/pcnfsd.conf`.**

   This file is used to contain configuration information for PCNFSD printing. (See “Configuring the PCNFSD Daemon” on page 169.) Refer to the man page `pcnfsd(1m)` for information about this file.

10. **Once `rpc.pcnfsd` starts, you must export the print spool directory created by `rpc.pcnfsd`.**

    For example:

```
# share --F nfs /var/spool
  # echo share --F nfs /var/spool >> /etc/dfs/dfstab
```

11. **If you are supporting user and group polices for your Solstice clients, create a directory for policy files called `/opt/MSPolicy`.**

▼ To Install `rpc.pcnfd` on a Server Running the SunOS 4.0 Operating System or Compatible Versions

1. **Move to the product installation page, to the section marked Server Components, and click SPARC or x86 to download the correct version of the server software to your machine.**

The compressed tar file is copied to your system (pkgs.sparc.tar.Z or pkgs.i386.tar.Z, depending on your operating system).

2. **Uncompress the file. For example, on a SPARC system, type**

```
uncompress pkgs.sparc.tar.Z
```

3. **Extract the files. For example, for a SPARC system, type**

```
tar xvf pkgs.sparc.tar
```

   This creates four packages: SUNWipop, SUNWlit, SUNWlicsw, and SUNWpcnfsd. You can then run the pkgadd utility in this directory to install then software on your system.

4. **Become superuser.**

5. **Make a working directory in the** /var **directory.**
   For example, enter mkdir /var/tmp/sunw

6. **Enter the shell command to install the** rpc.pcnfsd **daemon.**
   Enter ./addpcnfsd.sh to install rpc.pcnfsd.
   As you enter these commands, you are asked whether you want to start the daemon each time the machine is rebooted, and where you want to install the executable files. (The default directory is /usr/etc.)

7. **If necessary, create a** rpc.pcnfsd **configuration file** /etc/pcnfsd.conf**.**
   (See “Configuring the PCNFSD Daemon” on page 169.) Refer to the man page pcnfsd(8) for information about this file.

8. **Enter the** /usr/etc/exportfs /usr/spool/pcnfs **command to export the print-spool directory.**
   The directory /usr/spool/pcnfs is created by rpc.pcnfsd and must be exported. You should also add an entry to the /etc/exports file, so the directory is exported whenever the server reboots. For example:

```
# /usr/etc/exportfs /usr/spool
  # echo /usr/spool >> /etc/exports
```

Upgrading the PCNFSD Daemon

There are two versions of the PCNFSD protocol:

- Version 1 of PCNFSD – This version was developed prior to PC-NFS version 4.0. The `rpc.pcnfsd` version 1 daemon provides user authentication and basic printing services. This version can run only with the SunOS 4.0 operating system or compatible versions.
- Version 2 of PCNFSD – The latest version of the PCNFSD protocol, version 2 was developed for the 4.0 release of the PC-NFS™ product. It provides expanded user authentication and enhanced printing services. The current release of the `rpc.pcnfsd` daemon supports both version 1 and version 2 of the PCNFSD protocol. Version 2 runs on both SunOS 4.0 and 5.4 operating systems and compatible versions.

The current release of the `rpc.pcnfsd` daemon supports both version 1 and version 2 of the PCNFSD protocol. Source code and binary programs of this daemon are included on the CD-ROM for installation on a SunOS 4.0 or 5.4 operating system or compatible version. Daemons are in compressed UNIX `tar` files for installation on SunOS 4.0 operating systems and compatible versions.

Since version 2 of the daemon can support existing PC-NFS software users (with one compatibility issue, see Note following), you should replace existing version 1 `rpc.pcnfsd` server daemons with version 2. If you do not, users may find that certain features of Solstice Network Client will not work. To upgrade `rpc.pcnfsd` on SunOS 4.0 servers or compatible versions, follow the procedure “To Upgrade `rpc.pcnfsd` on a Server Running the SunOS 4.0 Operating System or Compatible Version” on page 168.

Note - The `rpc.pcnfsd` version 2 daemon recognizes only those printer names listed by the UNIX `lpstat -t` command. Run this command on the print server to determine the printer names that the `rpc.pcnfsd` daemon will recognize. This is different from the `rpc.pcnfsd` version 1, which allows you to use any names associated with a particular printer.

▼ To Determine if Version 2 Is Running

- **On a system running the SunOS 4.0 or 5.4 operating system or compatible version, enter:**

```
rpcinfo -u servername 150001 2
```

If version 2 of `rpc.pcnfsd` is running, you will see the following message:

```
proc 150001 vers 2 ready and waiting
```

If the server is running the old version of `rpc.pcnfsd` or if `rpc.pcnfsd` is not running, you will see the following message:

```
proc 150001 version 2 is not available
```

To Determine if Version 1 Is Running

- **On a system running the SunOS 4.0 operating system or compatible version, enter:**

```
rpcinfo -u servername 150001 1
```

If the server is running the old version of `pcnfsd`, you will see the following message:

```
proc 150001 vers 1 ready and waiting
```

In this case, upgrade to version 2.

If neither version is running, try starting the daemon by entering `/usr/etc/rpc.pcnfsd` and then check the version.

If that fails, you need to install `rpc.pcnfsd`.

Source code and binary versions of `rpc.pcnfsd` are distributed on your Solstice Network Client CD-ROM in compressed UNIX `tar` files. Before installing the daemon, check your server to see if `rpc.pcnfsd` is already present. If not, install it using the appropriate installation procedure.

With `pcnfsd` version 1, you were able to install `rpc.pcnfsd` so that it was started by the `inetd` superdaemon. The new `rpc.pcnfsd` daemon must execute a possibly lengthy configuration sequence each time its starts. To avoid delays—and possible time-outs—you should arrange for the daemon to be invoked from `/etc/rc.local` (SunOS 4.0 operating system or compatible versions) or by means of a script in the `init.d` directory (SunOS 5.4 operating system or compatible versions). Do not use `inetd`.

▼ To Upgrade `rpc.pcnfsd` on a Server Running the SunOS 4.0 Operating System or Compatible Version

1. **If the `rpc.pcnfsd` daemon is running, stop (kill) it.**
   a. **Become root.**
   b. **Determine the `rpc.pcnfsd` process ID number.**
      For example:

```
# ps -ax | grep rpc.pcnfsd
```

c. **Enter** `kill -9` ***processid number.***

2. **Rename the** `rpc.pcnfsd` **version 1 daemon.**
   For example, you might rename `/usr/etc/rpc.pcnfsd` to `/usr/etc/rpc.pcnfsd.v1`.

3. **Install** `rpc.pcnfsd` **version 2 according to the instructions in "To Install `rpc.pcnfd` on a Server Running the SunOS 4.0 Operating System or Compatible Versions" on page 165.**

4. **When you are satisfied that the new** `rpc.pcnfsd` **version is working correctly, delete the old version.**

Configuring the PCNFSD Daemon

To configure PCNFSD, you must edit the `pcnfsd` configuration file `/etc/pcnfsd.conf`. Modify this file if you want to perform any of these tasks:

- Rename the print spool directory
- Define "virtual" printers
- Disable the `wtmp` compile-time option
- Specify a UID range for authentication and printer security

For details about configuring `/etc/pcnfsd.conf`, refer to the `pcnfsd.1m` or `pcnfsd.8c` man page included on the Solstice distribution media.

For instructions on how to set up and configure print services, see Chapter 5.

Non-SunOS Platforms Installation

SunSoft supplies C source code for `rpc.pcnfsd` that you can run on most UNIX servers, including SunOS 4.0 systems and compatible systems. If your server is not one of these, you may need to adapt the source code to your system, and then compile and install the modified version.

Adapting `rpc.pcnfsd` to environments other than SunOS requires some understanding of what the program does and how it interacts with other software on the server. You may want to contact your system vendor to see if that company has a version of `rpc.pcnfsd` available for its system. See the section on porting `rpc.pcnfsd` in the *Solstice Network Client Installation and Licensing Guide.*

APPENDIX **C**

SNC Script Directives

Solstice Network Client includes a script interpreter, `sunwrun.exe`, that is installed into the directory `C:\Program Files\Solstice\Bin` during client installation. Since the script interpreter is designed to be read from the server, the system administrator should copy this file from the directory on the client to the `/opt/MSPolicy` directory on the authentication servers (servers running the `rpc.pcnfsd` daemon). Installing the script interpreter enables the network administrator to use new SNC scripts or pre-existing PC-Admin SNC scripts with the 32-bit clients running Solstice Network Client software.

The SNC script interpreter runs automatically at login on a Windows NT or Windows 95 system and at logout on a Window 95 system. The script interpreter interprets the SNC directives, which are, with a few exceptions, identical to the PC-Admin SNC directives. The script directives are listed and described in “SNC Script Directives” on page 172.

Script Interpreter Command

The syntax of the `sunwrun.exe` command is:

[*drive*:[*path*]]`sunwrun.exe [-ripn]` [*drive*:[*path*]]*file*`.snc`

You can specify multiple script file names on the command line. Each file name must end with the `.snc` extension. The interpreter will execute each file, in order, until a script exits with a non-zero exit code or all files are processed.

Options include:

`-r`	Causes the script interpreter to reset the shared environment before interpreting the first file.
`–i`	Causes the script interpreter to reset the shared environment after interpreting the last file.
`–p`	Causes the script interpreter to execute files only from the location specified in the `SNDRIVE` variable.
`–n`	Causes the script interpreter to exit immediately after executing the last script file, rather than waiting the default 5 seconds provided to enable the user to view the output.

SNC Script Directives

The SNC script directives are commands that are interpreted by the script interpreter. The directives are listed alphabetically and described in this section.

COPY *source_file destination_file*

Copies a file to a new location. You cannot use wildcards when specifying the source file name. If *destination_file* is a directory, the file is copied into the directory with the same name.

Example:

This example copies the Netscape bookmark file from a user's client computer to the user's home directory on the server.

```
COPY D:\Program Files\Solstice\Netscape\bookmark.htm %SNHOME%
```

DELETE *file1 dir1 file2 file3 ...*

Deletes a list of files, directories, or both. A directory must be empty before you delete it. No wildcards apply in specifying the name of files or directories to delete.

Example:

This example deletes the `temp` directory from your hard disk and home directory.

```
DELETE C:\temp %SNHOME%temp
```

ECHO [ON | OFF] ECHO *text_string*

Turns the interpreter line echo on or off, or displays *text_string*. ECHO operates like the DOS batch file ECHO. Each ECHO updates a scrolling dialog box. ECHO ON displays all lines as they are interpreted, including REM statements. The dialog box is displayed upon the first ECHO text statement and closes when the interpreter exits.

EXIT *exit_value*

Ends the interpretation of an SNC script. The numeric *exit_value* is returned to the calling SNC script. You can test the ERRORLEVEL with the IF directive.

Example:

This example exits the current SNC script with an ERRORLEVEL value of 3.

```
EXIT 3
```

EXPORT *varname*

Puts the variable *varname* into the environment of the script interpreter. Exported values are then available to the launched program. Environment variables are preserved across invocations in the registry.

The exported variables are not placed in the Windows global environment. However, any application that is launched or otherwise started, will have exported variables set in its environment.

In general, 32-bit applications should be using the registry for application-specific data and not relying on the environment.

Example:

This example exports the variable name, PATH.

```
EXPORT PATH
```

GOTO *label*

Jumps to a different location within the current SNC script. The *label* is a string. The location to jump to is denoted by :*label* on a line by itself.

Example:

This example goes to the line with the continue label if ERRORLEVEL is 0.

```
IF ERRORLEVEL 0 GOTO continue
ECHO ‘‘help, an error occurred!’’
EXIT 1
:continue
ECHO ‘‘Success!’’
```

IF [NOT] *condition statement*

Conditionally controls the interpretation of *statement* based on the value of *condition*.

Condition	Value
EXIST *filename*	True if *filename* exists; false otherwise. **Example:** `IF EXIST temp DELETE temp` Deletes the file `temp` if it exists.
ERRORLEVEL *number*	True if current error level is equal to *number*. **Example:** `IF ERRORLEVEL 0 GOTO` *label*
"*string1*" == "*string2*"	True if the strings match. Strings can contain a variable, such as %SNUSER%, which is expanded before testing for a match. Strings can also contain a literal % by having two %% in a literal—the first % escapes the second %. **Example:** `IF ''%SNUSER%'' == ''root'' EXIT` If the user is root, then exit.

INCLUDE *snc_filename*

Includes and interprets another SNC script. *snc_filename* is a fully qualified path to the file.

ERRORLEVEL is set upon returning from interpreting the listed SNC script if an error occurs or the EXIT directive is used.

Example:

This example includes and interprets the script `test.snc`.

```
INCLUDE C:\windows\test.snc
```

INI *ini_file_pathname section* [*entry*=[*value*]]

Adds, changes, or deletes entries or sections in the specified `.INI` file. In a single `INI` directive, you can add an entry to a section, or add a section and an entry. You can also delete a section, or delete an entry in a section.

In general, 32-bit applications should be using the Registry for application-specific data and not relying on the `.INI` files.

Example:

This example deletes the [nfsw] section in the SYSTEM.INI file.

```
INI C:\windows\system.ini nfsw
```

Example:

This example creates an app section in the WIN.INI file if it does not exist, and creates the Flag1 entry.

```
INI C:\windows\win.ini app Flag1=1
```

LAUNCH *filename* [*options*]

Specifies a file to be launched just before exiting the SNC script, where *filename* is a fully qualified path to the file, and *options* are any options the file may call.

If there are multiple LAUNCH directives, the last one takes effect.

No exit status is returned, except that ERRORLEVEL is set if the interpreter fails to find or execute the listed argument.

Example:

This example launches winipcg.exe file after it has processed the script.

```
LAUNCH C:\windows\winipcg.exe
```

LOGIN

Is parsed, but ignored.

LOGOUT

Is parsed, but ignored.

MKDIR *dirname1 dirname2*

Creates one or more directories. All directories in the path to a directory being created must exist. However, in a single directive, you can create a directory, then create a directory below it, and so on, by entering multiple arguments in order.

Example:

This example creates the directory C:\able\baker\charlie.

```
MKDIR C:\able C:\able\baker C:\able\baker\charlie
```

MOUNT [-o *option,option,...*] DRIVE *server:/dir1/dir2 drive*

NFS mounts a remote file system on the drive letter *drive*. The –o option can be followed by the options listed below, separated by commas.

Without options, the DRIVE directive lists the mounted drives.

The options are:

Option (Type)	Description
acdmax (INTEGER)	Sets the maximum number of seconds that NFS waits before checking to see if a folder attribute, such as modification time, has changed. A smaller value assures earlier detection that a folder has been modified. A larger value improves performance by decreasing the frequency of NFS operations.
acdmin (INTEGER)	Sets the minimum number of seconds that NFS waits before checking to see if a folder attribute, such as modification time, has changed. A smaller value assures earlier detection that a folder has been modified. A larger value improves performance by decreasing the frequency of NFS operations.
acoff (BOOLEAN)	Disables attribute caching. Caching can improve NFS file access time.
arch (BOOLEAN)	To conform to DOS conventions, you can set the archive bit to true.
acrmax (INTEGER)	Sets the maximum number of seconds that NFS waits before checking to see if a file attribute, such as file size, has changed. A smaller value assures earlier detection that a file has been modified. A larger value improves performance by decreasing the frequency of NFS operations.
acrmin (INTEGER)	Sets the minimum number of seconds that NFS waits before checking to see if a file attribute, such as file size, has changed. A smaller value assures earlier detection that a folder has been modified. A larger value improves performance by decreasing the frequency of NFS operations.
bsd (BOOLEAN)	Uses BSD directory folder creation syntax.
case=[yes, no]	Handles remote drive with case sensitivity in file names. Default is no case sensitivity. case=yes automatically sets cs (case sensitive). case=no automatically clears cs.

Option (Type)	Description
cf (BOOLEAN)	Uses only the preferred case (either upper or lower) for file name operations. If not specified, you can create files and folders in either uppercase or lowercase. Specifying cu and cf forces uppercase. If both options are specified, when created, the folder myfolder is automatically changed to MYFOLDER.
cs (BOOLEAN)	Looks up file names while preserving the case in which you entered the file name search key. When this option is used, file operations are case sensitive, which is faster than case-insensitive operations.
cu (BOOLEAN)	Instructs NFS Client to use uppercase letters as the preferred case for looking up and creating file names.
lock (BOOLEAN)	Specifies whether to use the built-in NFS capability to prevent others from changing files you are modifying. The default is no.
map=*mapchar*	Specifies a file name mapping character. **Example**: map=^
nfsver (INTEGER)	Specifies which version of NFS to use (0, 2, or 3). If the servers to which you most often connect support only one version, configure that version as a default. The default value 0 automatically tries v3 first and then v2. **Example**: nfsver=2 specifies NFS v2
port (INTEGER)	Default is 2049. The NFS specification suggests port number 2049 as the standard NFS server port. Your NFS servers may be configured to use another port number.
preserve	This option is ignored
retries (INTEGER)	Specifies the number of times an NFS client attempts to reach an NFS server. The default value is 5.
ro | rw	Mounts the directory in read-only or in read-write mode. Default is rw. The ro option connects drives so that you can read, but cannot write, their files.

Option (Type)	Description
`rsize (INTEGER)`	Specifies the size (in bytes) of a data block read from a file during an NFS data transfer. A larger size increases NFS performance if the underlying network hardware can handle the larger size. The default read and write size is 32,768 bytes for TCP, and 8 kilobytes for UDP. **Example:** This example sets the read size to 1024 bytes. `rsize=1024`
`share=[yes, no]`	Specifies whether to use the built-in NFS capability to prevent others from changing files that you are modifying. The default is `no`. `share=yes` automatically sets lock. `share=no` automatically clears lock.
`trans [TCP|UDP]`	Specifies transport. Using the UDP transport speeds up network traffic by reducing packet overhead. TCP works better when high reliability of packet transmissions is a requirement. If not set, the NFS client tries TCP first and then UDP. **Example:** `trans=TCP` sets the transport to TCP.
`type`	This option is ignored
`umask`	Sets the file creation mask. **Example:** `umask=022`
`wsize`	Specifies the size (in bytes) of a data block written to a file during an NFS data transfer. A larger size increases NFS performance if the underlying network hardware can handle the larger size. The default read and write size is 32,768 bytes for TCP, and 8 kilobytes for UDP. **Example:** `wsize=8192`, sets the write size to 8192 bytes.

Example:

The following example mounts the directory `saturn:/usr` on drive U, read-only, with a read size of 8 Kbytes, and with at least 10 retries before failing an NFS operation.

```
MOUNT –o ro,rsize=8192,retries=10 DRIVE saturn:/usr U:
```

MOUNT PRINTER

Is parsed, but ignored.

PAUSE *number*

Suspends the processing for *number* seconds.

Example:

This example sets a pause of 5 seconds.

```
PAUSE 5
```

REG DELKEY *keypath*

Deletes the named Registry key, *keypath*. This directive fails if there are subkeys.

If *keypath* contains spaces, enclose them in quotes.

keypath is the full path to the key containing the value. You can abbreviate `HKEY_LOCAL_MACHINE` to `HKLM` and `HKEY_CURRENT_USER` to `HKCU`.

Example:

This example deletes the named Registry key.

```
REG DELKEY HKEY_CURRENT_USER\Software\Netscape\MyKey
```

REG DELVAL *keypath value_name*

Deletes the value *value_name* in the Registry key *keypath*.

If *keypath* or *value_name* contain spaces, enclose them in quotes.

keypath is the full path to the key containing the value. You can abbreviate `HKEY_LOCAL_MACHINE` to `HKLM` and `HKEY_CURRENT_USER` to `HKCU`.

Example:

This example deletes `Myval` in the named Registry key.

```
REG DELVAL HKEY_CURRENT_USER\Software\Netscape\MyKey MyVal
```

REG NEWKEY *keypath*

Creates a new Registry key at the path *keypath*.

If *keypath* contains spaces, enclose them in quotes.

keypath is the full path to the key containing the value. You can abbreviate HKEY_LOCAL_MACHINE to HKLM and HKEY_CURRENT_USER to HKCU.

Example:

This example creates a new Registry key called:
HKEY_CURRENT_USER\Software\Netscape\MyKey

```
REG NEWKEY HKEY_CURRENT_USER\Software\Netscape\MyKey
```

REG *type keypath value_name value*

Adds a new *value* called *value_name*, of the specified *type* in the Registry.

If *keypath* or *value_name* contain spaces, enclose them in quotes.

keypath is the full path to the key containing the value. You can abbreviate HKEY_LOCAL_MACHINE to HKLM and HKEY_CURRENT_USER to HKCU.

type can be BINARY, MULTI, STRING, WORD.

Type	Meaning
BINARY	Specifies a string of twin hexadecimal values. (Registry type REG_BINARY) **Example:** REG BINARY HKCU\Software\sunw\cc\1.0\sunwnfs Binary_test 7465737400
MULTI	Specifies a set of strings separated by spaces. (Registry type REG_MULTI_SZ) **Example:** REG MULTI HKEY_CURRENT_USER\Software\Netscape\MyKey Srtings “My telephone number is 1234567” adds the strings My, telephone, number, is, and 234567 to the value Strings.

Type	Meaning
STRING	Specifies a string. (Registry type REG_SZ) **Example:** REG STRING HKEY_CURRENT_USER\Software\Netscape\MyKey test Hello adds the string Hello to the value test.
WORD	Specifies a integer in decimal or hexadecimal format. (Registry type REG_DWORD) Note: When a decimal number is entered it will be converted to hexadecimal and stored. When read back it will be in hexadecimal format, and leading zeros will be added to look exactly as it does in the Registry. *Example of writing a decimal value:* REG WORD HKCU\software\netscape\MYKey MyValue 4294967295 SET errorcode=%SNERRORLEVEL% IF NOT "%ERRORCODE%" == 0 GOTO ERROR *Example of reading the same value:* SET REG readvalue=HKCU\software\netscape\MyKey MyValue NOTSET IF NOT ERRORLEVEL 0 GOTO ERROR2 ECHO Value read is "%READVALUE%"

REM *comment text*

Specifies a comment line.

Example:

This example adds the comment, “Set environment variable.”

```
REM Set environment variable.
```

RESERVE

Is parsed, but ignored.

SET [*value_source*] *varname=value_specifier*

Sets the environment variable named *varname* with the value obtained from *value_source* according to *value_specifier*.

value_source can be ABS, INI, NIS, REG, or STR.

Value Source	Meaning
ABS	Specifies the default, in which value_specifier is used directly as the value. **Example:** `SET ABS TEMP=C:\temp` sets the global variable `TEMP` to `C:\temp`.
`INI` *filename* *section key* *default_value*	Uses a `.INI` file as the source of the value with which to set the variable. The value has four space-separated fields: *filename* – The name of the `.INI` file from which to obtain the value. *section* – The section in the `.INI` file from which to obtain the value. *key* – The entry from which to obtain the value. *default_value* – The value to use if a value cannot be obtained from the `.INI` file. **Example:** `SET INI C:\windows\win.ini mysection mykey myvalue`

Value Source	Meaning

`NIS`
nis_map_name key
default_value
	Sets a variable with a value from an NIS map or NIS+ table. This command looks up values in either or both NIS and NIS+, depending on the configuration of the local machine. The name service lookup order is honored. If the system is not using NIS or NIS+, an error is returned.
	The value has three fields separated by spaces:
	nis_map_name – The name of the NIS map or NIS+ table from which to obtain the value. To facilitate backward compatibility, you should use NIS map names. If the client is using NIS+, the script interpreter automatically converts NIS to NIS+ syntax. Table names are converted according to the following rules:
	■ The first period in the name is converted to an underscore:
	`auto.home => auto_home`
	■ The string `org_dir` is appended:
	`passwd => passwd.org_dir`
	`auto.dot => auto_dat.org_dir`
	key – The value of the key in the map from which to obtain the value.
	default_value – The value to use if a value cannot be obtained from the NIS map or NIS+ table.
	Example:
	`SET NIS HOMEDIR=auto.home`
	`%SNUSER% %SN_SERVER%:/tmp`
	Looks up a value of `%SNUSER%` in the `auto.home` map, and assigns it to `HOMEDIR`.
	If NIS+ is enabled on the client, `auto.home` is converted to `auto_home.org_dir`.
	If the lookup fails, `HOMEDIR` is set to the default value, `%SNSERVER%:/tmp`.

Value Source	Meaning
REG *varname=keypath* *value default*	Sets a variable with a value from the system Registry. The value has three space-separated fields: *keypath* – Full path to the key containing the value. You can abbreviate HKEY_LOCAL_MACHINE to HKLM and HKEY_CURRENT_USER to HKCU. *value* – Name of the value. *default* – Value used if the key or value is not found. If *keypath* or *value_name* contain spaces, enclose them in quotes. The command retrieves values of type REG_SZ, REG_DWORD, REG_MULTI, and REG_BINARY of up to 200 bytes. REG_DWORD values are returned as hexadecimal values. **Example:** SET REG *variable*=''HKLM\SOFTWARE*application**key*'' value NOTSET
STR *variable=option* *values*	*value_specifier* is a *substring_specification string* record. This space-separated record therefore has 2 fields. The *substring_specification* has three possible values: #, *, and N, where N is an integer digit. The first specification (#) specifies that the variable's value is the count of space-separated tokens in the *string*. The second specification (*) specifies that the variable's value is the *string* less the first token. This is analogous to a SHIFT LEFT operation, with the first token being discarded. The last specification (0-N) specifies that the variable's value is the Nth token in the *string*, thus serving as an INDEX operation. **Example:** Set FIVE to the fifth item in %LIST%, and set NUM to the number of items. Set RESTLIST to %LIST% less the first token. SET STR FIVE=5 %LIST% SET STR NUM=# %LIST% SET STR RESTLIST=* %LIST%

STOP

This directive is parsed, but ignored.

UMASK *octal_tuple*

Changes the file creation mask for the current user.

If the UMASK directive is used, then the value supplied is used as the default umask for all drive mounts. If it is not supplied, the system-wide default is used.

The umask setting may be overwritten on a per-mount basis, using the umask option to the MOUNT command.

Example:

This example changes the umask to 022.

```
UMASK 022
```

UNMOUNT [DRIVE *drive*: | PRINTER *lpt_device*:]

Unmounts a network drive or printer.

Example:

This example unmounts the directory mounted on drive U.

```
UNMOUNT DRIVE U:
```

Environment Variables Local to SNC Scripts

The following table lists the environment variables set on Solstice Network Client computers.

These variables are available to the SNC scripts and are saved in HKCU\Software\SUNW\CC\1.0\sunwnfs\Environment.

Variable	Value
SNCLASSID	Not used.
SNCLIENTID	Not used.
SNDRIVE	Drive letter of the drive where the directory /opt/MSPolicy is mounted.
SNERRORLEVEL	The error level returned by any SNC script directive. You must capture this value in the next directive, or it will be lost (overwritten).

Variable	Value
SNGROUP	Current user's UNIX primary group name. Numeric versions of this variable are available for systems not running NIS or NIS+.
SNGROUPS	Current user's UNIX secondary group names. Numeric versions of this variable are available for systems not running NIS or NIS+.
SNHOME	Current user's home directory on the server.
SNHOSTIPADDR	The IP address of the client. The SNHOSTNAME variable is always set to the Computer Name in the Network Identification property page, while SNHOSTIPADDR is always set to the IP address assigned to the client computer, even when using DHCP.
SNHOSTNAME	Client machine name.
SN_SERVER	Server that authenticates the user at login.
SNUSER	Current user's UNIX login name.
SNVERSION	Version of script interpreter.

Index

A

access
  denied when mapping network drive, 55, 56
  granting to shared resources, 73
  restricting, 155
administration mode, 6, 8
aliases
  created when browsing, 29
  creating, 29, 55, 56
  for automount maps, 29
  for multilevel directories, 29, 30
  for UNC names, 28, 36
  limitations, 29
  problems, 55
archive attribute, setting, 50
asynchronous readahead, 49
attribute cache, enabling, 48
authentication
  group ID/user ID, 160
  PCNFSD program, 163, 160
authentication server
  broadcasting for, 24, 48
  client management from, 107
  configuring
    dial-up connection, 14, 18
    TCP/IP settings, 58
  failure to connect to, 23
  obtaining credentials from, 153
  /opt/MSPolicy directory, 107
  outsi, 57
  selecting, 3
  setting up system policy files, 115, 116
  specifying, 153
automated installation, 6, 8
automount maps
  about, 154
  aliases for, 29
  auto_home, 39
  auto_master, 40
  browsing, 39, 41
  example of, 40
  syntax used, 28
Automounter
  about, 39
  setting time-out, 49

B

binary files, carriage returns and line feeds, 101
broadcasting, for authentication servers, 48
browsin, 55
browsing
  automount maps, 39, 41
  netwo, 56
  network printers
    on Windows 95, 81
    on Windows NT, 82
  network servers
    naming convention, 28
    no NFS servers listed, 57
    on Windows 95, 35
    on Windows NT, 36
    to create aliases, 55
    troubleshooting, 25

WebNFS servers, 46

C

cache
attribute, 48
data, 48
directory name lookup, 49
filename, 49
PC-CacheFS
cache-hit rate, 150
capacity, monitoring, 151
configuring, 4, 145
deleting and restoring, 146
directory, 144
flushing, 146
case handling, for file names, 50
Compact setup, choosing during installation, 3
components, selecting for installation, 3
concurrent licenses, 4
CONFIG.POL file, 115
connection options, applying, 54
COPY command, 172
credentials
conflict message, 56
used for authentication, 160
Custom setup, choosing during installation, 3

D

daemons
inetd, 168
LPD, 79
PCNFSD, 78
rpc.pcnfsd, 161, 162
data cache, setting read/write size, 48
data transfer, setting read/write size, 47
DELETE command, 172
desktop settings, managing, 105
devices, sharing, 73
DHCP
configuring for Windows 95, 58
configuring for Windows NT, 59
dial-up connection
authentication server, configuring, 14, 18
creating, 13, 18
installing, 12
NFS server, adding/removing, 16
TCP/IP configuration, 14
to PPP server
on Windows 95, 13
on Windows NT, 17
directories
caching, 147
multilevel, aliases for, 29
sharing, 73
directory name lookup cache, 49
disk space, used by PC-CacheFS, 146
DNS
as Windows default name service, 5
configuring, 57
domain name for NIS/NIS+ name server
on Windows NT, 59
specifying, 5, 41
drives
cached by PC-CacheFS, 4
mounting, SNC directive for, 176
reconnected on login, 43
viewing shared drives, 68
dynamic host configuration protocol, , *see* DHCP,

E

ECHO command, 173
environment variables
exported to an application, 173
setting, SNC directive for, 181
table of, 185
/etc/pcnfsd.conf file, 169
EXIT command, 173
EXPORT command, 173
exported folders and drives, viewing on Windows NT, 68

F

file access
authorizing, 160
on NFS servers, 154
file handle, public, 44
file locking/sharing, enabling, 3
file names
aliasing, 28
case-sensitive lookup, 50

mapping long file names, 49
NFS conventions, 28
file permissions, setting, 47
file sharing
enabling on Windows 95, 63
enabling on Windows NT, 62
file systems
accessing with NFS, 27
mounting with SNC directive, 176
file time-out, 147
Files and Folders properties, 49
firewall, with WebNFS, 44, 52
folder creation semantics, 51
folders
sharing with NFS, 73
viewing shared folders, 68

G

GID, assigned to new files, 51
global properties, applied to connections, 53
group membership, 161
group policies
about, 116
creating on Windows 95, 119

H

Home automount map, 40
host name, of NIS/NIS+ server, 41
HOSTS file, 5

I

idle time-out, for Automounter, 49
INCLUDE command, 174
inetd daemon, 168
INI command, 174
installation
automating, 8
information required for, 2
silent, 7
installation directory
deleting, 10
selecting, 2
installation script, creating, 8
IP address
of DNS server, 59
of NIS/NIS+ name server, 41, 59
of remote computer, 24

L

LAUNCH command, 175
license server, designating, 4
licenses
concurrent, 4
evaluation, 2
logging
NFS Server events on Windows 95, 75
NFS Server events on Windows NT, 70
print events, 93
login
failure
cannot log in to network, 23
no Login dialog box, 56
time, 3
to Solstice network, 131
to Windows 95, 135
to Windows NT, 131
troubleshooting, 141
logon scripts
about, 106, 119
creating, 120
examples of, 120
LPD Print Server
about, 93
setting up, 94
starting, 96
stopping, 97
troubleshooting, 102
LPD printing
adding shared printer, 97
enabling print requests, 95
LPR printing
adding printer port on Windows NT, 85
print protocol syntax, 83, 85

M

management tools, 105, 106
mandatory user profiles, setting up, 113
mapping a network drive
access denied, 55, 56
conflicting credentials, 56
on Windows 95, 31, 33

on Windows NT, 34
using a UNC file name, 34
using WebNFS, 45
vs. browsing, 35
mapping character, specifying, 47
Master automount map, 40
MKDIR command, 175
MOUNT command, 176
mount options
changing server connections, 54
order applied to connections, 54
setting preferences, 47, 53
WebNFS, 52
mounting directories
on Windows 95, 29
on Windows NT, 30
mounting drives, SNC directive for, 176
mounting network printers
client setup requirements, 79
on a UNIX system, 86
on Windows 95, 83
on Windows NT, 84
using LPR print protocol, 85
using PCNFSD print protocol, 84
MPR
and UNC format, 30
naming convention used, 28
multi-component lookup, 44
multilevel directories
aliases for, 29
mapping, 30
multiple provider router, , *see* MPR,

N

name service, 5
configuring, 40
NIS, 5
NIS+, 5
selecting during installation, 5
Windows default, 5
naming conventions
network resource, 28
UNC vs. NFS, 28
net use command, 87
network drives
mapping on Windows 95, 31
mapping on Windows NT, 32
mapping vs. opening, 154
saving in user profiles, 43
Network Event Log
configuring on Windows 95, 75
configuring on Windows NT, 71
Network Neighborhood
browsing automount maps, 41
browsing network servers, 35
Network Provider, 154
network traffic, reducing with PC-CacheFS, 151
NFS automount maps, 41
NFS Client
browsing for NFS servers, 35
setting permissions, 47
troubleshooting, 55
with client for Microsoft Network, 153
NFS file names, 28
NFS port, specifying with Portmapper, 52
NFS retransmissions, setting, 49
NFS Server
about, 155
accessing, 27, 28
on Windows 95
configuring Network Event Log, 76
configuring properties, 73
disabling logging, 76
enabling logging, 75
sharing resources, 72, 73
stopping/starting, 73
on Windows NT
configuring Network Event Log, 71
configuring properties, 64
enabling file sharing, 64
enabling logging, 70
removing access, 67
sharing resources, 66
starting and stopping, 65
troubleshooting, 156
NFS servers
adding from outside local subnet, 37
adding/removing in serial configuration, 16
browsing, 35, 36
not listed while browsing, 57
NFS version
selecting, 51

with WebNFS, 44
NIS/NIS+ name service
adding during installation, 5
configuring, 40, 41, 59
viewing maps, 39
NTUSER.MAN, mandatory user profile name, 113

O

operating system, required for server installation, 159
/opt/MSPolicy directory, 3
options, configuring NFS properties, 46
/opt/MSPolicy directory, 107, 161

P

passwords
changing on UNIX system, 131
changing on Windows 95, 135
changing on Windows NT, 131
changing UNIX password on Windows NT, 134
login, 160
synchronizing on Windows 95, 136
synchronizing on Windows NT, 133
troubleshooting, 140
PC-CacheFS
about, 143, 158
cache statistics, 152
configuring during installation, 4
designating the cache drive, 4
monitor, 144, 151
relative performance, 151
starting, 144
time-out, 147
PCNFSD print protocol
on Windows 95, 83
on Windows NT, 84
PCNFSD program, 160
inetd daemon, 168
porting to non-Sun servers, 170
running on a single server, 163
versions of, 167
PCNFSD server
authentication, 153
setting up system policy files, 115, 116
permissions
setting for shared printers, 91
using authentication server, 3
policy files, 161
port
assigning for WebNFS, 44
specifying for NFS, 52
port number, for license server, 4
Portmapper, 52
PPP connection
adding/removing NFS server, 16, 17
on Windows 95, 13
on Windows NT, 17
to PPP server, 15, 19
preferred case, setting, 50
Primary Network Logon, specifying, 154
print clients, troubleshoot, 102
print jobs
viewing on PC, 88, 99
viewing on UNIX workstation, 88, 99
print log file, for LPD Print Server, 100
print queue, viewing, 99
print servers
adding to Windows NT, 90
browsing for, 81
LPD, 93
setup requirements for, 78
troubleshooting, 102
printer drivers, configuring for shared printers, 91
printer port
adding on Windows NT, 84, 85
deleting on Windows NT, 85
for DOS printing, 87, 88
printer protocols
on Windows 95, 83
on Windows NT, 84
specifying, 83
printers
access, 160
browsing
on Windows 95, 81
on Windows NT, 82

configuring
about, 83
for DOS printing, 87, 88
on Windows NT, 91
road map, 78
displaying print requests, 157
logging problems, 157
mounting
alias convention, 81
on UNIX, 86
on Windows 95, 83
on Windows NT, 84
setting permissions, 91
setup requirements
for print clients, 79
for print servers, 78
spooling, 160
troubleshooting, 102
viewing logged print events, 93
viewing queues, 161
printers, *see* printers, shared
setup requirements,
printers, shared
adding to PC work environment, 97
adding to UNIX environment, 98
configuring local printer, 91
on a UNIX workstation, 98
on Windows 95, 63
on Windows NT, 90
supported by PCNFSD server, 161
turning off printer, 101
using LPD Print Server, 93, 156
printing, from a DOS application, 87
privileges, on exported directories, 69
profile path, on Windows NT, 110
ProfileList Registry key
updating user profiles, 109
user profile on Windows 95, 109
Profiles folder, 108
profiles, for users, 161
public file handle, 44, 52

Q

queues, printer, 161

R

read size
for data transfer, 47
specified for PC-CacheFS, 147
readahead, asynchronous, 49
reconnected drives, user-specific, 43
REG DELKEY command, 179
REG DELVAL command, 179
REG NEWKEY command, 179
Registry key
adding or deleting, SNC directive for, 180
local user profile, 109
relative performance, with PC-CacheFS, 151
remote hosts
access requests from, 68
limiting access privileges, 69
requirements
for client installation, 1
for server installation, 159
roaming user profiles
about, 110
on Windows 95, 112
on Windows NT, 110
RPC services, 160
rpc.pcnfsd daemon
configuring, 169
overview, 160
installing, 162, 163
upgrading, 168
version 2, 167
rpcinfo command, 51

S

script interpreter, command syntax, 171
scripts, , *see* SNC scripts,
security
NFS Client Properties, 47
provided by authentication server, 160
with NFS Server, 69
with PC-CacheFS, 144
serial connection
information required for setup, 11
setting up together with LAN
connection, 17
troubleshooting, 23, 25
serial number, from license certificate, 2

servers, 1
accessing with NFS, 28
authentication, 3, 48, 153
browsing, 35
license, 4
mount options, 54
NIS / NIS+, 5
WebNFS, 44
SET command, 181
setgid command, 51
setup type, choosing, 3
shared resources
granting access, 66, 73
restricting access, 156
silent installation, creating, 7
SNC scripts
about, 107
launching executable from, 175
list of, 172
spool, printing with PCNFSD, 160
subnet mask, specifying, 59
sunwrun.exe command, 171
synchronized passwords
enabling on Windows NT, 133
on Windows 95, 136
system policies
about, 106, 114
and user profiles, 116
CONFIG.POL file, 115
creating
on Windows 95, 118
on Windows NT, 117
with system policy editor, 115
file naming, 115
rules for updating on Windows, 115
system policy editor, using, 117
system policy files
on Windows 95, 118
on Windows NT, 116

T

TCP / IP protocol
and WebNFS, 44
dial-up connection configuration, 14
troubleshooting, 56
Windows 95 configuration, 57
Windows NT configuration, 58
time-out
Automounter, 49
PC-CacheFS, 147
transport options, selecting, 51
troubleshooting
login, 138, 141
LPD Print Server, 102
NFS Client, 55
passwords, 138
printing problems, 102
serial connections, 22, 25
TCP / IP, 55
tuning preferences, setting, 49
Typical setup, choosing during installation, 3

U

Ultrix operating system, 160
UMASK command, 184
uninstalling Solstice NFS Client, 9
universal naming convention (UNC)
file name mapping, 28
syntax, 28
UNIX system
accessing servers, 155
adding shared PC printer, 98
changing password
on Windows 95, 138
on Windows NT, 132
mounting shared PC printer, 86
synchronizing passwords, 136
viewing print jobs, 99
viewing print status, 88
UNMOUNT command, 185
user account, creating on Windows NT, 110
user authentication, 160
user configuration, 105
user policies, 3
user profiles, 3
about, 106, 108
and drive mapping, 43
customizing, 43
for multiple user accounts, 110
mandatory
setting up on Windows 95, 113
setting up on Windows NT, 113
on PCNFSD server, 161

on Windows 95, 108
on Windows NT, 108
roaming
about, 110
setting up on Windows 95, 112
setting up on Windows NT, 110
user views, 3, 105, 161
user work environment, enabling, 3

W

WebNFS
about, 44
browsing for servers, 46
client, 44
mapping a drive, 45
mount option, 52
pathname syntax, 45
server, 44
Windows default name service, 5
work environments, 105
write size
for data transfer, 47
specified for PC-CacheFS, 147