Solaris™ PC NetLink 2.0 Administration Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 U.S.A.
650-960-1300

Part No. 816-0266-10
March 2002, Revision A

Send comments about this document to: docfeedback@sun.com

Please
Recycle

Contents

1. Introduction to Solaris PC NetLink Administration 1

What's New in PC NetLink Version 2.0 1

About Your New Server 2

About Your New Administration Role 3

Windows NT Administration Tools Overview for Experienced Solaris System Administrators 4

User Manager for Domains 5

Server Manager 6

Event Viewer 6

System Policy Editor 7

User Profile Editor 7

PC NetLink Server Manager or the Solaris Command Line: Your Choice 8

PC NetLink Server Manager 9

Command-Line Interface for All Tasks 12

2. PC NetLink Administration at the Solaris Command Line 13

About the Show Commands Feature 14

▼ How to Use the PC NetLink Server Manager Show Commands Feature 14

About PC NetLink Commands 16

About the `net` Command 18

Administering Local and Remote Physical Hosts 18

- How to Administer a Local PC NetLink Physical Host 19
- How to Administer a Remote PC NetLink Physical Host 19
- How to Use PC NetLink Commands on a Windows Client 21

PC NetLink Command Usage 21

Specifying a PC NetLink Virtual Server 21

Paging Through Screens 21

Using Passwords With Commands 22

Using Command Confirmation 22

Using Abbreviations 23

Using Special Characters With Commands 23

Typing Path Names With Solaris `net` Commands 24

Typing Path Names at Client Computers 24

Understanding Command Syntax 24

Getting Help on `net` Commands 25

PC NetLink `net` Command Options 26

About `lanman.ini` File Entries 28

File Syntax 29

- How to Change a `lanman.ini` File Parameter 30

File Parameters 30

3. Configuring and Managing PC NetLink Software 37

About Logon and Logoff 39

Windows NT and Solaris Root Logon Privileges 39

- How to Start PC NetLink Server Manager 40
- How to Add a Solaris Server to PC NetLink Server Manager 41
- How to Log On to a Solaris Server Using PC NetLink Server Manager 42
- How to Log On to a Solaris Server From the Command Line 44

▼ How to Log Off a Solaris Server Using PC NetLink Server Manager 45

▼ How to Log Off a Solaris Server From the Command Line 45

About Starting and Stopping Services 46

▼ How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager 46

▼ How to Stop a PC NetLink Virtual Server Using PC NetLink Server Manager 47

▼ How to Start a PC NetLink Virtual Server From the Command Line 49

▼ How to Stop a PC NetLink Virtual Server From the Command Line 49

▼ How to Schedule Virtual Server Restart, Stop, or Start 50

▼ How to Start Individual Services 56

▼ How to Stop Individual Services 58

▼ How to Configure Startup for Individual Services 60

About Domain Configuration and Management 62

Adding, Removing, Renaming, and Moving Servers Within a Domain 64

Creating a New PC NetLink Virtual Server 64

Adding a Domain Workstation or Server Computer 65

Removing a Computer From a Domain 65

Changing the Name of a Domain or Server 66

Moving a Computer to a Different Domain 66

▼ How to Create an IP Address for a PC NetLink Virtual Server 66

▼ How to Create a New PC NetLink Virtual Server 67

▼ How to Delete a PC NetLink Virtual Server 74

▼ How to Rename a PC NetLink Virtual Server 75

▼ How to Move a Virtual Server to Another Domain 80

▼ How to Promote a BDC Within Its Domain 89

▼ How to Change the Role of a Server Within Its Domain 91

▼ How to Create a Directory Share 95

▼ How to Modify a Directory Share 96

▼ How to Delete a Directory Share 97

About Managing Policies 98

About Managing Virtual Server Policies 98

Computer Browsing 98

File Name Mapping 99

File Name Mapping Rules 100

Considerations for Using Mixed-Case Support 100

Tuning PC NetLink Parameters for Optimum Performance 101

Processes and Virtual Circuits 101

Client Workload 102

Solaris File System Integration 102

Ownership of Files and Directories 105

Managing Access Control List (ACL) Data 106

UPS Power Failure Notification 107

User Accounts 107

Copying User Accounts Using PC NetLink Server Manager 108

▼ How to Change Computer Browsing Policy 109

▼ How to Set Up File Name Mapping 111

▼ How to Tune PC NetLink for Optimum Performance 112

▼ How to Set Solaris File System Integration Policies 114

▼ How to Use UPS Power Failure Notification 116

▼ How to Edit User Accounts Policies 118

▼ How to Map Existing User Accounts 120

▼ How to Copy User Accounts From Solaris to PC NetLink Using PC NetLink Server Manager 121

▼ How to Copy User Accounts From PC NetLink to Solaris Using PC NetLink Server Manager 128

User Account Management Utilities 134

▼ How to Use the `ldifmerge` Utility 137

About Managing General Policies 138

NetBIOS 138

WINS Servers 138

WINS and NetBIOS Nodes 139

WINS Proxy 139

LAN Adapter (Lana) Numbers 139

NetBIOS Scope 140

Solaris Name Resolution and Domain Name Service (DNS) 140

PC NetLink Server Manager Security 140

Performance Monitoring and Alarms 141

▼ How to Configure the Windows Internet Name Service (WINS) 141

▼ How to Start or Stop WINS Using PC NetLink Server Manager 144

▼ How to Start or Stop WINS From the Command Line 146

▼ How to Configure a LAN Adapter (Lana) Device 146

▼ How to Configure Solaris Name Services 149

▼ How to Configure PC NetLink Server Manager Security Policy 152

▼ How to Configure PC NetLink Server Performance Monitoring and Alarms 153

▼ How to Monitor Physical Host Performance 156

▼ How to Investigate Performance Alarms 162

About Event Monitoring 163

Interpreting an Event 164

Event Header 164

Event Description 164

Event Types 165

Additional Data 165

Using PC NetLink Server Manager to View Events 166

Using Event Logs to Troubleshoot Problems 167

Monitoring PC NetLink Security Events 167

- How to Monitor Events Using PC NetLink Server Manager 168
- How to Monitor Events From the Command Line 169
- How to View Solaris Physical Host Information 170
- How to View or Change PC NetLink Virtual Server Configuration Options 171
- How to Add a Computer Account to a Domain 173
- How to Delete a Domain Member 175

4. Guide to Password Synchronization 177

About Password Synchronization 177

Suitable Environments 180

Setting Up Password Synchronization 181

- Task 1a of 6 – How to Configure the Password Filter on a Solaris PDC 181
- Task 1b of 6 – How to Configure the Password Filter on a Native Windows NT PDC 183
- Task 2 of 6 – How to Install and Start the Name Server Agent 184
- Task 3 of 6 – How to Install and Configure the PAM Module for Each Solaris Client 185
- Task 4 of 6 – How to Configure the Password Daemon 186
- Task 5a of 6 – How to Enable Password Synchronization Using PC NetLink Server Manager 187
- Task 5b of 6 – How to Enable Password Synchronization Using the Command Line 188
- Task 6 of 6 – How to Initially Synchronize Account Passwords 188

Troubleshooting Password Synchronization 189

General Suggestions 189

Isolating the Problem 190

Is the Name Server Agent Running on the Correct Host? 190

Is the Correct Port Available? 190

Is the `NetlinkPwdSyncDaemon` Set to the Correct IP Address? 191

Is the PAM Module Installed on Each Solaris Client? 191

Have You Manually Synchronized the Passwords? 191

Unsupported Windows NT Password Features 192

5. Setting Up Printing Services 195

About PC NetLink Printing Services 195

PC NetLink Printing Terms 196

PC NetLink Network Printing 197

Setting Up PC NetLink Printing 197

- Task 1 of 3 – How to Install a Solaris Printer 198
- Task 2a of 3 – How to Use PC NetLink Server Manager to Set Up the Solaris Printer as a PC NetLink Shared Printer 206
- Task 2b of 3 – How to Use Network Neighborhood to Set Up the Solaris Printer as a PC NetLink Shared Printer 207
- Task 3 of 3 – How to Make the PC NetLink Printer Available to Microsoft Windows Clients 208
- How to Remove a PC NetLink Shared Printer 208
- How to Remove a Solaris Printer 208
- How to Change Solaris Printer Properties 211

6. Implementing WINS and Maintaining Databases 213

About WINS and Its Function 214

About Name Resolution Services 214

NetBIOS and DNS Computer Names 215

NetBIOS Over TCP/IP (NetBT) Name Resolution 216

B-Node (Broadcast Node) 217

H-Node (Hybrid Node) 217

Other Combinations 217
WINS and Broadcast Name Resolution 218
WINS in a Routed Environment 218
WINS Proxy 222
WINS and Dial-Up TCP/IP Networking Clients 223
About WINS Server Planning 223
Planning for WINS Client Network Traffic 224
WINS Client Traffic on Routed Networks 225
Daily Startup of WINS Clients 225
Roving User 225
Estimating WINS Client Traffic 226
Planning for WINS Server Replication Across Wide Area Networks 226
Planning for WINS Server Performance 227
Planning Replication Partners and Proxies 227
Configuring WINS Servers and WINS Client Behavior 228
Configuring Replication Partners 230
Managing Static NetBIOS-to-IP Address Mappings 231
Viewing WINS Server Status 235
Viewing the WINS Database 235
Advanced Configuration Parameters for WINS 236
Registry Parameters for WINS Servers 236
Registry Parameters for Replication Partners 237
About Database Management 239
Compacting the WINS Database 239
Backing Up and Restoring the WINS Database 239
Cleaning Up the Databases 240
Database Maintenance Tasks 240
▼ How to Clean Up PC NetLink Databases 240

▼ How to Back Up PC NetLink Databases 248

▼ How to Restore Backed-Up Databases 254

▼ How to Back Up the Complete Virtual Server Image 258

▼ How to Restore a Complete Virtual Server Image 265

▼ How to View, Modify, or Delete Scheduled Tasks 268

7. Troubleshooting 271

About PC NetLink Troubleshooting Tools 272

Diagnostics Wizard 272

▼ How to Access the Diagnostics Wizard 273

Other PC NetLink Diagnostic Tools 278

Event Logs 279

Server Status 279

Performance Monitoring 279

Server Information 279

Solaris Information 280

PC NetLink Information 280

Cumulative Statistics 280

▼ How to Display Session Information From a Microsoft Windows NT Computer 281

▼ How to Close Sessions From a Microsoft Windows NT Computer 282

▼ How to Close Open Resources From a Microsoft Windows Computer 282

Print Subsystem Event Logs 283

Tools Providing Automatic Status on the Server 283

Alerter Service 283

Solaris System and PC NetLink Features 284

Command-Line Diagnostics and Repair Tools 284

`acladm` 284

`blobadm` 285

`lmshell` 285

`lmstat` 285

`ping` 286

`regconfig` 286

`regcheck` 287

`samcheck` 287

`srvconfig` 287

Troubleshooting Procedures 288

Isolating the Problem 288

▼ How to Check the Network 289

Step 1: Verify the Status of the Physical Network 289

Step 2: Verify the Transport Protocol Status 290

Step 3: Verify the NetBIOS Protocol Status 290

Step 4: Verify Solaris System Functionality 290

Step 5: Isolate Problems on the PC NetLink System 291

▼ How to Troubleshoot a Shared Resource 295

▼ How to Solve Problems With Unknown File Systems 296

A. PC NetLink Registry 299

PC NetLink Registry Structure 299

Using Registry Editor 301

Connecting to a Remote Registry 301

Viewing the Registry 302

Registry Editor Commands 302

Registry Keys and Values 308

PC NetLink Key Descriptions 308

Alert Parameters Entries 309

File Service Parameters Entries 309

Net Administration Parameters Entries 316

Parameters Entries 316

Process Parameters Entries 318

RPC Parameters Entries 322

Share Parameters Entries 323

User Service Parameters Entries 324

Directory Synchronization Entries 326

Alerter Service Parameters Entries 327

Browser Service Parameters Entries 328

EventLog Service Parameters Entries 329

Net Logon Service Parameters Entries 330

Netrun Service Parameters Entries 332

Directory Replicator Service Parameters Entries 333

UPS Service Parameters Entries 335

Local Security Parameters Entries 336

Lanman Server Parameters Entries 337

B. Performing Common Windows NT Administrative Tasks 339

PC NetLink Server Manager "How to" Help 339

Common Windows NT Administrative Tasks 340

- How to Join a Domain as a BDC When the PDC Is on a Different Subnet 340

  If a WINS Server Exists 340

  If a WINS Server Does Not Exist 341

- How to Add `LMHOST` Functionality to a PC NetLink Server Running as a BDC 341

- How to Set Up Directory Replication Between Servers on Different Domains 342

  Configuring the Import Server 343

Configuring the Export Server 345

▼ How to Set Up Windows NT Alerts and Security Auditing 347

Setting Up Alerts 347

Saving Alerts 347

Using Saved Settings 348

Setting Up Security Auditing 348

Viewing the Security Log 348

Preface

This book describes how to use Solaris™ PC NetLink[1] 2.0 software. It is intended for administrators of Solaris and Windows NT networks.

Before You Read This Book

Before attempting to use PC NetLink software, you should be familiar with Windows NT and Solaris system administration. Refer to your Windows NT documentation for complete information on using Windows NT tools.

How This Book Is Organized

Chapter 1 provides an introduction to PC NetLink software.

Chapter 2 describes how to use PC NetLink commands.

Chapter 3 provides general information about, and instructions for, configuring and managing your PC NetLink software.

Chapter 5 tells you how to set up a PC NetLink virtual server as a print server, and offers background information that will help you keep printing tasks running smoothly.

Chapter 6 provides detailed information about the Windows Internet Name Service (WINS) that PC NetLink software incorporates, and considers important performance issues that can help you plan your network's implementation of WINS.

1. Solaris PC NetLink software incorporates AT&T's Advanced Server for UNIX Systems.

Chapter 7 describes how to troubleshoot PC NetLink virtual servers and the Solaris physical hosts on which they run.

Appendix A provides an overview of the PC NetLink Registry structure, a description of Registry Editor, and descriptions of the PC NetLink Registry keys and values.

Appendix B provides instructions for accomplishing many basic Windows NT/PC NetLink administrative tasks that are not covered elsewhere in this book.

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices.

See one or more of the following for this information:

- *Solaris Handbook for Sun Peripherals*
- AnswerBook2™ online documentation for the Solaris operating environment
- Other software documentation that you received with your system

Typographic Conventions

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

Shell Prompts

Shell	Prompt
C shell	*machine-name*%
C shell superuser	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Related Documentation

Sun™ Cluster, Solaris, and PC NetLink software work together to provide a high availability environment for both Solaris users and Microsoft Windows users. You will find the following publications relevant.

Publication Title	Part Number
Solaris PC NetLink 2.0 Installation Guide	816-0327-10
Solaris PC NetLink 2.0 High Availability Guide	816-0276-10
Solaris PC NetLink 2.0 Release Notes	816-0277-10
Sun Cluster 2.2 System Administration Guide	806-0266-10
Sun Cluster 2.2 Release Notes	806-5345-10
Sun Cluster 2.2 Hardware Site Preparation, Planning, and Installation Guide	806-5346-10
Sun Cluster 2.2 Software Installation Guide	806-5342-10

Accessing Sun Documentation Online

A broad selection of Sun system documentation is located at::

`http://www.sun.com/products-n-solutions/hardware/docs`

A complete set of Solaris documentation and many other titles are located at:

`http://docs.sun.com`

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

`http://www.fatbrain.com/documentation/sun`

Sun Welcomes Your Comments

We are interested in improving our documentation and welcome your comments and suggestions. You can email your comments to us at:

`docfeedback@sun.com`

Please include the part number (816-0266-10) of your document in the subject line of your email.

CHAPTER 1

Introduction to Solaris PC NetLink Administration

The Solaris PC NetLink product[1] that you have installed within your network will be at once new and familiar to you, the administrator. This guide will introduce you to the product and to your new role as PC NetLink program administrator.

If you are already experienced with a previous version of PC NetLink software, you will not need to read this chapter, other than the next section about new features.

What's New in PC NetLink Version 2.0

This release of PC NetLink software includes several major new features added since Version 1.2.

- The ability to run up to ten PC NetLink virtual servers on each Solaris physical host, which offers the following advantages:
  - Better reliability
  - Easier migration and consolidation from NT to Solaris
  - Better scalability when consolidating multiple NT servers on a Solaris host
  - More effective use of equipment when PC NetLink is used in a high availability (HA) cluster

  For information about creating a new virtual server, see "How to Create a New PC NetLink Virtual Server" on page 67.
- Improved Access Control List (ACL) database scalability. See "Managing Access Control List (ACL) Data" on page 106.
- Enhanced monitoring of PC NetLink virtual servers in a high availability (HA) cluster. See the *Solaris PC NetLink 2.0 High Availability Guide*.

1. Solaris PC NetLink software incorporates AT&T's Advanced Server for UNIX Systems.

- Enhanced password synchronization, enabling a single password change to affect a user's accounts both on Solaris and Windows NT systems. For information about setting up password synchronization, see Chapter 4. Also see "How to Edit User Accounts Policies" on page 118.
- Enhanced directory synchronization, using Lightweight Directory Access Protocol (LDAP), in addition to the type of directory synchronization used in PC NetLink Version 1.2. See "User Accounts" on page 107, "How to Copy User Accounts From Solaris to PC NetLink Using PC NetLink Server Manager" on page 121, and "How to Use the ldifmerge Utility" on page 137.
- The ability to automatically mount users' UNIX home directories. See "How to Set Solaris File System Integration Policies" on page 114.
- Support for Domain Name Service (DNS) in NetBIOS. See "Solaris Name Resolution and Domain Name Service (DNS)" on page 140, and "How to Configure Solaris Name Services" on page 149.
- The ability to store UNIX group IDs using DOS attributes. See "How to Set Solaris File System Integration Policies" on page 114.
- An improved PC NetLink Server Manager graphical user interface (GUI).

About Your New Server

PC NetLink software is a set of Solaris operating environment services that enable powerful, highly scalable, highly reliable Sun computers to perform vital local area network (LAN) tasks within a Microsoft Windows, Windows NT, Windows 2000, or mixed-client environment. PC NetLink software acts as a *virtual server* that runs on the Solaris *physical host*. Using PC NetLink Version 2.0, you can create up to ten virtual servers on a single Solaris physical host.

As a server within a LAN, a Solaris physical host with PC NetLink software installed can provide file, print, authentication, member server, and primary and backup domain controller (PDC and BDC) services that enable the efficient sharing of computing resources among desktop computer users. Incorporating Microsoft technology, a PC NetLink virtual server works like a native Windows NT server in environments that include systems running Windows 2000, Windows NT Server, Windows NT Workstation, and Windows 98.

PC NetLink software implements many of the services that are offered by Windows NT Server 4.0. Among these services are:

- Windows NT PDC, BDC, and member server functionality
- Windows Internet Name Service (WINS)
- Microsoft Remote Procedure Calls (RPCs)

- Windows NT Directory Services (NTDS), including NT LanManager (NTLM) challenge/response, Security Accounts Manager (SAM) database, and so forth
- Windows NT Registry
- Microsoft NT file system (NTFS)-compatible file Access Control Lists (ACLs)
- Event logging

In addition, PC NetLink software offers user account synchronization between NTDS and related Solaris services.

The additional benefits of Sun computers running the Solaris operating environment include true preemptive multitasking and symmetric multiprocessing. The time-sharing, multiuser model employed by the Solaris operating environment ensures file system integrity and continued server availability—even if a user's application crashes.

About Your New Administration Role

Although it incorporates networking technology from Microsoft, the foundation of PC NetLink software is the Solaris operating environment. A PC NetLink virtual server is not an emulation of a Windows NT server, but rather a distributor of true Windows NT file and print services implemented on the Solaris operating environment.

Once you have set up your PC NetLink virtual server on the network, users of Microsoft Windows-based client computers won't notice that their network services are being provided by a Solaris, rather than Windows NT, server. Their Microsoft Windows clients' views of the Windows NT network servers will merely include one or more new servers that seem the same as the others.

In your role as an administrator of your Windows NT network, you won't notice any differences, either. You will continue to use the same Windows NT tools to perform the same Windows NT network administrative tasks that you ordinarily perform. But the presence of the PC NetLink virtual server in your Windows NT network does mean that you have one additional role that is not the same as Windows NT administration: PC NetLink administration.

The difference between administration of the physical host running PC NetLink software on your network and the Windows NT network services *provided by* your PC NetLink virtual server is both critical and occasionally subtle.

For example, you can set up a native Windows NT server as a Windows Internet Name Service (WINS) database server that resolves client computers' NetBIOS names to their IP addresses. As a Windows NT administrator, you have probably set

up and administered services on one or more WINS servers. Likewise, you can set up the PC NetLink virtual server as a WINS server and administer its Windows NT network role in the same way that you administer the native Windows NT server.

But note the subtle difference between PC NetLink and Windows NT administrative duties for WINS:

- PC NetLink *administration* – Enabling a Solaris computer to act as a WINS server, backing up, restoring, and creating a schedule for backing up the WINS database on that server
- *Windows NT network administration* – Managing the WINS service, such as configuring replication partners, adding static entries, and so forth

To complete the PC NetLink WINS-related tasks, you would use PC NetLink Server Manager or the command-line utility, documented in the PC NetLink online help or in this guide. To complete the Windows NT WINS administrative task, you would use the same Windows NT administration tool that you have always used—WINS Manager—and you would follow instructions in the tool's online help or in your Windows NT network administration documentation.

Similar to the WINS server example, you will find new administrative duties that are closely related to, but importantly different from, many of your ordinary Windows NT administrative tasks. This guide covers all of them. Additionally, Appendix B, "Performing Common Windows NT Administrative Tasks" on page 339, provides instructions for accomplishing several Windows NT administrative tasks.

Windows NT Administration Tools Overview for Experienced Solaris System Administrators

You may be an experienced administrator of a Windows NT network; in that event, you are already familiar with Microsoft NT administration tools and you can skip this section and proceed to the section, "PC NetLink Server Manager or the Solaris Command Line: Your Choice" on page 8.

For administrators of a Solaris network, however, this section is a summary of the Windows NT administration tools that you use to carry out your Windows NT network responsibilities. Becoming familiar with the functions of these tools will help you discern the difference between a Windows NT network administrative task and a PC NetLink administrative task.

Nearly all Windows NT network administrative tasks are carried out by way of several graphical user interface (GUI) tools. You can operate and administer a PC NetLink virtual server regardless of whether Windows NT is running on the network. However, client-based network administration tools running on Windows

NT Workstation, Microsoft Windows 98, and Windows 2000 enable remote administration of the Windows NT services provided by a PC NetLink virtual server.

To perform Windows NT network administrative tasks on a PC NetLink server from a Microsoft Windows 98-based client computer, you install Windows NT Server Tools. Remote administration is supported for all network functions. Windows NT Server Tools are available in the PC NetLink installation package.

All of the GUI-based tools for Windows NT network administration feature online help.

The most important and most commonly used Windows NT administration tools, and the common administrative tasks associated with them, are described in the following sections. (Depending on which tools package you use and which Windows NT version you are running, you may not have access to one or more of the tools listed in the following sections.)

User Manager for Domains

Windows NT network client computer users gain access to network resources with a single logon and password, from any computer in their own "domain" or other "trusted" domain. No matter which computer they use, their own user environment can be established for them by the Windows NT server at logon through the use of "user profiles." (Similar—though not equivalent—information in the world of the Solaris system administrator is stored in the `/etc/passwd`, `/etc/groups`, `.profile`, and `.cshrc` files.) This environment and various other user attributes are maintained by way of the Windows NT *User Manager for Domains* tool.

You use User Manager for Domains for many common tasks, including:

- Managing passwords, including resetting forgotten passwords
- Setting up logon hours
- Setting account expiration dates
- Managing user accounts, including creating, deleting, altering, naming, and disabling accounts
- Creating and modifying a path to the user's profile
- Creating logon scripts for users and specifying their home directories
- Managing groups, including creating, deleting, and changing them and their membership
- Managing security policy, including number of failed logons permitted, users' and groups' rights, and audit policy
- Managing trust relationships among Windows NT domains

Server Manager

Windows NT network resources—file services and print services, for example—are allocated from the servers to the client computers as *shares*. These shares are given names, and accounted for by way of these names. You manage shares and other server-based resources by way of the *Server Manager* tool.

You use Server Manager for many common tasks, including:

- Setting and managing share permissions for users, viewing a computer's shares, adding new shares, and stopping sharing directories
- Checking who is connected to which server, for how long, and which resources they have open
- Configuring the Windows NT Directory Replicator service
- Sending and managing administrative alerts
- Managing domains and domain controllers
- Managing services

Event Viewer

An *event* is any significant occurrence in the system or in an application. Some critical events are noted in on-screen messages.

An event that does not require immediate attention is noted in an *event log*. Event logging starts automatically. With an event log and the Windows NT tool called *Event Viewer*, you can troubleshoot various hardware and software problems, and monitor Windows NT security events. You also can archive logs in various file formats.

You use Event Viewer for many common Windows NT administrative tasks. Among Event Viewer's features, it:

- Reports all errors and exceptions
- Displays event logs for security, systems, and applications
- Displays event descriptions and details
- Sorts events by timeframe
- Filters events, displaying only those with characteristics you specify
- Searches for events
- Provides Windows NT error codes

System Policy Editor

On computers running Windows NT Workstation or Windows NT Server, the contents of the user profile are taken from the user portion of the Windows NT Registry. Another part of the Registry, the local computer portion, contains configuration settings that you can manage along with user profiles.

Using the *System Policy Editor*, you can create a *system policy* to control user work environments and actions and to enforce system configuration for all computers running Windows NT Workstation and Windows NT Server.

With system policies, you can control some aspects of user work environments without enforcing the restrictions of a mandatory user profile. You can restrict what users can do from the desktop, such as which options in Control Panel they can use, and customize parts of the desktop or configure network settings.

User Profile Editor

On computers running Windows NT Workstation or Windows NT Server, *user profiles* automatically create and maintain the desktop settings for each user's work environment on the local computer. (Although you can save user profiles in shared network directories on PC NetLink virtual servers, user profiles have no effect on those particular computers—only on the clients served by them.)

You can create and modify user profiles using the *User Profile Editor* tool.

In Windows NT, Windows 98, and Windows 2000, a user profile is created for each user when the user logs on to a computer for the first time. User profiles provide the following advantages to users:

- When users log on to their workstations, they receive the desktop settings as they existed when they logged off.
- Several users can use the same computer, with each receiving a customized desktop when they log on.
- User profiles stored on a server enable the profiles to follow users to any computer running the Windows NT or PC NetLink software on the network. These are called *roaming* user profiles (see Appendix B, "Performing Common Windows NT Administrative Tasks" on page 339).

As an administration tool, user profiles provide the following options:

- You can create customized user profiles and assign them to users to provide consistent work environments that are appropriate to their tasks.
- You can specify common group settings for all users.
- You can assign mandatory user profiles to prevent users from changing any desktop settings.

Other Windows NT tools available to many administrators include *WINS Manager*, *Registry Editor* (Regedit32), *Disk Administrator*, and *Performance Monitor*. Detailed information about these and the previously described Windows NT tools, as well as instructions for using them, are included in the tools' online help and your Windows NT network documentation.

PC NetLink Server Manager or the Solaris Command Line: Your Choice

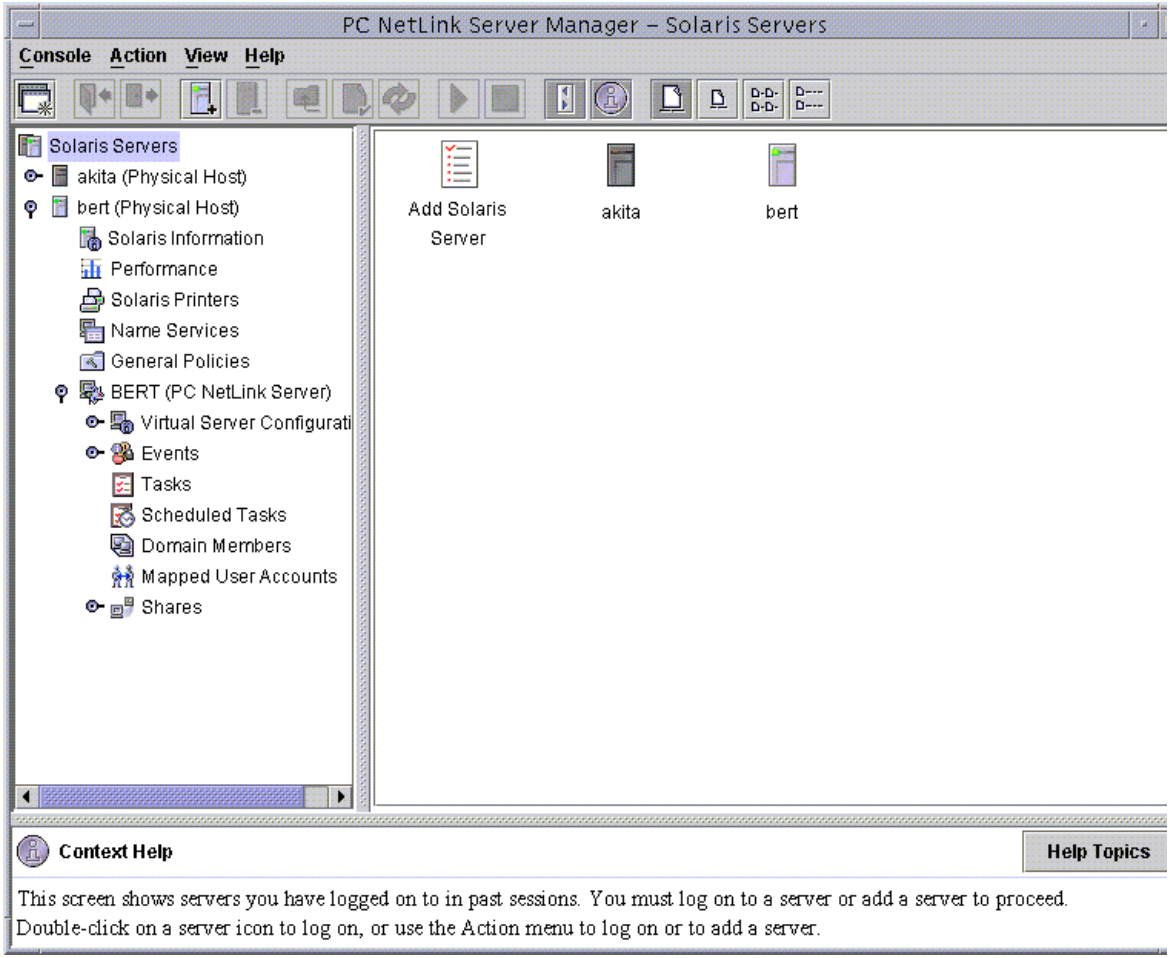
Aside from the administrative tasks that you routinely perform to keep your Windows NT or mixed-client network healthy—and for which you use the previously described Windows NT administration tools—you also need to perform some administrative tasks directly on your Solaris system-based physical host running PC NetLink software.

Suiting your background and preferences, PC NetLink administration provides a clear choice of methods: You can use a graphical user interface or the Solaris command line. This guide provides instructions on how to accomplish any administrative task on a PC NetLink virtual server by either method.

Note – Make sure that only one administrator at a time is making changes to any particular virtual server. Neither the command-line interface nor the PC NetLink Server Manager tool will preclude two or more administrators from simultaneously making changes—though the PC NetLink Server Manager tool will warn you if someone else with administrator privileges is logged on to a particular server.

PC NetLink Server Manager

Fitting comfortably within a Windows NT and Microsoft Windows environment, in which most routine and complex tasks are accomplished by way of graphical tools, is the PC NetLink administration tool, PC NetLink Server Manager, shown in the next figure.



You can manage all major aspects of PC NetLink administration, which is distinct from Windows NT network administration, by way of PC NetLink Server Manager—a distributed client-server application based on the Java™ programming language from Sun Microsystems. You install the server portion of PC NetLink Server Manager on the PC NetLink physical host, and the client portion on a Solaris (shown), Windows NT 4.0, Windows 98, or Windows 2000 client. (If you run PC

NetLink Server Manager on a Solaris machine, do so *locally*. Running the tool on a Solaris machine *remotely* may degrade interactive performance and result in less than optimal display.)

You can use PC NetLink Server Manager Version 2.0 to manage PC NetLink servers running PC NetLink Version 1.2, but features that are new in Version 2.0 will not be available. When you are connected to a physical host that is running PC NetLink Version 1.2, unavailable functions do not appear in the graphical user interface.

You cannot use PC NetLink Server Manager Version 1.2 to manage PC NetLink servers running PC NetLink Version 2.0.

Note – You cannot use the 2.0 version of PC NetLink Server Manager to administer servers that are running versions of PC NetLink software prior to Version 1.2. If you intend to keep a version of PC NetLink software prior to Version 1.2 on any physical host, then you must also keep the matching version of PC NetLink Server Manager—called "SunLink Server Manager" in Versions 1.0 and 1.1—on the network to administer it. Note also that you cannot use previous versions of PC NetLink Server Manager for PC NetLink 2.0 administrative tasks.

Among the most common and most important administrative tasks and concerns for which PC NetLink Server Manager is useful:

- *Logon and logoff* – To administer a PC NetLink virtual server from a remote client, you must have special user permissions on the physical host (which are known as *root* in the Solaris and UNIX world). PC NetLink Server Manager enables you to do this.
- *Virtual server startup and shutdown* – PC NetLink software includes a set of Solaris server processes that enables the virtual server to act as a Windows NT network server. PC NetLink Server Manager alerts you when you are attempting a task that requires shutdown of the PC NetLink virtual server, informs you about whether the server is running, and enables you to start and stop the virtual server without having to invoke any special Solaris commands. PC NetLink Server Manager also warns you when shutting down a virtual server might have unwanted consequences for other virtual servers running on the same physical host.
- *Domain configuration* – PC NetLink Server Manager covers most PC NetLink domain configuration tasks, including naming the virtual server and the domain, and specifying it as a PDC, BDC, or member server. You can also use the Windows NT Server Manager for PC NetLink configuration tasks.
- *Policy configuration* – PC NetLink Server Manager enables you to change various server policy parameters that are special to the PC NetLink virtual server, and provides context to help you understand the ramifications of policy changes that you put into effect.

- *Event management* – PC NetLink Server Manager's Events view, much like the Windows NT Event Viewer tool, enables you to check a variety of events related to PC NetLink operations.
- *Database management* – PC NetLink Server Manager enables you to manage and maintain the integrity of various Windows NT-related databases that are stored on your PC NetLink physical host—backing up and restoring them, for example. (Altering the content of these databases is a Windows NT administrative function, and not a PC NetLink administrative function.) Among the databases that you can clean up, back up, and restore with PC NetLink Server Manager are the ACL, the Registry, the SAM, and WINS.
- *NetBIOS* – Using PC NetLink Server Manager, you can set NetBIOS policies, including configuring the service as a WINS proxy.
- *Printing* – PC NetLink Server Manager includes a wizard that enables you to set up a Solaris printer, the first step toward setting up print services on a PC NetLink network.
- *Performance monitoring* – PC NetLink Server Manager includes a detailed graphical display of statistics related to the performance of the Solaris physical host that is running PC NetLink software.
- *Performance tuning* – PC NetLink Server Manager includes a tool that helps you manipulate various system settings and defaults to tune memory and speed for optimum performance.
- *Diagnostics* – A Diagnostics wizard automatically performs system tests to help you determine the cause of any problems you may encounter, and provides detailed information on how to resolve or work around the problem.
- *Copying user accounts* – PC NetLink enables copying PC NetLink user accounts to Solaris accounts, and copying Solaris user accounts to PC NetLink user accounts.
- *Backup* – A new Backup wizard enables you to back up and restore either the complete server image, or one or more databases only.
- *Virtual server creation and deletion* – You can create up to ten virtual servers on each Solaris physical host.
- *Printer and directory share management* – You can use PC NetLink software to manage Windows NT printer and directory shares.
- *Domain account management* – You can use PC NetLink software to manage domain accounts.
- *Mapping user accounts* – You can use PC NetLink software to map UNIX user accounts to Windows user accounts for specific users.
- *Online Help* – Detailed instructions for all tasks covered by PC NetLink Server Manager are available online.

Command-Line Interface for All Tasks

If you are an experienced administrator of Solaris systems or any other UNIX system, you already know the power of the command line. From the Solaris system superuser (root) prompt, you can type any number of commands to perform every administrative duty.

All of the traditional Solaris commands, and some new ones (including the Windows NT `net` commands), are available to you. For a rundown of the commands that are most relevant to PC NetLink administration, see Chapter 2, "PC NetLink Administration at the Solaris Command Line" on page 13. That chapter also provides general explanations of the use of Solaris commands to administrators whose Solaris experience is limited.

CHAPTER 2

PC NetLink Administration at the Solaris Command Line

This chapter describes how you can use PC NetLink commands, the `net` commands, and `lanman.ini` file editing to administer your PC NetLink virtual server at the Solaris physical host's root command prompt. It contains the following information:

- *PC NetLink commands* – This section describes the Solaris system commands that you can use to administer your PC NetLink virtual server at the physical host command prompt. (PC NetLink commands are installed in the `/opt/lanman/bin` and `/opt/lanman/sbin` directories.)
- `net` *command* – This section lists the `net` commands that are available to administer your PC NetLink virtual server at the physical host command prompt.
- `lanman.ini` *file* – This section is a table of values in the `lanman.ini` file that you can change by editing the file. Note that editing the vital `lanman.ini` file is a task for experienced administrators only.

Not covered in this chapter is information about the PC NetLink *Registry,* which plays a vital role in PC NetLink administration. The Registry is covered in Appendix A, "PC NetLink Registry" on page 299.

This chapter assumes that you have already installed and configured PC NetLink software on a Solaris physical host and installed PC NetLink Server Manager on a Solaris client, and that an Administrator account and password are available for your use.

Note – For the purposes of this Solaris system-centric chapter, the Microsoft Windows and Windows NT term "log on" is replaced with the Solaris term, "log in."

Instructions are included in this chapter for accomplishing the following tasks:

- "How to Use the PC NetLink Server Manager Show Commands Feature" on page 14
- "How to Administer a Local PC NetLink Physical Host" on page 19
- "How to Administer a Remote PC NetLink Physical Host" on page 19
- "How to Use PC NetLink Commands on a Windows Client" on page 21
- "How to Change a lanman.ini File Parameter" on page 30

Note – When a physical host has more than one PC NetLink virtual server configured, you must set the variable `PCNL_INSTANCE` before issuing a command to configure a specific virtual server, or use the `-I` *number* option with the command, where *number* is the instance number of the virtual server. (For `net` commands, use `/I:`*number*). If you do not, the command will fail.

About the Show Commands Feature

The PC NetLink graphical user interface tool for administration, PC NetLink Server Manager, includes a feature that is especially useful for administrators who use the command line. The *Show Commands* feature outputs the Bourne shell commands PC NetLink Server Manager invokes in the background while carrying out its tasks, and offers brief explanations about them. You can use the Show Commands feature as "training wheels" to become accustomed to PC NetLink commands, and you can easily copy the commands and paste them into the Solaris physical host command line or into script files.

▼ How to Use the PC NetLink Server Manager Show Commands Feature

1. **Start PC NetLink Server Manager on a Solaris client by typing the following command at the PC NetLink physical host command line:**

   ```
   /opt/lanman/sbin/slsmgr &
   ```

   (You can also use the Show Commands feature when using PC NetLink Server Manager on a client running the Microsoft Windows operating environment, but the command output is only useful at the Solaris command prompt.)

2. **If you have *not* already added a Solaris server to PC NetLink Server Manager, continue with Step 3; if you *have* added a server, skip the next step and continue with Step 4.**

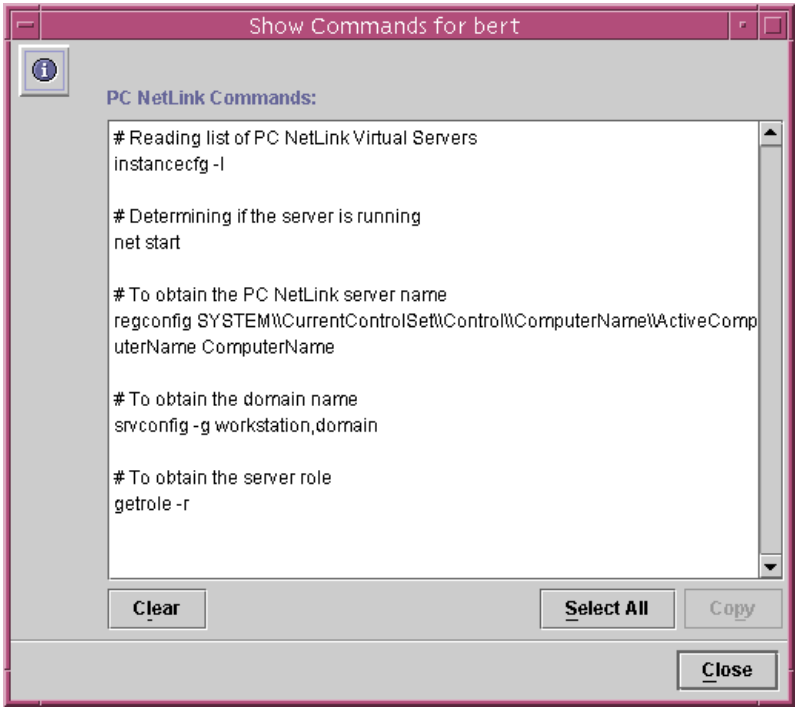
3. **Using the instructions in the section, "How to Add a Solaris Server to PC NetLink Server Manager" on page 41, add a Solaris server to the interface.**

   After adding a Solaris server, skip the next step and continue to Step 5.

4. **Using the instructions in the section, "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42, log on to the server.**

5. **Click the icon for a Solaris server (physical host), or one of its associated items, and choose Show Commands from the View menu.**

   A screen similar to the following appears.



Among the commands in the example above are those invoked by PC NetLink Server Manager to complete the foregoing task.

About PC NetLink Commands

You can use Solaris system commands at the physical host superuser command prompt to perform many administrative tasks.

Note – The commands listed in this chapter have not been translated into languages other than English.

TABLE 2-1 lists the Solaris system commands that you can use. For complete descriptions, syntax, and examples of the commands, consult the PC NetLink man pages. Make sure that your `MANPATH` variable is set as follows:

```
$MANPATH:/opt/lanman/man:/opt/SUNWlznb/man
```

With this variable set, you can find complete descriptions of each command by typing the following at the PC NetLink command prompt:

`man` *name-of-command*

TABLE 2-1 Solaris Commands for PC NetLink Administration

PC NetLink Command	Description
`acladm`	Creates, checks, prunes, fixes, and removes Access Control List (ACL) data.
`blobadm`	Displays statistical information, checks, and configures well-known or specified binary large object (BLOB) files.
`chacl`	Changes access control entry associated with the specified object(s).
`delshmem`	Deletes PC NetLink shared memory.
`elfread`	Displays event logs on the local PC NetLink server at the Solaris system console.
`euctosjis`	Converts the coding of characters from Extended UNIX Code (EUC) to Shift-JIS (S-JIS) encoding.
`getrole`	Displays the name of the local system's domain, its role within the domain, and the PDC of the domain.
`instancecfg`	Creates, lists, or deletes virtual server instances.
`joindomain`	Moves a PC NetLink server from one domain to another.
`ldif2sam`	Adds or deletes Solaris user accounts stored in an LDAP name service into or from the PC NetLink Security Accounts Manager (SAM) database.

TABLE 2-1 Solaris Commands for PC NetLink Administration *(Continued)*

PC NetLink Command	Description
`lmat`	Schedules commands or programs to run on a server at a specified time or date. (Note that the Solaris system `at` command also exists.)
`lmshare`	Manipulates a PC NetLink share file without server intervention.
`lmshell`	Provides the "look and feel" of an MS-DOS shell at the PC NetLink command prompt. Allows users to log in and link to other servers on the network, and to run a subset of DOS commands.
`lmstat`	Displays statistical information retrieved from the PC NetLink server's shared memory.
`lsacl`	Displays access control information associated with the specified object(s)/enumeration. The output of `lsacl` consists of two sections: the comments section and the ACL entries section.
`mapuname`	Maps and unmaps PC NetLink user names to and from Solaris system user names.
`nbdnsconfig`	Configures Domain Name Service (DNS) support.
`netevent`	Sends administrative or user alerts.
`passwd2sam`	Adds Solaris user accounts stored in a Solaris name service (FILES, NIS, NIS+) into the PC NetLink SAM database.
`promote`	Promotes a BDC to a PDC, and (with the `-d` flag) demotes a PDC to a BDC.
`pschkey`	Used to set the password used by the password daemon. This password must be the same for the password filter and the name server agent.
`pwdsync`	Used to report the password synchornization status of a given mapped account.
`regcheck`	Manipulates the PC NetLink Registry to enumerate Registry keys, to dump the contents of the Registry, or to check and repair Registry files.
`regconfig`	Queries or sets PC NetLink Registry key information.
`regload`	Creates a Registry file if one does not exist. Also reinitializes the Registry to system defaults.
`rmacl`	Deletes one or more entries from the ACL.
`sam2ldif`	Creates a `passwd` file containing PC NetLink user accounts to add into an LDAP name service.
`sam2passwd`	Creates a `passwd` file containing PC NetLink user accounts to add into a Solaris name service (FILES, NIS, NIS+).
`samcheck`	Checks or fixes the SAM database, or dumps the change log, built-in, account, or Local Security Authority (LSA) databases.

TABLE 2-1 Solaris Commands for PC NetLink Administration *(Continued)*

PC NetLink Command	Description
`setdomainname`	Changes the domain name of the local PC NetLink server.
`setservername`	Changes the name of the local PC NetLink server.
`sjistoeuc`	Converts the coding of characters from Shift-JIS (S-JIS) to Extended UNIX Code (EUC) encoding.
`srvconfig`	Displays or modifies PC NetLink configuration information stored in the `lanman.ini` file.
`winsadm`	Backs up, restores, compacts, or dumps the Windows Internet Name Service (WINS) database.
`winsconf`	Configures which WINS server PC NetLink will use.

About the `net` Command

You can perform many PC NetLink administrative tasks by using the `net` commands at the physical host's Solaris superuser command prompt. See TABLE 2-3 on page 26 for complete descriptions of the `net` commands. You should add the following to your `PATH`: `/opt/lanman/bin` and `/opt/lanman/sbin`.

The following sections summarize the `net` commands that are available from the Solaris root prompt, and describe syntax and usage conventions.

Administering Local and Remote Physical Hosts

When you administer a physical host while you are working at that server's command prompt, that server is called the *local* physical host. If you are administering a physical host from the command prompt of another server, the server being administered is called the *remote* physical host.

Some of your network client computer users may be designated as *account operators*, *print operators*, or *server operators*. These users have limited administrative or operator privileges that enable them to perform specific tasks. These privileges are sufficient to use the `net` command to administer a local server at the PC NetLink command prompt.

However, to use the `net` command to administer a *remote* PC NetLink physical host, you must be logged in to the remote host as an administrator with full administrative privileges. If you have different operators responsible for parts of your network and you do not want to assign them full administrative privileges, then they must log on to a physical host before administering it.

▼ How to Administer a Local PC NetLink Physical Host

To administer a local PC NetLink physical host using the `net` command:

1. **Log in as superuser to the Solaris physical host that is running the PC NetLink software.**
2. **At the Solaris system prompt, log in to the network:**

   `net logon` *username password*

   You need to log in to an account that has administrative privileges.
3. **Type the appropriate `net` command.**

   See a complete listing of `net` command options in the section, "PC NetLink net Command Options" on page 26.

Note – Remember to log off when you are finished administering the PC NetLink physical host by entering the `net logoff` command.

▼ How to Administer a Remote PC NetLink Physical Host

To perform server administrative tasks using the `net` command remotely, use the `net admin` command and the appropriate `net` command for the task. (Note that Step 3 of the following procedure describes two ways of entering the `net admin` command.)

To enter a `net` command remotely:

1. **Log in as superuser to the Solaris physical host that is running the PC NetLink software.**

2. **At the Solaris system prompt, log in to the network as Windows NT administrator or as a user with Windows NT administrative privileges by typing the following command:**

   `net logon` *username password*

   Operator privileges are not sufficient to perform this procedure.

3. **Type the `net admin` command using one of the following methods:**

   - Type a separate `net admin` command for each `net` command you want to execute. For example, to display statistics for a server named `account`, type the following:

     ```
     net admin \\account /command net statistics server
     ```

     This method is useful for batch files.

   - Type a `net admin` command followed by multiple `net` commands. For example, to execute multiple `net` commands on a Windows NT server or PC NetLink virtual server named `payroll`, type the following:

     ```
     net admin \\payroll /command
     ```

     This creates an *administrative command shell* from which you subsequently can issue `net` commands. The prompt changes to include the name of the Windows NT server or PC NetLink virtual server you are remotely administering; for example, `\\payroll`.

     Any `net` command that you type at this prompt is executed on the server that you specify. For example, at the prompt, type:

     ```
     [\\payroll] net share

     [\\payroll] net print
     ```

     where `\\payroll` is the prompt, and `net share` and `net print` are the commands.

4. **To exit the command shell and return to the system prompt, type `exit` or press CTRL+D.**

Note – You can use `net` commands that take a domain or computer name as an option for administering remote servers. This type of administration can be performed directly at the Solaris system command prompt without using the `net admin` command. For example, to display local groups on a remote domain named `market_dom`, you would type: `net localgroup /domain:market_dom`

▼ How to Use PC NetLink Commands on a Windows Client

1. **From the Start menu, choose Run.**
2. **Type the following:**

   `telnet` *pc-netlink-servername*

   where *pc-netlink-servername* is the actual host name of the PC NetLink physical host. For example, if you want to run PC NetLink commands from a Windows client PC and you have a PC NetLink physical host named "godot," you would type:

   ```
   telnet godot
   ```

3. **Using the telnet window that appears, follow the steps in "How to Administer a Remote PC NetLink Physical Host" on page 19.**

PC NetLink Command Usage

The following sections provide additional information about using PC NetLink commands at the server command prompt.

Specifying a PC NetLink Virtual Server

When a physical host has more than one PC NetLink virtual server configured, you must set the variable `PCNL_INSTANCE` before issuing a command to configure a specific virtual server, or use the `-I` *number* option with the command, where *number* is the instance number of the virtual server. (For `net` commands, use `/I:`*number*.) If you do not, the command will fail.

Paging Through Screens

Some displays provide more than one screen full of information. For example, the following command provides several screens of information on the `net share` command:

```
net help share /options
```

To display information one screen at a time, use the `more` command; for example:

```
net help share /options | more
```

After you have examined one screen of information and are ready to proceed, press the Spacebar to display the next screen of text.

Using Passwords With Commands

Some commands require a password as an option. You can provide a password as a command option by typing the password on the same line as the command itself. For example, to log on to the network with the user name `jim` and the password `kahuna`, you would type:

```
net logon jim kahuna
```

If you don't supply either the user name, the password, or both when you log on, the PC NetLink server will prompt you for the information.

For example, assume that you wanted to use the same resource described above, and typed only the user name:

```
net logon jim
```

The system then displays the following message:

```
Type your password:
```

When you enter a password at this prompt, the password does not appear on the screen as you type. This allows you to keep your password confidential, providing added security.

If you forget to type a password with a command that requires one, the system prompts you for it. Depending on the command that you type, the system may also prompt you for other pertinent information, such as your user name.

Using Command Confirmation

Some `net` commands require confirmation. The `/yes` and `/no` options help expedite `net` commands. When PC NetLink software reads one of these options, it does not pause to display the corresponding prompt. Instead, it accepts the `/yes` or `/no` option as your response to the prompt.

You can use `net` commands with `/yes` (`/y`) and `/no` (`/n`) options to create batch files and shell scripts that are not interrupted by PC NetLink prompts.

For example, if you use the `net logoff` command to log off the local area network with connections to remote shared resources intact, PC NetLink software displays a prompt similar to the following:

```
You have the following remote connections:

LPT1

Continuing will cancel the connections.

Do you want to continue this operation? (Y/N)  [Y]:
```

You can use the /yes and /no options with any net command to anticipate and respond to a prompt.

Using Abbreviations

The command reference pages in this chapter always use the full command names, command options, and service names. However, PC NetLink software recognizes abbreviations.

You can abbreviate any command option by typing enough letters to distinguish it from other command options. For example, the following is the syntax for the net accounts command:

net accounts [/forcelogoff:{*minutes*|no }] [/minpwlen:*length*] [/maxpwage:{*days*|unlimited}][/minpwage:*days*] [/uniquepw:*number*]

You can abbreviate the options, as illustrated in the following example:

```
net accounts /f:10 /minpwl:6 /ma:unlimited /minpwa:7 /u:3
```

You cannot abbreviate option values (for example, the unlimited option value for /maxpwage).

Using Special Characters With Commands

Some of the names or passwords that you need to enter may contain one or more special characters; for example, an ampersand (&). When you are at the Solaris system command prompt typing a name with a special character in a PC NetLink command, you must use an escape character (the backward slash [\ ]) before each special character. If you are at a client computer, you can surround the string containing the special characters in double quotation marks.

For example, to log in with the user name marksp and the password mrkt&dev from the system command prompt, you would type the following:

```
net logon marksp mrkt\&dev
```

Some commonly used Solaris system special characters include the following: asterisk (*); semicolon (;); pipe (|); square brackets ([ ]); parentheses [( )]; question mark (?); ampersand (&); caret (^); backward slash (\); greater-than and less-than signs (< >); blank ( ) and the “at” sign (@).

There are other Solaris special characters that you may encounter. For more information on special characters, consult your Solaris system documentation.

Typing Path Names With Solaris `net` Commands

The Solaris operating system uses a forward slash to separate names in a path. This is different from client computers running the Windows 98, Windows 2000, and Windows NT operating environments, which use backward slashes. Note, however, that the great majority of commands *will work* with either forward or backward slashes.

When typing path names at a Solaris system command prompt, you can use any of the following methods:

- *Single forward slashes* – Separate each element of the path with single forward slashes, like this:

  ```
  net share tmpshare=c:/tmp /us:10 /r:"Share for temporary use"
  ```

- *Double backward slashes* – Separate each element of the path with double backward slashes, like this:

  ```
  net share tmpshare=c:\\tmp /us:10 /r:"Share for temporary
  use"
  ```

- *Single quotation marks* – Separate each element of the path with a single backward slash and surround the whole path in single quotation marks, like this:

  ```
  net share 'tmpshare=c:\tmp' /r:"Share for temporary use"
  ```

  When including spaces in values, you may want to enclose the value in double quotation marks. For example, to change the comment for the `domain guests` group, you would type the following command:

  ```
  net group "domain guests" /comment: "All domain guests"
  ```

Typing Path Names at Client Computers

Client computers running the Windows 98, Windows 2000, and Windows NT operating environments use backward slashes to separate names in paths. For example:

```
net use f: \\product\data
```

Understanding Command Syntax

Directions in man pages for using PC NetLink commands are easier to understand and use if you keep the following concepts in mind:

- When an option is enclosed in braces ({}), the option is a required item in the syntax statement. For example, {yes|no} indicates that you must specify yes or no when using the command.
- When an option is enclosed in brackets ([ ]), it is an optional item in the syntax statement. For example, [*password*] indicates that a password may be used with the command, if desired.
- When a vertical bar (|) separates items within braces or brackets, only one of the options must be used. For example, {/hold | /release | /delete} indicates that only one of the three options must be used.
- When an ellipsis (...) appears in a syntax statement, it indicates that you can repeat the previous item(s). For example, /route: *devicename* [, ...] indicates that you can specify more than one device, putting a comma between the device names.
- Be sure to type forward slashes (/), backward slashes (\), commas (,), double quotation marks (" "), equal signs (=), colons (:), semicolons (;), and asterisks (*) as they are shown.
- Replace the pound sign (#) with a number.
- When you finish typing a command, press Enter (or Return). If you are typing a long command string, do not press Enter when your cursor gets to the edge of your screen; the cursor will "wrap around" and continue on the next line of your screen. Press Enter only after you finish typing the entire command string.

Getting Help on net Commands

Online help is available for all of the net commands that you can enter at the server command prompt. It provides command parameters, syntax, details about a command, and examples of the command in use. To obtain information about a net command option, type one of the following commands at the root prompt.

TABLE 2-2 Help on net Commands

Command	Description
net help	Names of available net commands.
net help *command*	Description, syntax, and options of the net command you selected.
net *command* /help	Description, syntax, and options of the net command you selected.
net help *command* /options	Detailed description of the options of the net command you selected.

PC NetLink `net` Command Options

The following table includes descriptions of the PC NetLink `net` command options that are available at the Solaris server command prompt.

TABLE 2-3 PC NetLink `net` Command Options

Command	Description
`net access`	Displays or modifies resource permissions on servers. Use this command only for displaying and modifying permissions on pipes and printer queues. Use `net perms` for managing permissions on all other types of resources.
`net accounts`	Displays the role of servers in a domain and displays or modifies password and login user requirements.
`net admin`	Runs a PC NetLink command or starts a command processor on a remote server. Usage note: In a situation in which a trust relationship does not exist between two domains, the logon (and user) authentication is done by the *remote* server for all the operations you perform on the remote server. For this reason, you must specify the remote server's administrator password when you use the `net admin` command to connect to it. However, once you have established a trust between the two domains, then the *trusted* domain is responsible for the logon and user authentication on behalf of the trusting domain. Thus, to set up a connection from the console of a trusted domain server to a trusting domain server, the logon password you use should be of the *local* domain administrator rather than that of the remote domain administrator. (You can ignore the password field if you have logged on to the local domain.)
`net auditing`	Displays and modifies the auditing settings of a resource.
`net browser`	Displays the list of domains that are visible from a local server or the list of computers that are active in a domain.
`net computer`	Displays or modifies the list of computer accounts in a domain. You can also type this command as: `net computers.`
`net config`	Displays the controllable services that are running.
`net config server`	Displays or changes settings for the server service while it is running.
`net continue`	Reactivates suspended services when typed at a server, and reactivates shared printers that have been disabled by `net pause` when typed at a client computer.
`net device`	Displays or modifies resource permissions on servers. Use this command only for displaying and modifying permissions on pipes and printer queues. Use `net perms` for managing permissions on all other types of resources.

TABLE 2-3 PC NetLink `net` Command Options *(Continued)*

Command	Description
`net file`	Displays the names of all open shared files and the number of file locks, if any, on each file. You can also use this command to close shared files. When used without options, this command lists all of the open files at a server. You can also type this command as `net files`.
`net group`	Adds, displays, or modifies global groups. You can also type this command as `net groups`.
`net help`	Provides lists of network commands and topics for which you can get help, or provides help for a specific *command* or *topic*.
`net helpmsg`	Provides help for a network error message.
`net localgroup`	Adds, displays, or modifies local groups in domains. You can also type this command as `net localgroups`.
`net logoff`	Logs off a user name from the network.
`net logon`	Logs in a user name to the server and sets the user name and password for the user's client. If you do not specify a user name with this command, the default user name will be your Solaris system login name.
`net password`	Changes the password for a user account on a server or in a domain.
`net pause`	Suspends services or disables printers at a server. Usage note: After you have followed the instructions in Chapter 4 of this guide to set up your Solaris printer, establish it as a PC NetLink shared printer, and make it available to your Microsoft Windows clients, do *not* use the `net pause` command as a method to pause the print queue. That command is interpreted by PC NetLink software as a command to disable the printer rather than merely to pause the queue. Instead, to pause the queue by way of the command line, use the `net print /hold` command.
`net perms`	Displays or modifies resource permissions and ownership information on servers. The resources on which this command currently operates are shares, directories, and files.
`net print`	Displays or controls print jobs and printer queues; also sets or modifies options for a printer queue. See the usage notes in this table for the `net pause` and `net share` commands.
`net send`	Sends a message to connected client computers.
`net session`	Lists or disconnects sessions between a server and clients. When used without options, this command displays information about all of the sessions with the local server. You can also type this command as `net sessions`.

TABLE 2-3 PC NetLink `net` Command Options *(Continued)*

Command	Description
`net share`	Creates, deletes, modifies, or displays shared resources. Use this command to make a resource available to clients. When used without options, this command displays information about all of the resources being shared on the server. Usage note: Using the `net share` command to remove a printer share removes the share, but does not remove the printer. To remove the printer, use the `net print` command.
`net sid`	Performs translations between account names and their corresponding security identifiers (SIDs).
`net start`	Starts a service or, if used without options, displays a list of services that are running. The services that you can start are Alerter, Computer Browser, Directory Replicator, EventLog, Net Logon, Netrun, Server, Time Source, and WINS.
`net statistics`	Displays or clears the Statistics log.
`net status`	Displays a server's computer name, configuration settings, and a list of shared resources.
`net stop`	Stops a network service.
`net time`	Synchronizes the client's clock with that of a server or domain, or displays the time for a server or domain.
`net trust`	Establishes and breaks trust relationships between domains, and lists trust information for a specified domain.
`net user`	Adds, modifies, or deletes user accounts or displays user account information.
`net version`	Displays the version of network software currently running on the computer at which the command is issued.
`net view`	Displays a list of servers or displays resources being shared by a server.

About `lanman.ini` File Entries

This section lists and describes the `lanman.ini` file parameters that you can modify to change PC NetLink virtual server configuration and performance. (Other configuration values are stored in the PC NetLink Registry, as well; see Appendix A, "PC NetLink Registry" on page 299.) The configuration values within the `lanman.ini` file are vital to the proper operation of the PC NetLink virtual server, and editing this file is a task that should be performed *only by experienced administrators*.

When PC NetLink software is first installed, the `lanman.ini` file (`/etc/opt/lanman/`*number*`/lanman.ini`) contains some default parameter values. Other parameters and the titles of the sections in which they reside are added whenever you change the PC NetLink configuration. Only parameters that have been changed to values other than their default values are added to the `lanman.ini` file. If a parameter does not appear in the file (or is commented out with a semicolon), it is set to its default value. The file location is `/etc/opt/lanman/`*number*`/lanman.ini`, where *number* is the instance number.

Before attempting to change any of the parameters available in the `lanman.ini` file, it is useful to understand the relationship between the `lanman.ini` file entries and server defaults.

Every virtual server parameter has a default setting. To display and edit default settings, a utility program called `srvconfig` is provided in the `/opt/lanman/sbin` directory.

You can edit the `lanman.ini` file to set parameters to values other than the defaults. The value assigned to any parameter in the `lanman.ini` file always supersedes the default value for that parameter. Note that no changes will actually take effect until you have stopped and then restarted the server.

When you want to set the value of a parameter to something other than the default by directly editing the `lanman.ini` file, locate (or add) the appropriate section title in the file, and then add the desired *parameter=value* entry.

File Syntax

Within each section of the `lanman.ini` file, parameters are listed as follows:

- The name of each parameter is at the beginning of a line, followed by an equal sign and the value assigned to it: *parameter=value*.
- Comments start with a semicolon (`;`). If a semicolon precedes a parameter on the line, that parameter is ignored.
- When a list of values is assigned to a parameter, the values are separated by commas: *parameter=value,value,value, ...* (There are some exceptions to this rule, which are noted in the description of the appropriate parameters.)
- When a value consists of a path, the path may be absolute, starting with a forward slash (`/`). If a path does not start with `/`, it is assumed to be relative to the `lanman` directory.
- If a numeric value begins with 0 (the numeral), it is octal; if it begins with an "X," it is hexadecimal; if it begins with a numeral from 1 to 9, it is decimal.
- When a parameter has no assigned value (nothing to the right of the equal sign), the value is 0 for a parameter that requires a number and null for a parameter that requires a character string.

- A null value is not valid for all parameters.

▼ How to Change a `lanman.ini` File Parameter

1. **Use the `srvconfig` command to display default settings for the server parameters:**

   ```
   /opt/lanman/sbin/srvconfig -p | more
   ```

   Note – When a physical host has more than one PC NetLink virtual server configured, you must set the variable `PCNL_INSTANCE` before using the `srvconfig` command, or use the `-I` *instance* option. If you do not, the command will fail.

   ---

2. **Edit the `lanman.ini` file using vi or a similar text editor.**

   The file location is `/etc/opt/lanman/`*number*`/lanman.ini`, where *number* is the instance number. You may have to add a section heading to the file; for example `[lmxserver]`. You then need to add a *parameter*=*value* pair to the appropriate section of the `lanman.ini` file. (See the section, "About lanman.ini File Entries" on page 28.)

3. **Stop and restart the virtual server for the new values to take effect.**

   For more information about the `srvconfig` command, type `man srvconfig` at the system prompt.

File Parameters

The following tables describe the configurable parameters in the `lanman.ini` file. The parameters are grouped according to the section of the `lanman.ini` file in which they reside.

The `lanman.ini` file contains additional parameters that are not included in the following tables. These parameters are for debugging purposes and you should not modify them.

TABLE 2-4 `[lmxserver]` Section Parameters

Parameter	Description, Values, and Default Setting
`anncmailslot`	The name of the mail slot used for periodic server announcements. Values: A path up to a maximum of 256 characters. Default: `\\*\MAILSLOT\LANMAN` Note that backward slashes must be doubled on input or else the entire input line must be enclosed in single quotation marks. (Type *text*`\\`*text* or `'`*text*`\`*text*`'` to enter text with a single backward slash.)
`appsources`	The names of the modules that can write to the Application log. Default: The server initializes the value of this parameter at startup.
`countr`	The country code for server-generated messages. Default is 001. Other values: Asia—099; Australia—061; Belgium—032; Canada—002; Denmark—045; Finland—358; France—033; Germany—049; Italy—039; Japan—081; Latin America—003; Netherlands—031; Norway—047; Portugal—351; Spain—034; Sweden—046; Switzerland—041; United Kingdon—044; United States—001
`dll_dir`	The path to the directory containing message text files used by PC NetLink Solaris system commands. Default: `/opt/lanman/shares/asu/system32`
`lang`	Defines the character set that PC NetLink software uses for processing client requests. Default: `en_US`
`listenextension`	The extension that the Solaris system Listener program, by default, applies to the name of the server computer. This parameter is ignored if the `listenname` parameter in the `[server]` section is used. Values: 0-13 characters and a null value are acceptable. Default: `.SERVE`
`listennamechk`	If set to yes, it forces any name specified with the `listenname` parameter to be different than the Solaris machine name or the Solaris machine name with a `.serve` extension in order to avoid name conflicts with the Solaris Listener. Default: Vendor specific
`lmaddonpath`	The directory for dynamic libraries bound into the server program and called at various times during server execution, as described in the `/usr/include/lmx/lmaddon.h` header file. The server looks for these dynamic libraries on startup. Values: A path up to a maximum of 256 characters. Default: `/opt/lanman/lib/addon/lmaddon`

TABLE 2-4 `[lmxserver]` Section Parameters *(Continued)*

Parameter	Description, Values, and Default Setting
`lmgetmsg_path`	Search order for message text files used by PC NetLink. Default: `netmsg.dll`, `kernel32.dll`, `locallspl.dll`, `asumsg.dll`
`lptmpdir`	The location of the spooling directory for temporary files used by the Solaris system's LP (printer) subsystem. Default: `/var/spool/lp/tmp/`*uname* where *uname* is the server's Solaris system name. (This is not changeable by users.)
`mapaclblob`	Configures whether to use memory-mapped file operations when accessing the PC NetLink Access Control List database. Values: yes, no. Default: yes
`mapchangelogblob`	Configures whether to use memory-mapped file operations when accessing the PC NetLink Change Log database. Values: yes, no. Default: no
`maplsablob`	Configures whether to use memory-mapped file operations when accessing the PC NetLink Local Security Authority database. Values: yes, no. Default: no
`mapregistryblob`	Configures whether to use memory-mapped file operations when accessing the PC NetLink Registry database. Values: yes, no. Default: no
`mapsamblob`	Configures whether to use memory-mapped file operations when accessing the PC NetLink Security Accounts Manager database. Values: yes, no. Default: no
`maxfilesize`	The maximum file size, in kilobytes, that the Solaris system redirector will allow a "local Solaris user" to create on a local system. Values: 100 - unlimited. Default: 2097152
`msgforward`	Specifies if PC NetLink software implements message forwarding between clients. Implementation of message forwarding is not recommended. Values: yes (implement forwarding) or no (do not implement forwarding). Default: no
`nativelm`	An additional field in the session setup request/response. Default: PC NetLink
`nativeos`	An additional field in the session setup request/response. Default: UNIX *x.x* Generic (where *x.x* is the release number)

TABLE 2-4 `[lmxserver]` Section Parameters *(Continued)*

Parameter	Description, Values, and Default Setting
`netaddonpath`	The directory in which the PC NetLink program looks for dynamic libraries on startup. Dynamic libraries found in the directory are bound into the PC NetLink program and used to access the various network interfaces on the server computer. Sample source for a network interface file is located in the default directory. Values: A path up to a maximum of 256 characters. Default:`/opt/lanman/lib/addon/networks`
`nethelpfile`	The location of the help file used by the `net help` command (relative to `/var/opt/lanman/msgfiles`). Default: `/opt/lanman/msgfiles/net.hlp`
`netmsgwait`	The interval, in seconds, that the server waits for a response when it sends a message that requires one. Values: 0 - unlimited. Default: 300
`network`	The network device names and NetBIOS name-passing type for the network(s) the server should use. Values: Sets of four items separated by commas, each set of four separated from the next by a space. The following four items are in each set: 1. The device name for virtual circuit access. 2. The device name for datagram network access. 3. A digit identifying the NetBIOS interface convention used by the two devices above. Currently there is only one convention compiled into the server: 0 = OSI NetBIOS convention. 4. The name of the transport provider, as returned by the `nlsprovider` system call. (For networks not configured to accept incoming connections through the Solaris system Listener program, this can be any arbitrary string.)
`prebinduxredir`	Controls the name that the Solaris system `net` command binds when it uses the Solaris system redirector (`uxredir`). If this parameter is set to yes, the server pre-binds a NetBIOS name that will be used by all Solaris system `net` commands. Because this name is pre-bound, the `net` command does not need to bind its own name, and this quickens the Solaris system's `net` access to the server. If this parameter is set to no, then each `net` command will use its own unique name with somewhat slower performance resulting. Values: yes, no. Default: yes
`secsources`	The names of the modules that can write to the Security log. Default: The server initializes the value of this parameter at startup.

TABLE 2-4 [lmxserver] Section Parameters *(Continued)*

Parameter	Description, Values, and Default Setting
srvstathelpfile	The location of the help file used by the Activity Monitor. Default: /opt/lanman/msgfiles/srvstat.hlp
stacksize	The size of the stack, in bytes, for each task internal to the server. Values: 12000 - unlimited. Default: 20000
syssources	The names of the modules that can write to the System log. Default: The server initializes the value of this parameter at startup.

TABLE 2-5 [Fsi] Section Parameters

Parameter	Description, Values, and Default Setting
fsaddonpath	The location of dynamic link libraries (DLLs) that support file systems on the server. Values: A path up to a maximum of 256 characters. Default: /opt/lanman/lib/addon/fsaddon
fslibname	The subdirectory of the directory identified by fslibpath where new file systems are located. Values: A path up to a maximum of 256 characters. Default: lmfsiops.so
fslibpath	The location of new file systems on the server. Values: A path up to a maximum of 256 characters. Default: /usr/lib/fs
fsmap	File system type identifiers that map unknown file systems to known file system types. Values: A comma-separated list of mappings. Default: unknown:s5,nfs:nfs,sfs:vxfs,cdfs:vxfs
fsnosupport	Maps unknown file system to specified file system. Default: s5
remotemounts	The names of file system types that indicate remotely mounted file systems. Default: nfs

TABLE 2-6 [Workstation] Section Parameters

Parameter	Description, Values, and Default Setting
domain	The name of the domain that includes the server. Values: Any name of up to 15 characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; @ ‘ Default: <*servername*>_dom

TABLE 2-7 [Server] Section Parameters

Parameter	Description, Values, and Default Setting
listenname	If set, this is the server's name on the network. If not set, the PC NetLink system may receive client connections from the Solaris Listener on the Solaris machine name with a .serve extension (such as liberty.serve). This is implementation dependent. The Solaris system machine name can be determined by using the uname -n command. To change the value of the listenname parameter, use the setservername command. For more information about this command, type man setservername at the PC NetLink command prompt. Values: Any name of up to 15 characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; @ ' Default: null
maxclients	Identifies the maximum number of simultaneous client sessions that the server must support. Default: 2000.
srvservices	The list of keywords for the services that start automatically when the server is started. Because services are started in the order they appear in the srvservices entry, you must ensure that netlogon appears before any services that require it. Default: alerter, netlogon, browser

CHAPTER 3

Configuring and Managing PC NetLink Software

This chapter provides general background information about, and instructions for, configuring and managing your PC NetLink software. Note that the instructions in this chapter pertain only to your PC NetLink program, not to Windows NT network configuration or management.

You can accomplish most tasks in this chapter in two ways: by using the PC NetLink Server Manager tool, or by logging in to the physical host that is running PC NetLink and typing commands at the Solaris root command prompt.

Major topics covered in this chapter include:

- Logon and logoff
- Startup and shutdown
- Domain configuration and management
- Policy management
- Event monitoring

Instructions are included in this chapter for accomplishing the following tasks:

- "How to Start PC NetLink Server Manager" on page 40
- "How to Add a Solaris Server to PC NetLink Server Manager" on page 41
- "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42
- "How to Log On to a Solaris Server From the Command Line" on page 44
- "How to Log Off a Solaris Server Using PC NetLink Server Manager" on page 45
- "How to Log Off a Solaris Server From the Command Line" on page 45
- "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46
- "How to Stop a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 47
- "How to Start a PC NetLink Virtual Server From the Command Line" on page 49

- "How to Stop a PC NetLink Virtual Server From the Command Line" on page 49
- "How to Schedule Virtual Server Restart, Stop, or Start" on page 50
- "How to Start Individual Services" on page 56
- "How to Stop Individual Services" on page 58
- "How to Configure Startup for Individual Services" on page 60
- "How to Create an IP Address for a PC NetLink Virtual Server" on page 66
- "How to Create a New PC NetLink Virtual Server" on page 67
- "How to Delete a PC NetLink Virtual Server" on page 74
- "How to Rename a PC NetLink Virtual Server" on page 75
- "How to Move a Virtual Server to Another Domain" on page 80
- "How to Promote a BDC Within Its Domain" on page 89
- "How to Change the Role of a Server Within Its Domain" on page 91
- "How to Change Computer Browsing Policy" on page 109
- "How to Set Up File Name Mapping" on page 111
- "How to Tune PC NetLink for Optimum Performance" on page 112
- "How to Set Solaris File System Integration Policies" on page 114
- "How to Use UPS Power Failure Notification" on page 116
- "How to Edit User Accounts Policies" on page 118
- "How to Map Existing User Accounts" on page 120
- "How to Configure the Windows Internet Name Service (WINS)" on page 141
- "How to Start or Stop WINS Using PC NetLink Server Manager" on page 144
- "How to Start or Stop WINS From the Command Line" on page 146
- "How to Configure a LAN Adapter (Lana) Device" on page 146
- "How to Configure Solaris Name Services" on page 149
- "How to Configure PC NetLink Server Manager Security Policy" on page 152
- "How to Configure PC NetLink Server Performance Monitoring and Alarms" on page 153
- "How to Monitor Physical Host Performance" on page 156
- "How to Investigate Performance Alarms" on page 162
- "How to Monitor Events Using PC NetLink Server Manager" on page 168
- "How to Monitor Events From the Command Line" on page 169
- "How to View Solaris Physical Host Information" on page 170
- "How to View or Change PC NetLink Virtual Server Configuration Options" on page 171
- "How to Add a Computer Account to a Domain" on page 173

■ "How to Delete a Domain Member" on page 175

About Logon and Logoff

To perform PC NetLink Solaris administrative tasks or Windows NT administrative tasks—whether from the physical host's command line, the PC NetLink Server Manager tool, or from a remote client—you must be authorized by the server. Network resources are protected at several levels by different processes.

Depending on the type of privileges that the administrative task you want to accomplish requires, you need to log on by identifying yourself with both a special user name and a password that accompanies it. Purely PC NetLink administrative tasks, such as changing the name of a PC NetLink system, require that you log on with the Solaris superuser name, root. Windows NT administrative tasks, such as changing an NT server's configuration, additionally require special Windows NT administrator privileges and passwords.

Windows NT and Solaris Root Logon Privileges

To administer Windows NT data, some of your network users may be designated as *account operators*, *print operators*, or *server operators*. These users have limited Windows NT administrative or operator privileges that enable them to perform specific tasks. These privileges are sufficient to use the `net` command to administer a *local* server at the physical host's command prompt, as well.

However, *remote* Windows NT administrative access to a PC NetLink server is protected by additional logon security, which requires you to be a member of a specially privileged group, *Administrators*. Once you have identified yourself to the server, it checks your user name and password against the server directory database.

You can use PC NetLink Server Manager or the Solaris command line to log on to, or log off from, your PC NetLink system. To perform any administrative task, you must log on as root first, and then, in some cases, also provide your Windows NT administrator name and password. Note that using the PC NetLink command line requires you first to log on as root to the Solaris system that hosts the PC NetLink server software, and then, using your Windows NT administrator user name and password, to log on to the network with the `net` command.

▼ How to Start PC NetLink Server Manager

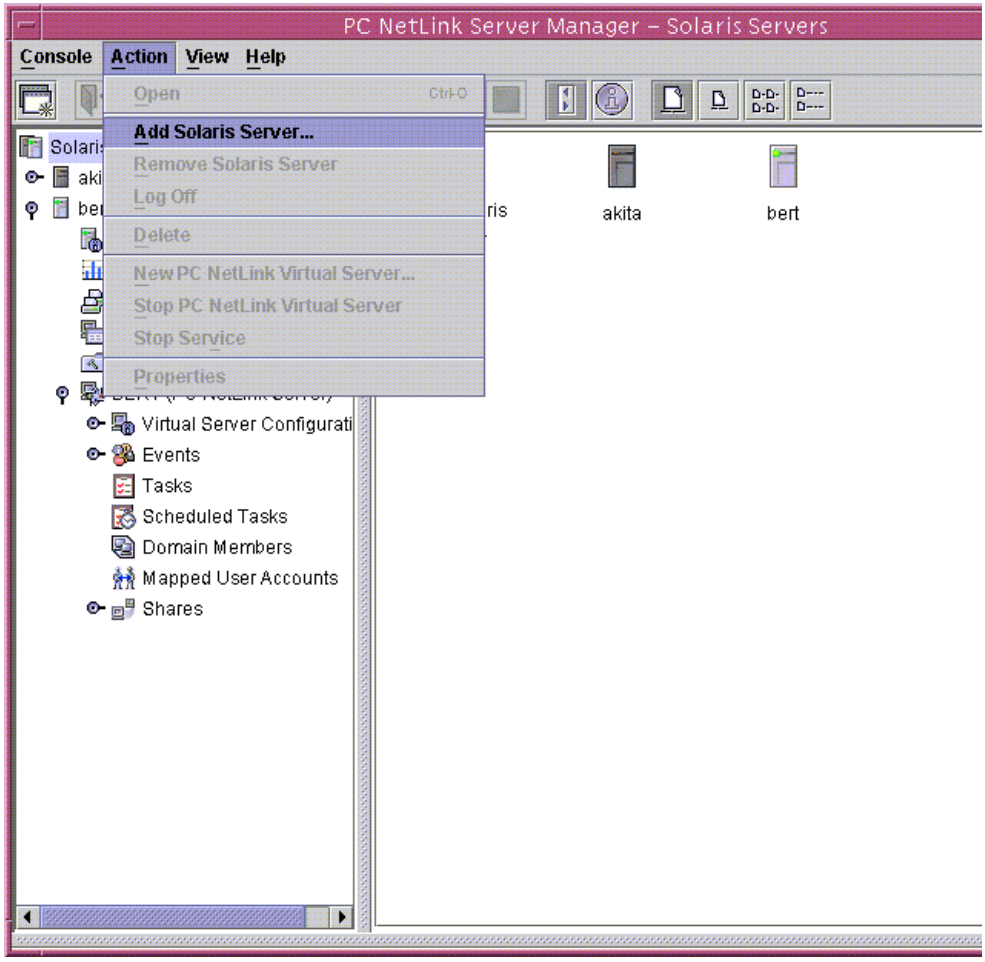
- **Do one of the following, depending on the computer you are using:**
  - Using a Microsoft Windows system, double-click the PC NetLink Server Manager icon. (If you have chosen not to have icons placed on the Start menu or your desktop, select the PC NetLink Server Manager folder from the Programs menu, and then double-click the icon.)
  - Using a Solaris system, type the following at the command prompt:
    `/opt/lanman/sbin/slsmgr`

    To use a maximum heap size for PC NetLink Server Manager that is larger than the default value of 32 Mbytes, use the option `-m` *number*, where *number* is the number of Mbytes to use for the PC NetLink Server Manager maximum heap size. To change the maximum heap size for PC NetLink Server Manager running on Microsoft Windows, you must launch the application from a command window rather than by using the Start menu or a shortcut.

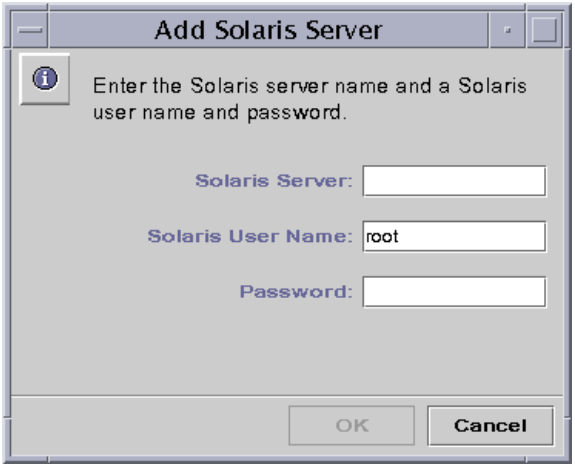
▼ How to Add a Solaris Server to PC NetLink Server Manager

1. **From the Action menu, choose Add Solaris Server, or double-click the Add Solaris Server icon in the Results pane.**

   If this is the first time you have started PC NetLink Server Manager, the Add Solaris Server dialog box will appear automatically, making this step unnecessary.



The following screen appears.



2. **Type in the name of the Solaris server you want to add to PC NetLink Server Manager.**
3. **Type the root password for the system (the root user name is already entered by default), then click OK.**

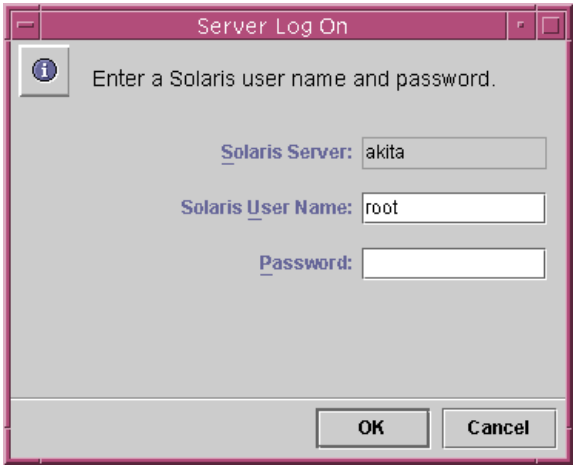
   You are logged on to the specified server, which is added to the list of Solaris servers.

▼ How to Log On to a Solaris Server Using PC NetLink Server Manager

1. **Do one of the following:**
   - In the Solaris Servers list in the Navigation pane (left side) of PC NetLink Server Manager, click the name of any PC NetLink physical host.
   - Double-click a physical host in the Results pane (right side) of PC NetLink Server Manager.
   - Highlight a physical host in the Results pane (right side) of PC NetLink Server Manager, and choose Log On from the Action menu.
   - With the mouse pointer over the icon of a physical host in the Results pane (right side), right-click and choose Log On from the menu.

Note – The step above assumes that this is not the first time that you have run PC NetLink Server Manager. If this is the first time, then the system prompts you to add a server—a procedure that also logs you on to the system. See "How to Add a Solaris Server to PC NetLink Server Manager" on page 41.

The Server Log On dialog box appears.



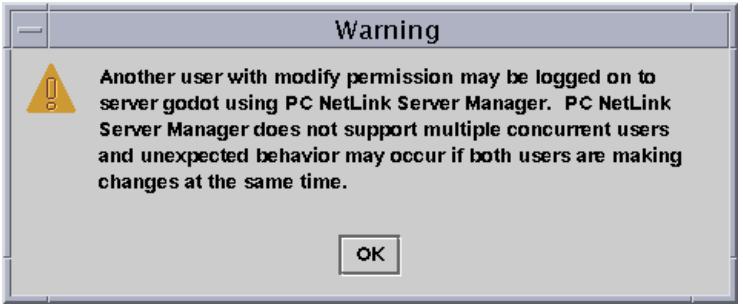
Note – The Server Log On dialog box will also appear whenever you attempt to perform an administrative task on a PC NetLink system to which you are not logged on. To make any changes, you must log on as root.

2. **In the text field provided, type the root password.**

   Although you can log on with a non-root user name, PC NetLink administrative functions require root privileges. A root account in a Solaris system is equivalent to an Administrators group account in a Windows NT system, with full administrative privileges. Therefore, if you log on with a user name other than root (which is the default), you will not be able to make any administrative changes to the system.

3. **Click OK.**

   If another user with administrative privileges is logged on when you attempt to log on, a message similar to the following is displayed.



   Only one administrative user at a time should use the PC NetLink program to make changes. Unless you need to make an immediate change, or you want only to monitor PC NetLink behavior, you should not log on.

▼ How to Log On to a Solaris Server From the Command Line

1. **At the Solaris prompt of the physical host that is running PC NetLink software, type the following command:**

   ```
   system% su
   Password:
   system#
   ```

2. **At the new system prompt, log on to the network as Administrator or as a user with administrative privileges by typing the following command:**

   ```
   system# net logon username password
   ```

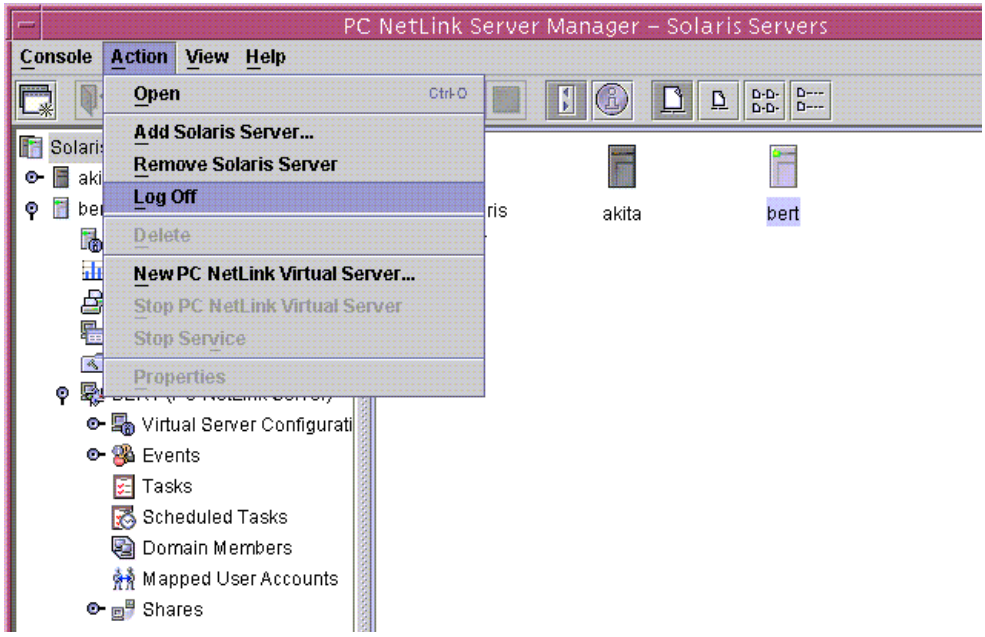
   Substitute a privileged user name for *username*, and substitute the privileged user's correct password for *password*.

   Note – To perform administrative tasks on any *remote* PC NetLink system, you must be logged on as a member of the Administrators group. Operator privileges are not sufficient for remote administration.

   To avoid displaying the password on your screen, you can omit it from this command. The system will prompt you for the password, but will not display it as you type it.

▼ How to Log Off a Solaris Server Using PC NetLink Server Manager

- **With the server or any of its associated items highlighted, choose Log Off from the Action menu.**



▼ How to Log Off a Solaris Server From the Command Line

- **Type the following command:**

  `system#` **`net logoff`**

  If you used the `su` command to switch to the root account, type **`exit`** to return to the account from which you switched.

About Starting and Stopping Services

The PC NetLink program provides the following Windows NT services:

- Alerter
- Computer Browser
- Directory Replicator
- Event Log
- Net Logon
- Netrun
- Spooler
- Timesource
- Windows Internet Name Service (WINS)

To perform a number of administrative tasks, you must first shut down some or all of these services, and then restart the services after performing the tasks.

In a native Windows NT environment, you use the Services command in Server Manager to start and stop each of the services available on the computer, determine whether a service starts automatically, and control some service startup parameters.

You can use the Windows NT Server Manager's Services Startup dialog box to configure when and how a service is started, and optionally, to specify the user account that the service will use to log on. By default, most services log on using a special system account. (Of the services provided with PC NetLink software, only the Directory Replicator service logs on using a specific user account.)

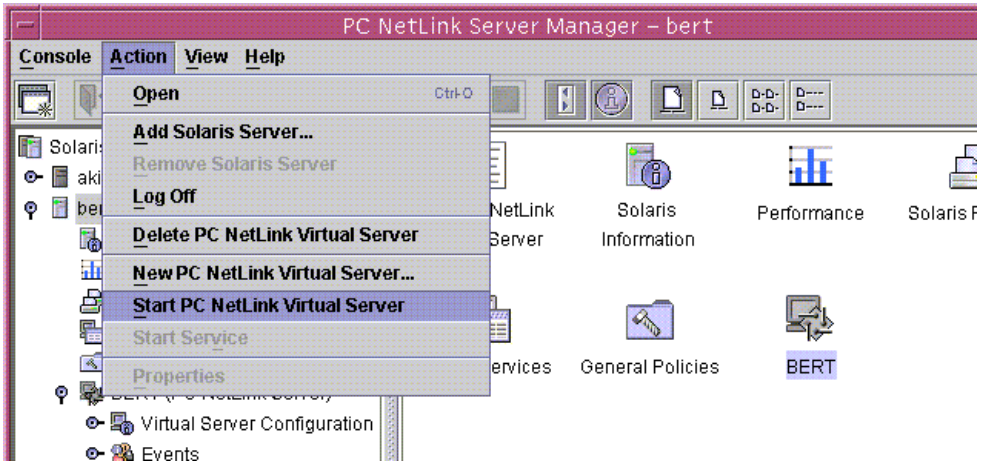
To start and stop your PC NetLink program, as well as individual services that are specifically supplied by it, you use either PC NetLink Server Manager, the physical host's Solaris command line, or your Windows NT Server Manager.

▼ How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that you want to start.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **With the name of the PC NetLink virtual server highlighted, choose Start PC NetLink Virtual Server from the Action menu.**



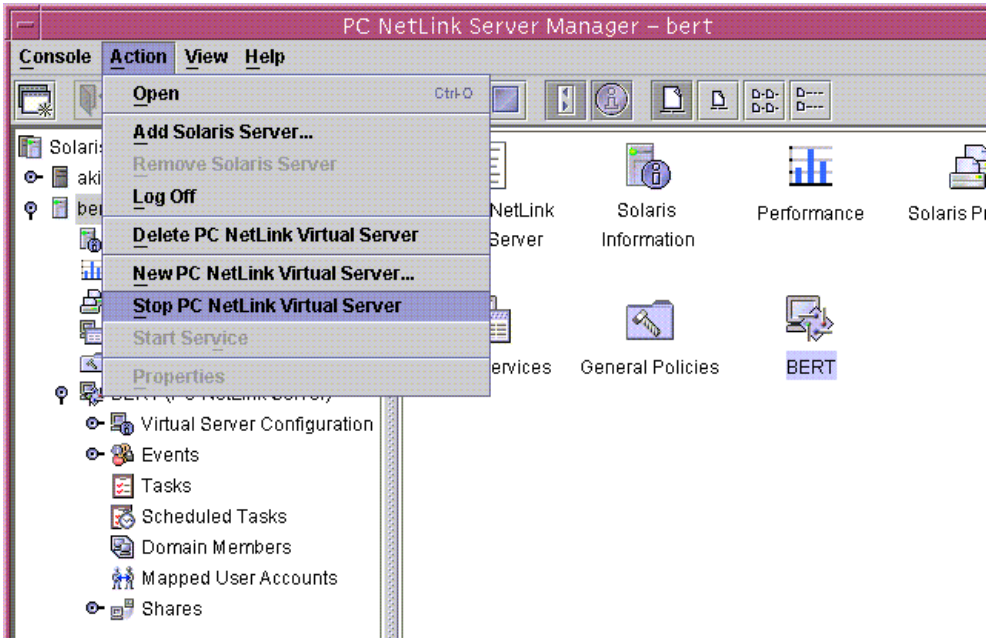
Note – PC NetLink Server Manager wizards for various administrative tasks offer you the option of having the wizard itself shut down and start up PC NetLink processes. If you choose this option when using these wizards, you do not need to start up or shut down the processes manually.

▼ How to Stop a PC NetLink Virtual Server Using PC NetLink Server Manager

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that you want to stop.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

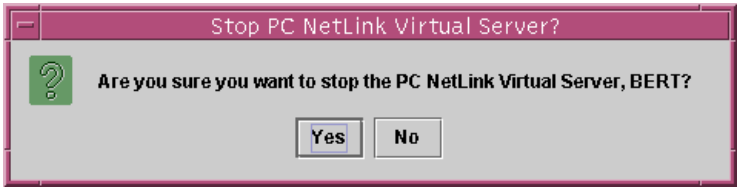
2. **With the name of the PC NetLink virtual server highlighted, choose Stop PC NetLink Virtual Server from the Action menu.**



Note – PC NetLink Server Manager wizards for various administrative tasks offer you the option of having the wizard itself shut down and start up PC NetLink processes. If you choose this option when using these wizards, you do not need to start up or shut down the processes manually.

---

3. **Choose Yes to confirm that you want to stop the PC NetLink virtual server, or No to cancel the operation.**



▼ How to Start a PC NetLink Virtual Server From the Command Line

1. **Log on as root to the Solaris physical host for the PC NetLink virtual server that you want to start.**

   For instructions, see "How to Log On to a Solaris Server From the Command Line" on page 44.

2. **At the system prompt, type the following:**

   ```
   system# /opt/lanman/bin/net start server
   ```

Note – When a physical host has more than one PC NetLink virtual server configured, you must set the variable `PCNL_INSTANCE` before issuing a command to configure a specific virtual server, or use the `-I` *number* option with the command, where *number* is the instance number of the virtual server. (For `net` commands, use `/I:`*number*.) If you do not, the command will fail.

▼ How to Stop a PC NetLink Virtual Server From the Command Line

1. **Log on as root to the Solaris physical host for the PC NetLink virtual server that you want to stop.**

   For instructions, see "How to Log On to a Solaris Server From the Command Line" on page 44.

2. **At the system prompt, type the following:**

   ```
   system# /opt/lanman/bin/net stop server
   ```

Note – When a physical host has more than one PC NetLink virtual server configured, you must set the variable `PCNL_INSTANCE` before issuing a command to configure a specific virtual server, or use the `-I` *number* option with the command, where *number* is the instance number of the virtual server. (For `net` commands, use `/I:`*number*.) If you do not, the command will fail.

▼ How to Schedule Virtual Server Restart, Stop, or Start

In addition to using the Action menu or Solaris command line to stop or start a virtual server, you can use a PC NetLink Server Manager wizard: Server Stop and Start. This wizard is useful for restarting the server, or for scheduling server restart, stop, or start at a later time or according to a schedule.

Note – Scheduled tasks are not supported in a high availability (HA) environment.

---

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server for which you want to schedule restart, stop, or start.**

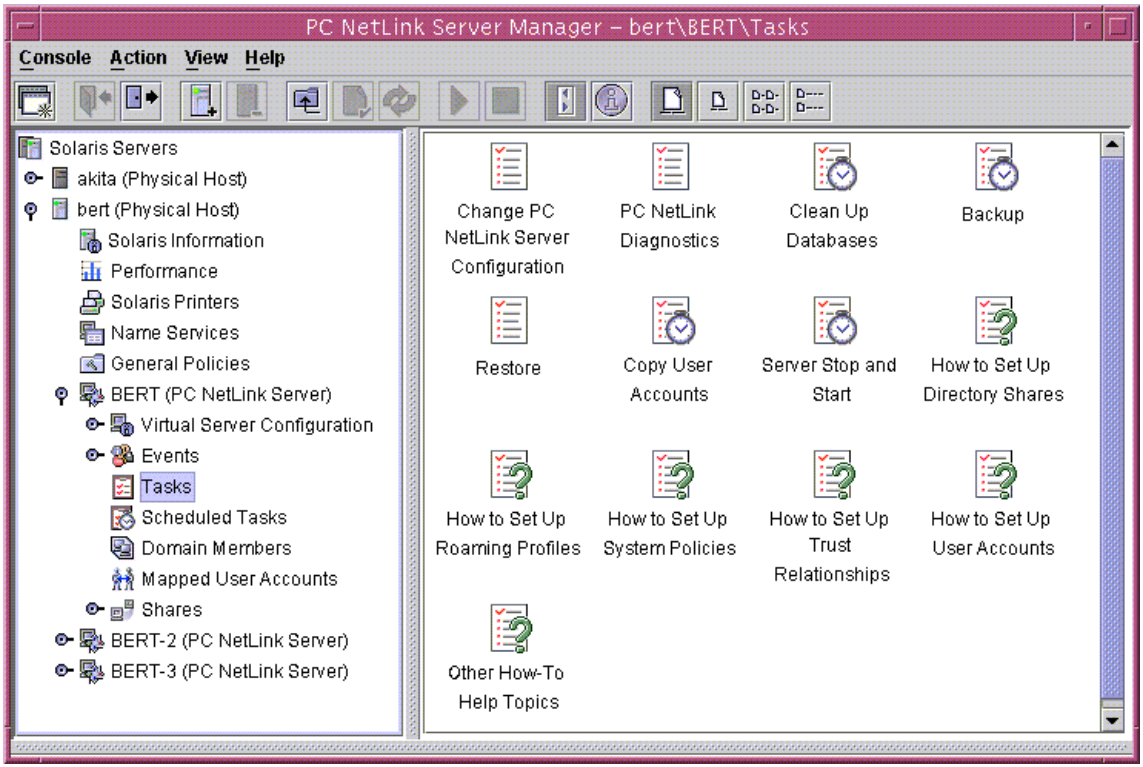
   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Tasks.**

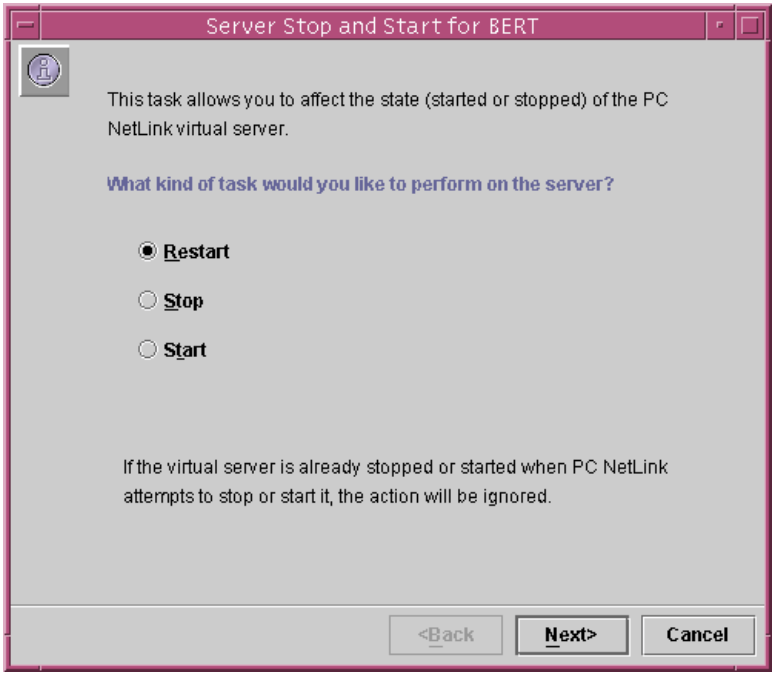
   A screen similar to the following appears.



Note that some of the tasks—including Server Stop and Start—are marked with a clock face. This indicates that these are tasks that you can run immediately, or automatically on a periodic schedule that you create.

4. **Double-click Server Stop and Start.**

   The following screen appears.



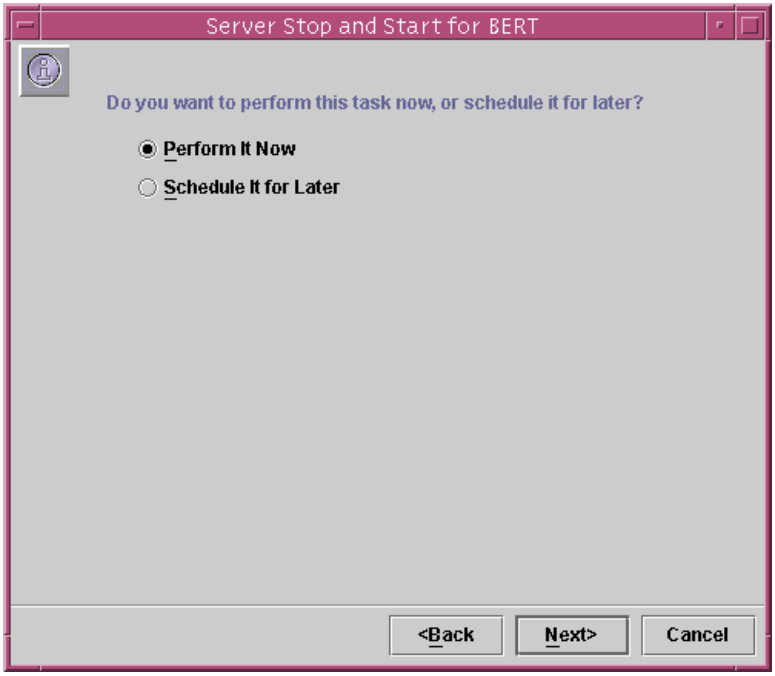
5. **Select which task you want to perform: Restart, Stop, or Start.**

   If the virtual server is already stopped or started when PC NetLink attempts to stop or start it, the action will be ignored.

6. **Click Next.**

   If you continue the procedure by clicking Next, the resulting screen prompts you for scheduling information.

.



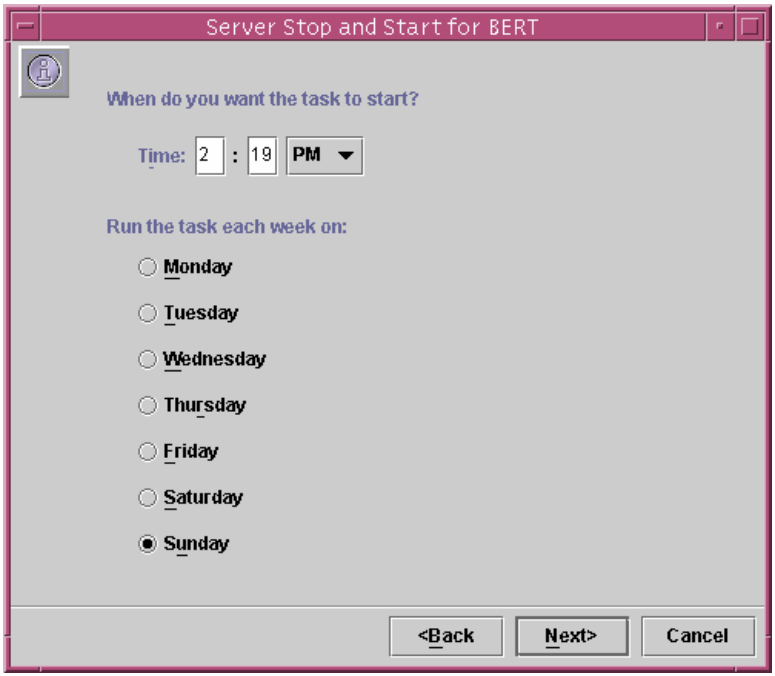
7. **Select Perform It Now or Schedule It for Later, and then click Next.**

Note – Scheduled tasks are not supported in a high availability (HA) environment.

---

8. **Depending on the selection you made, do one of the following:**
   - *Perform It Now* – Skip to Step 12.
   - *Schedule It for Later* – Continue with Step 9.
9. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

   A screen similar to the following appears.



The example shows the choices you must make when scheduling the task to be run weekly. Depending on your selection, you must furnish the following information about when you want the task to be run:

- *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date.
- *Daily* – The time of day.
- *Weekly* – The time of day and the name of the day.
- *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only.

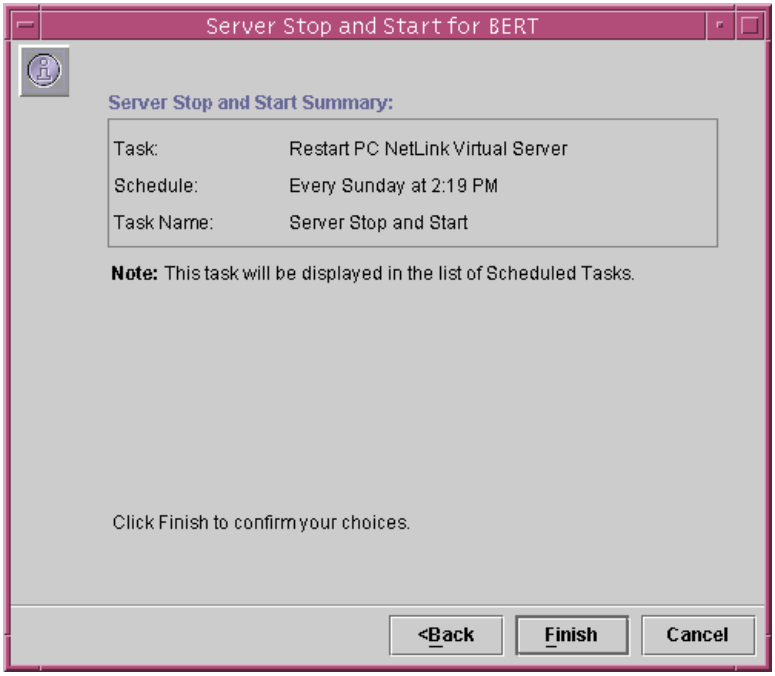
10. **Click Next.**

11. **In the text field of the resulting screen, type a name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

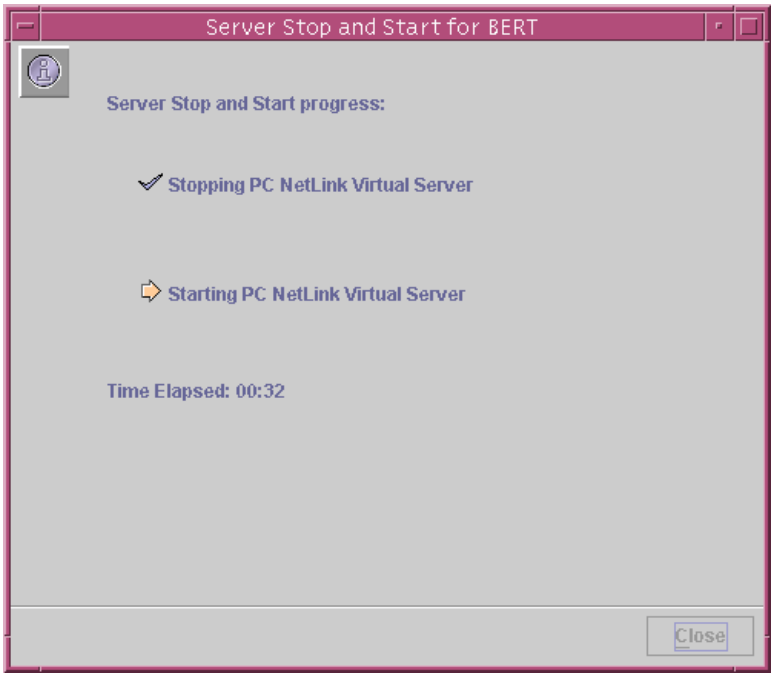
12. **Click Next.**

    A summary screen similar to the following appears.



13. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

▼ How to Start Individual Services

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose service you want to start.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

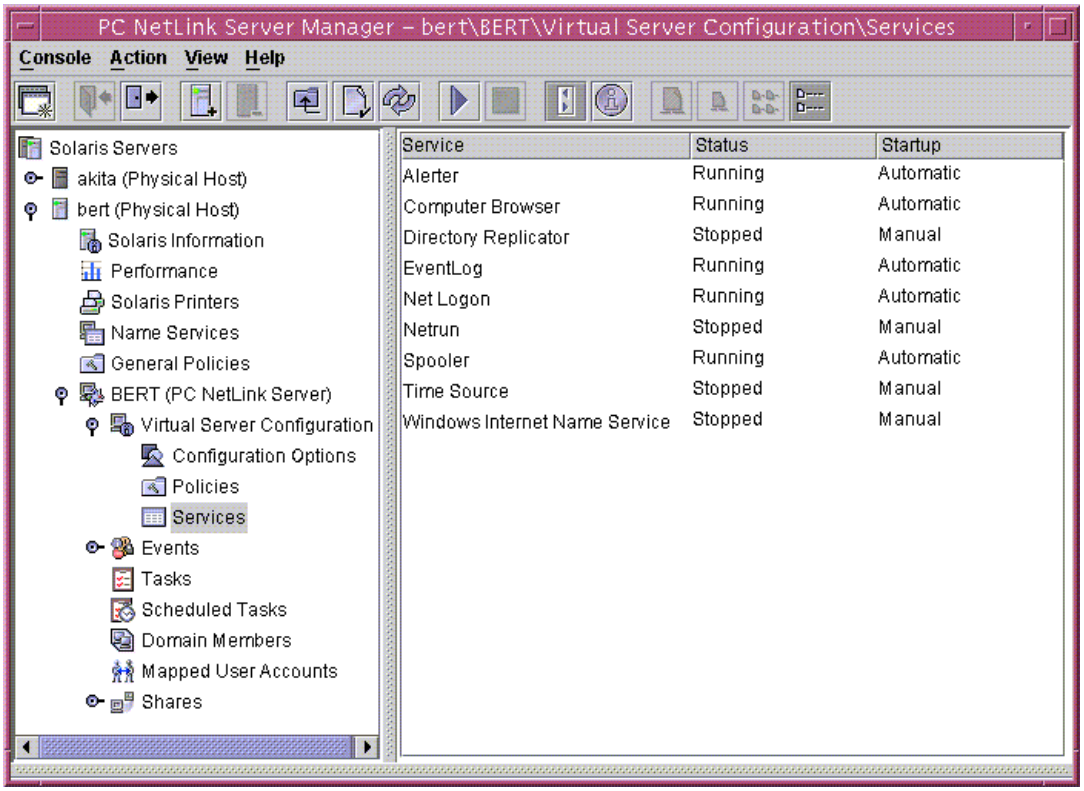
2. **In the Results pane, double-click the icon that represents the PC NetLink virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

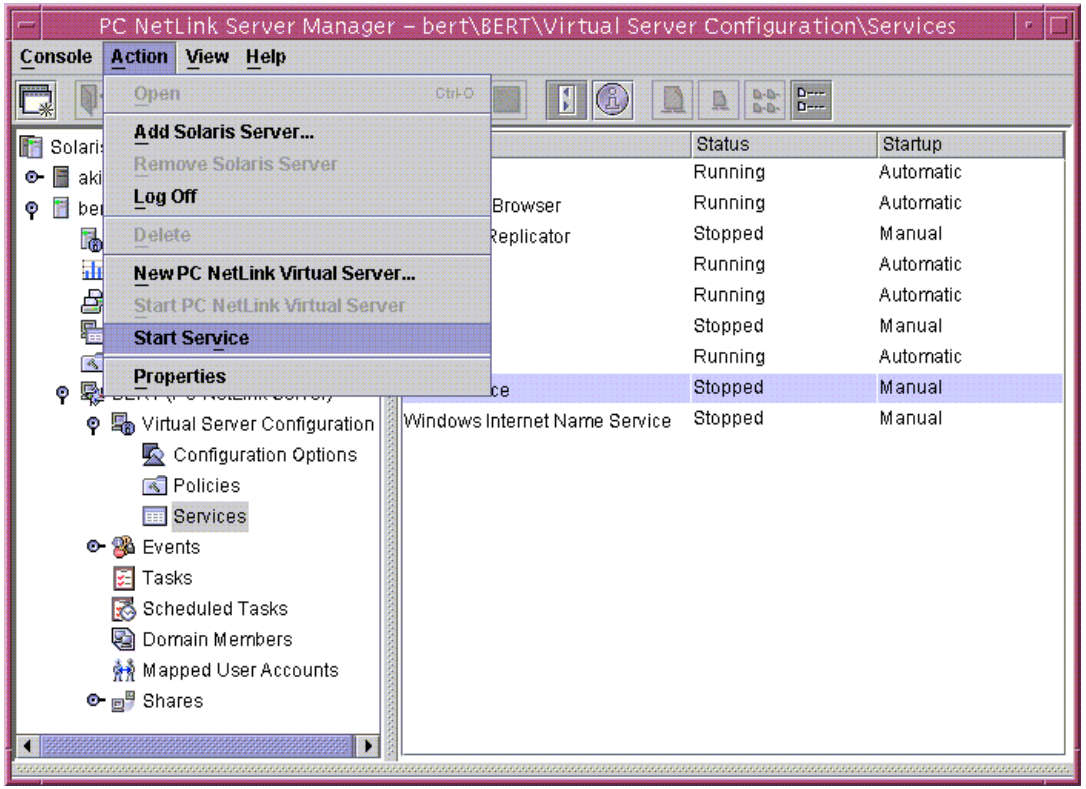
3. **Double-click Virtual Server Configuration.**

4. **Double-click Services.**

   The Results pane changes, displaying a list of individual PC NetLink services, their status, and their startup method—either manual or automatic.



5. **Highlight the service that you want to start, then choose Start Service from the Action menu.**



Note – The WINS server can run on only one instance in the domain at a time. If you attempt to start a second WINS server instance, you receive an error.

▼ How to Stop Individual Services

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose service you want to stop.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

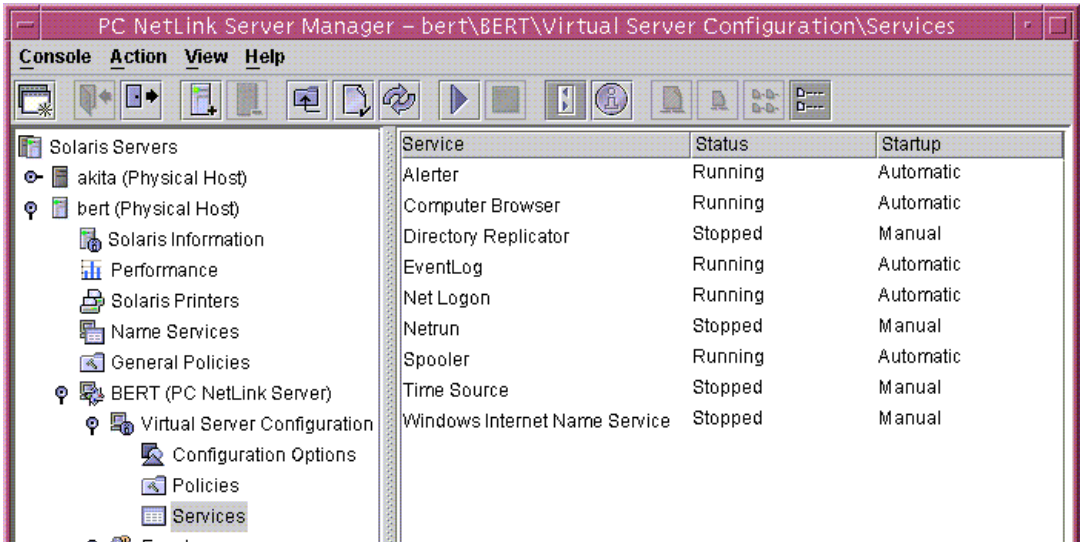
2. **In the Results pane, double-click the icon that represents the PC NetLink virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

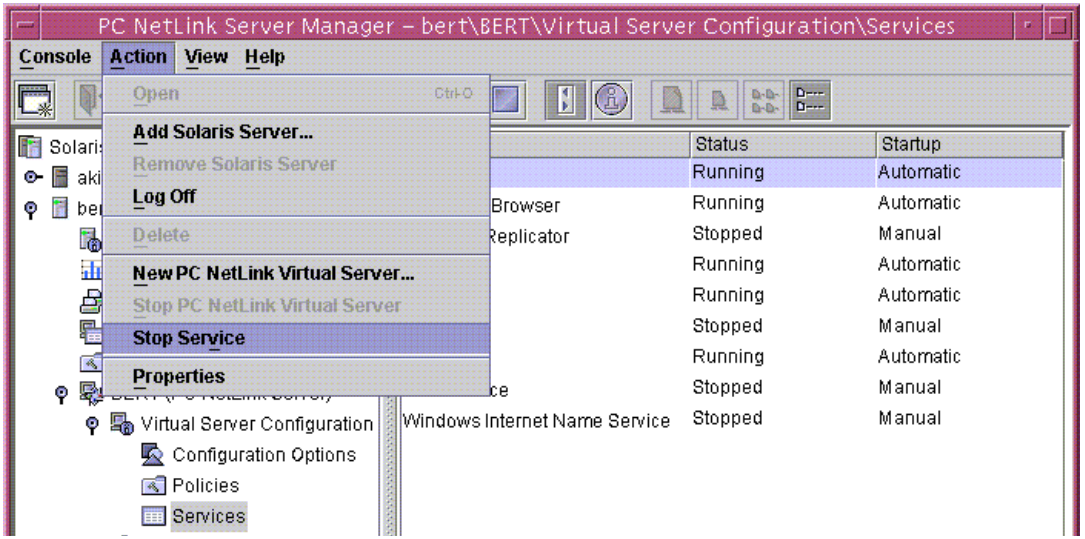
3. **Double-click Virtual Server Configuration.**

4. **Double-click Services.**

   The Results pane changes, displaying a list of PC NetLink services, their status, and their startup method—either manual or automatic.



5. **Highlight the service that you want to stop, then choose Stop Service from the Action menu.**



6. **Choose Yes to confirm that you want to stop the service, or No to cancel the operation.**

▼ How to Configure Startup for Individual Services

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose service you want to configure.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

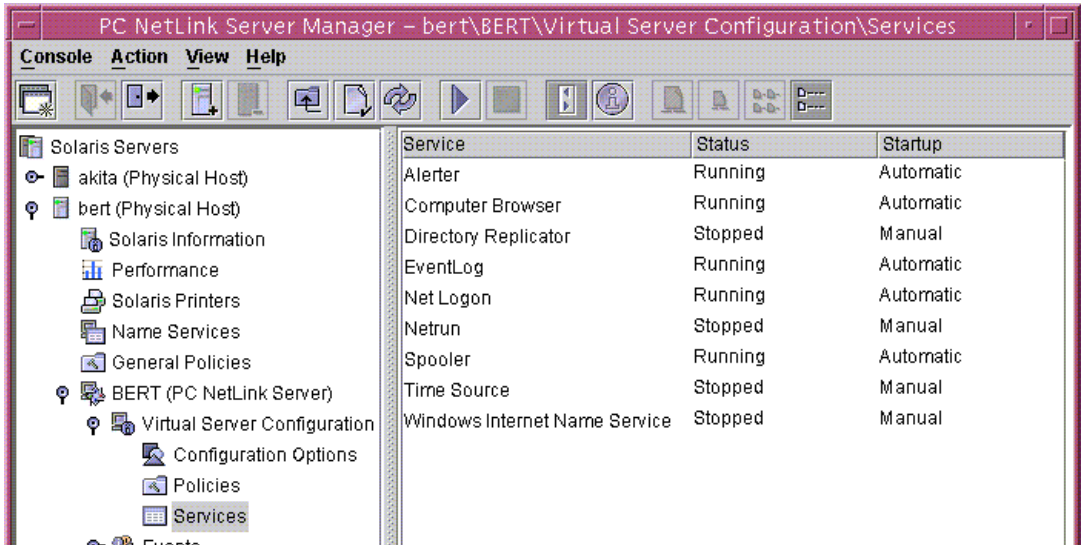
2. **In the Results pane, double-click the icon that represents the PC NetLink virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

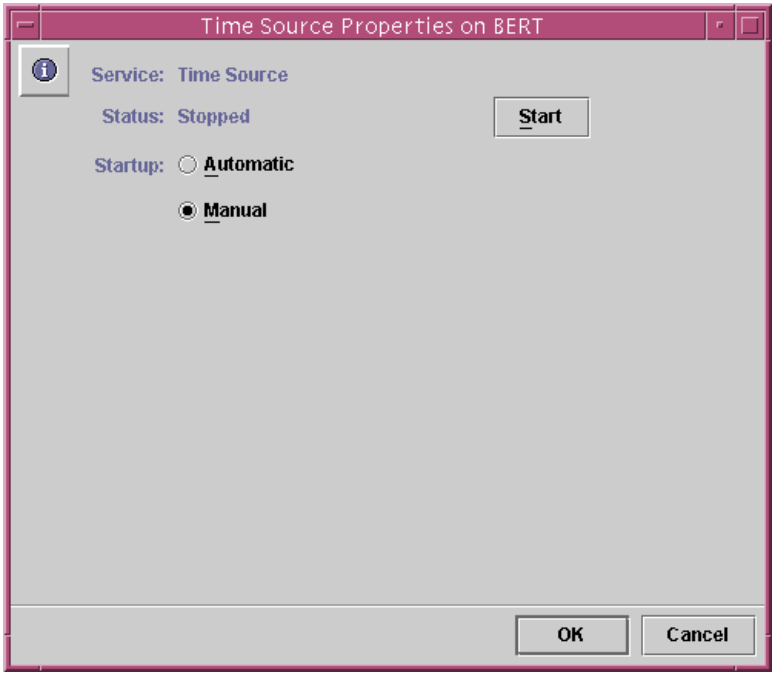
4. **Double-click Services.**

   The Results pane changes, displaying a list of PC NetLink services, their status, and their startup method—either manual or automatic.



5. **Double-click the name of the service whose startup method you want to change.**

   A screen similar to the following appears.



6. **Select either the Manual or the Automatic button, then click OK.**

   Automatic startup means that the service will start when you start PC NetLink.

About Domain Configuration and Management

A *domain* is a logical grouping of network servers and other computers that share common security and user account information. Within domains, you create one user account for each user. Users then log on to a domain, not to individual servers within the domain.

A domain is the administrative unit of PC NetLink directory services. The term, domain, does not refer to a single location or specific type of network configuration. Computers in a single domain can share physical proximity on a small local area network (LAN) or can be located in different corners of the world, communicating over any number of physical connections, including dial-up lines, ISDN, fiber, Ethernet, Token-Ring, frame relay, satellite, and leased lines.

Every PC NetLink virtual server in a Windows NT network must be given one of the following roles in the domain:

- *Primary domain controller (PDC)* – A PDC distributes user account information to backup domain controllers and validates network logon requests. There can be only one primary domain controller per domain. A server that is a domain controller requires a unique IP address.
- *Backup domain controller (BDC)* – A BDC receives user account information from the primary domain controller and validates network logon requests. Using either the PC NetLink Server Manager or the Windows NT Server Manager tool, you can promote a BDC to primary if the primary domain controller is not accessible. Note, however, that the primary domain controller must be the first server that is installed in a domain, and it must be up and running before you install a backup domain controller. A server that is a domain controller requires a unique IP address.
- *Member server* – Also known as a *standalone server*, a member server is a computer that is running PC NetLink (or Windows NT) server software, but has no domain controller role whatsoever. Because a member server has no controller role within its domain, you can move it at will to any other domain or workgroup. Member servers do not participate in user logon validation; therefore, they offer more computing resources than PDCs or BDCs for acting as file and print servers, for example. If you know that you will need to move a particular server to a different domain in the future, you should install it as a member server.

If you used *Express* installation, the program created a PC NetLink virtual server that acts as a *primary* domain controller in a new domain. If you used *Custom* installation, you chose the virtual server's role. As administrator, you can change the role, the name, and the domain of virtual servers. If you or another administrator have created additional virtual servers on a physical host, these virtual servers can belong to the same or different domains, and have the same or different roles. (However, only one virtual server per domain can act as a primary domain controller.) Member servers on a physical host can share the same IP address.

Note – On first startup of PC NetLink software after initial installation, the default name of the Administrator account is the English word, "Administrator." If you are using a localized version of the PC NetLink program, you must still type the English word when you log on for the first time. "Administrator" is not translated. After you have logged on, you can then change the words as you desire.

In addition to setting up the PC NetLink virtual server as a PDC, the Express installation defaults specify that:

- The virtual server name is the same as the host name of the Solaris system (it appears in UPPERCASE).
- The server domain name is *HOSTNAME*_DOM.

You can change any of the defaults by using the instructions in the next few sections.

Note – Keep in mind that the instructions in this book are for Solaris servers and PC NetLink virtual servers *only*. For native Windows NT servers, you use the utilities provided in Windows NT Server Tools, Windows NT Administrative Tools, or Windows NT Server to promote and demote domain controllers; synchronize backup domain controllers with the PDC; add, remove, and rename domain controllers; and manage domain security, including account policy, audit policy, and trust relationships. Because these Windows NT tools are also effective within a domain that includes PC NetLink virtual servers, it is advisable to use them for most domain configuration tasks.

Adding, Removing, Renaming, and Moving Servers Within a Domain

If you used the Express installation program, you created a new domain within your Windows NT network, which was automatically designated as a PDC. You can add other computers and virtual servers to the domain.

You must add a computer running Windows NT Server or Windows NT Workstation software or a PC NetLink virtual server to the domain before it can participate in domain security. When you add a computer to a domain, the PC NetLink program creates a computer account for it. If the added computer is a BDC, it requests a copy of the domain directory database from the PDC. A member server does not store copies of the database.

Creating a New PC NetLink Virtual Server

A new feature in PC NetLink Version 2.0 enables you to create up to ten PC NetLink virtual servers on a Solaris physical host. The virtual servers can be in the same domain or in different domains, and can be backup domain controllers, member servers, or primary domain controllers (although there can be only one primary domain controller for each domain).

You do not use the installation procedure to create additional virtual servers, you use PC NetLink Server Manager or the `instancecfg` command at the Solaris physical host's root command prompt.

Before creating a new PC NetLink virtual server, you must decide on which Solaris physical host you want the new virtual server to run. Although a virtual server can run on any Solaris physical host in your network, you should consider load balancing and the host's configuration. In addition, some PC NetLink policies are configured for each physical host rather than for each virtual server. These policies include:

- NetBIOS
- PC NetLink Server Manager security
- Performance and alarms

Adding a Domain Workstation or Server Computer

To add a computer account to a domain, you must be logged on to a user account that has the appropriate user privileges. With the appropriate privileges, you can add workstations, servers, and PC NetLink virtual servers to domains after installation.

To add a PC NetLink virtual server to a domain, you can use either PC NetLink Server Manager or the `joindomain` command. You must be logged on as root. To reconfigure a PC NetLink virtual server to be a BDC in an existing domain without reloading the server software, you must furnish the Windows NT password for the target domain's Administrators or Account Operators group. The PDC must be running in the domain that is being joined.

You can also create a domain account for a computer so that when the computer joins the domain, the user will not need to furnish the Windows NT password. In this way, you can avoid giving the user this information when it is not required for other tasks. See "How to Add a Computer Account to a Domain" on page 173.

Removing a Computer From a Domain

You can remove accounts for workstations, BDCs, and member servers from a domain—but you cannot remove the PDC until you promote a BDC. See "How to Delete a Domain Member" on page 175.

When you remove a computer running Windows NT Workstation or Windows NT Server as a member server from a domain served by a PC NetLink domain controller, use PC NetLink Server Manager or the Network option in Windows NT Server Manager to delete the computer's account from the directory database or move it to a new workgroup or domain. This prevents the computer from participating in domain security.

Caution – To remove a *native* Windows NT BDC from a domain, you must delete the computer account and reinstall Windows NT Server or Windows NT Workstation on that computer, indicating the new domain. Do not continue to use a BDC that has been removed from a domain until you have reinstalled the operating environment software. For a PC NetLink virtual server BDC, however, you do *not* need to reinstall the software.

Changing the Name of a Domain or Server

You can locally change the domain name for every computer in a domain, move computers from one domain into another, or change the name of the server itself. To do so, you use either PC NetLink Server Manager, or the `setdomainname` or `setservername` command at the Solaris server's root command-line prompt. (For information about the commands, type `man setdomainname` or `man setservername` at the Solaris command prompt.)

Moving a Computer to a Different Domain

To change the domain to which a PC NetLink virtual server belongs, you use either PC NetLink Server Manager or the `joindomain` command locally at the physical host's root command prompt. (For information about the `joindomain` command, type `man joindomain` at the Solaris command prompt.)

After you have moved a workstation or member server from one domain served by a PC NetLink domain controller to another by way of either the `joindomain` command or PC NetLink Server Manager, you should delete its computer account from the PDC in its former domain.

Note that while a *native* Windows NT BDC cannot change domains unless Windows NT Server is reinstalled, PC NetLink BDCs can change domains without requiring the software to be reinstalled.

▼ How to Create an IP Address for a PC NetLink Virtual Server

If you plan to run multiple virtual servers on a Solaris physical host, you must configure multiple Internet Protocol (IP) addresses. A server that is a domain controller requires a unique IP address, but member servers on the same physical host can share an IP address.

To configure a virtual server's IP address:

1. **Request an available IP address on your subnet.**
2. **Using the command line, log on as root to the Solaris physical host for the PC NetLink virtual server.**
3. **Create the file** `/etc/hostname.`*devicedevice-number*`:`*alias-number* **and edit it with the host name assigned to the IP address you have reserved.**

   For example, the file might be named `/etc/hostname.hme0:1` and its contents might be `bert-2.`
4. **Add this IP address and host name to your local** `/etc/hosts` **file.**

   For example, the `hosts` file might contain the following:

```
#
# Internet host table
#
127.0.0.1      localhost
129.148.184.74 bert    loghost
129.148.184.157 bert-2
```

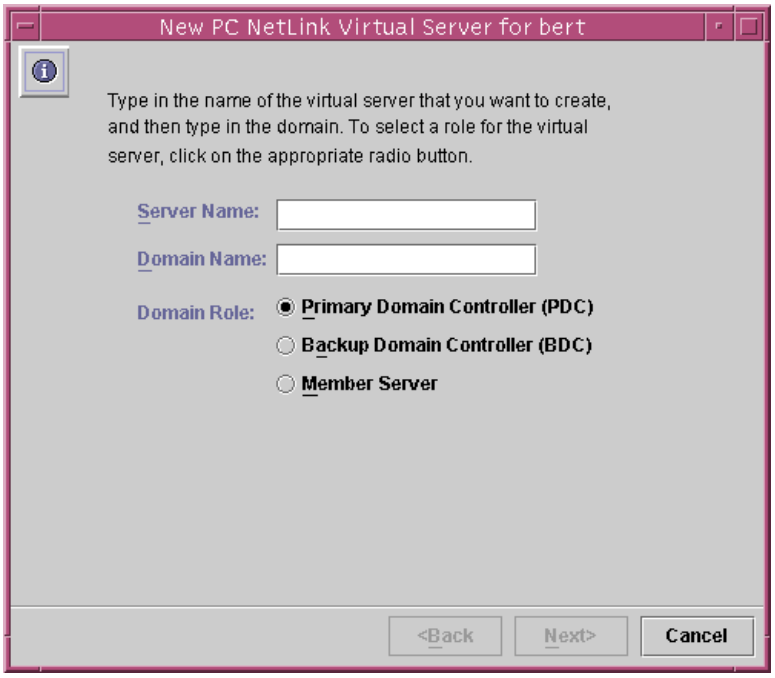
5. **Reboot the Solaris physical host.**

▼ How to Create a New PC NetLink Virtual Server

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host on which the PC NetLink virtual server that you want to create will run.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.
2. **In the Results pane, double-click New PC NetLink Virtual Server.**

   You can also choose New PC NetLink Virtual Server from the Action menu. A screen similar to the following appears.



3. **In the Server Name field, type a name for the new virtual server.**

   The interface will not allow you to use the following characters in a server name:

   - Space
   - Tab
   -] (right bracket)
   - [(left bracket)
   - / (slash)
   - \ (back slash)
   - * (asterisk)
   - : (colon)
   - + (plus sign)
   - ; (semicolon)
   - < (less-than sign)
   - > (greater-than sign)
   - , (comma)
   - ? (question mark)
   - " (double quote)
   - = (equal sign)

4. **In the Domain Name field, type the domain name for the new virtual server.**

   You can create a new domain, or make the new virtual server a member of an existing domain.

   The interface will not allow you to use certain characters in a domain name. See Step 3 for a list of invalid characters.

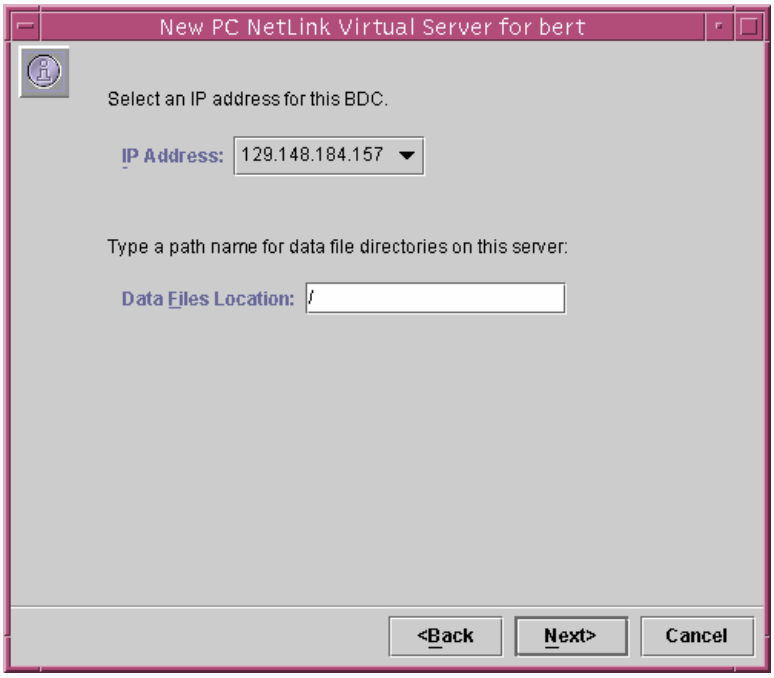
5. **Click the appropriate Domain Role button to designate the role of the server in the domain, according to the following guidelines:**

   When you create a new virtual server, you have three options: PDC, BDC, or Member Server. However, you cannot create a new virtual server as a primary domain controller if it will be a member of an existing domain that already has a primary domain controller.

   - If you make the server the PDC in a new domain, you will be prompted to create a password for its Administrator account.
   - If you make the server either a BDC or a member server in an existing domain, you will be prompted to furnish the PDC name and the password for the PDC's Administrator account if there is not already a valid computer account for that server on the PDC.
   - If you make the server a member server in a new or existing domain, you will be prompted to furnish a password to be used for the local administrative account on the member server.

6. **Click Next.**

   The following screen appears. (However, in a high availability (HA) environment, the software prompts you to select an HA logical host before this screen appears.)



7. **In the IP address menu, select an address from the list.**

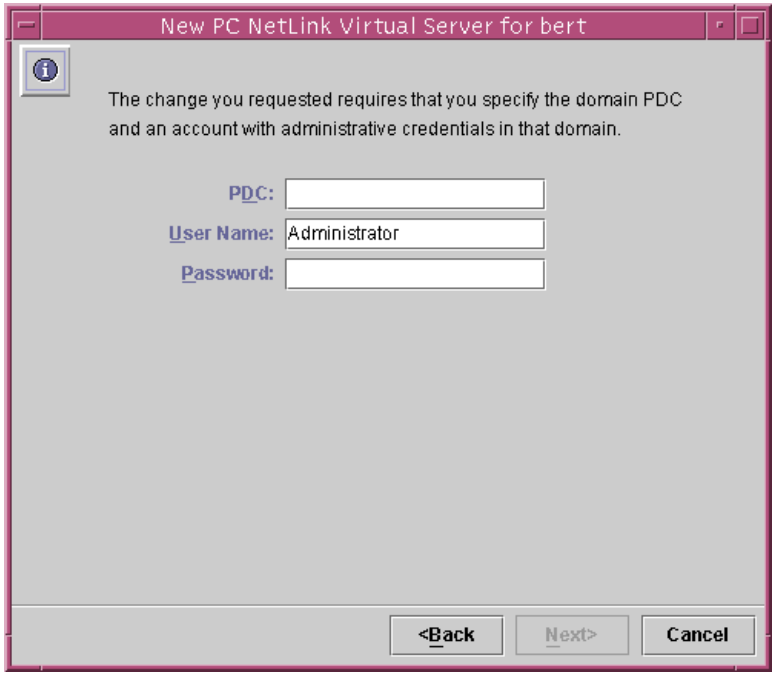
   Only addresses that are available to the new instance are listed. A server that is a domain controller requires a unique IP address.

8. **Type a path name for data file directories.**

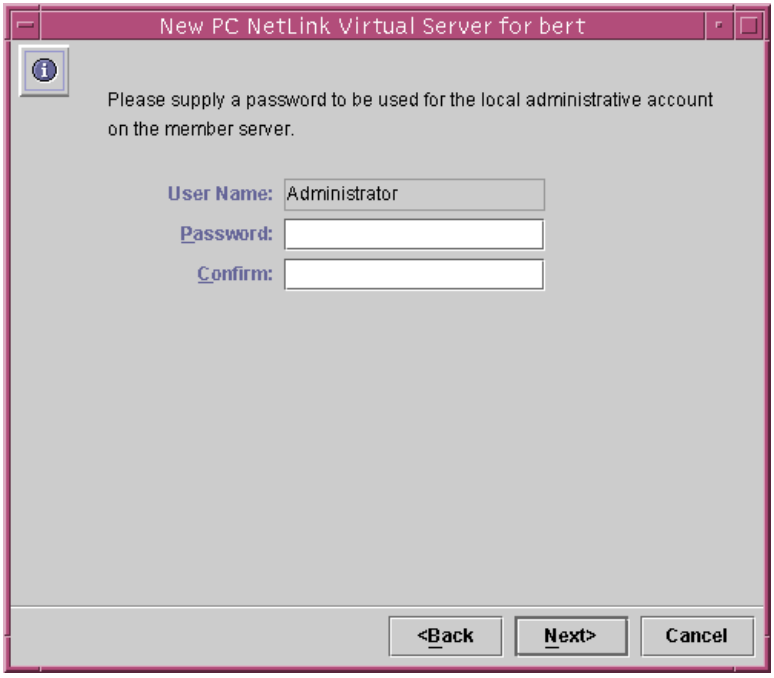
9. **Click Next.**

10. **Do one of the following:**

- *If you are creating a BDC or member server*, a screen appears that asks for information about the domain's PDC. Type the required information.

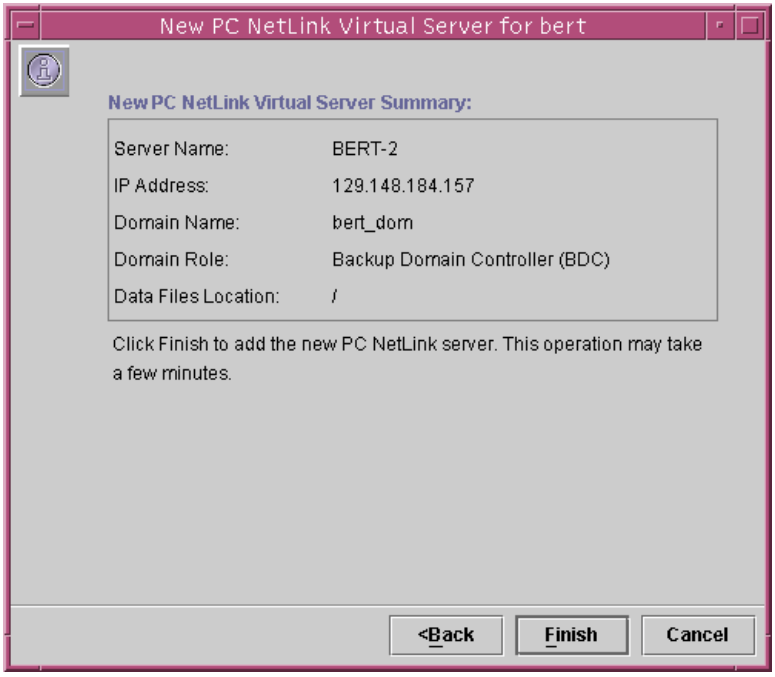


- *If you are creating a member server*, a screen appears that asks for a password for the local administrative account on the member server. Type the required information.



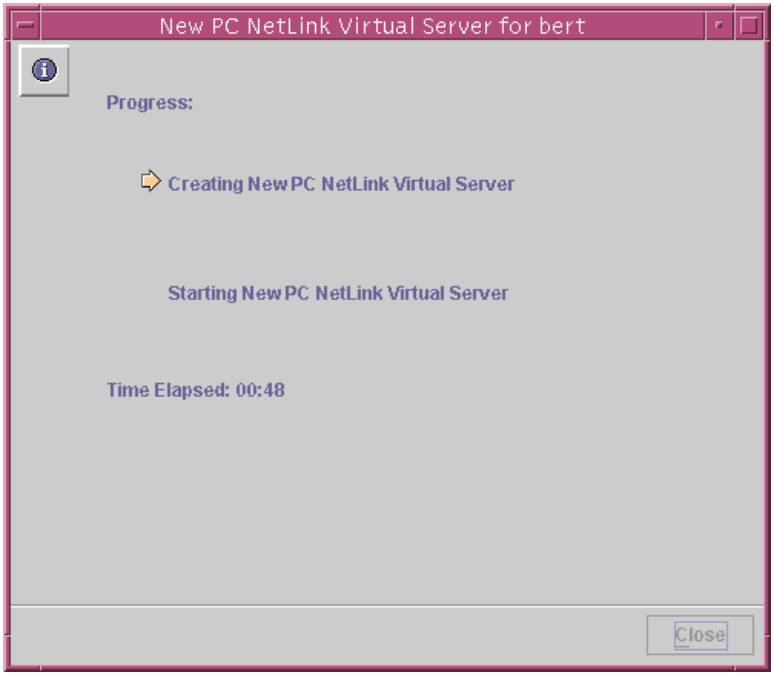
11. Click Next

The resulting screen summarizes the choices you have made.



12. **Click Finish to proceed with the virtual server creation, Back to make changes, or Cancel to abandon the procedure.**

    If you click Finish, the resulting screen informs you of the progress of the virtual server creation, marking pending activity with an arrow and completed activity with a check mark When the wizard finishes working, the new virtual server should have been created and started.



▼ How to Delete a PC NetLink Virtual Server

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that you want to delete.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, select the icon that represents the PC NetLink virtual server that you want to delete.**

3. **Choose Delete PC NetLink Virtual Server from the Action menu.**

   The software prompts for a confirmation. Users must be informed that the PC NetLink virtual server will be shut down, that client connections will be lost, and the instance will be irrevocably deleted. Note that it is possible to use this command to delete all virtual servers on a physical host.

▼ How to Rename a PC NetLink Virtual Server

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server whose name you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the PC NetLink virtual server.**

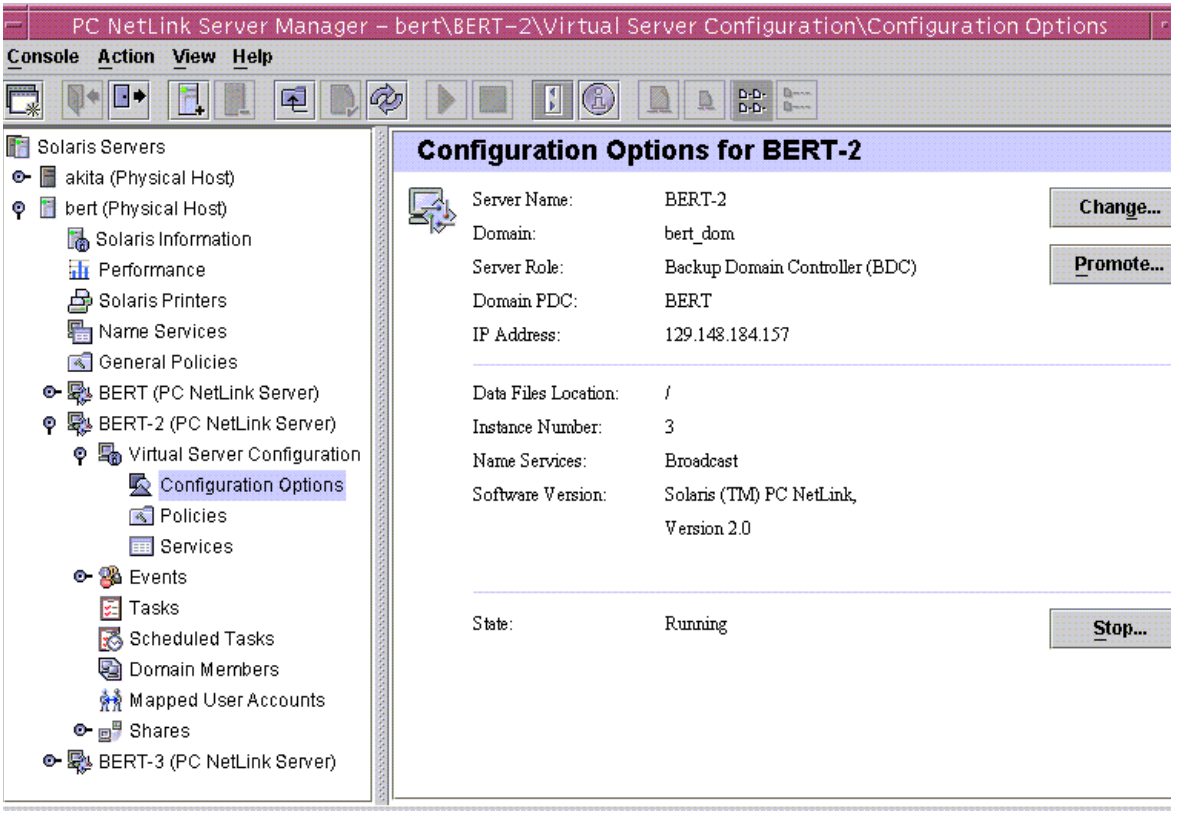
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

   The Results pane changes, displaying a list of three categories.

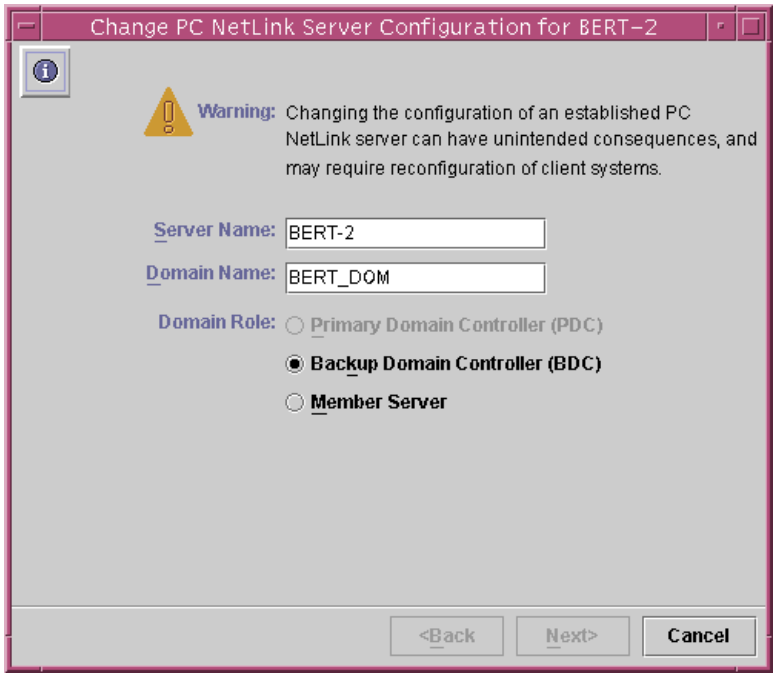
4. **Double-click Configuration Options.**

   The Configuration Options window appears, listing the virtual server's name, its IP address, the domain name, the system's role within the domain, and the version of PC NetLink software that it is running. It also displays the data files location and virtual server instance number on the physical host. If the system is either a BDC or a member server, the name of the domain's PDC is also listed. The State of the server can be either Running or Stopped.



5. **Click Change.**

   A screen similar to the following appears.



   Note that this same task wizard appears when you use the alternative method of changing server configuration; that is, by double-clicking Tasks and then double-clicking Change PC NetLink Server Configuration.

6. **In the Server Name text field, type the new server name, and then click Next.**

   See "How to Create a New PC NetLink Virtual Server" on page 67 for a list of disallowed server name characters. Note that merely changing the name of a PDC does not permit you also to change its role within its current domain.

   A screen appears that allows you to change the IP address of the server (optional).

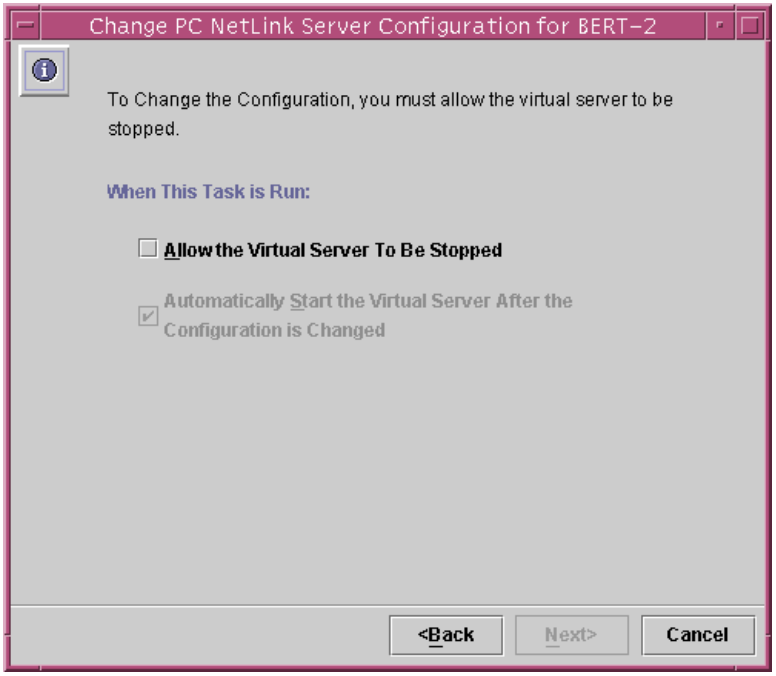
7. **Choose a new IP address for the virtual server (optional), and then click Next.**

8. **Depending on the role of the server whose name you are changing, do one of the following:**

   - *If you are changing the name of a PDC* – Skip to Step 10.
   - *If you are changing the name of a BDC or member server* – You must furnish information about the domain's PDC to add the new computer account to the directory database. Proceed to Step 9.

9. **Type the password for the domain PDC's Administrator account, and then click Next.**

   The resulting screen informs you that the PC NetLink program must be stopped and then restarted for the changes to become effective.

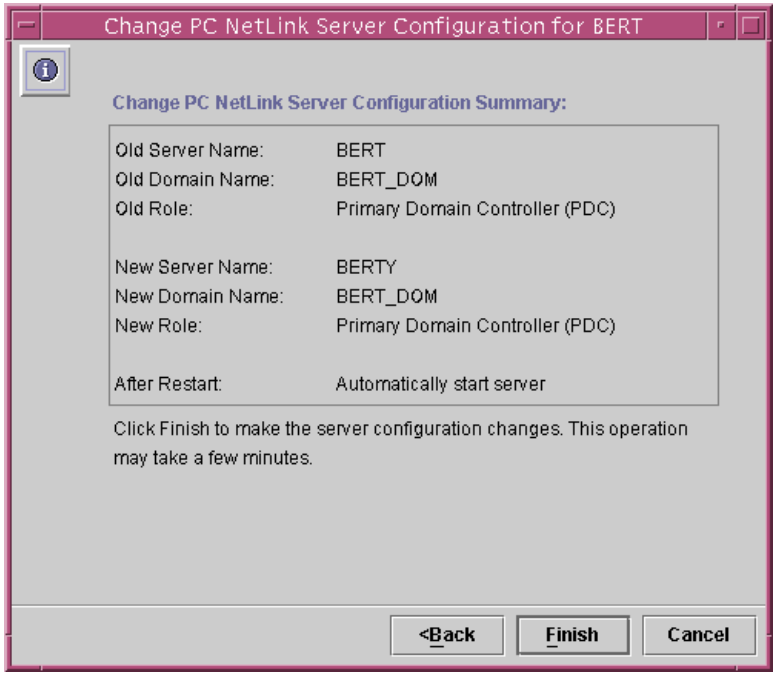


10. **Select Allow the Virtual Server To Be Stopped.**

    You must select this to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the configuration change. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the configuration change.

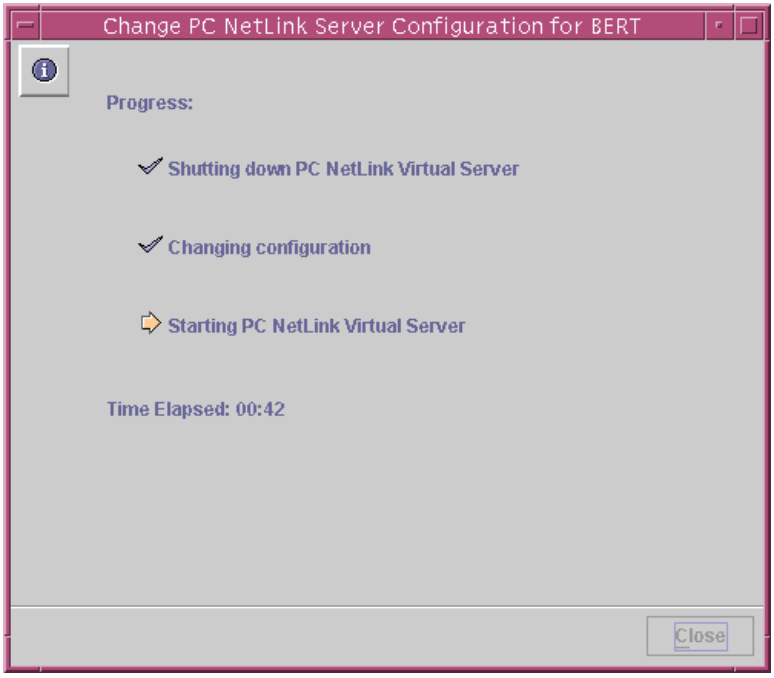
11. **Click Next to proceed with the name change, Back to make changes, or Cancel to abandon the procedure and leave the virtual server name and domain name unchanged.**

    If you continue the procedure by clicking Next, the resulting screen summarizes the choices you have made.



12. **Click Finish to proceed with the name change, Back to make changes, or Cancel to abandon the procedure and leave the server name and domain name unchanged.**

    The resulting screen informs you of the progress of the configuration change, marking pending activity with an arrow and completed activity with a check mark.



13. **(Optional) If you did *not* choose to have the PC NetLink virtual server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

▼ How to Move a Virtual Server to Another Domain

1. **Using PC NetLink Server Manager, log on to the Solaris physical host for the PC NetLink virtual server whose domain you want to change.**

    For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

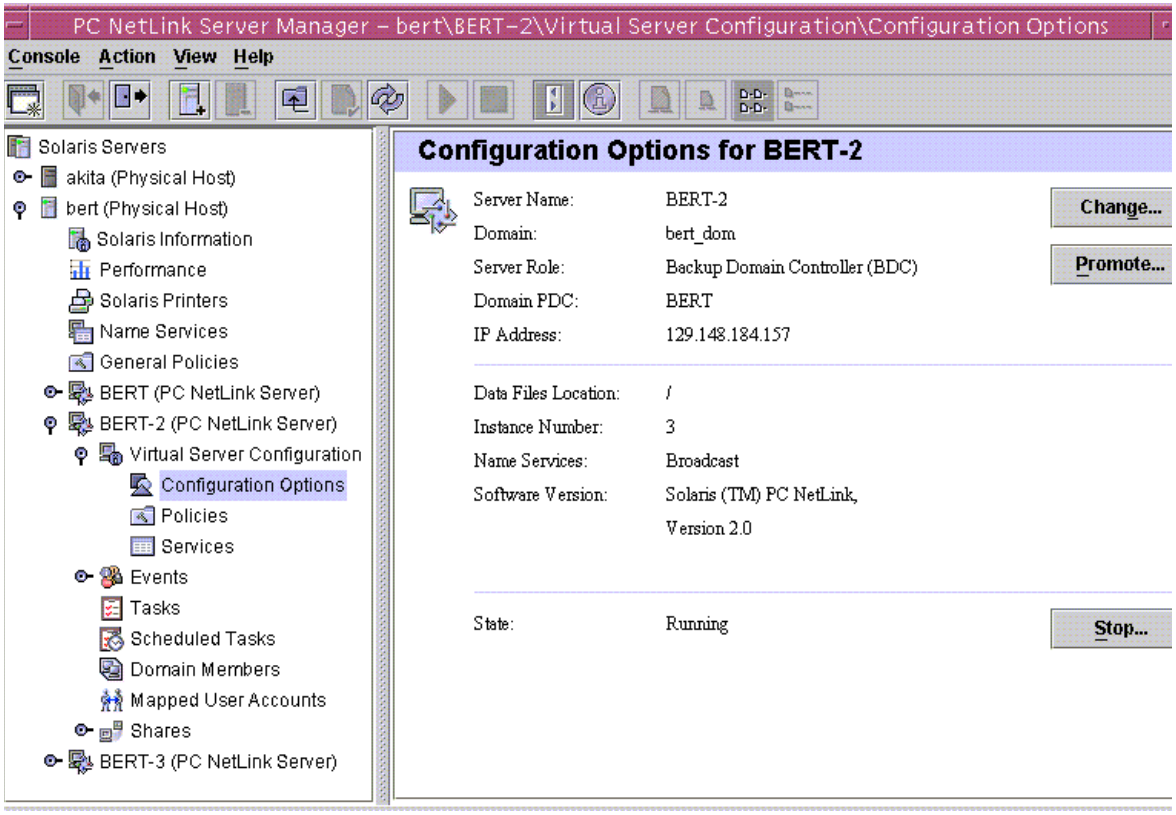
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

   The Results pane changes, displaying a list of three categories.

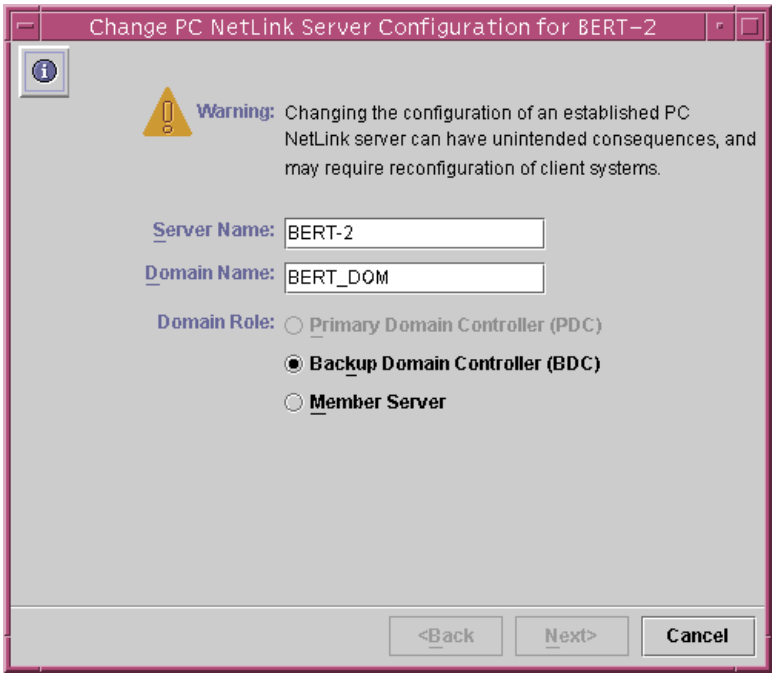
4. **Double-click Configuration Options.**

   The PC NetLinkConfiguration Options window appears, listing the PC NetLink system's server name, the domain name, the system's role within the domain, and the version of PC NetLink software that it is running. If the system is either a BDC or a member server, the name of the domain's PDC is also listed. The State of the server can be either Running or Stopped.



5. **Click Change.**

   A screen similar to the following appears.



6. **In the Domain Name text field of the dialog box, change the server's domain name according to the following guidelines:**

   - By changing the domain name of the server, you are effectively reassigning it to the domain whose name you type.
   - By changing domains, you may also designate a new role for the server within its new domain.
   - A domain name can be up to 15 characters long, but cannot include the following characters:
     - Space
     - Tab
     -] (right bracket)
     - [(left bracket)
     - / (slash)
     - \ (back slash)
     - * (asterisk)
     - : (colon)
     - + (plus sign)
     - ; (semicolon)

- < (less-than sign)
- > (greater-than sign)
- , (comma)
- ? (question mark)
- " (double quote)
- = (equal sign)

- To complete a change to the name of a domain served by a PC NetLink domain controller, you must use this procedure on *every* PC NetLink virtual server within the domain, then use the Network option in the Windows NT Control Panel to change the domain name on every Windows NT Workstation and Windows NT Server computer within the domain. For Windows 98 clients, you change the name of the Windows NT domain in the Network Properties of Microsoft Network Client. You must then reestablish existing trust relationships.

7. Click the appropriate Domain Role button to designate the role of the server in its new domain, according to the following guidelines:

When you change the virtual server's domain, you have three options: PDC, BDC, or Member Server.

- If you make the server the PDC in its new domain, you will be prompted to create a *new* password for its Administrator account.
- If you move an existing domain's PDC into a different domain, you must also promote the BDC in the existing domain to become that domain's PDC. See "How to Promote a BDC Within Its Domain" on page 89.
- If you make the server either a BDC or a member server in the domain to which you are moving it, you will be prompted to furnish the password for that domain PDC's Administrator account if there is not a vaild computer account of that role for this server already.
- If you make the server a member server in its new domain, you will be prompted to furnish a *new* password to be used for the local administrative account on the member server.

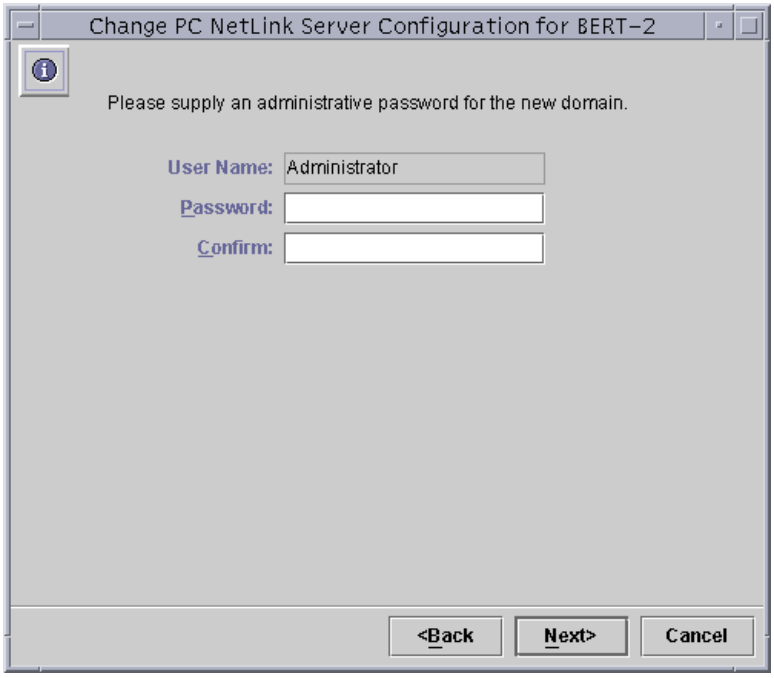
8. Click Next.

A screen appears that allows you to change the IP address of the server (optional).

9. Choose a new IP address for the virtual server (optional), and then click Next.

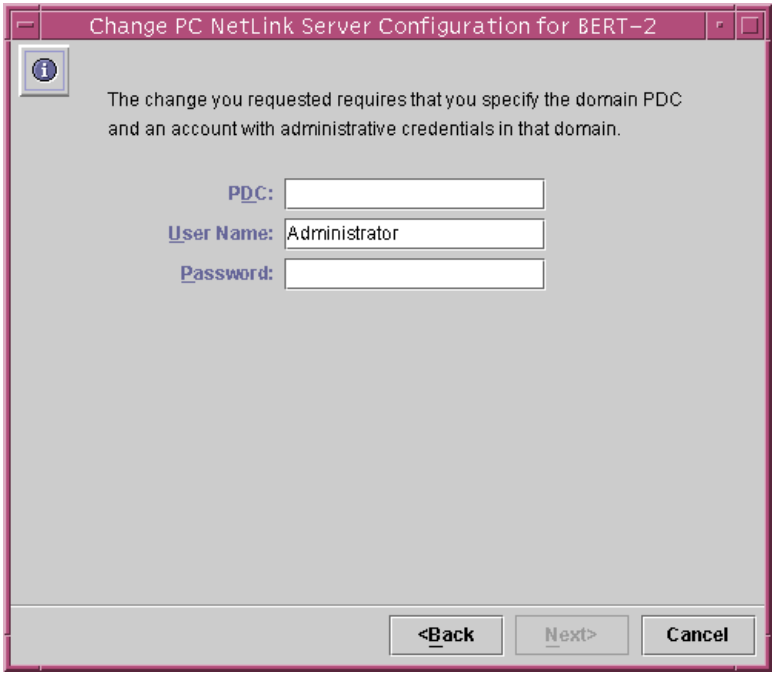
10. **Depending on the role you selected for the server in its new domain, do one of the following:**

    - *If PDC*, furnish the *new* password for the server's new role in both password text fields in the following screen.

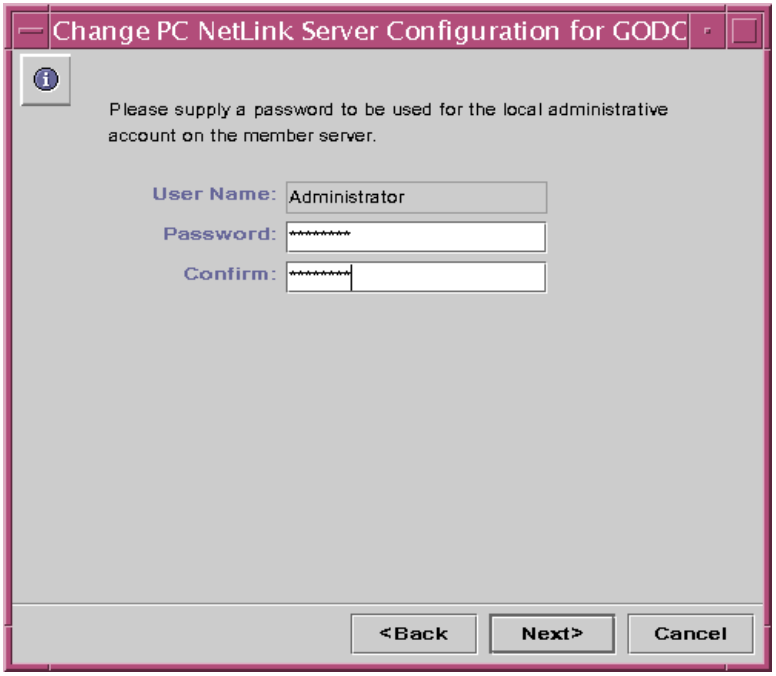


Note that you cannot assign more than one PDC to a single domain. If you are moving an existing domain's PDC to another domain, remember to promote the existing domain's BDC to become the domain's PDC. See "How to Promote a BDC Within Its Domain" on page 89. A server that is a domain controller requires a unique IP address.

- *If BDC or Member Server*, type the Administrator account user name and password for the PDC that exists in the domain to which you are moving the server, if there is not already a valid computer account for that server on the PDC. A server that is a domain controller requires a unique IP address, but a member server does not.

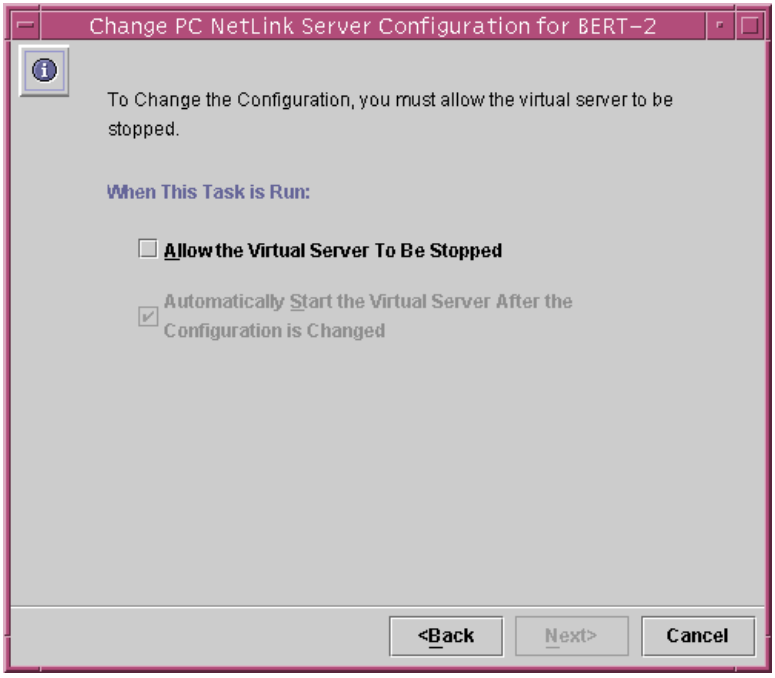


- *If Member Server,* you must also furnish a *new* password to be used for the local administrative account on the member server.



11. **Click Next.**

The resulting screen informs you that the PC NetLink virtual server must be stopped and then restarted for the changes to become effective.

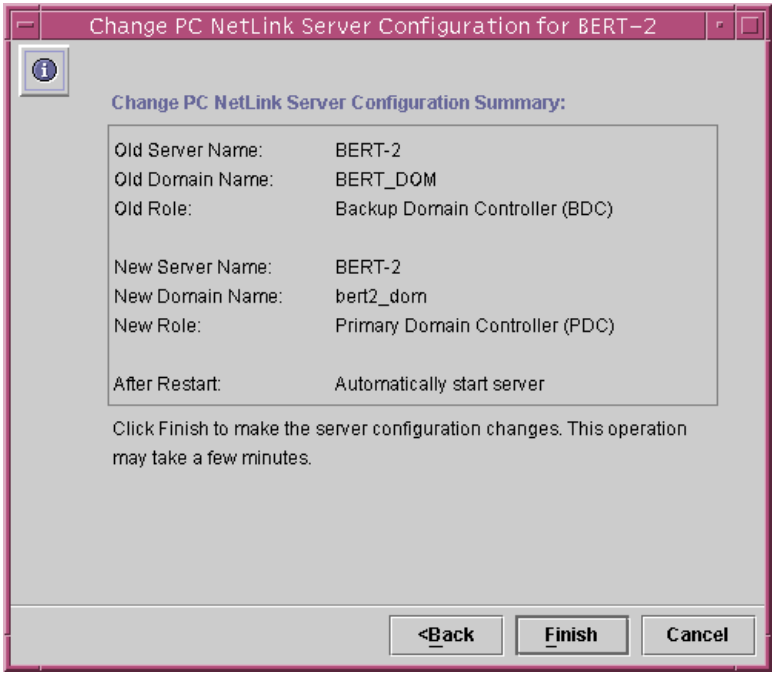


12. **Select Allow the Virtual Server To Be Stopped.**

You must select this to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the configuration change. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the configuration change.

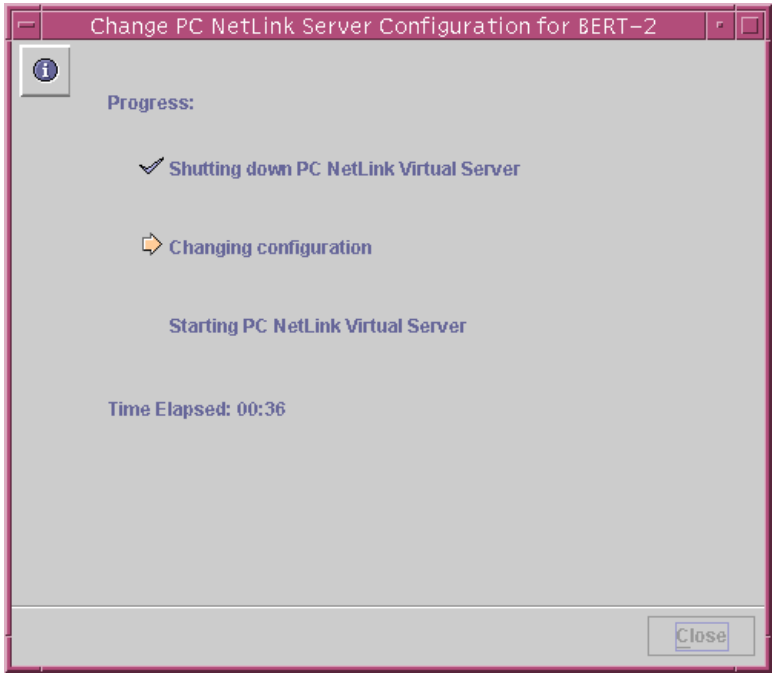
13. **Click Next to proceed with the configuration change, Back to make changes, or Cancel to abandon the procedure and leave the server configuration unchanged.**

    If you continue the procedure by clicking Next, the resulting screen summarizes the choices you have made.



14. **Click Finish to proceed with the name change, Back to make changes, or Cancel to abandon the procedure and leave the configuration unchanged.**

    The resulting screen informs you of the progress of the configuration change, marking pending activity with an arrow and completed activity with a check mark.



15. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

▼ How to Promote a BDC Within Its Domain

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that you want to promote.**

    For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

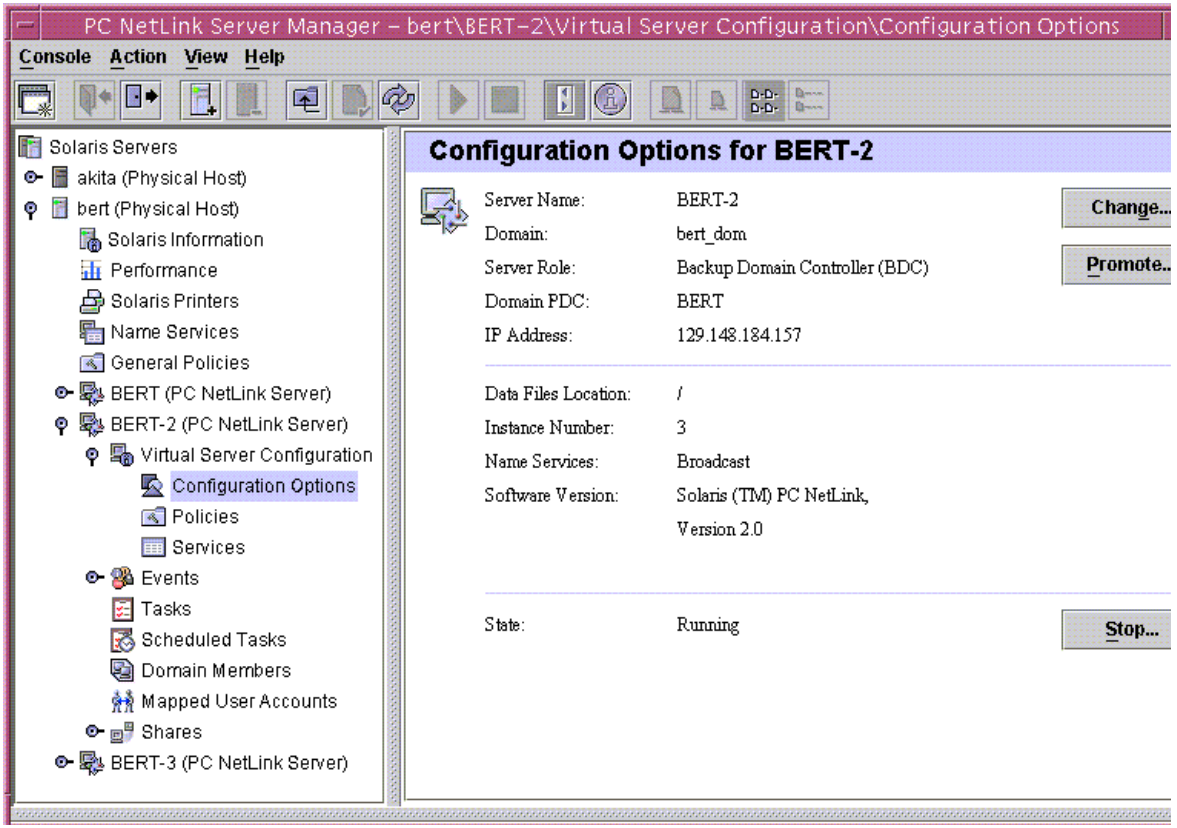
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

   The Results pane changes, displaying a list of three categories.

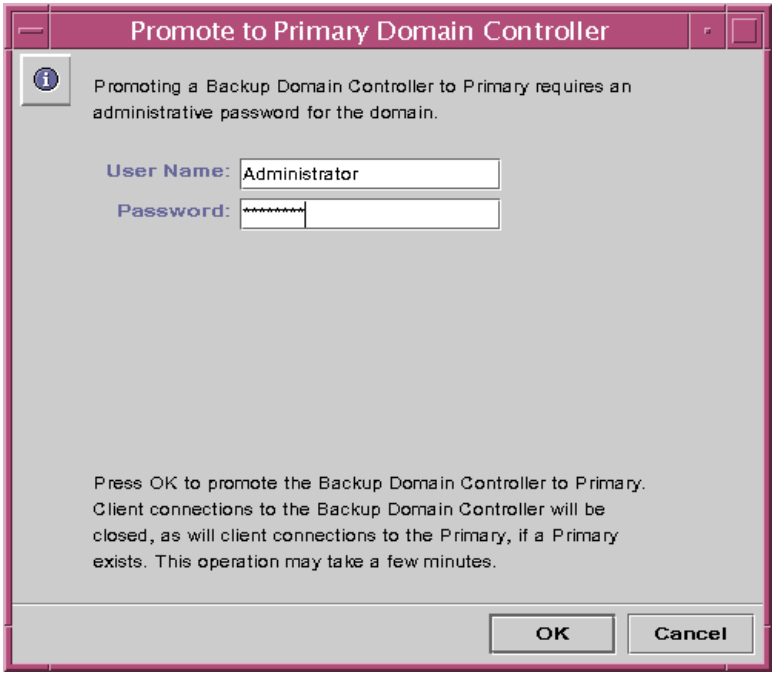
4. **Double-click Configuration Options.**

   The PC NetLink Configuration Options window appears, listing the PC NetLink system's server name, the domain name, the system's role within the domain, the version of PC NetLink software that it is running, and the name of the domain's PDC. The State of the server can either be Running or Stopped. In the example below, the server's name is BERT-2 and its role is BDC in the bert_dom domain. The domain's PDC is the server named BERT.



5. **Click Promote to change the role of a backup domain controller to a primary domain controller.**

   The following screen appears, prompting for the password for the Administrator account on the *current* PDC.



6. **Click OK to continue the promotion, or Cancel to halt it.**

   If you click OK, all client connections to the BDC and the current domain's PDC will be closed while the configuration change, which takes several minutes, is being made.

▼ How to Change the Role of a Server Within Its Domain

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that you want to promote.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

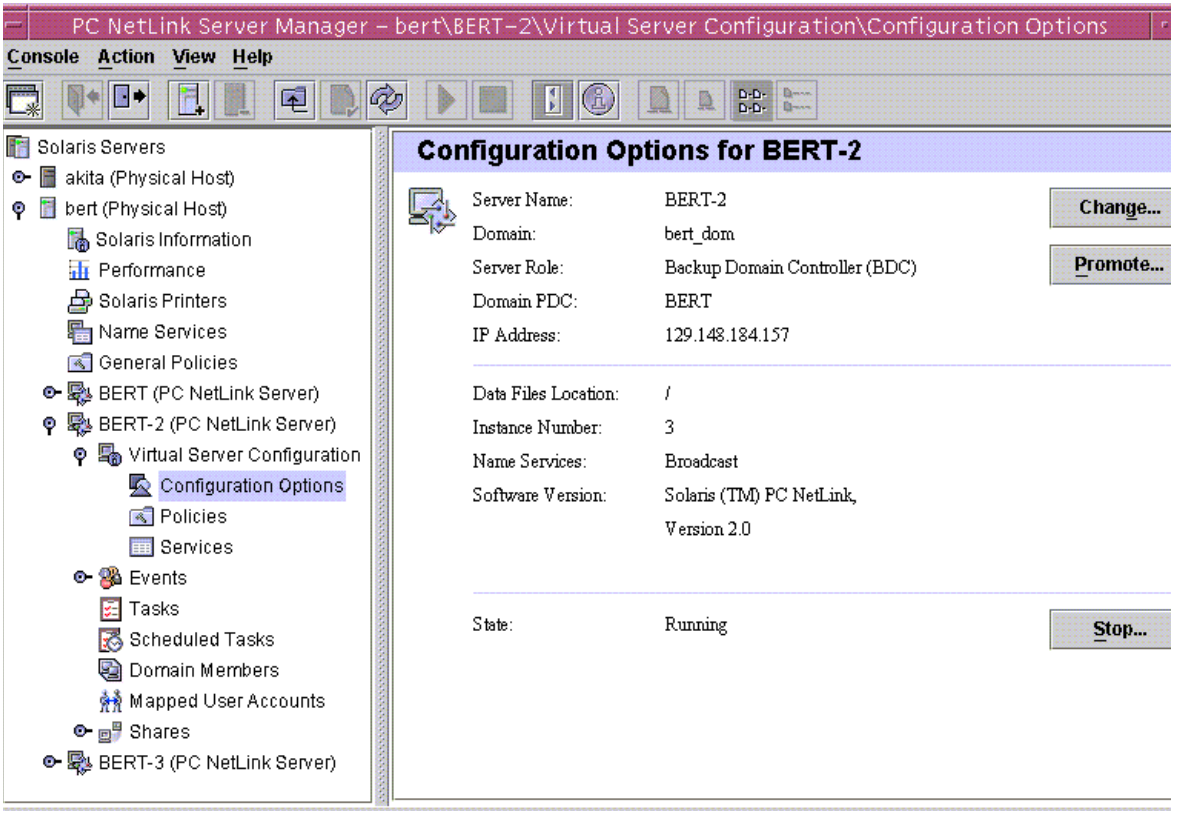
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

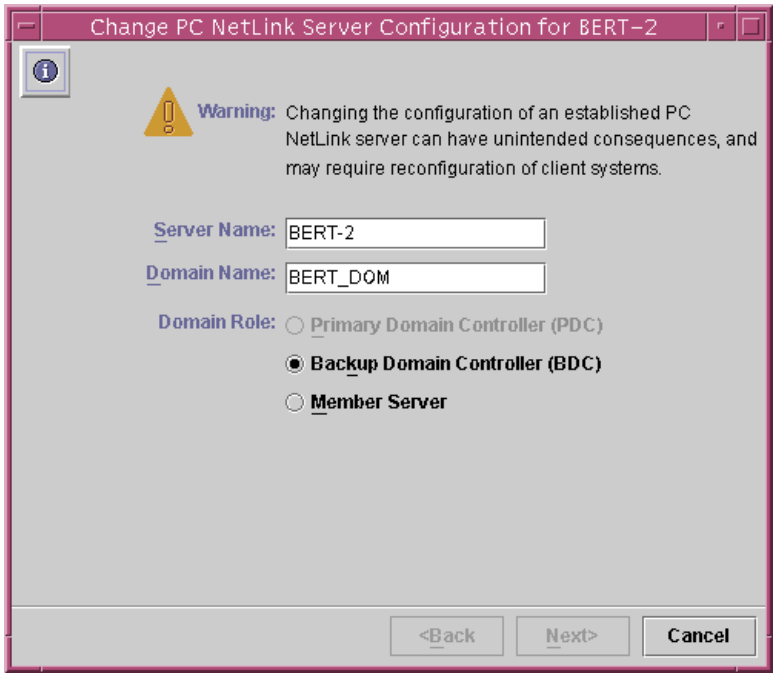
   The Results pane changes, displaying a list of three categories.

4. **Double-click Configuration Options.**

   The PC NetLink Configuration Options window appears, listing the PC NetLink system's server name, the domain name, the system's role within the domain, and the version of PC NetLink software that it is running. If the system is either a BDC or a member server, the name of the domain's PDC is also listed. The State of the server can either be Running or Stopped. In the example below, the virtual server's name is BERT-2 and its role is BDC in the bert_dom domain.



5. **Click Change to change the role of a backup domain controller or member server.**



6. **Click on the radio button for the new server role.**

   A screen appears that allows you to change the IP address of the server (optional).

7. **Choose a new IP address for the virtual server (optional), and then click Next.**

8. **Click Next.**

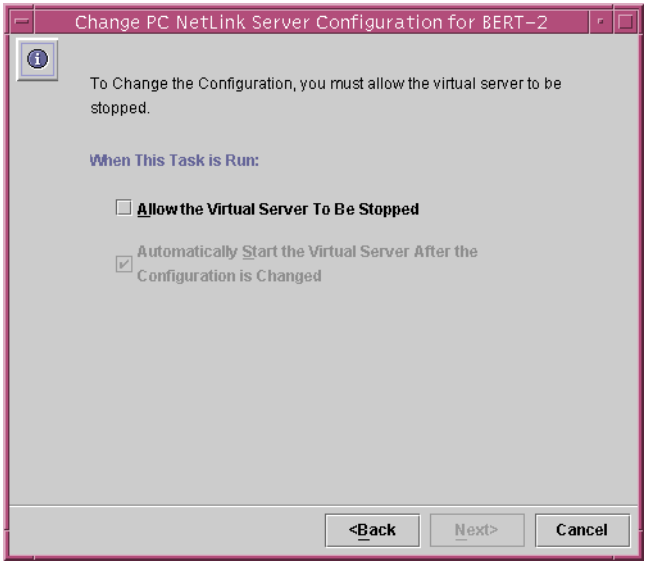
   If there is not a vaild computer account of that role for this server already, a screen appears that prompts you for the password for the Administrator account on the domain PDC.

9. **Type the password and click Next.**

10. **If you are changing the server's role to member server, type the password to use for the new administrative account in the next screen, and confirm it.**

11. **Click Next.**

    The resulting screen informs you that the PC NetLink program must be stopped and then restarted for the changes to become effective.



12. **Select Allow the Virtual Server To Be Stopped.**

    You must select this to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the configuration change. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the configuration change.

13. **Click Next to proceed with the configuration change, Back to make changes, or Cancel to abandon the procedure and leave the server configuration unchanged.**

14. **If you continue the procedure by clicking Next, the resulting screen summarizes the choices you have made. If the changes are what you intend, click Finish.**

    All client connections to the server will be closed while the configuration change, which takes several minutes, is being made. If you chose not to automatically restart the server, you must restart the server manually to complete the configuration change.

▼ How to Create a Directory Share

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server on which you want to create a directory share.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **In the Results pane, double-click Shares.**

4. **Double-click Directory Shares.**

5. **Double-click Share a Directory.**

6. **In the dialog box, type a name for the new directory share.**

   Note that you cannot use the following characters in a directory share name:

   - / (slash)
   - \ (back slash)
   - " (double quote)
   - : (colon)
   - | (vertical bar)
   - < (less-than sign)
   - > (greater-than sign)
   - ? (question mark)
   - * (asterisk)
   - [(left bracket)
   -] (right bracket)
   - + (plus sign)
   - = (equal sign)
   - ; (semicolon)
   - , (comma)

7. **Type the directory to share, or browse for it.**

8. **Click Next.**

9. **In the next screen, specify how many users can access this share at a time, and add a comment if desired.**

10. **Click Next to proceed, Back to make changes, or Cancel to abandon the procedure and leave the server configuration unchanged.**

    If you continue the procedure by clicking Next, the resulting screen summarizes the choices you have made.

11. **Click Finish to proceed with the operation, Back to make changes, or Cancel to abandon the procedure and leave the configuration unchanged.**

    The resulting screen informs you of the progress of the configuration change, marking pending activity with an arrow and completed activity with a check mark.

▼ How to Modify a Directory Share

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that has the directory share.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **In the Results pane, double-click Shares.**

4. **Double-click Directory Shares.**

5. **Double-click the directory share you want to modify.**

6. **Modify one or more of the settings in the Properties dialog box, then click OK.**

   The directory share is modified. Note that you cannot use the following characters in a directory share name:

   - / (slash)
   - \ (back slash)
   - " (double quote)
   - : (colon)
   - | (vertical bar)
   - < (less-than sign)
   - > (greater-than sign)
   - ? (question mark)
   - * (asterisk)
   - [(left bracket)
   -] (right bracket)
   - + (plus sign)
   - = (equal sign)
   - ; (semicolon)
   - , (comma)

▼ How to Delete a Directory Share

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server that has the directory share.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **In the Results pane, double-click Shares.**

4. **Double-click Directory Shares.**

5. **Select the share you want to delete.**

6. **Choose Delete Directory Share from the Action menu.**

   The directory share is deleted.

About Managing Policies

You can define the following six sets of PC NetLink policies individually for each virtual server on a Solaris physical host:

- Computer browsing
- File name mapping
- Performance tuning
- Solaris file system integration
- UPS power failure notification
- User accounts policy

You can also define the following three sets of PC NetLink policies that affect all virtual servers running on a Solaris physical host:

- NetBIOS
- PC NetLink Server Manager security
- Performance and alarms

The instructions in this guide for managing these policies relate to, and affect, only your PC NetLink program—not the Windows NT network itself. You continue to administer Windows NT network policies in the manner and with the tools to which you are accustomed. Windows NT policies that are not covered in this guide include:

- User password (account)
- Audit
- Trust relationships

About Managing Virtual Server Policies

You set each policy described in this section independently for each virtual server.

Computer Browsing

Computer browsing is the process of checking domains, workgroups, and computers to look for shared directories and printers. Networks, domains, workgroups, computers, and shared directories are organized in a tree structure. You choose a network name to display available domains and workgroups, a domain or workgroup name to display available computers, or a computer name to display its shared directories.

A *master browser* maintains the tree-structure list and updates the *backup browsers*. Users of network client computers are viewing this list when they look at their Network Neighborhood.

Computer browsing policy for a PC NetLink virtual server involves setting the frequency that the master browser updates its list, the frequency that a backup browser copies the list from the master browser, and the level of browsing event detail that you want to be included in the System log.

File Name Mapping

In Solaris system files and directories, you can have names of up to 255 characters, far greater than the MS-DOS operating system 8.3 standard. To ensure access to all Solaris files by all applications, the PC NetLink program provides *file name mapping*: Each file or directory with a name that does not conform to the MS-DOS 8.3 standard automatically is given a second name that does conform.

Note, however, that the PC NetLink program does not generate short names for *share* names that do not conform to MS-DOS naming standards, but only for files and directories with long names. When naming a share, use the 8.3 standard to avoid potential file name conflicts.

PC NetLink file name mapping allows applications that do not support long file names to access files with such names. These applications refer to files that have long names by their shorter names.

Note – If an application that does not support long file names opens a file with a long name and then saves the file, the long name is lost and only the short name remains.

PC NetLink file name mapping is composed of the following three elements:

- Mixed-case support
- Mapping Solaris system file names to the 8.3 convention
- Mapping Solaris system file names containing characters that are unacceptable in Windows NT to names that are acceptable to Windows NT

The challenge of mapping between name spaces is resolved on Solaris systems by concatenating a truncated file name with a pseudo-unique suffix, which is generated dynamically from the i-node number of the Solaris system file.

File Name Mapping Rules

For mapping Solaris system file names to 8.3-type file names, the following default rules apply:

- Spaces are removed from the name.
- Periods are removed, except for the last one followed by at least one character.
- Invalid characters are replaced by underscores (_).
- The name, not including suffix, is truncated; a tilde (~) separator and a combination of numbers (0 - 9) and letters (A - Z) are appended.
- The suffix (the characters following the tilde separator) is truncated to three characters.

For example, the file name *longfilename.txt* and i-node number of 11455, would have a mapped name of *long~8u7.txt*.

For mapping from Solaris system file names to Windows NT-style file names, the following default rules apply:

- Invalid characters are replaced by underscores (_).
- A mapping separator (a tilde by default) and a combination of numbers (0 - 9) and letters (A - Z) are appended to the name, not including the extension.
- The extension is preserved.

For example, the file name *k<l<m.expression* and i-node number of 8461 would have a mapped name of *k_l_m~6j1.expression*.

Considerations for Using Mixed-Case Support

A decision on whether your virtual server should continue to support mixed-case file names—which is the default in the PC NetLink program—should be considered carefully. Mixed-case support allows clients to have access to file names on Solaris systems that contain uppercase characters, but turning off this feature could improve server performance.

It is inadvisable to switch frequently between enabled mixed-case support and disabled mixed-case support on the same server. While mixed-case support is enabled, clients can create files with mixed-case names. These files will become unavailable to them as soon as mixed-case support is disabled. If mixed-case support is changed from enabled to not enabled, every existing file name should be made lowercase.

Do not create file names in the same directory that are identical except for case. Although the Solaris operating environment is case-sensitive, PC NetLink mixed-case support causes the server to preserve case but behave in a case-insensitive way, just like Windows NT. Microsoft product users are not aware of the possibility of

having case-insensitive similar file names in a directory, because Windows NT does not allow such files. As a result, users may become confused if they access incorrect files or are denied access to files they need.

Tuning PC NetLink Parameters for Optimum Performance

Tuning the performance of a complex computer system is a difficult task requiring specialized knowledge. The Performance Tuning interface of PC NetLink Server Manager (see "How to Tune PC NetLink for Optimum Performance" on page 112) lets you make some simple adjustments. You can also view ongoing performance data by way of PC NetLink Server Manager, and adjust performance thresholds that, when exceeded, generate alarms (see "How to Monitor Physical Host Performance" on page 156).

Editing appropriate parameters in the PC NetLink Registry and the `lanman.ini` file gives you much more control over performance, but this should only be undertaken by knowledgeable persons.

Following is a cursory introduction to the concepts involved. For a full treatment of the subject, refer to *Sun Performance and Tuning*, Prentice Hall, ISBN 0130952494.

Processes and Virtual Circuits

PC NetLink software runs on a Solaris-based server and provides file and print services to PC clients. For the purposes of tuning system performance, it helps to think of PC NetLink as a collection of *processes*, each being an independent agent responsible for handling requests from one or more clients.

When a client requests a service—perhaps the opening of a file—PC NetLink software establishes a connection between the requesting client and the appropriate process. That connection is known as a *virtual circuit*.

Of the several factors that can affect performance, the two most important may be the total number of processes running on the computer and the number of virtual circuits per process.

The situation is analogous to a large telephone switchboard in the days before electronic switches replaced human operators. Each process can be thought of as an operator, with each call arriving at the switchboard being a virtual circuit.

If the number of phone calls is great, the average time it takes for the operator to respond to a specific call increases, reducing performance.

One way to prevent the operators from being bogged down is to limit the number of simultaneous calls that can arrive at the switchboard. In essence, this is what the slider does in the PC NetLink Server Manager Performance Tuning tab labeled Speed-Memory Balance (see page 113).

As you adjust this slider, you change two Registry parameters called `MinVCPerProc` and `MaxVCPerProc` (see "Registry Keys and Values" on page 308 in Appendix A, "PC NetLink Registry"), limiting the number of virtual circuits per process. These changes, which take effect upon restarting PC NetLink software, are dynamically reflected in the Technical Details display area.

Of course, reducing the number of virtual circuits per process may mean that you'll need more processes to handle the overall volume of client requests.

A given server can handle only so many processes. Each process requires a fixed amount of memory and computational resources. You can do serious harm to your system by pushing it to run more processes than it can accommodate. To help you prevent this, the statistic, Maximum Processes per Server (Derived), is shown in the Technical Details display area.

Note that the `lanman.ini` file parameter, `maxclients` (see "File Parameters" on page 30) also has a bearing on the total number of processes running on the server at any time.

Client Workload

Some applications make unusually high demands on PC NetLink for file and print services. These applications include engineering CAD programs, video server software, and benchmarking tools.

When clients run demanding applications like those, PC NetLink's responsiveness may be less than what you would expect given the number of clients being supported. In such cases you may need to set Performance Tuning policy's Speed-Memory Balance slider further toward Optimize for Speed to achieve reasonable performance. See "How to Tune PC NetLink for Optimum Performance" on page 112 for details.

Solaris File System Integration

You can control the access that users have to files and directories on PC NetLink servers by securing them through *permissions*.

Every permission that you set specifies the access that a group, user, or others can have to the directory or file. For example, when you set Read permission for the group called `Coworkers` on the file `MY_IDEAS.DOC`, the users in that group can display the file's data and attributes, but they cannot edit the file or delete it.

The PC NetLink program offers the following permissions that you can set on directories and files for users, groups, and others:

- *Read (R)* – Allows individuals or groups to see the file or contents of a folder, but not to edit, delete, or execute it

---

Note – In the Solaris operating environment, Read permission is far more restrictive than the similarly named permission in the Windows NT environment. In the Windows NT environment, Read permission is advisory only—a user on a Windows NT client machine would still be able to edit a nominally Read-only file. In the Solaris environment—the environment in which all PC NetLink files and directories are stored and managed—a user would be prohibited from editing a Read-only file. You can override the more restrictive Solaris permissions to become fully compatible with Windows NT-style permissions, however. See "How to Set Solaris File System Integration Policies" on page 114 for instructions.

- *Write (W)* – Allows individuals or groups to see and edit the file or contents of a folder
- *Execute (X)* – Allows individuals or groups to run executable programs, but not to see or edit the code itself
- *Full Access (RWX)* – Allows individuals or groups to see, edit, and run any file, directory, or executable program so designated
- *No Access* – Denies all permission (achieved by not setting any of the above permissions)

You establish permissions on files and directories, but the permissions that you establish actually affect the computer users. The Solaris operating environment differentiates among people to whom the permissions apply:

- *User* – If you own a Solaris system file or directory, you can assign it access permissions for yourself. For example, to prevent unauthorized users from executing a program, you can assign Execute permission to yourself only.
- *Group* – This setting, in the context of the PC NetLink program, is not the same as Group permission in the Solaris operating environment. In the Solaris file system, Group permission grants to other members of your Solaris group access to files and directories that you own. In the PC NetLink environment, however, *Windows NT* groups—not Solaris groups—are created, and Solaris Group permission has no effect on them.

- *Other* – You can assign access permissions to files and directories that you own for all Solaris system users other than yourself and the users in your group. Depending on your needs, you can allow these other users to read or change your files and directories or you can prevent such access. Restricting access to others does not affect your own access to the files and directories.

Standard permissions are combinations of individual permissions that depend on the nature of the files and directories and the makeup of groups. To work effectively with PC NetLink file and directory security, keep the following points about setting permissions in mind:

- Users cannot use a directory or file unless they have been granted permission to do so or belong to a group that has permission to do so.
- Permissions are cumulative, except that setting a No Access permission—not indicating Read, Write, or Execute on a file or directory—overrides all other permissions. For example, if the `Coworkers` group has Write permission for a file while the `Finance` group has only Read permission, and John is a member of both groups, John will be granted Read and Write permissions. However, if you remove the `Finance` group's only permission for the file to effectively become No Access, John will not be able to use the file—even though he is a member of a group that has access to it.
- When you create files and subdirectories in a PC NetLink directory, they inherit permissions from the directory. For example, if you add a file to a directory that allows the `Coworkers` group Write permission and the `Finance` group Read permission, the same permissions will apply to the file.
- The user who creates a file or directory is ordinarily the owner of that file or directory—though you can change that default. The owner can control access to the file or directory by changing the permissions set on it.
- The easiest way to administer security is to set permissions for groups, not individual users. Typically, a user needs access to many files. If the user is a member of a group that has access to the files, you can terminate the user's access by removing the user from the group rather than by changing the permissions on each of the files. Note that setting permissions for an individual user does not override the access granted to the user through groups to which the user belongs.

Note – When you copy PC NetLink files or directories, security permissions set on them are discarded in addition to ownership and auditing information. The files inherit a new set of permissions from the directory into which you have copied them. If the new directory does not specify permissions for files, only a file's owner (the person who copied the file) will have permission to use the file.

In addition to files and directories, shares carry their own permissions in a Windows NT environment. In case of permission conflicts among files, directories, and shares, clients see the *most* restrictive permissions among the conflicting sets.

Ownership of Files and Directories

Every file and directory has an *owner*. The owner controls how permissions are set on the file or directory and can grant permissions to others.

When a file or directory is created, the person creating the file or directory automatically becomes its owner. It is expected that administrators will create most files on network servers, such as when they install applications on the server. Therefore, most files on a server will be owned by administrators, except for data files created by users and files in users' home directories.

Ownership can be transferred in the following ways:

- The current owner can grant an implied ownership ability to other users by setting Write permission on the files or directories for Group or Others. This enables other people to copy the file, and "inherit" ownership of the duplicate.
- An administrator can take ownership of any file on the computer at any time. For example, if an employee leaves the company suddenly, the administrator can take control of the employee's files, no matter what permissions have been set.

Note – Although an administrator can take ownership, the administrator cannot transfer ownership to others. This restriction keeps the administrator accountable.

The administrator also can take file ownership by using the `net perms` command. For more information, type `net help perms` at the PC NetLink command prompt.

In addition to files and directories, computer *processes* also have an owner. A computer process is initiated whenever an executable program is run, and the process is known to the system by a unique identifier. In the Solaris environment, this is called a *Process Identifier*, or *PID*.

Unlike file or directory ownership, however, process "ownership" changes whenever the program is executed. While an executable program—a spreadsheet, for example—is originally owned by the person who installed it on the network, its User and Group PID ownership changes when a person runs it. The spreadsheet process owned by root at installation will now be owned by the user and the user's group at execution. Because this change in process ownership has security implications, the PC NetLink program enables you to regulate it.

File-locking is also an important security concern, particularly in your heterogeneous environment of Windows NT and Solaris. While PC NetLink software accords the same file-locking security on network-based files and directories as Windows NT does, locked files may still be accessible directly from a Solaris computer account. PC NetLink software enables you to preclude that from happening, though it is not set by default as it may degrade overall system performance. If your network includes users who will access files from both

Windows NT and Solaris network client machines, you should change this setting to honor Windows NT file-locking from Solaris accounts. See "How to Set Solaris File System Integration Policies" on page 114.

During PC NetLink installation, DOS attribute groups were created. If your site uses a Solaris name service such as NIS in the Solaris environment, you should put the group information into the name service maps.

If DOS attributes are stored in groups, when a user creates files using a Windows NT Workstation and writes to a directory on the Solaris system, the owner is the user who creates the file and the default group is `DOS---`. The `DOS---` group is not recognized by Solaris servers that are not running PC NetLink software. While the user information is, in fact, retrieved from the name service maps, the group information will not be correctly displayed unless the listing of the file is performed on the PC NetLink system itself (default lookup: `files nis`). If you are viewing these files from another Solaris system, the group ID will not be resolved correctly. By putting the group information into the name service maps, you allow the files to be consistent between the local system files and the maps.

If DOS attribute storage is using some other means, then files and directories will not be created using `DOS---` groups.

Managing Access Control List (ACL) Data

PC NetLink Version 2.0 software provides enhanced ACL scalability by storing Windows NT-style ACL information in Solaris hidden files. ACL information for a file */pathprefix/directory/filename* is stored in the location */pathprefix/directory/*`.LMX:/`*filename*`/::$SD`.

If you upgrade from PC NetLink Version 1.2 software, the installation moves your existing ACL information from the single PC NetLink private database used in that version to hidden files used by Version 2.0 software. However, a downgrade installation will not restore the old private database and ACL information will be lost unless restored from a backup. Be sure to back up your data before installing Version 2.0 software.

The PC NetLink Version 2.0 ACL database contains entries for non-file entities only, such as shares. For this reason, backing up the ACL database is still important.

You can restore ACL database information backed up from PC NetLink Version 1.2 to a system running PC NetLink Version 2.0 by using the command `acladm -u`. See the man page for `acladm` for more information.

You can use the program `/opt/lanman/sbin/fsattr` to ensure that ACL files and directories have the correct ownership, primary group, and permissions, and to remove ACL files left over from files that have been removed.

UPS Power Failure Notification

You can send a power failure message to all Windows NT network users who are connected to a computer by using the Send Message command on the Computer menu in Windows NT Server Manager. For example, you can do this before you disconnect one or more users or before you stop the server service on that computer.

Using PC NetLink Server Manager, you can warn users of impending server shutdown because of power loss when an uninterruptible power supply (UPS) service is available.

For alerts to be sent, the Alerter service must be running on the PC NetLink server from which the alert is originated. See "How to Start Individual Services" on page 56. For client machines to receive the alerts, their Microsoft Windows Messenger service must be running.

Note – The UPS Power Failure Notification feature depends on the particular UPS power monitoring software that comes with your specific UPS product. PC NetLink software provides power failure notification to clients when it receives a `SIGPWR` (Signal 19) in the `lmx.ctrl` process that is running on the PC NetLink machine. When you set up your UPS monitoring software, you must modify it to send a `SIGPWR` (or `kill -19`) to the process ID of the `lmx.ctrl` process. See the man pages for `signal`, `ps`, and `kill` for further information.

User Accounts

You can associate new PC NetLink user accounts with Solaris user accounts on the Solaris system that is running PC NetLink software. To create this type of association, you use the PC NetLink Server Manager tool or the `mapuname` command. (For more information about the `mapuname` command, type `man mapuname` at the PC NetLink command prompt.) After you map a PC NetLink user account to a Solaris system user account, any file that the PC NetLink server user creates will be owned by the Solaris system user account.

Note – This option is useful only to those sites that use the `mapuname` command to associate Windows NT and Solaris accounts, and that keep their Solaris accounts in a local `/etc/passwd` file (that is, those who do *not* use the NIS name service). If this is the case and you choose this option, then if you use the Windows NT User Manager tool to change the user's Windows NT home directory to a shared path on the PC NetLink system, it edits `/etc/passwd` so that the user's Solaris account has the same home directory on the server.

Having both PC NetLink and Solaris system user accounts allows your Solaris system files to be owned by your Solaris system user account and to be accessed through your PC NetLink user account. You should map Solaris system user accounts to PC NetLink software users on the Solaris systems where their home directories reside—this is the default, though you can change it.

Assigning Solaris system user accounts to PC NetLink user accounts ensures that Solaris system user accounts are created only when necessary. It also gives administrators complete control over the mapping of PC NetLink user accounts to Solaris system user accounts.

You use the PC NetLink Server Manager tool to assign Solaris system user accounts automatically to new PC NetLink user accounts. See "How to Edit User Accounts Policies" on page 118. The Solaris system user account name that is assigned to the PC NetLink user account will be the same as, or similar to, the PC NetLink user account name. Differences can arise in cases of long, duplicate, or special character PC NetLink user account names.

If you were to map a PC NetLink user account to a nonexistent Solaris system user account, or if the Solaris system account for a PC NetLink user is deleted, the PC NetLink user will not have access to any shared resources on the Solaris system. To ensure that the PC NetLink user can continue to access the system, delete the account mapping or re-map the user to another Solaris system user account.

As administrator, you also have the ability to enable or disable users with Solaris accounts from logging on to the Solaris system, and to choose whether to synchronize PC NetLink home directories with users' Solaris home directories.

Note – You should avoid sharing any user's UNIX home directory on more than one PC NetLink system. Only the Windows NT user whose account is mapped to a particular UNIX account can access that UNIX account's home directory. Dynamic home directory sharing by the automounter can automatically give users access to their own UNIX home directories.

Copying User Accounts Using PC NetLink Server Manager

PC NetLink Server Manager allows you to selectively copy Windows NT Security Accounts Manager (SAM) user records to and from Solaris name service user records, and also allows you to schedule this activity.

When you run the Copy User Accounts task to copy user accounts from Solaris to PC NetLink, it is a complete process. When you run this task to copy user accounts from PC NetLink to Solaris, it creates a file that lists accounts that you must manually add to Solaris using the Solaris command line; it *does not* actually copy the accounts.

▼ How to Change Computer Browsing Policy

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server whose computer browsing policy you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

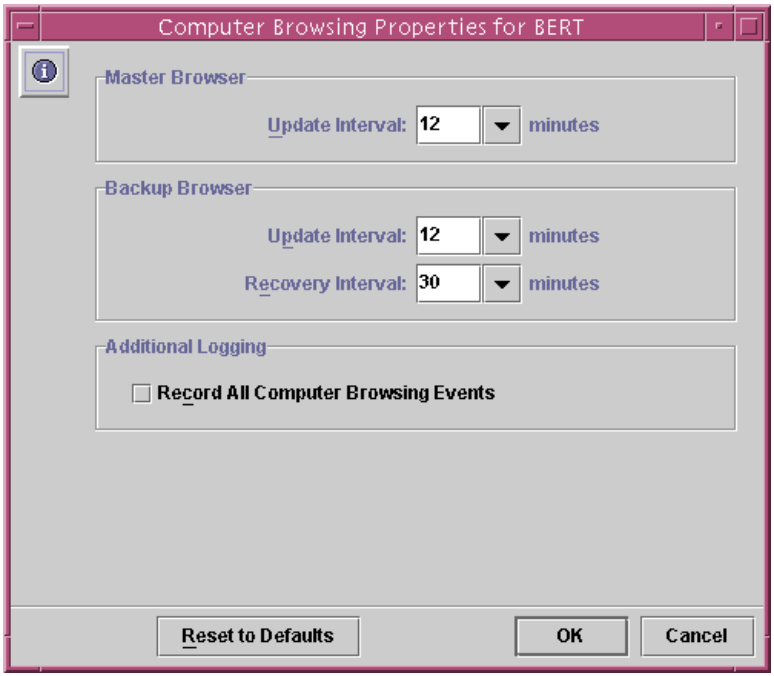
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

4. **Double-click Policies.**

5. **Double-click Computer Browsing.**

   The following screen appears.



6. **Using the provided drop-down lists and check box, make any changes to the Master Browser and Backup Browser update and recovery intervals, and list of browsing events that should be included.**

   Checking Record All Computer Browsing Events makes the event list more inclusive than the default.

   Note that you must enter a value greater than "0" for both the Master and the Backup Browsers' update intervals.

7. **Click OK, Cancel, or Reset to Defaults.**

   If you click OK to make any changes, PC NetLink Server Manager will automatically stop and then restart your browsing service to make the changes effective.

▼ How to Set Up File Name Mapping

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server whose file name mapping policy you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the server.**

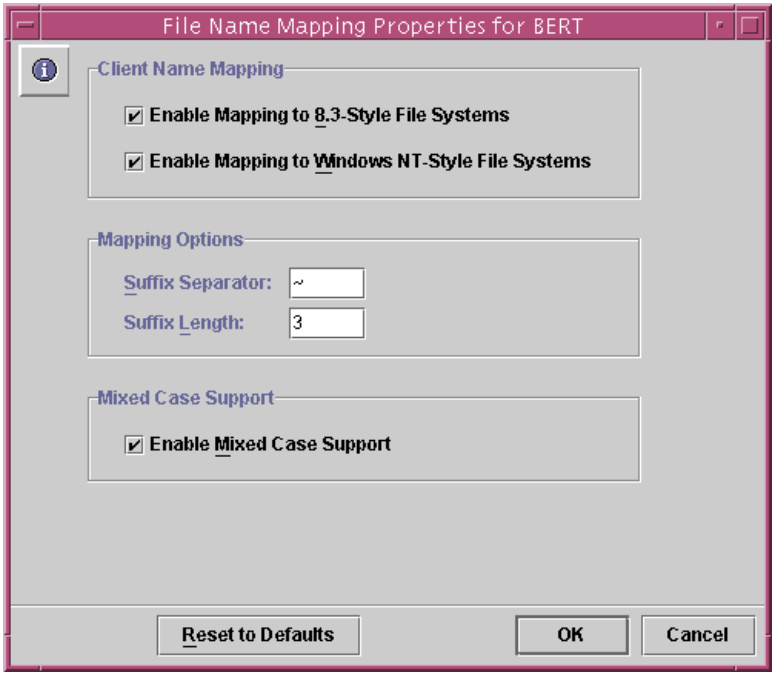
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

4. **Double-click Policies.**

5. **Double-click File Name Mapping.**

   The following screen appears.



6. **Create or change file name mapping policies according to the following guidelines:**
   - Check Enable Mapping to 8.3-Style File Systems if some of your client machines run applications that require that name format.
   - Check Enable Mapping to Windows NT-Style File Systems so that Solaris file names with characters that are invalid in Windows NT are changed to "legal" characters.
   - Type a new value in the Suffix Separator text field if you have reason to change the default; the default separator is a tilde (~).
   - Type a new value in the Suffix Length text field if you have reason to change the default from three. This value does *not* include the separator.
   - Check Enable Mixed Case Support if you want to allow file names to be created with both uppercase and lowercase characters, and you want case to be a factor in finding files. Note that checking this box may degrade performance.
7. **Click OK, Cancel, or Reset to Defaults.**

▼ How to Tune PC NetLink for Optimum Performance

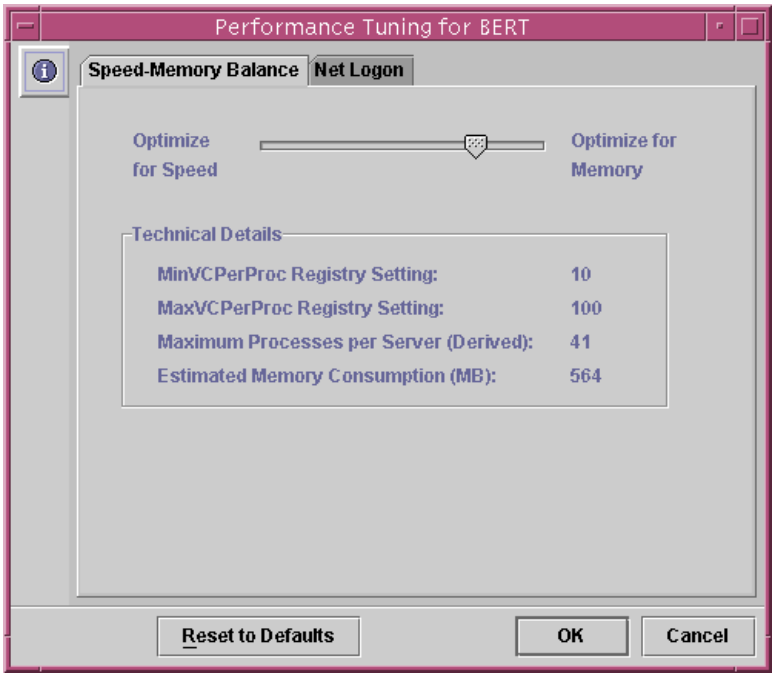
1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose performance you want to tune.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Virtual Server Configuration.**
4. **Double-click Policies.**

5. **Double-click Performance Tuning.**

   A screen similar to the following appears.



Note – Default PC NetLink settings enable optimum performance of most virtual servers in most cases. Do not adjust the default settings unless you are an experienced system administrator. For background information on PC NetLink performance parameters, see "Tuning PC NetLink Parameters for Optimum Performance" on page 101.

---

6. **Adjust performance-related parameters according to the following guidelines, organized by the Performance Tuning policy's tabs:**

   - *Speed-Memory Balance* – The default settings are those specified in the PC NetLink Registry, and are appropriate for most cases. For the default values associated with the Registry entries affected, see the section, "Registry Keys and Values" on page 308 in Appendix A, "PC NetLink Registry," and consult the entries for `VCDistribution`, `MinVCPerProc`, and `MaxVCPerProc`.

     To change the default values, either to optimize for speed or for memory, use the sliders according to the following guidelines:

- The farthest left setting maximizes speed. Do not use this setting unless your system has at least 4 gigabytes of RAM. This may be an appropriate setting to handle unusual client workloads.
- The farthest right setting minimizes memory consumption, but results in slower system response. You may need to use this setting if your system has less than 1 gigabyte of RAM.

Read the Context Help associated with other slider positions for explanations of the intermediate settings.

- *Net Logon* – Select Automatically Disconnect Idle Net Logon Connections to establish a timeout, which is disabled by default.

▼ How to Set Solaris File System Integration Policies

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose Solaris file integration policies you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

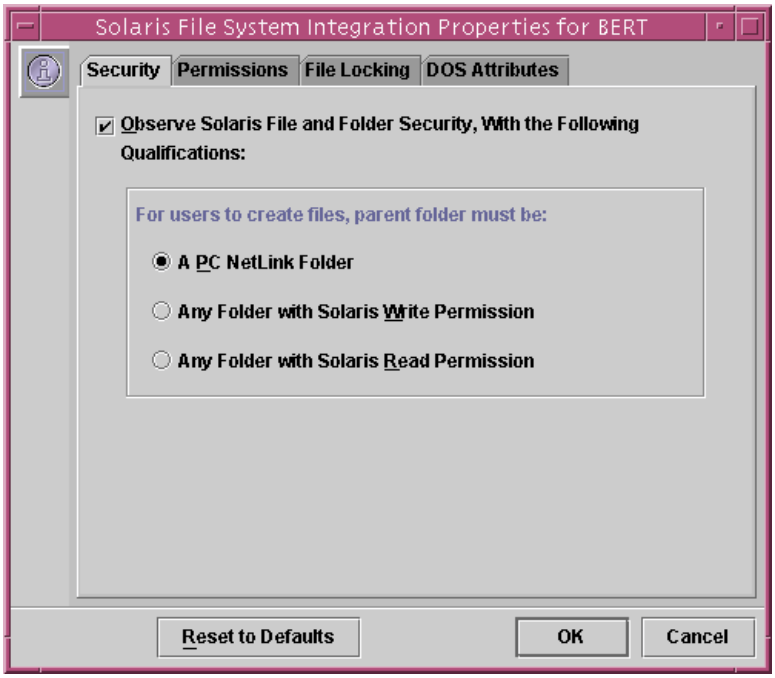
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

4. **Double-click Policies.**

5. **Double-click Solaris File System Integration.**

   The following screen appears.



6. **Set PC NetLink file creation policies according to the following guidelines, using the Security, Permissions, File Locking, or DOS Attributes tabs:**

   - *Security* – To establish policy for file creation within PC NetLink folders:
     - *Ignore Solaris permissions* – Leave unchecked the Observe Solaris File and Folder Security...Qualifications option to ignore Solaris permissions. With this option unchecked, Windows NT file and directory permissions are the only permissions that will prevail over file and directory creation and access for reading. PC NetLink software users with appropriate Windows NT permissions can create files within PC NetLink folders.
     - *Observe Solaris permissions* – Check Observe Solaris File and Folder Security...Qualifications and then select one of the three radio buttons to set parent folder requirements:
       – PC NetLink – This option reuires users to have Solaris Write permission to create a file within a PC NetLink folder only—it will not affect any other Solaris file system folder. This is the most restrictive option, in that it does not grant any permissions in any other Solaris directories or files.

- *Any Folder with Solaris Write Permission* – This option eases the restriction, by enabling PC NetLink software users to create files within PC NetLink folders and any other Solaris file system folder for which they have Write permission.
- *Any Folder with Solaris Read Permission* – This option specifies that only minimal Solaris permissions be in place on any PC NetLink folder or any other Solaris folder. In effect, this option grants Write permission to any Solaris operating environment-based folder.

- *Permissions* – To establish default User, Group, and Other file and folder permissions, check the box next to the permissions that you want to set.
- *File Locking* – To cause PC NetLink software to observe Windows NT file locking—thereby preventing users with Solaris accounts from accessing the locked files—check Reflect Client-Created Record Locks in Solaris File System. (Note that checking this box may slow down performance.)
- *DOS Attributes* – to establish the policy for storing DOS attributes:
  - To store DOS attributes, check Store DOS Attributes and choose how to store them by selecting the Solaris Groups, UNIX Execute Bits, or Solaris File System radio button. These settings behave as follows:
    - *Solaris Groups* – This option uses the "DOS-xxx" group IDs to store DOS attributes. As a result, the UNIX group IDs are discarded.
    - *UNIX Execute Bits* – This option stores DOS attributes for files in UNIX execute bits. DOS archive, system, and hidden attributes are represented as UNIX user, group, and other execute bits, in that order. DOS attributes for directories are not stored.
    - *Solaris File System* – This option stores DOS attributes in hidden files in the Solaris file system using POSIX ACLs.
  - To *not* store DOS attributes, leave Store DOS Attributes unchecked. Any file created or modified by a PC NetLink user will be assigned the group IDs of the Solaris account to which the PC NetLink user is mapped. If the PC NetLink user account is unmapped, new files are assigned the group IDs of the `lmworld` account.

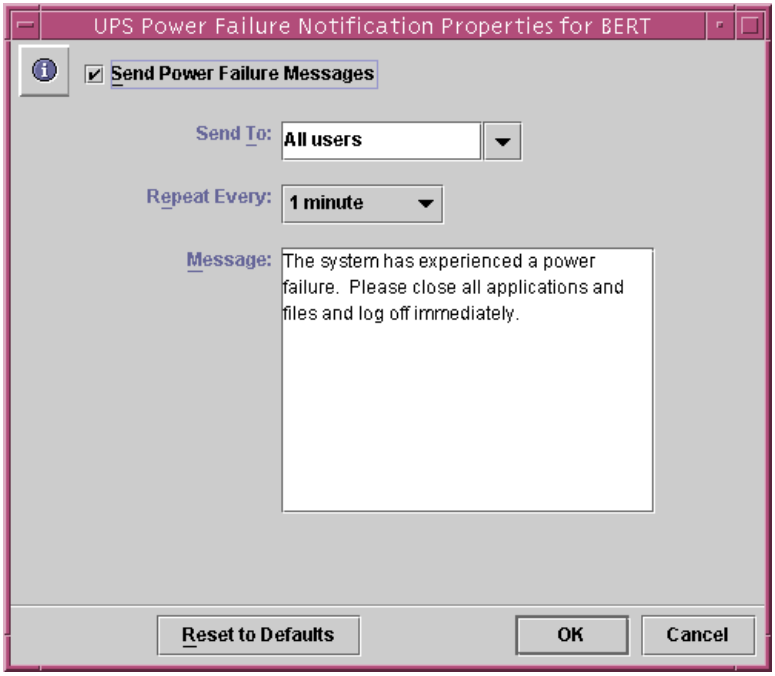
7. **Click OK, Cancel, or Reset to Defaults.**

▼ How to Use UPS Power Failure Notification

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose UPS power failure notification policy you want to change.**

   For instructions, see “How to Log On to a Solaris Server Using PC NetLink Server Manager” on page 42. Also see the Note on page 107 for important information about the UPS policy.

2. **In the Results pane, double-click the icon that represents the virtual server.**
   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Virtual Server Configuration.**
4. **Double-click Policies.**
5. **Double-click UPS Power Failure Notification.**
   The following screen appears.



6. **Check Send Power Failure Messages.**
7. **Either select from the drop-down list, or type directly into the text field, the NetBIOS names of all the users or systems that you want to notify.**
   Select All Users if you want to send the message to everyone.
8. **Using the drop-down list, designate how often you want the notification to be repeated.**
9. **In the Message text field, type the message that you want to send.**
10. **Click OK, Cancel, or Reset to Defaults.**

▼ How to Edit User Accounts Policies

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose user account mapping policy you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

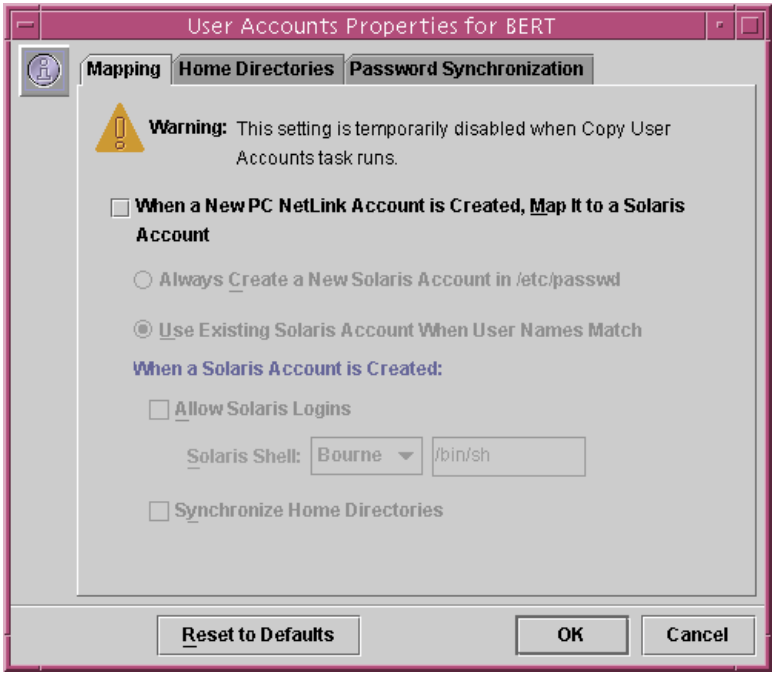
   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

4. **Double-click Policies.**

5. **Double-click User Accounts.**

   The following screen appears.



6. **Click the Mapping tab to establish or edit user account mapping policies according to the following guidelines:**

   - Check When a New PC NetLink Account is Created, Map It to a Solaris Account in order to automatically create a unique Solaris account for a user simultaneously with the creation of his or her new account in the Windows NT domain served by the PC NetLink system. If you check this option, you then have other options, described in the remainder of this list.
   - Select the option Always Create a New Solaris Account in /etc/passwd, or the option Use Existing Solaris Account When User Names Match. Note that a Solaris account exists independently of both Windows NT and PC NetLink systems.

Note – Checking the Always Create a New Solaris Account in /etc/passwd option will cause the system to create a new Solaris account by way of a local `/etc/passwd` file *only*. If your site uses a Solaris name service such as NIS, do *not* check this option.

   - Select whether to permit a user with a Solaris account to use that account independently of NT and PC NetLink software, by checking Allow Solaris Logins or leaving it unchecked. If you select to permit Solaris logins, use the Solaris Shell drop-down list to choose a command shell, or choose Other and type the shell name in the text field.
   - Select Synchronize Home Directories for automatic synchronization of PC NetLink home directories with Solaris home directories.

Note – The Synchronize Home Directories option is useful only to those sites that use the `mapuname` command to associate Windows NT and Solaris accounts, and that keep their Solaris accounts in a local `/etc/passwd` file (that is, those who do *not* use the NIS name service). If this is the case and you choose this option, then if you use the Windows NT User Manager tool to change the user's Windows NT home directory to a shared path on the PC NetLink system, User Manager edits the `/etc/passwd` file so that the user's Solaris account has the same home directory on the server.

See "User Accounts" on page 107 for background information on these policies. To map existing user accounts, see "How to Map Existing User Accounts" on page 120.

7. **Click the Home Directories tab to edit the policy for automounting home directories.**

   To automatically mount home directories of PC NetLink mapped users, check Automatically Mount Solaris Home Directories of Mapped Users, and type a comment for the dynamic UNIX home directory share if desired.

Note – You can also control how PC NetLink software shares home directories by using the `regconfig` utility. The shares created by the automounter will be visible to PC users who are logged in and have a mapped user account on Solaris. For each such user, when they log in to a PC NetLink server that has the automounter turned on, their Solaris home directory will appear as a Windows share (with a share name the same as their user name). Each user sees only their own share; the administrator sees none of them. After the automounter performs the mapping, this type of share looks and behaves exactly like other PC NetLink shares in either NT Server Manager or Network Neighborhood (this includes security settings).

8. **Click the Password Synchronization tab to edit the policy for password synchronization.**

   Select the Enable Password Synchronization check box to turn password synchronization on or off for mapped accounts. Password synchronization must be configured for this check box to have any effect. For information about setting up password synchronization, see Chapter 4.

9. **After making changes in one or more tabs, click OK, Cancel, or Reset to Defaults.**

   When you click Reset to Defaults, the software resets defaults for the current tab only.

▼ How to Map Existing User Accounts

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server on which you want to map existing user accounts.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

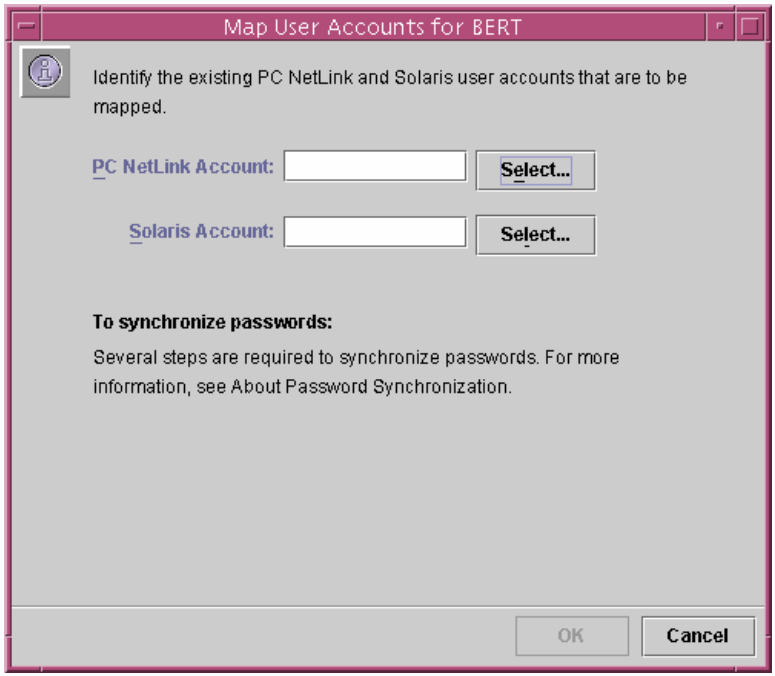
2. **In the Results pane, double-click the icon that represents the virtual server on which you want to map existing user accounts.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Mapped User Accounts.**

4. **In the window that appears, double-click the icon for Map User Accounts.**

   The following screen appears.



5. **Enter the names of the existing PC NetLink account and the Solaris account, or click Select to browse accounts.**

6. **Click OK.**

▼ How to Copy User Accounts From Solaris to PC NetLink Using PC NetLink Server Manager

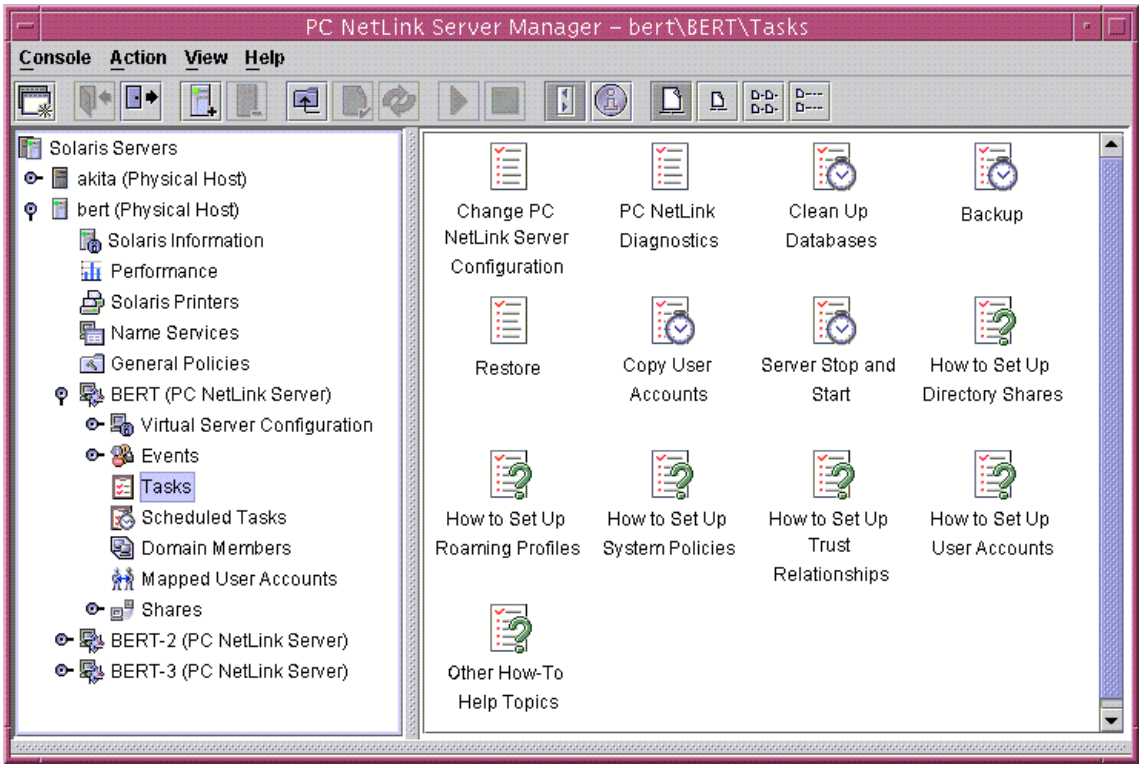
1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server on which you want to copy user accounts.**

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Tasks.**

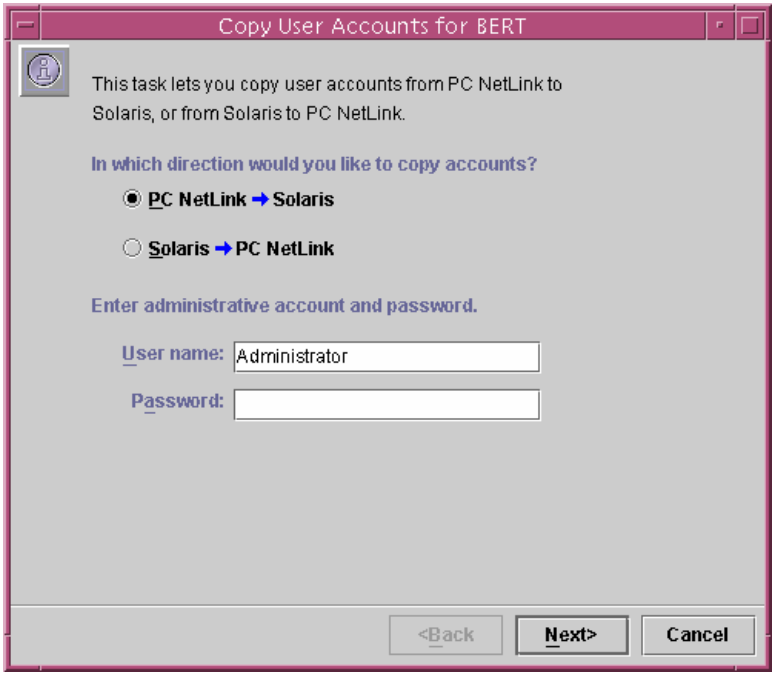
   A screen similar to the following appears.



Note that some of the tasks—including Copy User Accounts—are marked with a clock face. This indicates that these are tasks that you can run immediately, or automatically on a periodic schedule that you create.

4. **Double-click Copy User Accounts.**

   The following screen appears.

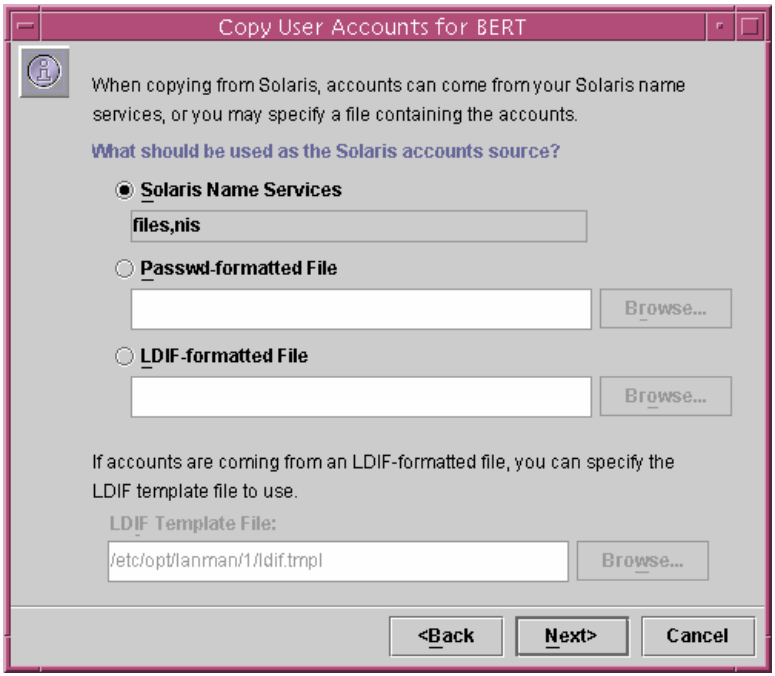


5. **Click Solaris -> PC NetLink.**

6. **Type an administrative account and password.**

7. **Click Next.**

   The following screen appears.



8. **Specify the source for accounts to copy.**

   Click Solaris Name Services to get accounts directly from Solaris name services.

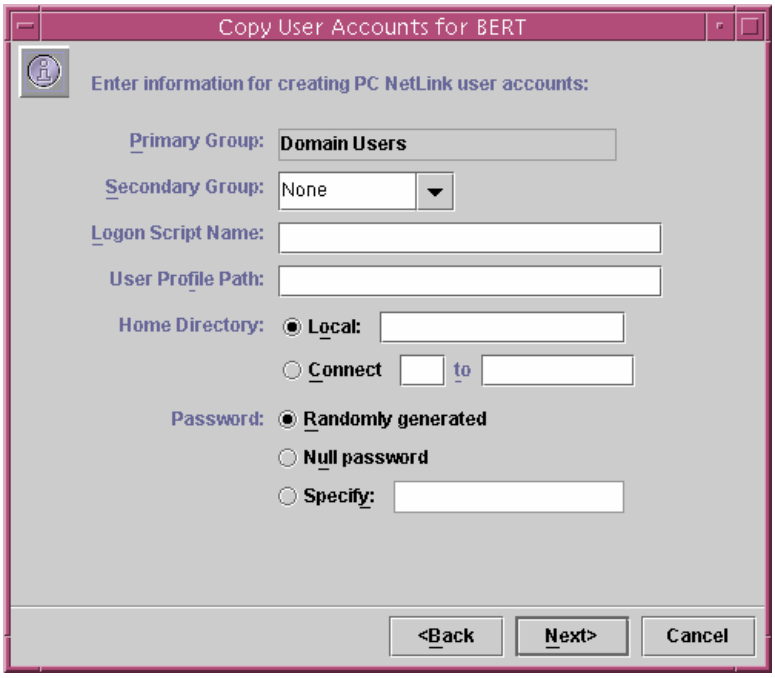
   To use a file that contains the accounts, click Passwd-formatted File or LDIF-formatted File. After selecting a file type, click Browse to see the names of existing files, or type a file name in the text field. If you are using an LDIF-formatted file, you must also specify an LDIF template to use.

9. **Click Next.**

10. **Click Generate List Automatically to include all PC NetLink accounts not in Solaris when this task is run, or click Specify User Accounts and Load Users to list accounts. Then, check the accounts you want to copy.**

11. **Click Next.**

The following screen appears.

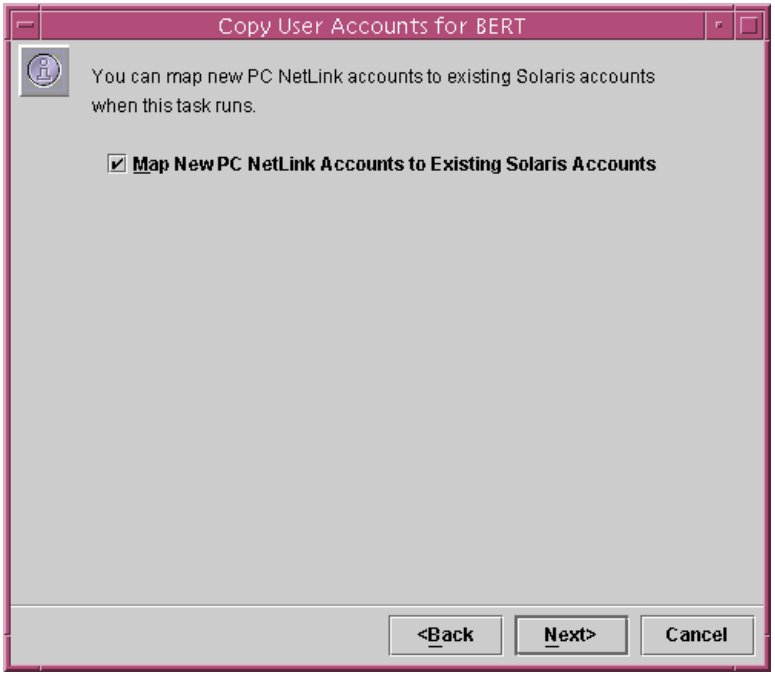


12. **Enter information for creating PC NetLink user accounts (optional).**

- Choose a secondary group from the drop-down menu for the accounts that will be copied.
- Type a logon script name to use and a user profile path from the drop-down menu.
- Click Local to specify the path to local home directories, or click Connect and specify a drive letter to allow a remote path to be mounted as a mapped network drive.
- For account passwords, click on Randomly generated, Null password, or Specify to enter an initial password for all the accounts.

13. **Click Next.**

    The following screen appears.



14. **Click Map New PC NetLink Accounts to Existing Solaris Accounts if you want to use this feature.**

    Mapping is required if you plan to subsequently synchronize passwords.

15. **Click Next.**

    The resulting screen prompts you for scheduling information.

16. **Select Perform It Now or Schedule It for Later, and then click Next.**

Note – Scheduled tasks are not supported in a high availability (HA) environment.

---

17. **Depending on the selection you made, do one of the following:**

    - *Perform It Now* – Skip to Step 22.
    - *Schedule It for Later* – Continue with Step 18.

18. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

    If you specified individual accounts in Step 10, the only possible choice is Just Once.

19. **Depending on your selection, furnish the following information about when you want the task to run:**

    - *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date.
    - *Daily* – The time of day.
    - *Weekly* – The time of day and the name of the day.
    - *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only.

20. **Click Next.**

21. **In the text field of the resulting screen, type a name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

22. **Click Next.**

    A summary screen appears.

23. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.

Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

▼ How to Copy User Accounts From PC NetLink to Solaris Using PC NetLink Server Manager

---

Note – This procedure creates a file that lists accounts to manually add to Solaris using the Solaris command line. Unlike the operation for copying user accounts from Solaris to PC NetLink, this operation is not sufficient to actually copy the accounts.

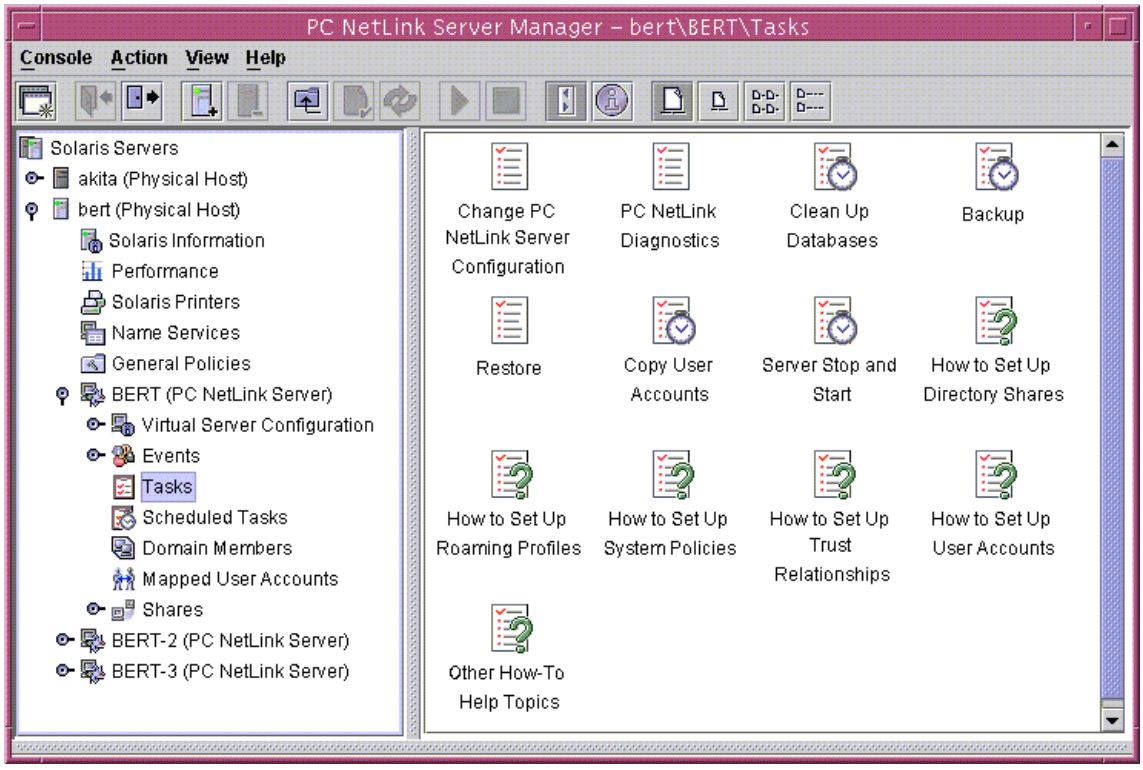
---

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server on which you want to copy user accounts.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Tasks.**

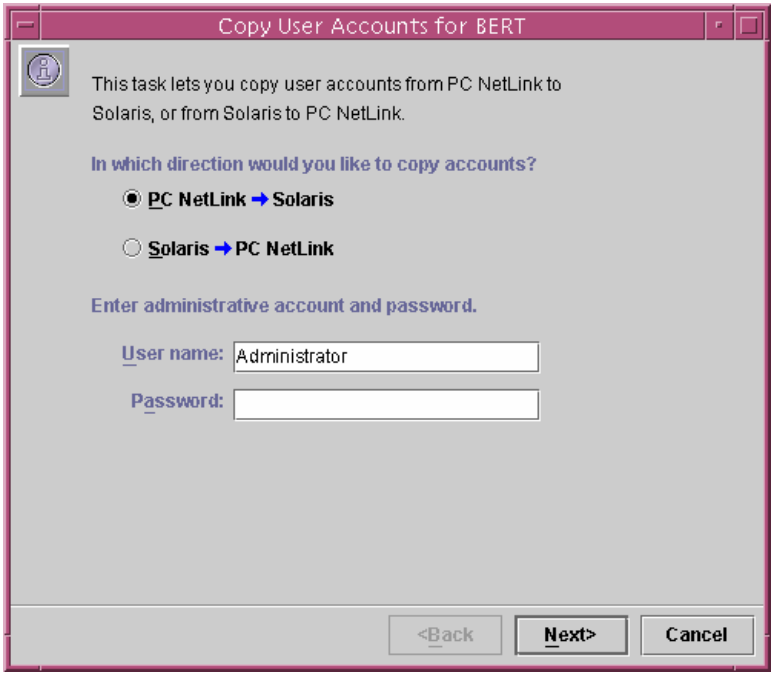
   A screen similar to the following appears.



Note that some of the tasks—including Copy User Accounts—are marked with a clock face. This indicates that these are tasks that you can run immediately, or automatically on a periodic schedule that you create.

4. **Double-click Copy User Accounts.**

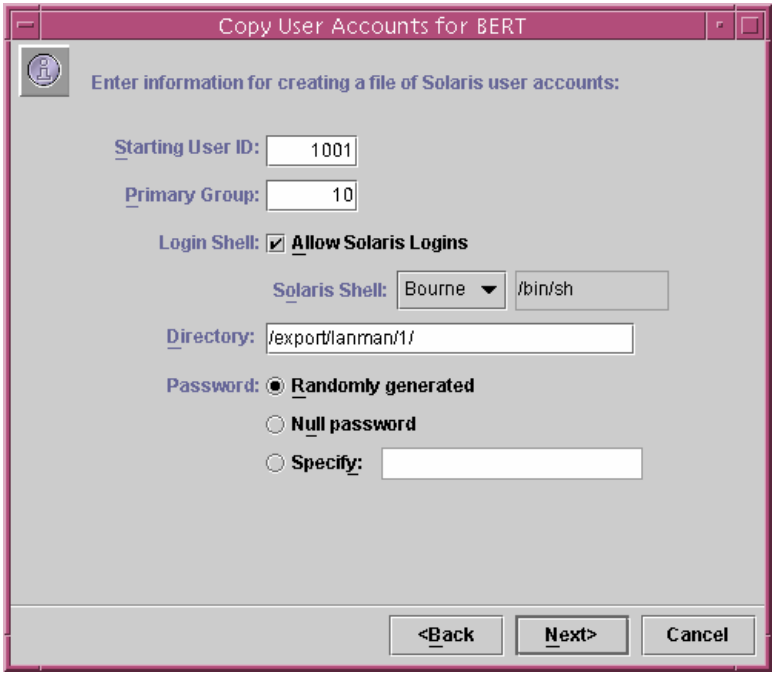
   The following screen appears.



5. **Click PC NetLink -> Solaris, if it is not already selected.**
6. **Type an administrative account and password.**
7. **Click Next.**
8. **Click Generate List Automatically to include all PC NetLink accounts not in Solaris when this task is run, or click Specify User Accounts and Load Users to list accounts. Then, check the accounts you want to copy.**

9. **Click Next.**

   The following screen appears.

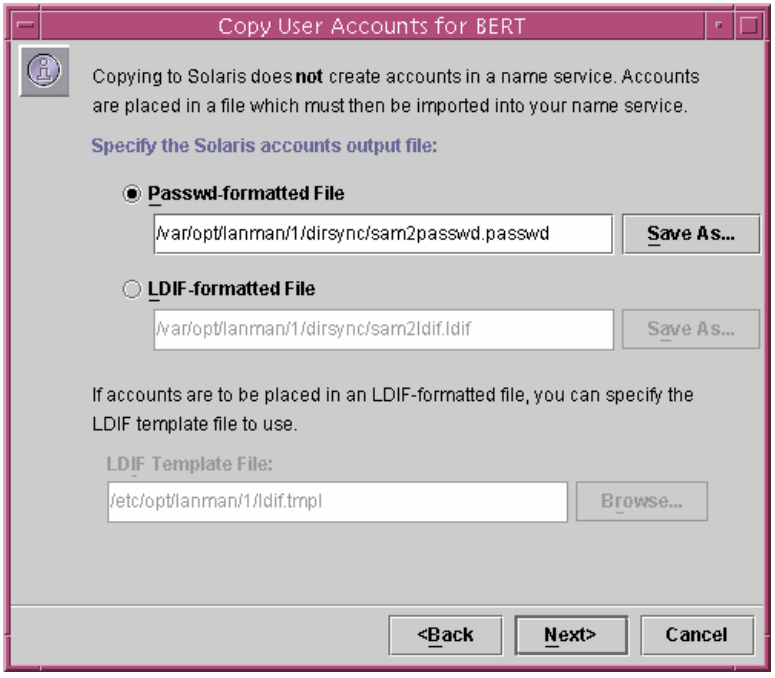


10. **Type the information for creating a file that lists user accounts to add to Solaris (optional).**

    - Type a starting user ID number and primary group number for the accounts that will be copied.
    - Click Allow Solaris Logins if desired, and specify a Solaris shell for the accounts to use.
    - In the Directory field, type the path to use for users' home directories.
    - For account passwords, click on Randomly generated, Null password, or Specify to enter an initial password for all the accounts.

11. **Click Next.**

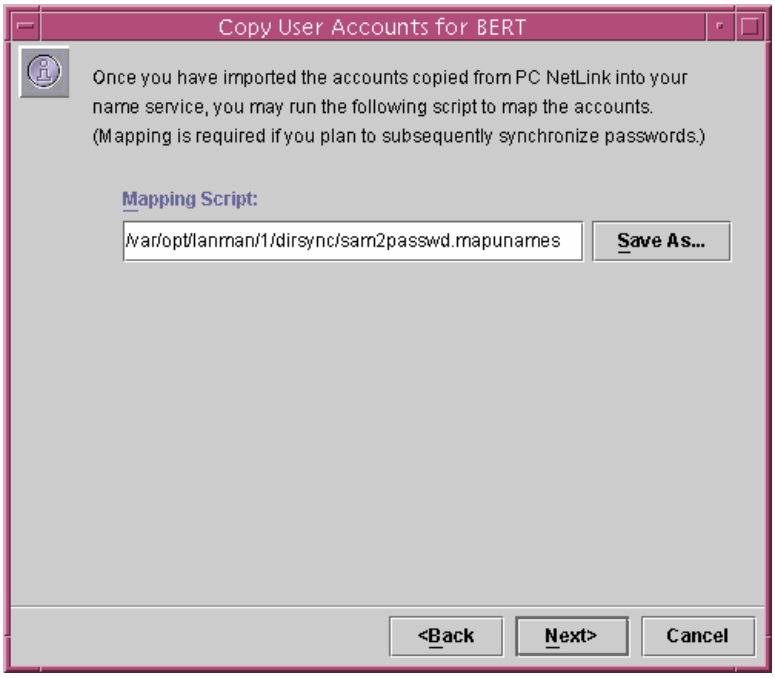
    The following screen appears.



12. **Select whether to create a passwd-formatted file or an LDIF-formatted file. Then click Browse to see the names of existing files, or type a file name in the text field.**

13. **Click Next.**

    The following screen appears.



14. **Type the name of a mapping script in the text field, or click Browse to view existing files.**

    Once you have imported the accounts copied from PC NetLink into your name service, you can run the mapping script to map the accounts. (Mapping is required if you plan to subsequently synchronize passwords.)

15. **Click Next.**

    The resulting screen prompts you for scheduling information.

16. **Select Perform It Now or Schedule It for Later, and then click Next.**

Note – Scheduled tasks are not supported in a high availability (HA) environment.

---

17. **Depending on the selection you made, do one of the following:**
    - *Perform It Now* – Skip to Step 22.
    - *Schedule It for Later* – Continue with Step 18.

18. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

    If you specified individual accounts in Step 8, the only possible choice is Just Once.

19. **Depending on your selection, you must furnish the following information about when you want the task to run:**

    - *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date.
    - *Daily* – The time of day.
    - *Weekly* – The time of day and the name of the day.
    - *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only.

20. **Click Next.**

21. **In the text field of the resulting screen, type a name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

22. **Click Next.**

    A summary screen appears.

23. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.

Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

User Account Management Utilities

Besides using PC NetLink Server Manager to copy user accounts, you can use several PC NetLink utilities to accomplish this task.

PC NetLink software provides two Solaris user account management utilities for use in transferring existing Windows NT SAM user records to and from Solaris name service user records:

- `sam2passwd`
- `passwd2sam`

PC NetLink software also provides three user account management utilities for use in transferring existing Windows NT SAM user records to Lightweight Directory Access Protocol (LDAP) Data Interchange Format, known as LDIF format, for use with tools that use the LDAP protocol:

- `sam2ldif`
- `ldif2sam`
- `ldifmerge`

Neither the `sam2ldif` nor the `ldif2sam` utility communicates directly with an LDAP database. It is up to the LDAP administrator to either read the LDIF data into the LDAP server or generate LDIF from the LDAP server. These utilities do not deal with authentication, and therefore should work with any type of LDAP authentication used. Further, since the LDIF files contain security and password information, administrators must be responsible for moving and protecting these files in a secure way.

`passwd2sam`

The `passwd2sam` user account management utility places user account information that is stored in a Solaris name service—such as FILES or NIS—into the PC NetLink SAM database. If the PC NetLink system is configured as a BDC in an existing Windows NT domain, `passwd2sam` operations will transfer to the domain's PDC.

Note – Using this utility does *not* add users' passwords to the PC NetLink SAM database, because passwords are one-way encrypted; that is, they cannot be decrypted for automatic transfer from one account to the other.

The `passwd2sam` user account management utility supports three modes of operation:

- It adds Solaris user accounts into the PC NetLink SAM database. This is the default mode of operation. Solaris user accounts can be added from the running Solaris name service or by a user-specified `/etc/passwd` formatted input file.
- It deletes Solaris user accounts from the PC NetLink SAM database. Solaris user accounts are deleted from the PC NetLink program by a user-specified `/etc/passwd` formatted input file.
- It finds and disables Windows NT domain user accounts that have been added by `passwd2sam` and subsequently deleted from a Solaris name service. This mode will find and disable PC NetLink user accounts that have been removed from a Solaris name service.

You must format all input files to `passwd2sam` as `/etc/passwd` entries. See the `passwd2sam`(1) man page for details on invocation options and arguments.

sam2passwd

The `sam2passwd` user account management utility records PC NetLink user accounts, and then creates the following `/etc/passwd` formatted file containing the PC NetLink user accounts:

`/var/opt/lanman/dirsync/sam2passwd.passwd`

This file contains nonprivileged PC NetLink user accounts that you can add to Solaris name service maps or to a local `/etc/passwd` file (on which you then run the `/user/bin/pwconv` command).

The `sam2passwd` utility is provided to assist you in migrating user accounts into your running Solaris name service, but does not actually perform the operation. See the `sam2passwd`(1) man page for details on invocation options and arguments.

sam2ldif

The `sam2ldif` user account management utility allows transfer of SAM user records to a LDAP server. This utility functions similarly to the `sam2passwd` utility, but generates text in LDAP Data Interchange Format (LDIF) rather than in `/etc/passwd` format. This LDIF output can then be read into an LDAP server. This will allow the SAM user information to be shared with other services that use LDAP to store user data. The `sam2passwd` utility outputs only the information needed by the Solaris operating environment, such as the user ID number, group ID number, shell, and home directory. However, the `sam2ldif` utility outputs all the information that the Windows NT operating environment normally stores for each user in the SAM database (that is, the entire USER_INFO_3 record). See the `sam2ldif`(1) man page for complete information about this utility.

ldif2sam

The `ldif2sam` utility allows transfer of LDAP user records to SAM user records. This utility functions similarly to the `passwd2sam` utility, but it reads in text in LDIF format rather than in `/etc/passwd` format. It then updates the SAM database according to the information it reads. Similar to `sam2ldif`, this utility outputs all the information that the Windows NT operating environment normally stores for each user in the SAM database (that is, the entire USER_INFO_3 record). If any of these fields change in the LDAP database, an administrator can use this utility to update the SAM database according to those changes. See the `ldif2sam`(1) man page for complete information about this utility.

ldifmerge

The ldifmerge utility takes two LDIF files as inputs. It compares records in these two files to determine which records should be deleted, modified or added. It then creates a third output file that is the mergence of the two, using LDIF "changetype" attributes to differentiate between additions, deletions, and modifications.

The LDIF file generated by the sam2ldif utility contains all records in the SAM database and does not indicate which records should be added, deleted, or modified in the LDAP database. Without a merge utility there would be no way to determine which records should be deleted. Furthermore, records that had not changed would be included in the LDIF file, causing records to be overwritten with an identical copy, which is unnecessary. When the ldifmerge utility creates its output file, it merges the files by determining which records have been added or deleted, and it also checks the files for modifications.

▼ How to Use the ldifmerge Utility

1. **Use the sam2ldif utility to generate a file in LDIF format that contains all users in the SAM database.**
2. **Use an LDAP tool such as ldapsearch to create a file in LDIF format that is a representation of the LDAP database.**

   This will show the current state of the LDAP database with respect to which users it contains and what each user's attributes are.
3. **Run the ldifmerge utility on the two files generated in Step 1 and Step 2, respectively.**

   This generates LDIF code, which the ldapmodify utility can read into the LDAP database. The LDIF code generated by this utility includes special directives called "changetypes" to indicate how to handle a particular LDAP entry. For example, the following LDIF code changes a single attribute:

```
dn: uid=jrosen,ou=users,dc=east,dc=sun,dc=com
changetype: modify
replace: uidnumber
uidnumber: 123456
```

The `ldifmerge` utility accepts the following command-line options.

Option	Description
`-o`	Original LDIF file.
`-n` *file*	New LDIF file. This should be a file that was generated by the `sam2ldif` utility.
`-m` *file*	Merged file. This file will overwrite an existing file with the same file name.

About Managing General Policies

The policies in this section are general policies that you set for a Solaris physical host.

NetBIOS

NetBIOS, which stands for Network Basic Input/Output System, is a session-layer interface used by applications to communicate. Its logical naming system permits computer network interfaces to establish connections, and ensures reliable data transfer between computers once the connections exist.

PC NetLink NetBIOS policy properties affect all virtual servers on a physical host.

WINS Servers

A Windows Internet Name Service (WINS) server is a machine that maintains a database of available network resources and the computers that own them. A computer seeking such a resource "asks" the WINS server to look up the address of the machine that owns the resource.

A network can have no WINS servers, or it can have any number of them. See a fuller discussion of WINS in Chapter 5, "Implementing WINS and Maintaining Databases" on page 213.

WINS and NetBIOS Nodes

By default, PC NetLink software brings up each network interface in Broadcast node (b-node). In this mode, a computer seeking a network service or resource broadcasts a general request to the network, seeking a response from the machine that owns the resource or service. Each computer receiving such a request responds with its address.

This mode has the advantage of not requiring WINS servers, but it generates a lot of network traffic. Broadcast node does not work across subnets.

WINS servers use the NetBIOS Hybrid node (h-node). In this mode, a computer seeking a network service or resource sends that request directly to a specified WINS server, which in turn looks up the address of the machine that owns the resource.

WINS Proxy

WINS proxies are useful in networks comprising several subnets, where some of the computers on those subnets are running in Broadcast node. A WINS proxy fields local requests for services located on a different subnet, caching network addresses and communicating with the WINS server when necessary.

You can also configure the NetBIOS service to use WINS servers to resolve NetBIOS names by typing the IP address of the primary and secondary WINS servers. You can configure only the primary WINS server, or both. The WINS server addresses can be the IP address of the local PC NetLink system running the WINS service, or another PC NetLink system running the WINS service, or a Windows NT server running the WINS service.

If either primary or secondary WINS servers are configured, you can use the WINS proxy setting to allow this PC NetLink system to provide WINS proxy service to other computers that have not been configured to use WINS servers to resolve NetBIOS names. Be discreet in using this option, as it joins the NetBIOS name spaces for both b-node and h-node NetBIOS nodes on the local subnet, and can cause unexpected name conflicts.

LAN Adapter (Lana) Numbers

LAN Adapter (Lana) numbers are part of the logical naming system established by NetBIOS. PC NetLink software assigns Lana numbers automatically to each network interface, choosing a number that is unique within the particular computer.

You can configure one NetBIOS Lana for each available network interface card. You should plan ahead to choose the particular network interfaces that you want to be assigned NetBIOS Lanas.

NetBIOS Scope

NetBIOS scope is a seldom-used feature that limits the computers with which a particular network device can communicate.

The chief use of scope is in wide area networks (WANs) or other large networks, where it can prevent conflicts caused by two or more network interfaces having the same NetBIOS name.

Consider a network belonging to a shoe manufacturer where two machines, both earmarked for use by sales personnel, exist on the same subnet.

One machine is used by those selling sneakers, and the other by those selling boots. If both machines had the NetBIOS name "sales," problems would result. However, if one machine is given the scope name "sneakers" and the other "boots," then both machines could retain the NetBIOS name "sales" without any conflict. Note however, that both machines could then only communicate with other machines possessing the same scope.

Solaris Name Resolution and Domain Name Service (DNS)

A new feature in PC NetLink 2.0 enables forwarding of NetBIOS name lookups to the Solaris name services listed in the file `nsswitch.conf`. As part of this feature, you can add Domain Name Service (DNS) to the end of the list if it is not already there. You can also specify DNS configuration settings. See "How to Configure Solaris Name Services" on page 149.

You can also use the `nbdnsconf` command to configure DNS support. See the man page for `nbdnsconfig`.

PC NetLink Server Manager Security

Another security consideration involves users' privileges to administer the PC NetLink program by way of the PC NetLink Server Manager tool. You can choose settings that affect security on subsequent PC NetLink Server Manager sessions. The Data Integrity setting uses public key signatures to protect data passed between the server and the client. Authentication takes place behind the scenes and involves rechecking credentials with each transaction. See "How to Configure Solaris Name Services" on page 149.

PC NetLink Server Manager security policy properties affect all virtual servers on a physical host.

Performance Monitoring and Alarms

Performance monitoring policy enables you to control how virtual servers on a physical host report information about system performance, and under what conditions alarms are sent. These policy settings affect all virtual servers on a physical host.

The Generate Alarms setting enables you to specify whether PC NetLink sends alarms by e-mail, and the e-mail address to use. PC NetLink alarm notification policy settings affect all virtual servers on a physical host.

▼ How to Configure the Windows Internet Name Service (WINS)

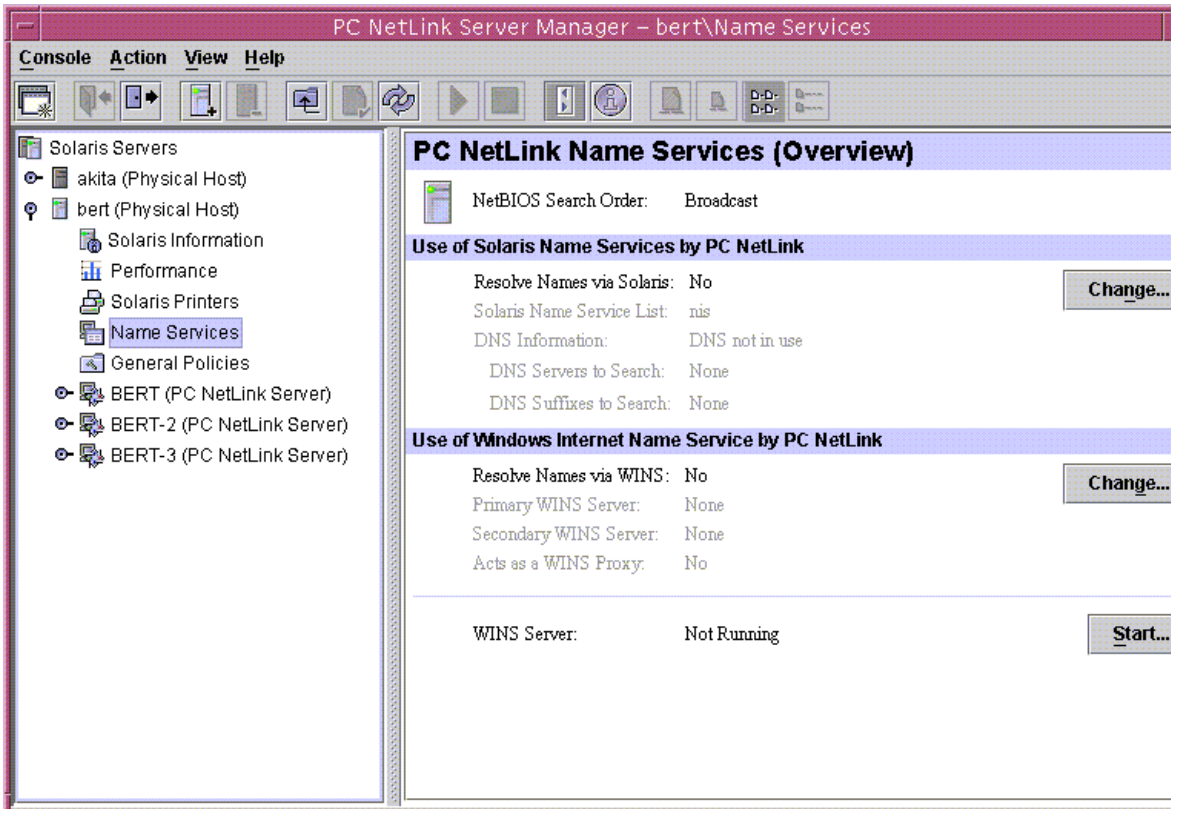
You configure the Windows Internet Name Service on a system-wide basis; the policy affects all virtual servers on a physical host.

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose WINS configuration you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

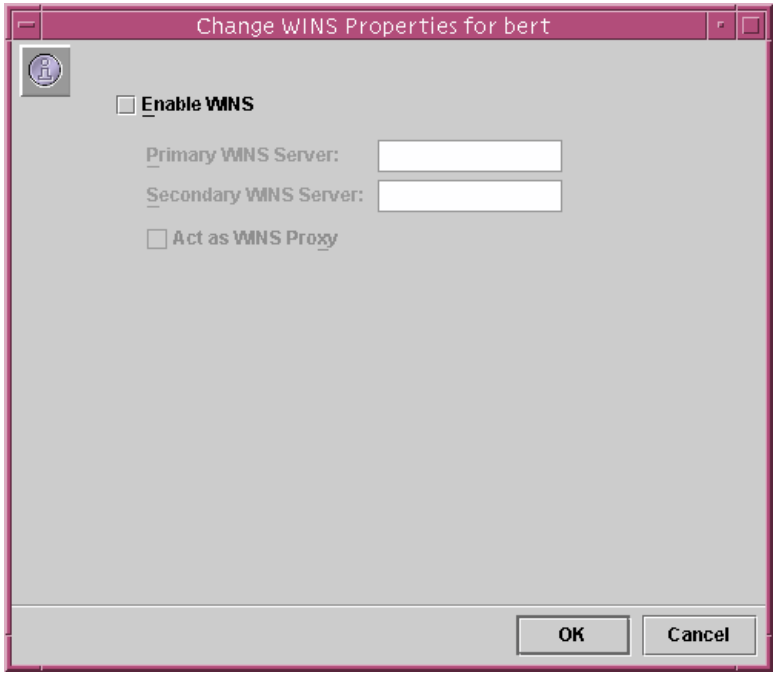
2. **In the Results pane, double-click Name Services.**

   A screen that lists current name services configuration appears, similar to the following.



3. **Click Change in the Use of Windows Internet Name Service by PC NetLink pane.**

   The following screen appears.



4. **To enable WINS on the local system, click the check box next to Enable WINS.**

   The screen changes to activate three WINS configuration choices:

   - Primary WINS Server
   - Secondary WINS Server
   - Act as WINS Proxy

5. **In the corresponding text fields, type in the IP addresses for the primary and, optionally, secondary WINS servers.**

   See "WINS Proxy" on page 139 for a description of primary and secondary WINS servers.

6. **Choose whether you want the system to act as a WINS proxy.**

   See "WINS Proxy" on page 139 for a description.

7. **Click OK.**

   The following screen appears, notifying you that the PC NetLink program and the NetBIOS driver must be restarted for changes to take effect.

8. **Choose whether to stop and restart the server and the NetBIOS driver immediately or to restart them later.**

   None of the changes you have designated will become effective until the next time you start the PC NetLink program.

   If a user restarts NetBIOS using PC NetLink Server Manager, all virtual servers running on the physical host will be stopped and then automatically restarted.

   Only one WINS server can run on a Solaris physical host, regardless of the number of virtual servers running on that physical host.

Note – If you have designated your PC NetLink server as a WINS server, the Enable WINS option does not start the WINS service automatically after the PC NetLink program is restarted. You need to start the service manually by typing `net start wins` at the system's command line, or by using PC NetLink Server Manager.

▼ How to Start or Stop WINS Using PC NetLink Server Manager

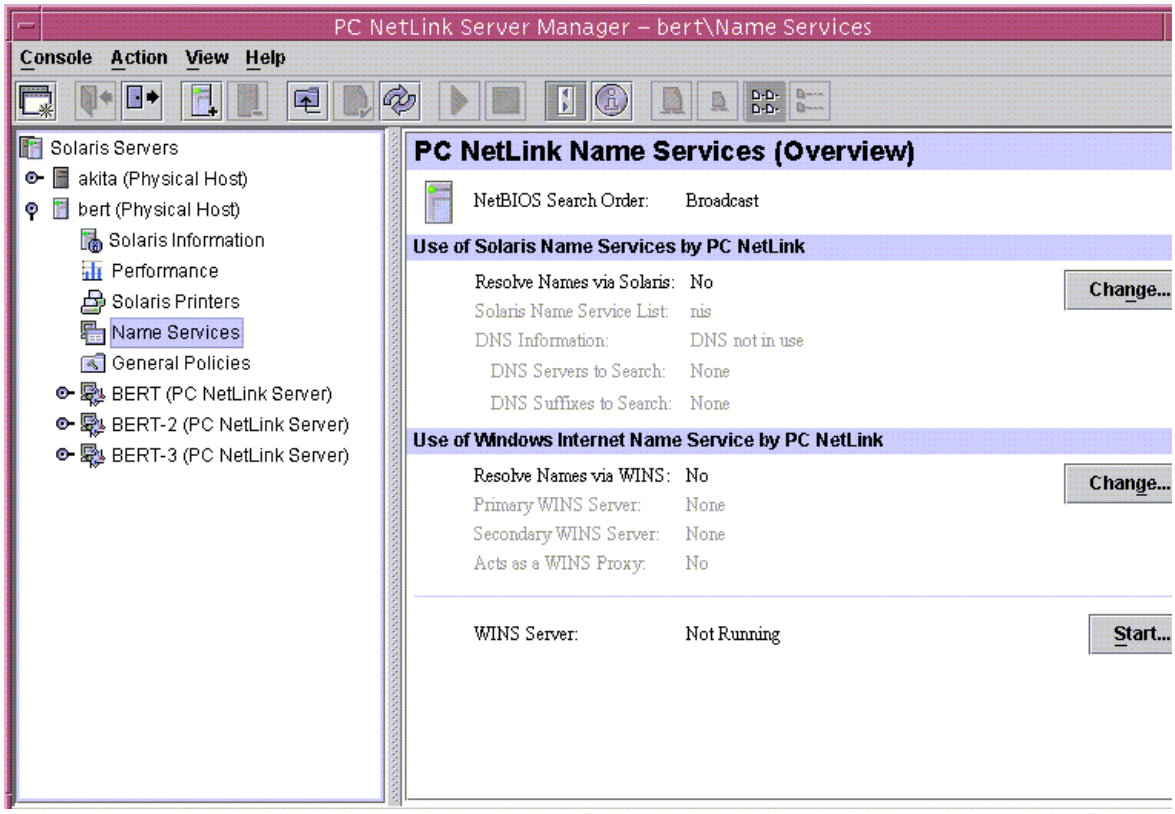
Only one WINS server can run on a physical host.

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose WINS configuration you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click Name Services.**

   A screen that lists current name services configuration appears, similar to the following.



3. **Click the button at the bottom of the window.**

   Depending on whether the WINS server is currently running, the button text reads either Start or Stop. When starting a WINS server, you can specify the virtual server on which it will run.

▼ How to Start or Stop WINS From the Command Line

Only one WINS server can run on a physical host.

- **At the PC NetLink command line, type one of the following commands:**

```
net start wins
net stop wins
```

▼ How to Configure a LAN Adapter (Lana) Device

You configure NetBIOS policy on a system-wide basis; the policy affects all virtual servers on a physical host.

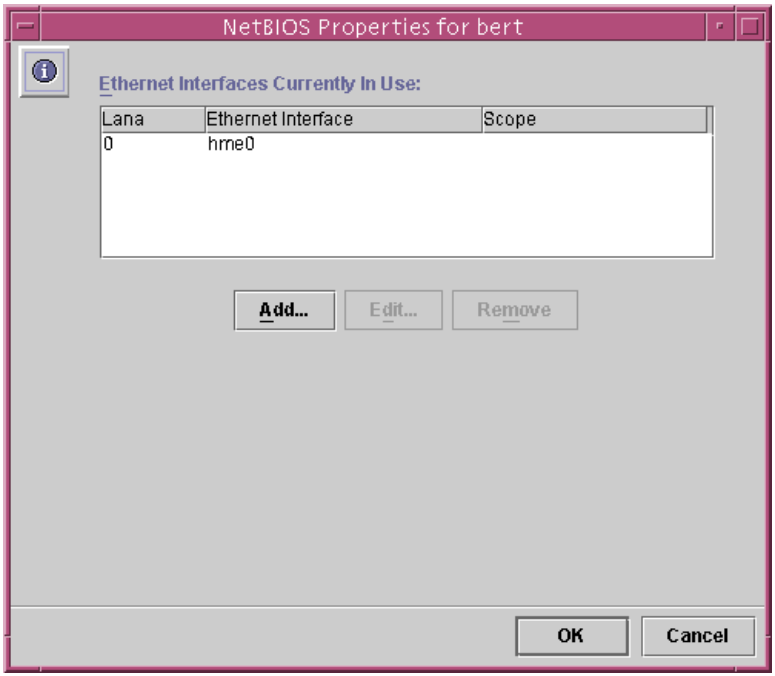
1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose NetBIOS policy you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the General Policies icon.**

3. **Double-click NetBIOS.**

   The following screen appears.



4. **In the Ethernet Interface table, click to highlight the name of the device that you want to configure.**

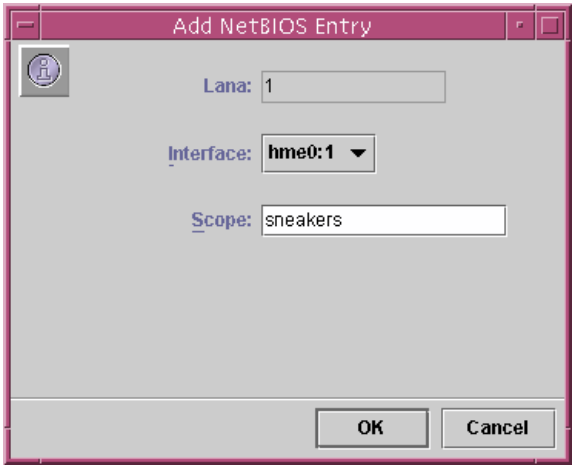
   For background information on NetBIOS, see "NetBIOS" on page 138.

5. **Depending on whether you want to add, edit, or remove an interface and its Lana entry, do the following:**

   - If you want to *add* an interface and Lana entry, go on to the next step.
   - If you want to *edit* an interface and Lana entry, go to Step 7.
   - If you want to *remove* an interface and Lana entry, go to Step 8.

6. **Click Add.**

   The following screen appears.



   a. **Click the drop-down Interface list to choose the available interface you want to add.**

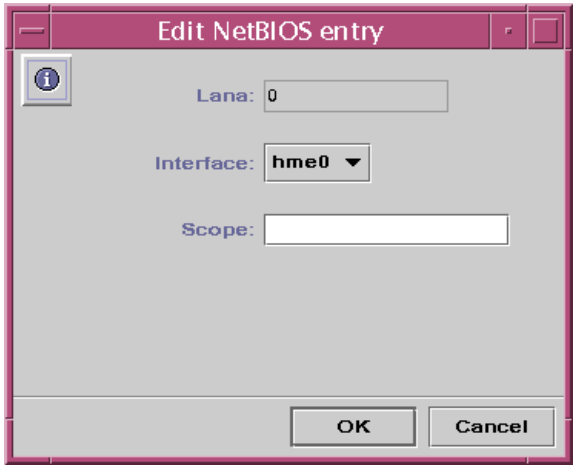
   b. **(Optional) In the Scope text field, type the name of the scope that you want the added device to serve.**

      The scope name can contain a maximum of 63 characters consisting of the uppercase or lowercase letters A-Z, the numerals 0-9, and all standard symbols.

   c. **Click OK.**

7. **Select the entry you want to edit and then click Edit.**

   The following screen appears.



   a. **Click the drop-down Interface list to assign a different available interface to the local system.**

   b. **(Optional) In the Scope text field, edit or create the name of the scope that you want the edited device to serve.**

      The scope name can contain a maximum of 63 characters consisting of the uppercase or lowercase letters A-Z, the numerals 0-9, and all standard symbols.

   c. **Click OK.**

8. **Select the entry you want to remove and then click Remove.**

   Note that PC NetLink Server Manager will not permit you to remove a Lana entry if it is the *only remaining* Lana entry.

▼ How to Configure Solaris Name Services

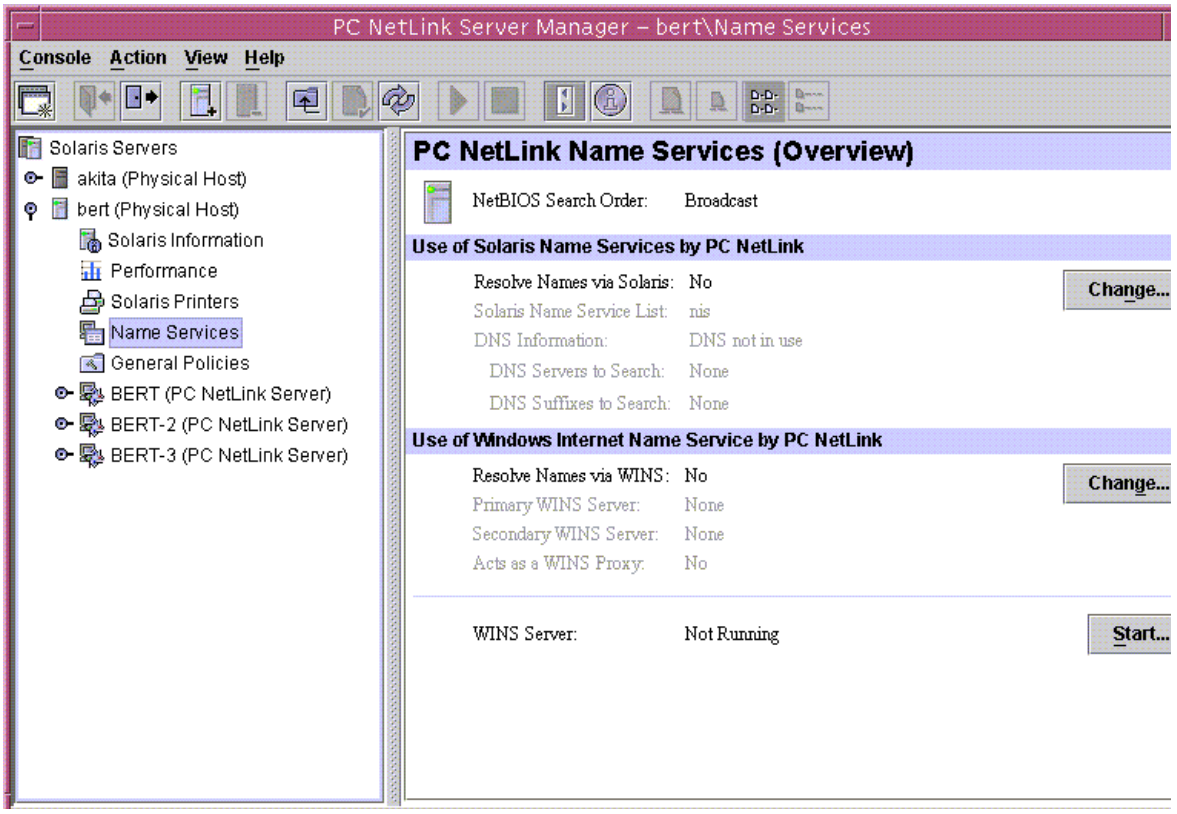
You configure Solaris name services policy on a system-wide basis; the policy affects all virtual servers on a physical host.

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose name services policy you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

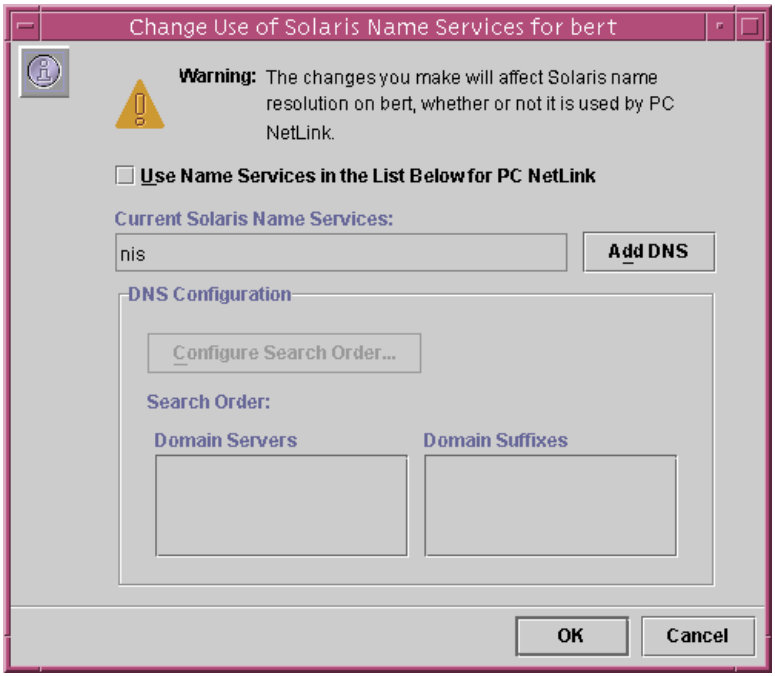
2. **In the Results pane, double-click Name Services.**

   A screen that lists current name services configuration appears, similar to the following.



3. **Click Change in the Solaris Name Services pane.**

   The Change Use of Solaris Name Services window appears, similar to the following.



4. **Check the box Use Name Services in the List Below for PC NetLink.**

   You *must* check Use Name Services in the List Below for PC NetLink in order to use DNS, even if DNS is the only service you want to use. If "dns" is not in the list of name services, the button to the right of the list reads Add DNS; if "dns" is in the list, the button reads Remove DNS.

   Solaris name services are read from the file `nsswitch.conf`. To change the list of services, other than adding or deleting DNS, you need to edit that file.

5. **Click Add DNS or Remove DNS to change the configuration.**

6. **Click Configure Search Order to configure the DNS server search order.**

   In the window that appears, you can specify up to three DNS server IP addresses to search, and up to six domain suffixes. Select an entry and click on Up or Down as necessary to configure the search order.

7. **Click OK.**

   The Change Use of Solaris Name Services window reappears. You can specify DNS server names and suffixes in the fields provided.

8. **Click OK to complete the configuration change, or click Cancel to cancel the operation.**

▼ How to Configure PC NetLink Server Manager Security Policy

You configure PC NetLink Server Manager security policy on a system-wide basis; the policy affects all virtual servers on a physical host.

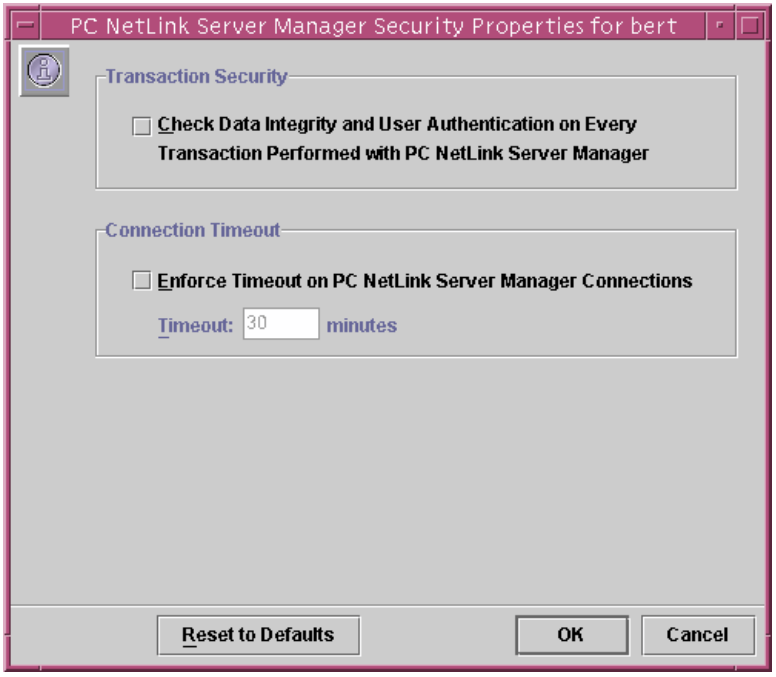
1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose PC NetLink Server Manager security policies you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **Double-click General Policies.**

3. **Double-click PC NetLink Server Manager Security.**

   The following screen appears.



4. **Do one or both of the following:**
   - Check the Transaction Security box to require client authentication for PC NetLink Server Manager transactions and to invoke public key signatures to protect data that is passed between the server and clients.
   - Click the Connection Timeout box to specify a period of time after which PC NetLink Server Manager connections expire. Specify the time period, in minutes, in the provided text field.
5. **Click OK, Cancel, or Reset to Defaults.**

▼ How to Configure PC NetLink Server Performance Monitoring and Alarms

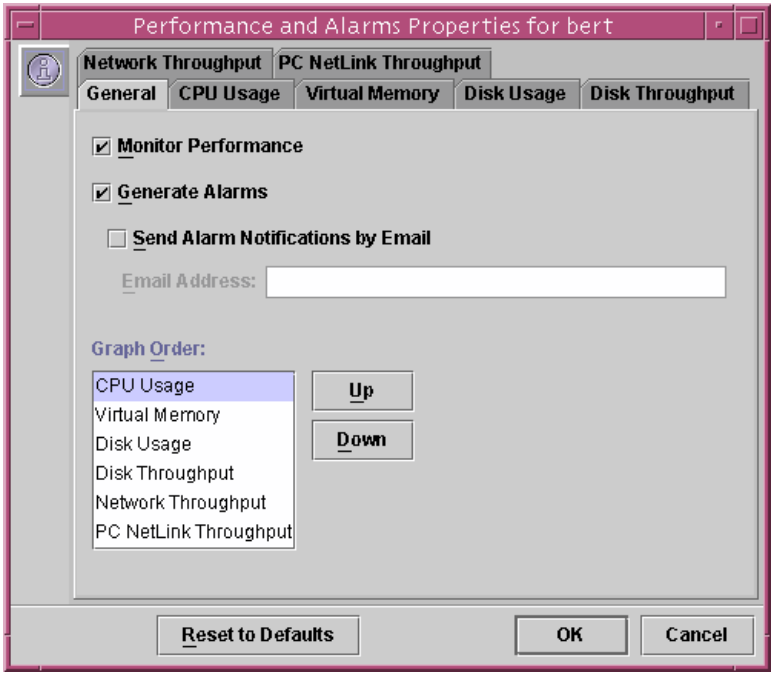
You configure PC NetLink server performance monitoring and alarms on a system-wide basis; the policy affects all virtual servers on a physical host.

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose performance and alarms policies you want to change.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.
2. **Double-click General Policies.**

3. **Double-click Performance and Alarms.**

   A window similar to the following appears.



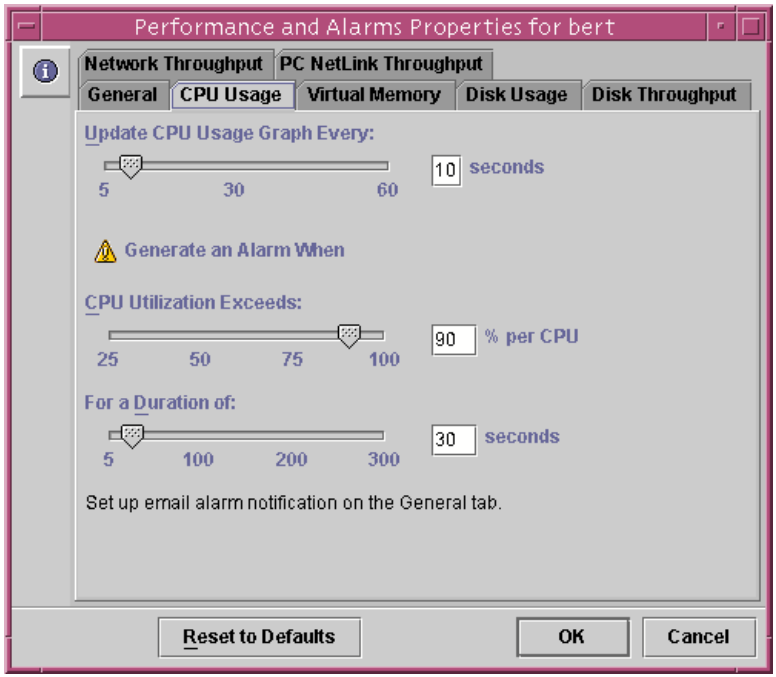
4. **Check or uncheck Monitor Performance and Generate Alarms according to the performance monitoring and performance alarm policy you want to set for this PC NetLink server. You can also check Send Alarm Notifications by Email and type an email address.**

5. **Depending on your policy, do one of the following:**

   - If you are finished electing whether to monitor performance or show alarms and are satisfied with the defaults, click OK to put the policy into effect or Cancel to make no changes and dismiss the dialog box. Continue with Step 8.
   - If you have elected to generate alarms but want to adjust the threshold at which alarms are generated, continue with Step 6.

6. **Click the tab that represents the performance parameter whose alarm threshold you want to change.**

   In the following example, CPU Usage is the parameter to be adjusted.



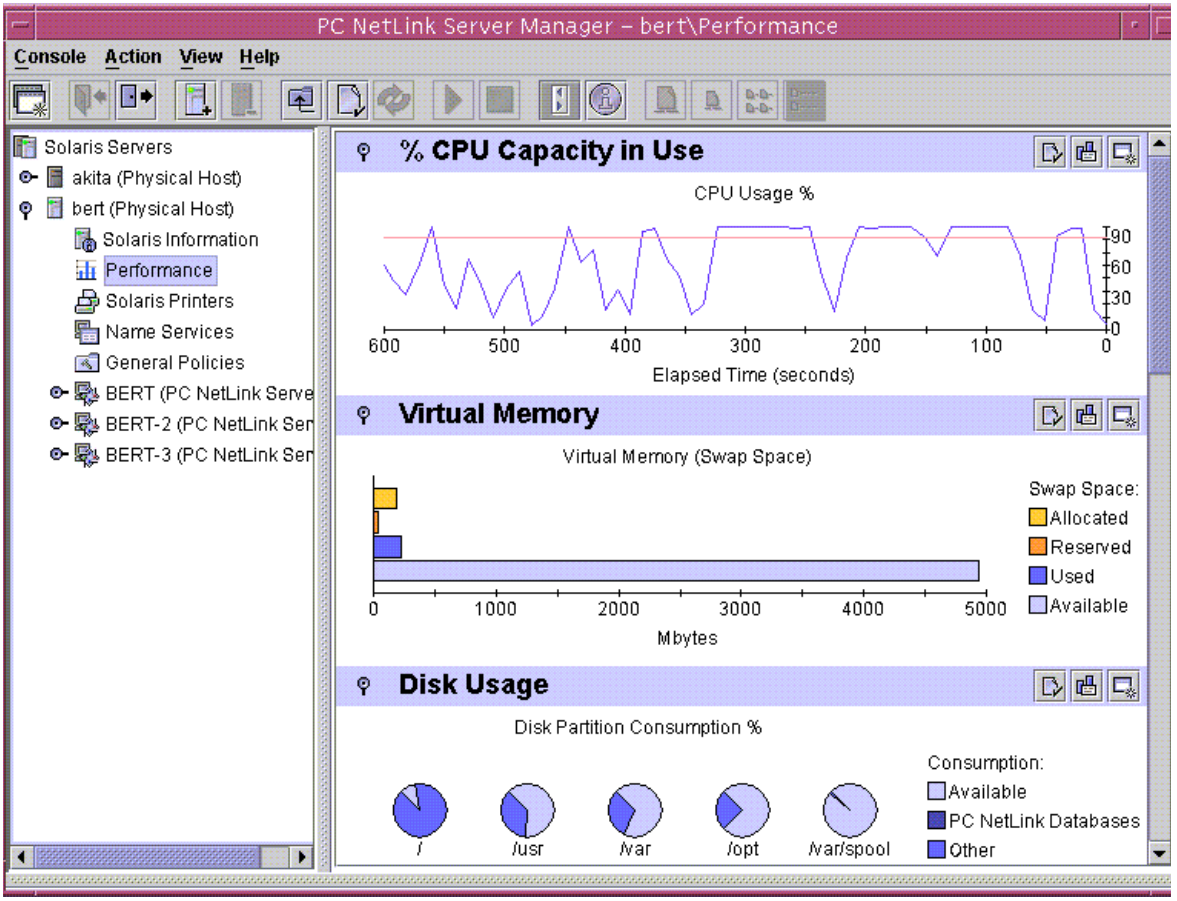
7. **Using the sliders, adjust performance alarm thresholds according to your policy.**

8. **Click OK to dismiss the window and make the changes effective, Cancel to dismiss the window and leave thresholds unchanged, or Reset to Defaults. If you choose Reset to Defaults, click OK to dismiss the window.**

▼ How to Monitor Physical Host Performance

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose performance information you want to view.**
2. **In the Results pane, double-click Performance.**

   A screen similar to the following appears.



The graphical display reports various established performance parameters at intervals that you can set. The displayed parameters are:

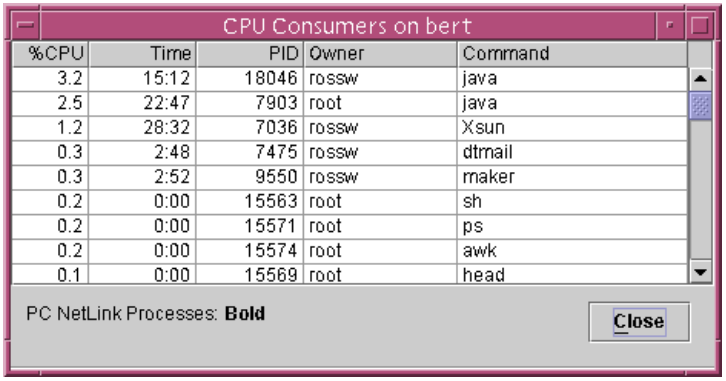
- *% CPU Capacity in Use* – This line graph measures utilization of the monitored server's CPU over a set period of time. Time (in seconds) is measured on the X (horizontal) axis and percentage of total CPU capacity is measured on the Y (vertical) axis. This display also accounts for multiple CPUs. The range of the Y

axis is 0 to 100*n*, with *n* representing the number of CPUs. For example, if you were to keep the default alarm threshold set at 90%, and you have a two-CPU system, then you will see the alarm threshold line at 180%: 90% times two CPUs.

- *Virtual Memory (also known as swap space)* – This bar chart illustrates the amount of virtual memory that is allocated, reserved, used, and available to the monitored server. When you place the mouse pointer over any of the bars, a number appears indicating the absolute value of the bar.
- *Disk Usage* – These pie charts illustrate available disk space, disk space consumed by PC NetLink databases, and total other disk space consumed on each of the server's *local* disk partitions. When you place the mouse pointer over any of the pie charts, a number appears indicating the absolute value of the chart.
- *Disk Throughput* – Measuring transfers-per-minute, kilobytes-per-minute, and average service time, these bar graphs illustrate utilization of each *local* disk partition in the monitored system. When you place the mouse pointer over any of the bars, a number appears indicating the absolute value of the bar.
- *Network Throughput* – This line graph reports transmission of network packets, packet collisions, and packet transmission errors over the course of time, measured in seconds.
- *PC NetLink Throughput* – This line graph reports the average service times, in milliseconds, of PC NetLink services to Windows NT clients, and, measured in seconds, bytes received over time from Windows NT clients and sent to clients by the monitored PC NetLink server. PC NetLink throughput is displayed for an individual virtual server. If the physical host has multiple instances, you can select which server's throughput to display by choosing its instance number from the drop-down menu provided.

Each of the parameters offers more detailed "drill-down" views of the generated statistics. You reveal these views by clicking the following icon:

This icon is the center of the three icons that are at the extreme right of the parameters' title. Representative of the drill-down detailed view is, for example, the listing of CPU consumers on a PC NetLink physical host named "bert," which is the drill-down view of the % CPU Capacity in Use parameter.



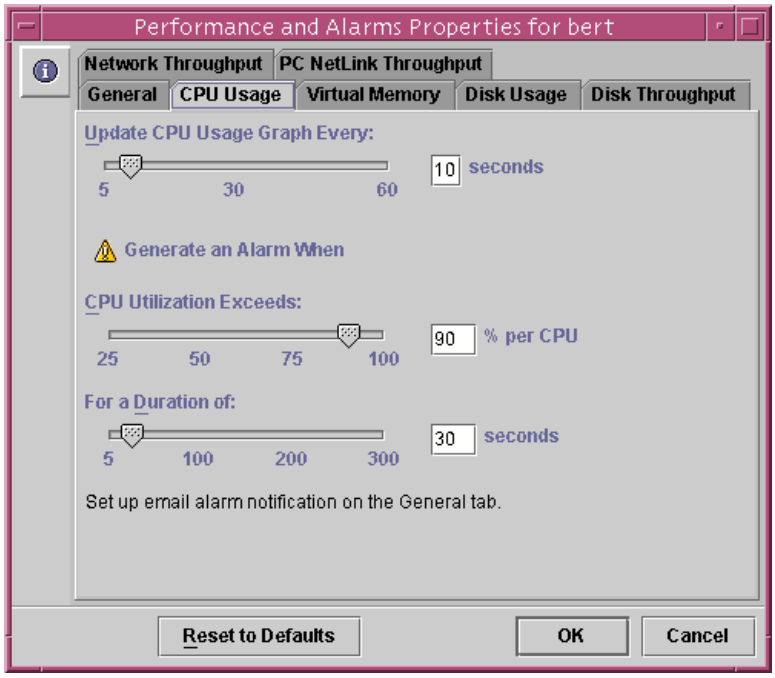
In all of these displays, exclusive PC NetLink processes are shown in boldface type.

To focus your attention on one specific performance parameter, you can use the "tear-off" window feature. This feature creates a separate window with information pertaining only to the parameter you selected. To display a tear-off window, you click the icon at the right of the group of three icons discussed above. It looks like the following:

Clicking the icon at the left of the group of three icons reveals the Performance Properties window, which you will use in the following step. It looks like the following:

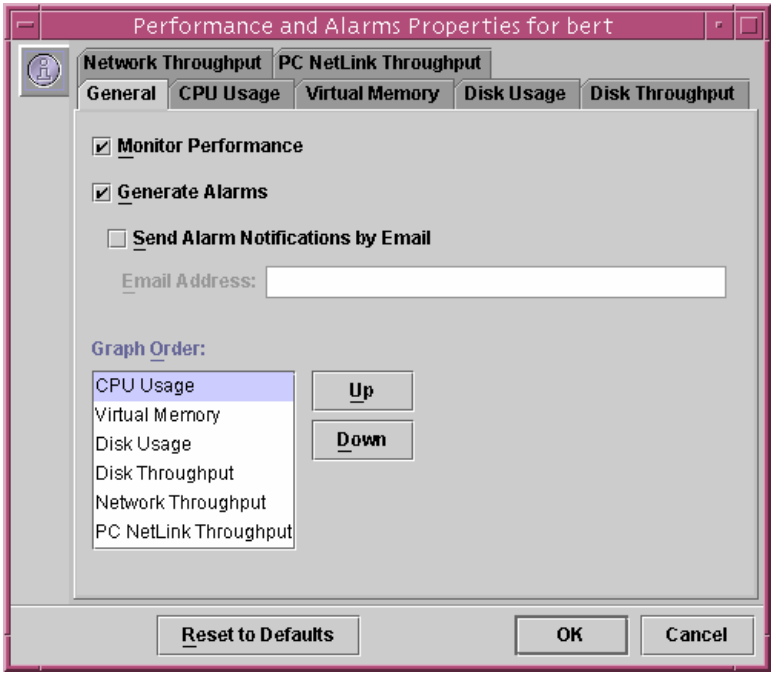
3. **In the title bar of any of the performance parameter displays, click the Performance Properties window icon.**

   The following window appears.



4. **Click the General tab.**

   The following window appears.

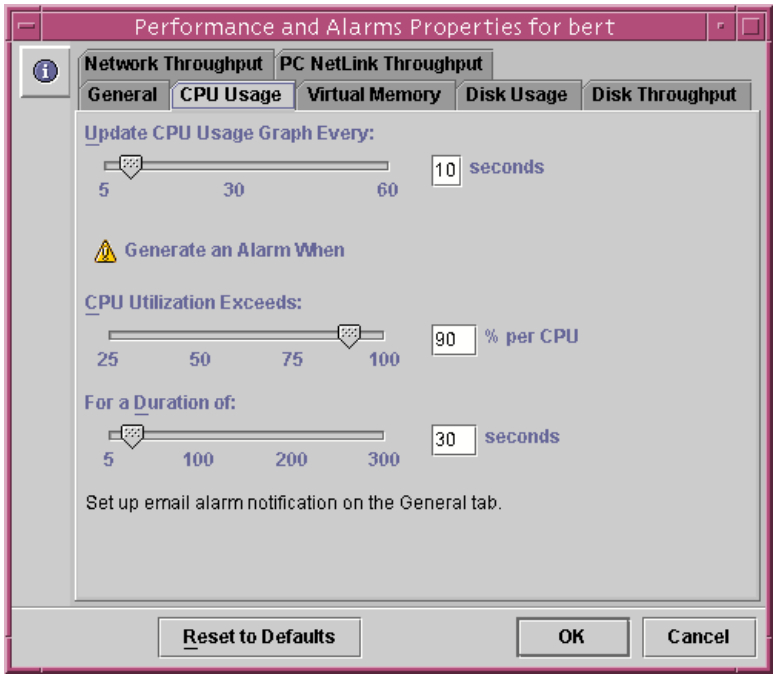


5. **Check or uncheck Monitor Performance and Generate Alarms according to the performance monitoring and performance alarm policy you want to set for this PC NetLink server. You can also check Send Alarm Notifications by Email and type an email address.**

6. **Depending on your policy, do one of the following:**
   - If you are finished electing whether to monitor performance or show alarms and are satisfied with the defaults, continue with Step 9.
   - If you have elected to generate alarms but want to adjust the threshold at which alarms are generated, continue with Step 7.

7. **Click the tab that represents the performance parameter whose alarm threshold you want to change.**

   In the following example, CPU Usage is the parameter to be adjusted.



8. **Using the sliders, adjust performance alarm thresholds according to your policy.**

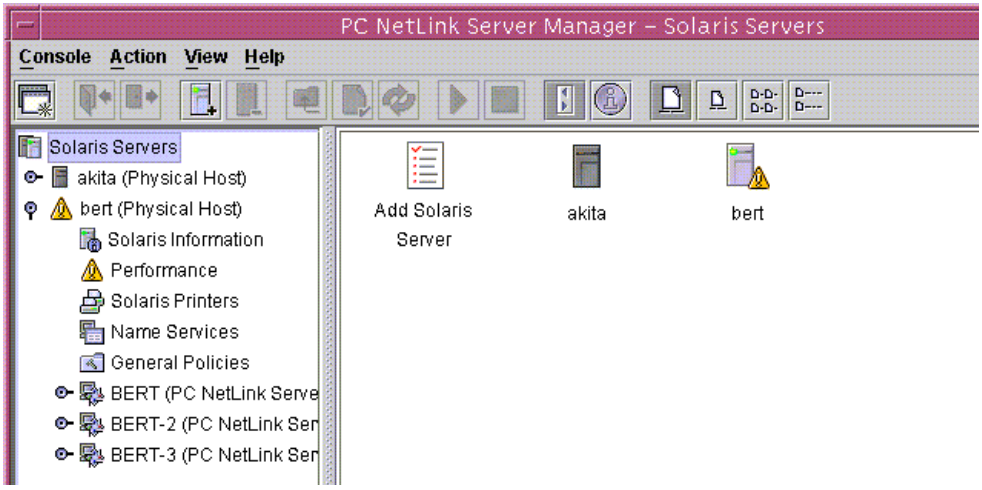
9. **Click OK to dismiss the window and make the changes effective, Cancel to dismiss the window and leave thresholds unchanged, or Reset to Defaults. If you choose Reset to Defaults, click OK to dismiss the window and set the default values.**

▼ How to Investigate Performance Alarms

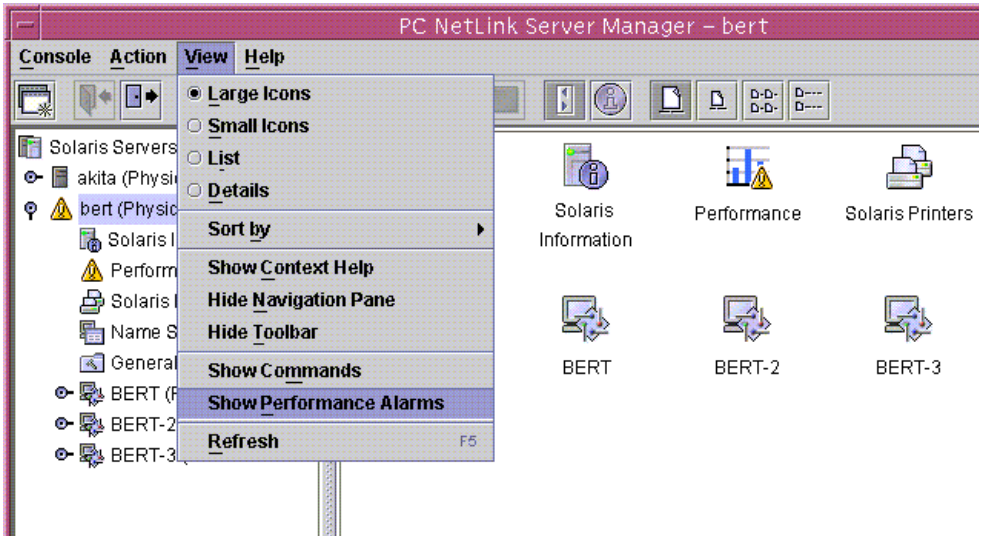
1. **In the main Results pane and Navigation pane of PC NetLink Server Manager, look for any Solaris server with an alarm symbol.**

   In the following illustration, the Solaris server named bert has an alarm associated with it (in this case it is shown in both panes). Alarm icons also appear in performance graph toolbars.

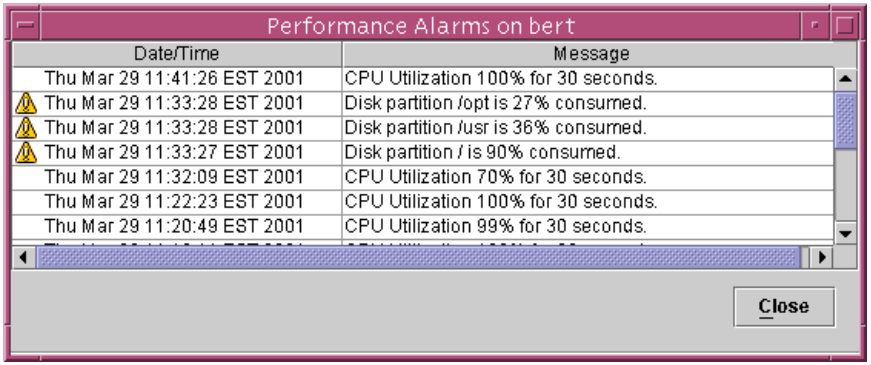
   .



2. **With the name of the server highlighted, choose Show Performance Alarms from the View menu.**



A screen similar to the following appears. (Note that the Disk Usage alarm threshold, for purposes of this illustration, has been set to an impractically low level of 25% for 300 seconds. The default of 95% for 300 seconds is more realistic under normal conditions.)



About Event Monitoring

An *event* is any significant occurrence in the system (or in an application). Such events are *NT events*, which you can also see in the NT Event Viewer. Some critical events are noted in on-screen messages. An event that does not require immediate attention is noted in an *event log*. Event logging starts automatically every time you start the PC NetLink program. With an event log displayed by the PC NetLink Server Manager tool, you can troubleshoot various problems and monitor PC NetLink security events.

PC NetLink software records events in the following types of logs:

- *System log* – Contains events logged by PC NetLink system components. For example, the failure of a service to start during startup is recorded in the System log. The types of events that are logged by system components are determined by the PC NetLink program.
- *Security log* – Contains various security-related data, such as valid and invalid logon attempts and events related to resource use, such as creating, opening, or deleting files or other objects.
- *Application log* – Contains events logged by applications. For example, a database program might record a file error in the Application log. Application developers decide which events to monitor.

System and Application logs can be viewed by all users; Security logs are accessible only to system administrators.

Interpreting an Event

Event logs consist of a *header*, a *description* of the event (based on the event type), and *additional data*. Most Security log entries consist of the header and a description.

PC NetLink Server Manager displays events from each log separately. Each line shows information about one event, including date, time, source, category, event ID, user account, and computer name.

Event Header

An event header contains the following information:

- *Date* – The date the event occurred.
- *Time* – The time the event occurred.
- *Source* – The software module that logged the event, which can be either an application name or a component of the system or of a large application, such as a service name.
- *Category* – A classification of the event by the event source. This information is used primarily in the Security log.
- *Event* – A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the log service is started. The first line of the description of such an event is "The Event log service was started." The event ID and the source of the event can be used by product support representatives to troubleshoot system problems.
- *User* – The user name of the user on whose behalf the event occurred. If the event is not logged by a user, then the Security ID of the logging entity is displayed.
- *Virtual Server* – The name of the virtual server on which the event occurred.

Event Description

The format and contents of the event description vary, depending on the event type. The description is often the most useful piece of information, indicating what happened or the significance of the event.

Event Types

The PC NetLink Server Manager logs indicate the event types:

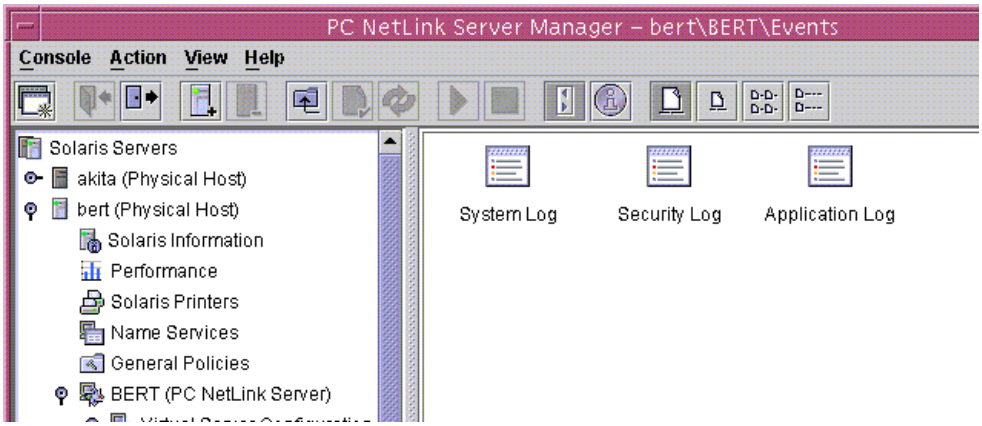
- *Error* – Significant problems, such as a loss of data or loss of functions. For example, an Error event is logged when a service was not loaded during PC NetLink startup.
- *Warning* – Events that are not necessarily significant, but that indicate possible future problems. For example, a Warning event is logged when the server is low on key resources.
- *Information* – Infrequent significant events that describe successful operations of major server services. For example, when a service starts successfully, it would log an Information event.
- *Success Audit* – Audited security access attempts that were successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
- *Failure Audit* – Audited security access attempts that failed. For example, if a user tried to access a network drive and failed, the attempt is logged as a Failure Audit event.

Additional Data

The data field contains binary data that you can display in bytes or words. The application that was the source of the event record generates this information. Because the data appears in hexadecimal format, only someone who is familiar with the source application can interpret its meaning.

Using PC NetLink Server Manager to View Events

You determine which event log to view by switching between the System, Security, and Application logs that are available in the Events group within PC NetLink Server Manager.



- *Selecting a log* – Double-click the appropriate log icon for event viewing. You can choose to view the logs of any PC NetLink server after you have logged on to it. Once you have opened a log, you can sort by any column by clicking on the column head—and reverse-sort by clicking the column head again.
- *Refreshing the view* – When you first open a log file, PC NetLink Server Manager displays the current information for that log. This information is not updated automatically. To see the latest events and to remove overwritten entries, choose Refresh from the View menu or click the Refresh button in the toolbar.
- *Viewing details about events* – For many events, you can view more information by double-clicking the event. The Event Detail dialog box shows a text description of the selected event and any available binary data for the selected event. This information is generated by the application that was the source of the event record. Because the data appears in hexadecimal format, its meaning can be interpreted only by someone who is familiar with the source application. Not all events generate such data.

Note – To control the types of security events that are audited, you set Audit policies by way of your Windows NT tools. You do not use PC NetLink Server Manager to set Audit policies; therefore, this guide does not include those instructions.

Using Event Logs to Troubleshoot Problems

Careful monitoring of event logs can help you to predict and identify the sources of system problems. Logs also can confirm problems with Windows NT application software. If a Windows NT application crashes, an Application event log can provide a record of activity leading up to the event.

The following are guidelines for using event logs to diagnose problems:

- Determine how frequently an error occurs. If a particular event seems related to system problems, search the event log to find other instances of the same event or to judge the frequency of an error.
- Note Event IDs. These numbers match a text description in a source message file. Product support representatives can use this number to understand what occurred in the system.

Monitoring PC NetLink Security Events

You enable auditing from the Windows NT User Manager for Domains Auditing Policy dialog box. Through auditing, you can track PC NetLink security events. You can specify that an audit entry is to be written to the Security event log whenever certain actions are performed or files are accessed.

An audit entry shows the activity that occurred, the user who performed the action, and the date and time of the activity. You can audit both successful and failed attempts. The audit trail can show who actually performed actions on the network and who tried to perform actions that are not permitted.

Events are not audited by default. If you have Administrator permission, you can specify which types of system events are audited through the Windows NT User Manager for Domains tool.

The Audit policy determines the amount and type of security logging that PC NetLink software performs. For file and object access, you can specify which files and printers to monitor, which types of file and object access to monitor, and for which users or groups. For example, when File and Object Access auditing is enabled, you can use the Security tab in a file or folder's Properties dialog box to specify which files are audited and what type of file access is audited for those files.

▼ How to Monitor Events Using PC NetLink Server Manager

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server whose event logs you want to view.**

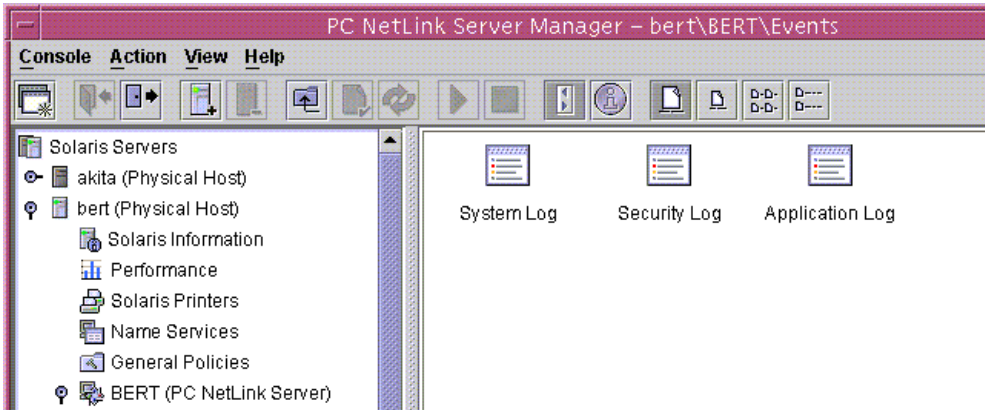
   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Events.**

   The following screen appears.



4. **Double-click the name of the log that you want to view.**

5. **Double-click any line in the log to see more details about the particular event.**

   For background information about interpreting events, see "Interpreting an Event" on page 164.

▼ How to Monitor Events From the Command Line

You can use the PC NetLink `elfread` command to read System, Security and Application logs. This command is especially useful when troubleshooting a PC NetLink system that has failed to start. (Events of this type typically are written to the System log.) Use the `elfread` command as a backup to the PC NetLink Server Manager, which is the recommended method of viewing log files when the server is running.

- **At the PC NetLink command prompt, type the following command:**

  `elfread [-od]` *logname*

  Replace *logname* with one of the following log types: System, Security, or Application.

  To display the log file contents listing the oldest event first, use the `-o` option. To display detailed information about events, use the `-d` option.

  If no options are specified, a summary of all events in the specified log is displayed in reverse chronological order.

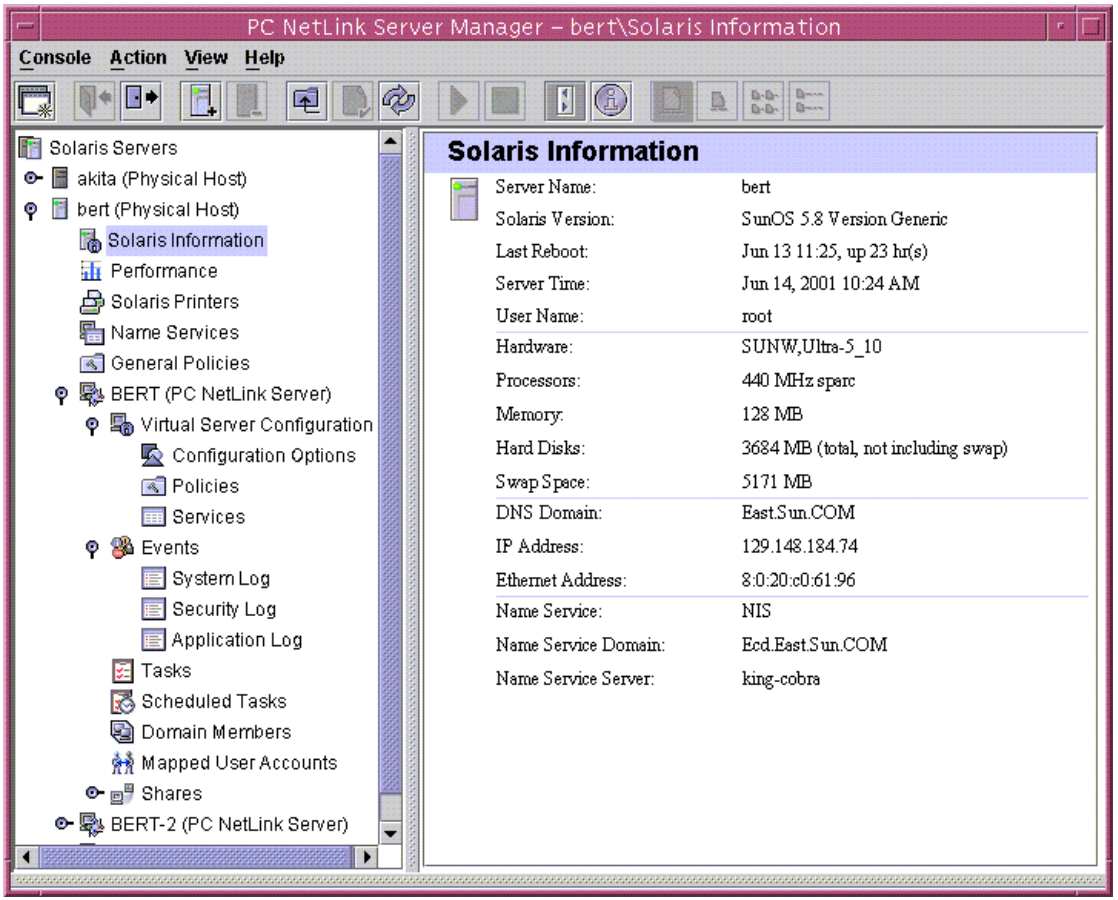
▼ How to View Solaris Physical Host Information

1. **Using PC NetLink Server Manager, log on as root to the Solaris server whose Solaris information you want to view.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click Solaris Information.**

   The following screen appears.



The data displayed in the Solaris Information view is current, though not automatically updated. To update the view with the most recent data, choose Refresh from the View menu or click the Refresh button in the toolbar. The following information is provided:

- Server name
- Solaris operating environment version
- The last time the system was rebooted
- The current date and time on the server
- The name of the *current* user
- The hardware description
- The system's processors type
- The amount of random access memory
- Total (not including swap) space on disks
- Swap space
- DNS domain name
- Internet Protocol (IP) address of the system
- Ethernet address of the system
- The name service currently in use
- The name service domain name
- The name of the name service server

▼ How to View or Change PC NetLink Virtual Server Configuration Options

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server whose PC NetLink information you want to view.**

   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

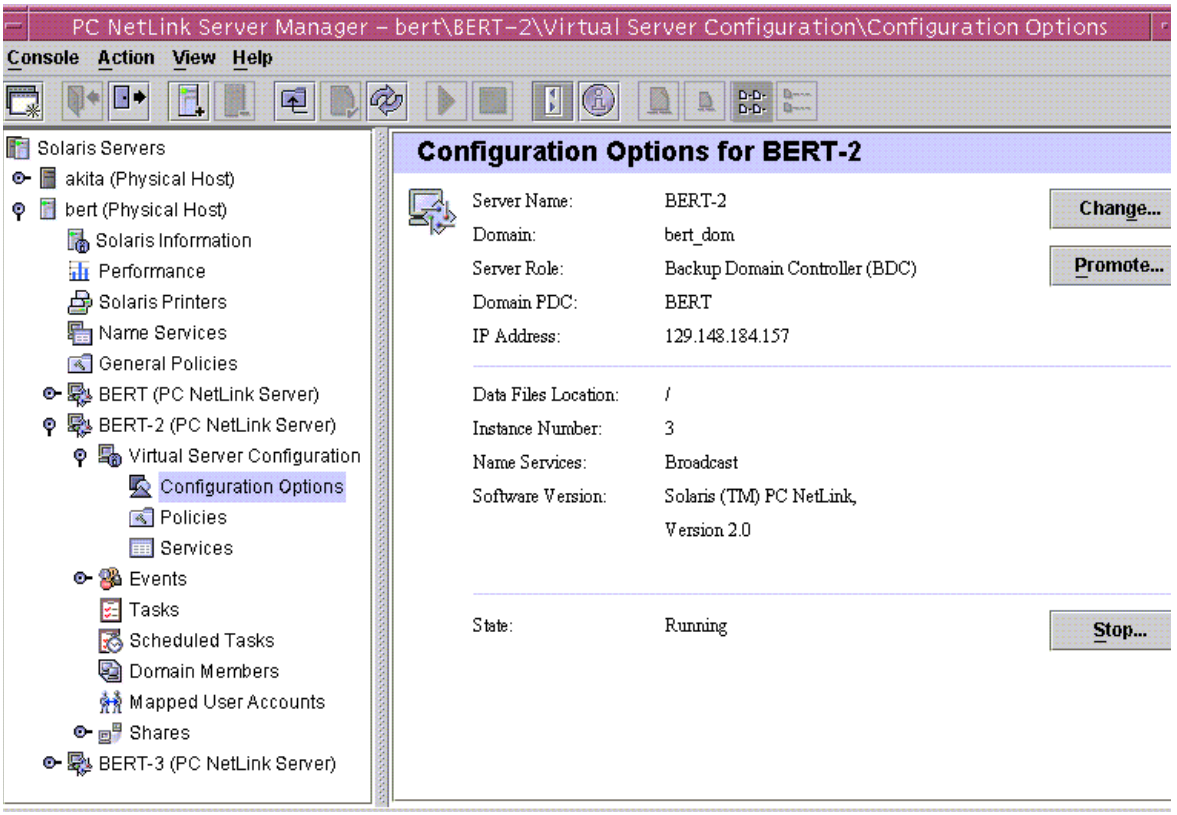
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Virtual Server Configuration.**

4. **In the Results pane, double-click Configuration Options.**

   The following screen appears.



The data displayed is current, though not automatically updated. To update the view with the most recent data, choose Refresh from the View menu or click the Refresh button in the toolbar.

The following information is provided:

- PC NetLink server name
- PC NetLink server's domain name
- PC NetLink server's role
- The name of the domain PDC, if the server is a BDC or member server
- PC NetLink server Internet Protocol (IP) address
- Data files location (directory path on the physical host)
- Server instance number
- Name service currently in use
- PC NetLink software version number
- State of the server (stopped or running)

- High Availability is shown if the server is configured for high availability.

In addition to furnishing you with vital information, the Configuration Options window includes three buttons from which you can initiate various administrative tasks:

- *Change* – By clicking this button, you can initiate changes to the configuration of the PC NetLink system, including its server name, domain name, and domain role. See the section, "About Domain Configuration and Management" on page 62, along with the instructions that are included in that section. See "How to Create a New PC NetLink Virtual Server" on page 67 for a list of disallowed server name characters.
- *Promote* – Clicking this button, which is available only for BDCs, enables you to upgrade the role of the server within its domain. See the section, "How to Promote a BDC Within Its Domain" on page 89.
- *Stop (Start)* – Depending on whether the PC NetLink program is running or stopped, this button enables you to stop or start the program. See the section, "About Starting and Stopping Services" on page 46, along with the instructions that are included in that section.

▼ How to Add a Computer Account to a Domain

1. **Using PC NetLink Server Manager, log on to the Solaris physical host for a PC NetLink virtual server that is in the domain to which you want to add a member.**

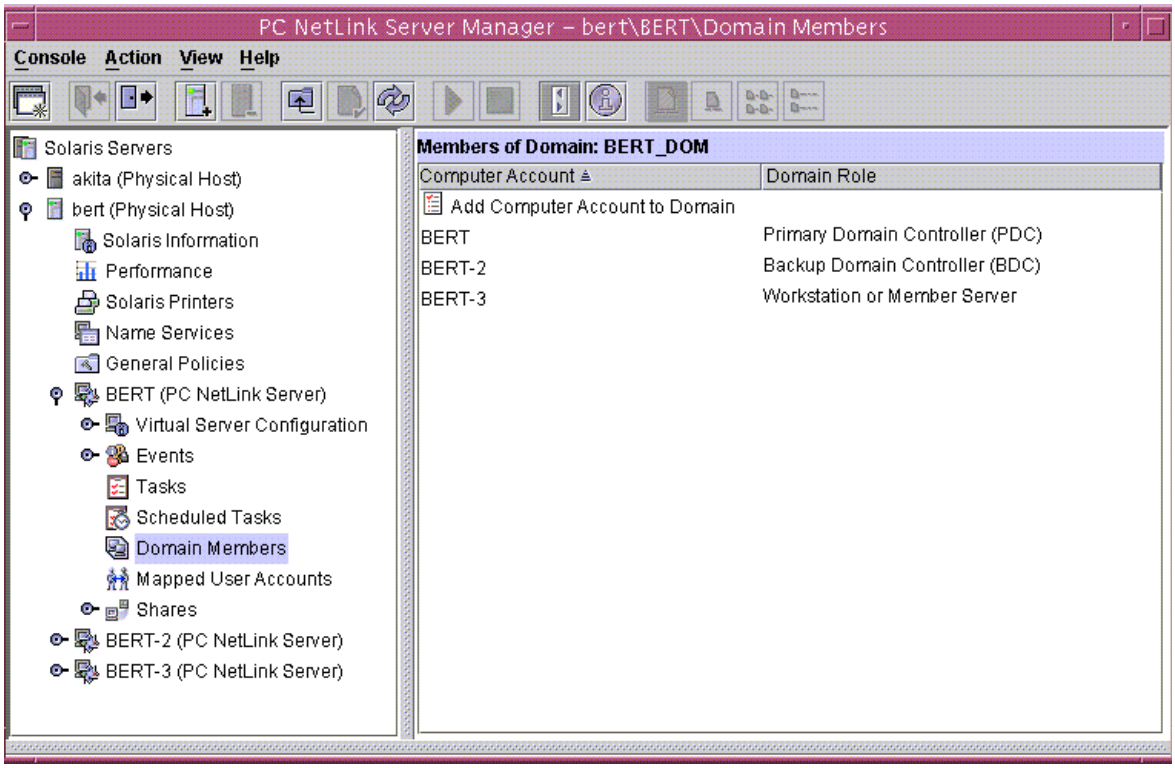
   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents a PC NetLink PDC or BDC in the domain.**

   The Results pane changes, displaying a list of seven administrative categories.

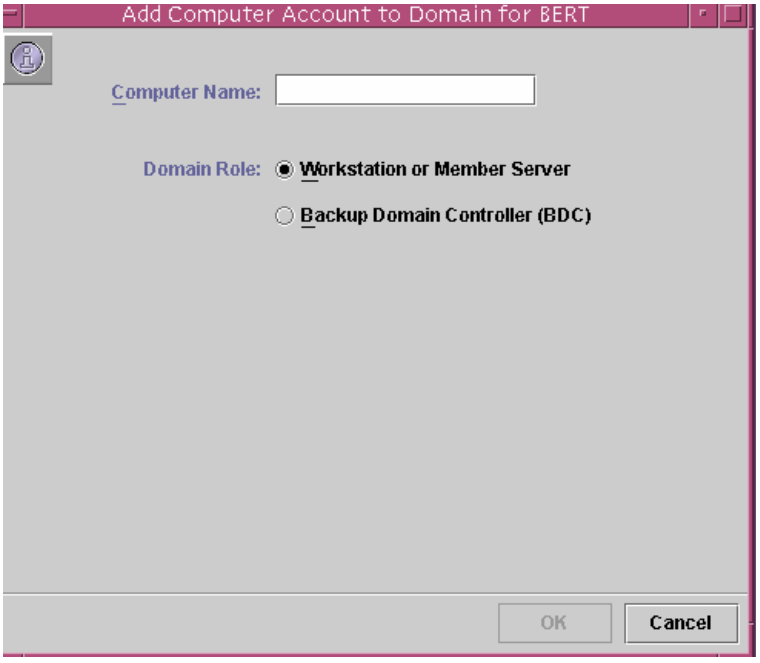
3. **Double-click Domain Members.**

   A screen similar to the following appears.



4. **Double-click Add Computer Account to Domain.**

The following screen appears.



5. **Enter the computer name and choose a domain role, then click OK.**

▼ How to Delete a Domain Member

1. **Using PC NetLink Server Manager, log on to the Solaris physical host for a PC NetLink virtual server that is in the domain from which you want to delete a member.**

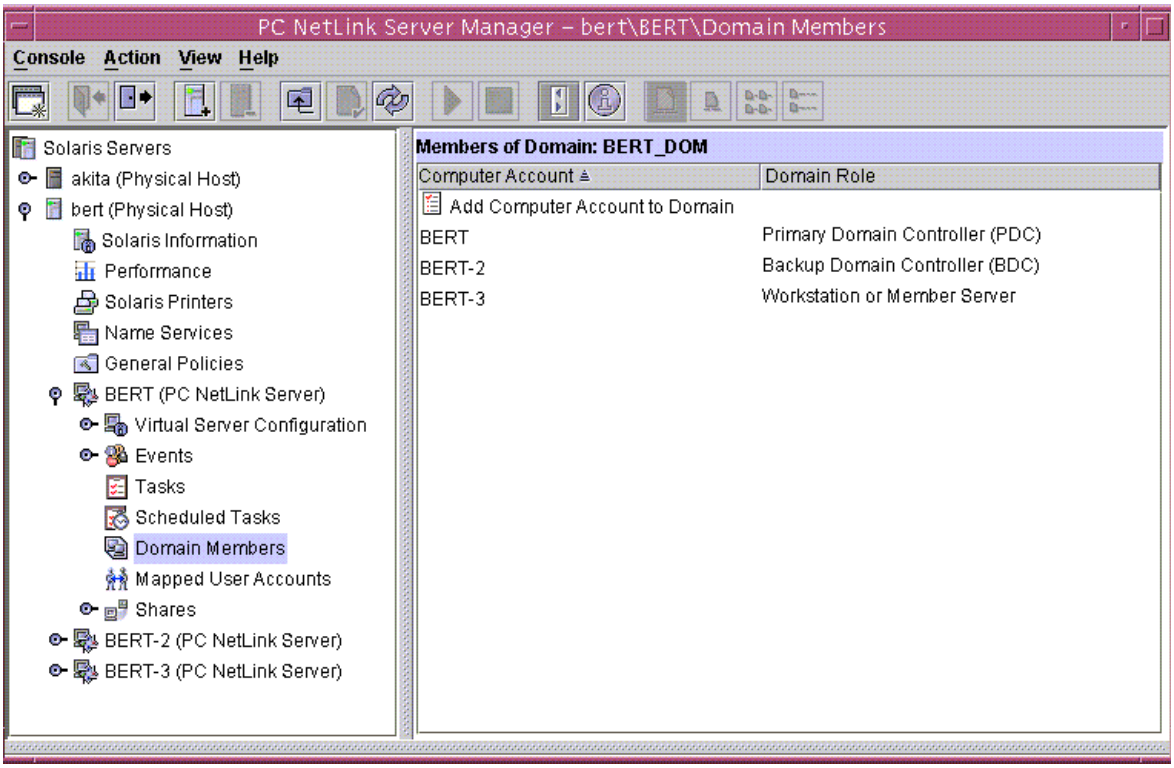
   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents a PC NetLink PDC or BDC in the domain.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Domain Members.**

   A screen similar to the following appears.



4. **Select the name of the domain member you want to delete and then choose Delete Domain Member from the Action menu.**

CHAPTER 4

Guide to Password Synchronization

This chapter provides information about configuring and using password synchronization.

Instructions are included in this chapter for accomplishing the following tasks:

- "Task 1a of 6 – How to Configure the Password Filter on a Solaris PDC" on page 181
- "Task 1b of 6 – How to Configure the Password Filter on a Native Windows NT PDC" on page 183
- "Task 2 of 6 – How to Install and Start the Name Server Agent" on page 184
- "Task 3 of 6 – How to Install and Configure the PAM Module for Each Solaris Client" on page 185
- "Task 4 of 6 – How to Configure the Password Daemon" on page 186
- "Task 5a of 6 – How to Enable Password Synchronization Using PC NetLink Server Manager" on page 187
- "Task 5b of 6 – How to Enable Password Synchronization Using the Command Line" on page 188
- "Task 6 of 6 – How to Initially Synchronize Account Passwords" on page 188

About Password Synchronization

Password synchronization enables PC NetLink 2.0 users to easily maintain one password for their mapped PC NetLink and Solaris accounts, by automatically applying any password change to both accounts.

Password synchronization employs several components to propagate password changes. As an administrator, you must manually install and configure these components before you can initialize password synchronization for PC NetLink 2.0 users:

- The *password filter* receives and forwards password change requests to the password daemon. You must install the password filter on your primary domain controller (PDC).
- The *name server agent* changes the Solaris password in your Solaris name service. You must install and start the name server agent on the machine acting as your name server master.
- The *PAM module* forwards password change requests from Solaris clients to the password daemon. You must install the PAM module on each Solaris client machine that will use PC NetLink and password synchronization.
- The *password daemon* receives all password change requests from Solaris and Windows NT, and can be located on any PC NetLink domain controller. The password daemon is loaded during your initial PC NetLink 2.0 installation.

In the sample configuration in FIGURE 4-1, you can follow the path of a password change by a Windows NT client in the PC NetLink 2.0 password synchronization environment. In this example, the password daemon and the password filter are running on a Solaris primary domain controller (PDC).

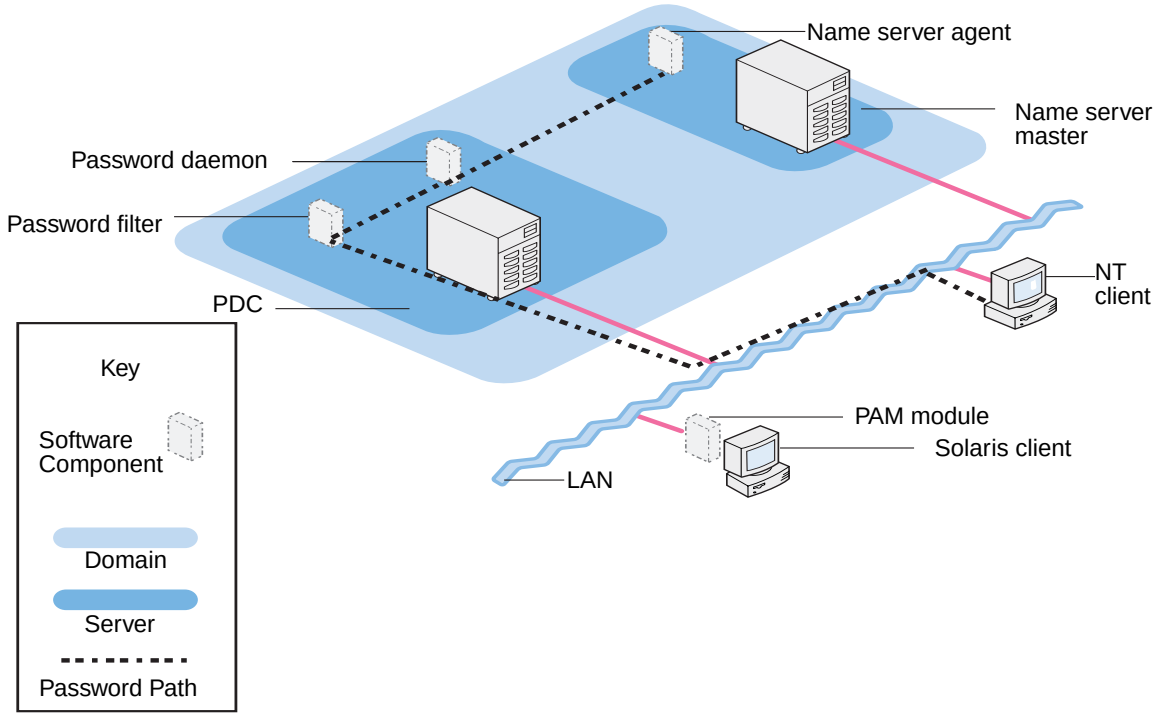


FIGURE 4-1 Password Change by a Windows NT Client With Password Synchronization Configured

In the sample configuration in FIGURE 4-2, you can follow the path of a password change by a Solaris client in the PC NetLink 2.0 password synchronization environment. In this example, the password daemon and the password filter are running on a Solaris PDC.

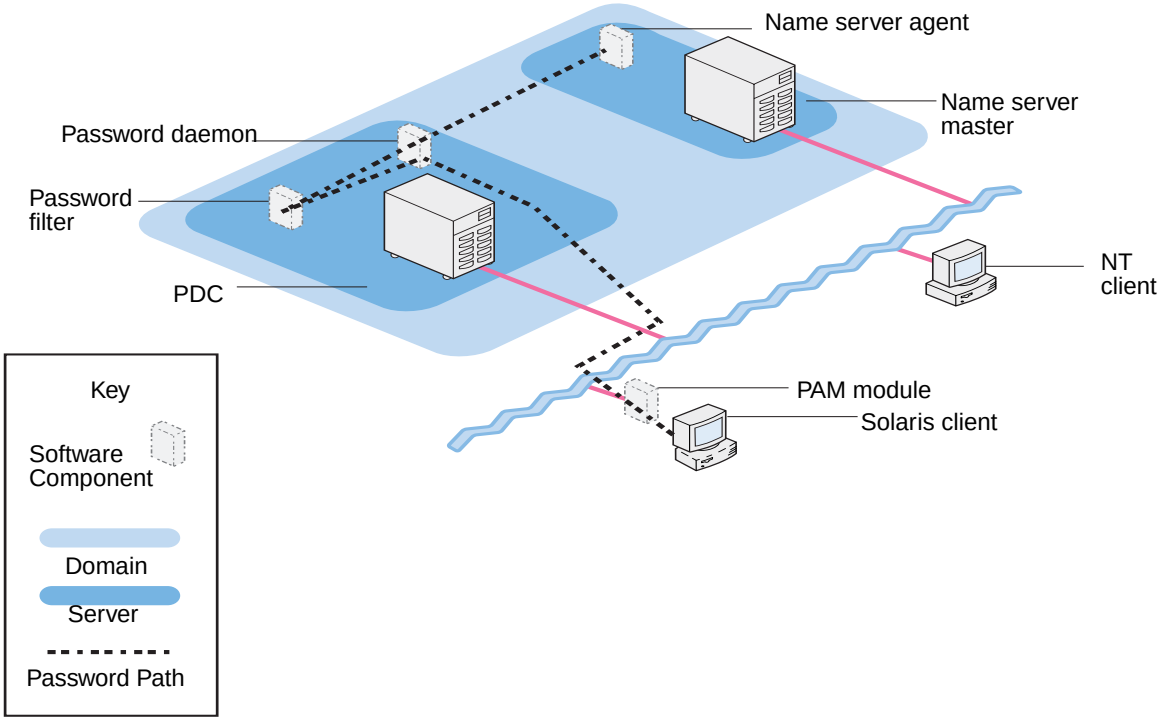


FIGURE 4-2 Password Change by a Solaris Client With Password Synchronization Configured

Suitable Environments

Password synchronization is a feature that requires precise configuration. You need to be familiar with your site's PC NetLink setup, including server roles, IP addresses, and administration privileges.

Your environment is suitable for password synchronization if:

- You run only one Solaris name service (NIS *or* Files). PC NetLink software can synchronize passwords for only one Solaris name service. While your system may be configured to use multiple name services, you cannot synchronize passwords across name services.
- You have mapped Windows NT accounts and Solaris accounts in a one-to-one ratio (you can only synchronize passwords from one Windows NT account to one Solaris account).
- You have only one Solaris domain but want to synchronize passwords within one or more NT domains.

Note – Trusted domain accounts are not synchronized, and only Windows NT accounts in the local domain are synchronized.

Setting Up Password Synchronization

Configuring your system for password synchronization involves six multistep tasks:

1. Configuring the password filter
   a. On a Solaris PDC
   b. On a native Windows NT PDC
2. Installing and starting the name server agent
3. Installing and configuring the PAM module
4. Configuring the password daemon
5. Enabling password synchronization
   a. Using the command line
   b. Using PC NetLink 2.0 Server Manager
6. Initially synchronizing account passwords

Note – If you are using a native Windows NT server for your primary domain controller (PDC), you need to configure the password filter differently. Follow the procedure "Task 1b of 6 – How to Configure the Password Filter on a Native Windows NT PDC" on page 183.

▼ Task 1a of 6 – How to Configure the Password Filter on a Solaris PDC

1. **Log on as root to the Solaris physical host that is running the domain PDC.**
2. **Change directories to** `/opt/lanman/sbin`**.**

Caution – Only *experienced* administrators should edit the Registry.

3. **Set the** `Notification Packages` **Registry parameter to** `libsyncfilt.so` **using this command:**

```
# ./regconfig -vs SYSTEM/CurrentControlSet/Control/Lsa
"Notification Packages" REG_MULTI_SZ libsyncfilt.so
```

Note – If you are operating a multi-instance environment, you must repeat this command for each virtual server that will use password synchronization, by using the `-I` *number* option or by setting the PCNL_INSTANCE variable before each command.

4. **Use the following command to verify that the PC NetLink password filter is correctly located in the list of password filters:**

```
# ./regconfig -vs SYSTEM/CurrentControlSet/Control/Lsa
"Notification Packages"
```

Note – If you are using other password filters, the password synchronization filter, `libsyncfilt.so`, must be located first in the list of password filters.

5. **Create the** `AuthenticationToken` **Registry key:**

```
# ./regconfig -a SYSTEM/CurrentControlSet/Services/
AdvancedServer/DirectorySyncParameters AuthenticationToken
```

6. **Set the** `AuthenticationToken` **Registry parameter to a password for the password filter:**

```
# ./regconfig -vs SYSTEM/CurrentControlSet/Services/
AdvancedServer/DirectorySyncParameters AuthenticationToken
REG_MULTI_SZ password
```

This password must be the same for the name server agent and the password daemon.

Note – If you are operating a multi-instance environment, you must repeat this command for each virtual server that will use password synchronization, by using the `-I` *number* option or by setting the PCNL_INSTANCE variable before each command.

▼ Task 1b of 6 – How to Configure the Password Filter on a Native Windows NT PDC

1. **Log on as Administrator to the Windows NT PDC.**
2. **Browse to `/mswin/intel32` on your PC NetLink CD, or to the Tools share directory at `/opt/lanman/shares/tools/passsync_setup` to locate the file `PasswdSync.exe`.**
3. **Double-click `PasswdSync.exe`.**

   Complete the steps in this wizard to install the `syncflt.dll` file in the directory `Winnt/system32`.
4. **Type a password in the dialog box to set the Authentication Token registry parameter to a password for the password synchronization system.**

   This password must be the same for the name server agent and the password daemon. This password is stored in the Registry parameter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdvancedServer\DirectorySyncParameters\AuthenticationToken`.
5. **Verify that the `Notification Packages` Registry parameter is set to `syncflt`, as follows:**

Caution – Only *experienced* administrators should edit the Registry.

   a. **Start the Windows NT Registry editor, `regedt32`, which is usually in the directory `C:\Winnt\system32`.**

   b. **Select `Notification Packages` under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.**

Note – If you are using other password filters, the password synchronization filter, `syncflt`, must be located first in the list of password filters.

6. **From the same location,** `SYSTEM\CurrentControlSet\Services\AdvancedServer\DirectorySyncParameters`, **double-click on** `NetlinkPwdSyncDaemon`.
7. **Type the IP address of the machine running the password daemon.**
   This setting tells the password filter where to forward password change requests.
8. **Click OK.**
9. **Restart the native Windows NT PDC so that these changes take effect.**

▼ Task 2 of 6 – How to Install and Start the Name Server Agent

1. **Log on as root to the Solaris physical host acting as your Solaris name server master.**
2. **Locate the** `SUNWlzps` **package on your PC NetLink CD or other source, in the** `/PCNL/sparc` **directory.**
3. **Copy the** `SUNWlzps` **package to the** `/var/spool/pkg` **directory on the machine acting as your name server master using this command:**

```
# cp -r SUNWlzps /var/spool/pkg
```

4. **Install the** `SUNWlzps` **package on the name server master by typing:**

```
# pkgadd SUNWlzps
```

5. **Issue this command to configure the name server agent authentication token:**

```
# /opt/SUNWlzps/bin/nsachkey
```

6. **When prompted, type a password for the password synchronization system.**
   This password must be the same for the password filter and the password daemon.
7. **Start the name server agent using this command:**

```
# /etc/init.d/lmxnsa start
```

▼ Task 3 of 6 – How to Install and Configure the PAM Module for Each Solaris Client

---

Note – You must perform all steps in this procedure on each Solaris client machine that will use PC NetLink and password synchronization.

---

1. **Log on as root to the Solaris client machine.**
2. **Locate the `SUNWlzpm` package on your PC NetLink CD or other source, in the `/PCNL/sparc` directory.**
3. **Copy the `SUNWlzpm` package to the `/var/spool/pkg` directory on the Solaris client machine using this command:**

```
# cp -r SUNWlzpm /var/spool/pkg
```

4. **Install the `SUNWlzpm` package using this command:**

```
# pkgadd SUNWlzpm
```

5. **Edit the `/etc/pam.conf` file to correspond to the version of Solaris software you are running.**

   a. **Under Password Management, comment out the following line:**

   ```
   # other    password required /usr/lib/security/$ISA/pam_unix.so.1
   ```

   b. **Depending on the version of the Solaris operating environment that you are running, add one of the following lines to the Password Management section of the file:**

   - For the Solaris 2.7 or 2.8 operating environment, add the following line under Password Management:

     ```
     other     password required /usr/lib/security/$ISA/pam_lmx.so.1
     ```

   - For the Solaris 2.6 operating environment, add the following line under Password Management:

     ```
     other     password required /usr/lib/security/pam_lmx.so.1
     ```

   For your information, sample versions of the file `pam.conf` are located in the `/opt/SUNWlzpm/bin` directory, named `pam.conf.2.6` and `pam.conf.2.7`. Use `pam.conf.2.7` as the sample file for both the Solaris 2.7 and 2.8 operating environments.

6. **To configure the PAM module, change directory to** `/opt/SUNWlzpm/bin` **and type:**

```
# ./pamlmxcfg
```

7. **When prompted, type the IP address of each Solaris physical host that has the password daemon installed, per domain, one at a time.**

   The system prompts for addresses repeatedly; after you have typed all the addresses, type Control-C. (These addresses will appear as a comma-separated list in the file `/opt/SUNWlzpm/lib/pamlmx.conf`.)

▼ Task 4 of 6 – How to Configure the Password Daemon

The password daemon is installed from the `SUNWlzs` package to the `/opt/lanman/lib` directory during PC NetLink 2.0 installation. The password daemon can reside on any PC NetLink domain controller, including the PDC.

1. **Log on as root to the Solaris physical host.**
2. **Change directories to** `/opt/lanman/sbin`**.**
3. **Create the** `NetlinkPwdSyncDaemon` **Registry key:**

```
# ./regconfig -a SYSTEM/CurrentControlSet/Services/
AdvancedServer/DirectorySyncParameters NetlinkPwdSyncDaemon
```

4. **Set the** `NetlinkPwdSyncDaemon` **Registry parameter to the IP address of the host where the password daemon resides, using this command:**

```
# ./regconfig -vs SYSTEM/CurrentControlSet/Services/
AdvancedServer/DirectorySyncParameters NetlinkPwdSyncDaemon
REG_MULTI_SZ ip.address.of.passworddaemonhost
```

Note – You can configure your system so that the password daemon and the password filter reside on different hosts. In that case, you must perform Step 3 on the machine running the password filter, then continue with Steps 4 and 5 on the machine hosting the password daemon.

---

5. **To set the password daemon authentication token, type the following command:**

```
# /opt/lanman/sbin/pschkey
```

6. **When prompted, type a password for the password synchronization system.**
   This password must be the same for the password filter and the name server agent.
7. **Restart the PC NetLink server, using the following command:**

```
# /etc/init.d/ms_srv restart
```

▼ Task 5a of 6 – How to Enable Password Synchronization Using PC NetLink Server Manager

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host.**
2. **Double-click the appropriate PC NetLink server icon in the Navigation pane.**
3. **Double-click the Virtual Server Configuration icon.**
4. **Click the Policies icon.**
5. **Double-click the User Accounts icon in the Results pane.**
6. **Select the Password Synchronization tab.**
7. **Check the Enable Password Synchronization option.**
8. **Click OK.**

Note – If you are operating a multi-instance environment, you must repeat Steps 2 through 8 for each virtual server.

▼ Task 5b of 6 – How to Enable Password Synchronization Using the Command Line

To enable password synchronization you must change the Registry parameter `SyncPasswordsToSolaris` from the default value, 0, to 1, on the PC NetLink domain controller that you decide to make responsible for password synchronization.

Caution – Only *experienced* administrators should edit the Registry.

1. **Using the command line interface, log on as root to the Solaris physical host.**
2. **Change directories to `/opt/lanman/sbin`.**
3. **At the command prompt, type:**

```
# ./regconfig -vs SYSTEM/CurrentControlSet/Services/
AdvancedServer/DirectorySyncParameters SyncPasswordsToSolaris
REG_DWORD 1
```

Note – If you are operating a multi-instance environment, you must issue this command for each instance using the `-I` *number* option, or by setting the PCNL_INSTANCE variable before each command.

▼ Task 6 of 6 – How to Initially Synchronize Account Passwords

1. **Map Solaris user accounts to PC NetLink accounts.**

   To map user accounts, use PC NetLink Server Manager or the `mapuname` command. See the PC NetLink Server Manager More Help topic "How to Set Up User Accounts" or the man page for the `mapuname` command for more information.

2. **Manually synchronize the passwords for each pair of user accounts to initialize their synchronized state.**

   First, you must ensure that the passwords are different. Then, you must manually change either the Windows NT password to match the Solaris password, or change the Solaris password to match the Windows NT password.

3. **Verify that the passwords have become synchronized using these commands:**

```
# cd /opt/lanman/sbin
# ./pwdsync -v Solaris-user-account
# ./pwdsync -v DOMAIN-NAME:NT-user-account
```

If the passwords are synchronized, the system displays:

"Solaris-user-account `is password synchronized"`

"DOMAIN-NAME:NT-user-account `is password synchronized"`

You can also view or edit the synchronized state of mapped user accounts in PC NetLink Server Manager, under Mapped User Accounts for the appropriate PC NetLink virtual server.

4. **Test a pair of accounts to see if password changes are propagating correctly.**

Change a password from a Solaris client, then verify that synchronization occurred by logging on to that account from a Windows NT client, using the new password. Perform the same check, starting from a Windows NT client, changing the password, and verifying the change from a Solaris client.

Troubleshooting Password Synchronization

The following sections provide general and specific troubleshooting tips you can use to isolate a problem with password synchronization.

General Suggestions

Password synchronization is a complex feature that relies upon the correct installation and configuration of several components. Before assuming that there is a specific problem, it is worthwhile to perform some basic checks.

- *Verify your setup* – It is worthwhile to review the setup procedures to make sure each component is correctly installed and running on the appropriate hosts. A common configuration problem is using an invalid IP address for the password daemon.

- *Know your environment* – Because password synchronization operates in a domain on multiple machines, potentially with multiple system administrators, it is important to verify IP addresses, domain roles, PC NetLink server configurations, and Authentication Token passwords.

Isolating the Problem

Is the Name Server Agent Running on the Correct Host?

The name server agent must be installed and started on the Solaris host acting as your name server master. You can easily check if the name server agent is running by typing the following command at the system command prompt:

```
% ps -ef | grep lmx
```

The system display should include the following (at a minimum)::

```
root 18680     1  0 09:57:04 ?        0:00 lmx.nsa
```

This display indicates that a required server process is in fact running. If this process is not running, start it by using the following command::

```
% /etc/init.d/lmxnsa start
```

Is the Correct Port Available?

It is possible that the port used by `lmx.ntpw` is occupied. If this port is in use by another process, the password daemon does not function properly. Use the following command to check the status of the port:

```
% netstat -a | grep 6793
```

If the port is available, the system display should include:

```
   *.6793      *.*      0        0 24576            0 LISTEN
server.6793    *.*      0        0 24576            0 LISTEN
```

Is the NetlinkPwdSyncDaemon Set to the Correct IP Address?

The NetlinkPwdSyncDaemon should be set to the IP address of the host where the password daemon resides. Verify that the IP address is for the correct machine, and that it was entered properly. To view the current configuration of the NetlinkPwdSyncDaemon, log on as root to the Solaris physical host and type:

```
# /opt/lanman/sbin/regconfig -vs SYSTEM/CurrentControlSet/
Services/AdvancedServer/DirectorySyncParameters
“NetlinkPwdSyncDaemon”
```

If the current IP address is incorrect, use this command to reset the parameter:

```
# /opt/lanman/sbin/regconfig -vs SYSTEM/CurrentControlSet/
Services/AdvancedServer/DirectorySyncParameters
“NetlinkPwdSyncDaemon” REG_MULTI_SZ correct.ip.address
```

Is the PAM Module Installed on Each Solaris Client?

The PAM module must be installed on any Solaris client that uses password synchronization. The PAM module forwards password change requests from Solaris clients to the password daemon. If the PAM module is not installed on the Solaris client, password propogation from the Solaris client will not occur.

Have You Manually Synchronized the Passwords?

Once you have set up password synchronization and mapped user accounts, you must manually change either the Windows NT password to match the Solaris password, or change the Solaris password to match the Windows NT password.

For example, you have an existing Solaris user account, juser, with a password of lucky1. You create and map a Windows NT account for juser, with the account name juser, and a password of changeme. You must manually change one of juser’s passwords to match the other. Change juser’s Windows NT password from changeme to lucky1.

Once you have manually synchronized the passwords, any password changes by juser are automatically propagated by the software.

Have You Looked at the `passsync` Logfile for Additional Information?

PC NetLink password synchronization maintains a logfile of errant password change activity in `/var/opt/lanman/`*number*`/dirsync/passsync.log`, where *number* is the instance number. This file contains errors encountered while attempting a password change from either Solaris or Windows NT. The following table provides a list of the potential Windows NT error codes output to the logfile and their meaning::

TABLE 4-1 Windows NT Status Code Description

Windows NT Status	Error Code	Descriptions
`STATUS_ILL_FORMED_PASSWORD`	0xC000006B	New password is poorly formed, for example, it contains characters that cannot be entered from the keyboard.
`STATUS_ACCOUNT_RESTRICTION`	0xC000006E	An account restriction, such as minimum password age, has been encountered.
`STATUS_ACCOUNT_LOCKED_OUT`	0xC0000234	Account has been locked out; no change allowed.
`STATUS_PASSWORD_RESTRICTION`	0xC000006C	Password did not meet a password integrity check and was rejected by a password filter.
`STATUS_PWD_TOO_SHORT`	0xC000025A	Password did not meet minimum length requirements.
`STATUS_ACCESS_DENIED`	0xC0000022	User does not have the appropriate access to complete the operation.
`STATUS_WRONG_PASSWORD`	0xC000006A	User entered incorrect current Windows NT password.

Unsupported Windows NT Password Features

Password History

PC NetLink password synchronization does not support and cannot handle password history (uniqueness) restrictions set on Windows NT accounts.

When a password change is requested from Windows NT, the password filters are notified of the change. These password filters push the password change to Solaris, prior to Windows NT performing a history check on the given account. If the password change is then rejected by Windows NT, based on a password history violation, Solaris is not notified of the rejection, and the passwords are no longer synchronized. In this case, Solaris accepts the new password and Windows NT rejects the change and retains the old password.

Permit Blank Password

The general rule for password synchronization in PC NetLink is that a password change must meet the password criteria standards for both Windows NT and Solaris. Windows NT permits a blank password, but the Solaris utilities `passwd` and `rlogin` do not permit NULL or blank passwords. Disable or do not use the Windows NT Permit Blank Password feature with PC NetLink password synchronization.

If enabled, the Permit Blank Password feature creates the following scenario. Setting the Windows NT password to NULL or blank will also set the password to NULL in the Solaris naming service, that is, Files or NIS. Because the Solaris utilities `passwd` and `rlogin` do not allow for NULL or blank passwords, a Solaris client would be unable to log in to a system or change the password if it has been changed to NULL or blank from Windows NT. If this occurs, change the password from the Windows NT client from NULL/blank back to a conforming non-blank password that is accepted on both Solaris and Windows NT.

CHAPTER 5

Setting Up Printing Services

This chapter tells you how to set up a PC NetLink virtual server as a print server for Windows clients, and offers background information that will help you keep print tasks running smoothly. The process for setting up a Solaris printer to work in the network comprises three tasks:

- "Task 1 of 3 – How to Install a Solaris Printer" on page 198
- "Task 2 of 3 – How to Set Up the Solaris Printer as a PC NetLink Shared Printer;" see either of the following:
  - "Task 2a of 3 – How to Use PC NetLink Server Manager to Set Up the Solaris Printer as a PC NetLink Shared Printer" on page 206
  - "Task 2b of 3 – How to Use Network Neighborhood to Set Up the Solaris Printer as a PC NetLink Shared Printer" on page 207
- "Task 3 of 3 – How to Make the PC NetLink Printer Available to Microsoft Windows Clients" on page 208

You need to perform the first two setup tasks only once per printer. The final task, making the new printer available to Windows clients, requires that each client machine user add the printer.

This chapter also explains:

- "How to Remove a PC NetLink Shared Printer" on page 208
- "How to Change Solaris Printer Properties" on page 211

About PC NetLink Printing Services

PC NetLink printing offers the following features:

- You can browse the network for available network printers using PC NetLink Server Manager. Double-click the Solaris Printers icon in the Results pane for a physical host to see Solaris printers; double-click Printer Shares in the Shares Results pane for a virtual server to see printer shares.
- As an administrator, you can administer PC NetLink print servers, printers, documents, and printer drivers remotely.
- As an administrator, after your first client installs the printer, you do not have to install printer driver files on other Windows NT, Windows 98, and Windows 2000 client computers to enable them to use a PC NetLink print server; this installation happens automatically because the driver is installed on the printer driver share. If all printing clients are running Windows NT, Windows 98, or Windows 2000, it only is necessary to install printer driver files in one place—at the PC NetLink print server.
- Clients can print to all networked printers that have their own direct Ethernet interface and have been configured as PC NetLink system printers.

Note – You cannot share a printer that is connected to a Solaris physical host that is not running PC NetLink software.

PC NetLink Printing Terms

In PC NetLink terminology, a *shared printer queue* is the mechanism through which a collection of print devices is accessed by LAN users with appropriate permissions. A *print device* is the actual hardware that produces printed output. Print devices can be connected directly to the server (via parallel port), to the network (via a network adapter card), or to a client computer on the network.

The Solaris operating environment, which your PC NetLink server runs, provides *LP Printer* functionality that mediates between the PC NetLink system, which sends clients' print requests to the LP service, and the print devices to which the LP service directs the requests. Users access print devices by sending their print jobs over the network to shared printer queues, which in turn forward the jobs to print devices.

In Windows NT terminology, a *printer* is the software interface between the operating system and the print device. The printer defines where the document will go before it reaches the print device (to a local port, to a file, or to a network printer share), when it will go, and various other aspects of the printing process.

In PC NetLink terminology, the shared printer queue is the software interface between the application and the print device. When you administer a PC NetLink print server from Windows NT, a "printer" actually represents a shared printer queue.

A *printer driver* is a program that converts graphics commands into a specific printer language, such as PostScript™. When you *add a printer*, you are installing a printer driver and making the printer (shared printer queue) available on the network by sharing it.

A *print server* is the computer that receives documents from clients.

Spooling is the process of writing the contents of a document to a file on disk. This file is called a *spool file*.

The PC NetLink program supports all of the print devices that the *local spooling system* supports. The local spooling system is the process that runs on the PC NetLink server's Solaris system, which handles system printing.

Network-interface print devices have their own network cards; they need not be physically connected to a print server because they are connected directly to the network.

PC NetLink Network Printing

The PC NetLink program supports true network printing. When Windows NT, Windows 98, and Windows 2000 clients connect to a correctly configured PC NetLink print server, the printer driver is automatically installed on the client computer if necessary, if the driver was copied to the server during printer installation.

If you install a newer or different printer driver on a PC NetLink server or a Windows NT, Windows 98, or Windows 2000 client computer, you must update the printer driver manually to have the new version copied on to your computer. You remove and then add the printer to download the printer driver automatically.

Setting Up PC NetLink Printing

Establishing a printer (print device) as a PC NetLink shared printer involves three groups of tasks:

- Configuring the printer as a Solaris printer
- Designating the printer as a shared PC NetLink printer
- Making the new printer available to individual clients

Note – Even though it is possible to configure a printer by way of the Solaris command line, it is recommended for experienced Solaris system administrators only. If you do not fit that description, you are advised to use the PC NetLink Server Manager method only.

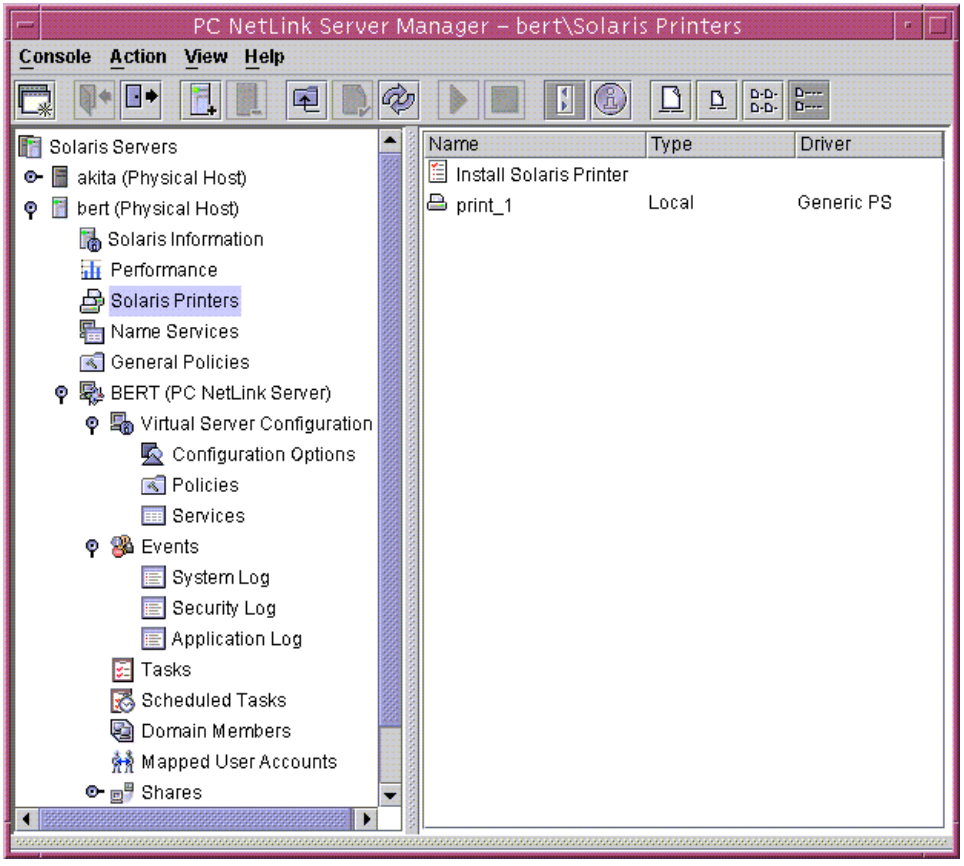
▼ Task 1 of 3 – How to Install a Solaris Printer

1. **Using PC NetLink Server Manager, log on as root to a Solaris physical host.**

   In the following examples, the server "bert" is a Solaris physical host.

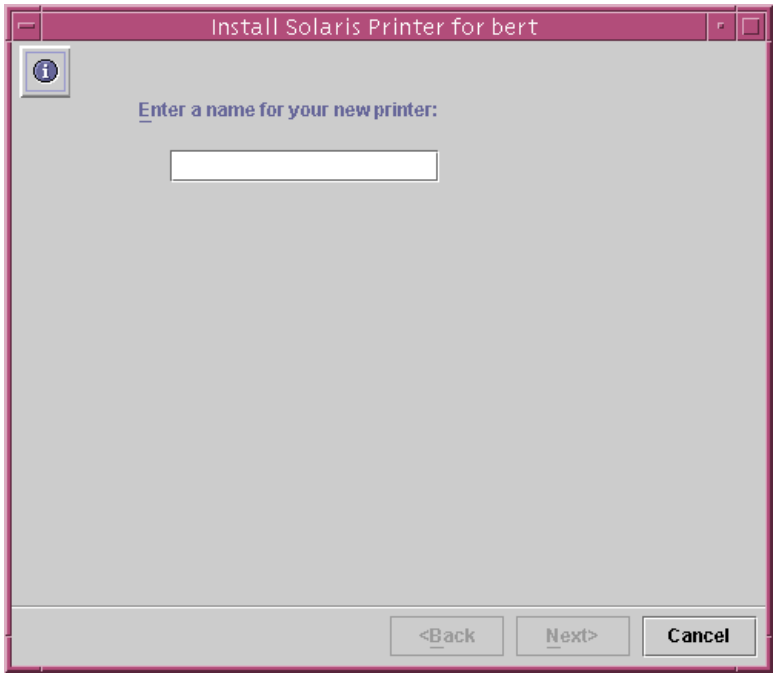
2. **Double-click Solaris Printers in the Results pane.**

   A screen similar to the following appears, listing any *locally spooled* Solaris printers and displaying the Install Solaris Printer wizard icon.



3. **Double-click Install Solaris Printer.**

   The following dialog box appears.



4. **Type a name for the new printer in the provided field, and then click Next.**

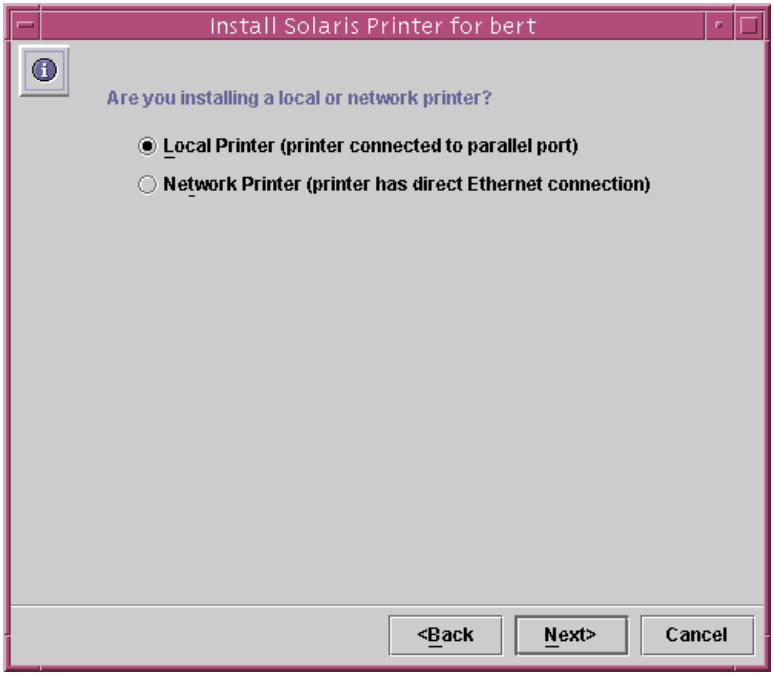
   The name you choose will be its Solaris queue name. A printer name must be between 1 to 14 characters and can be made up of only the letters A through Z (uppercase, lowercase, or mixed case), the numerals 0 through 9, or an underline (_). The tool will only permit "legal" characters in the text field, and will not permit going on to the next step unless you type at least one character.

   The printer name you type is checked against all existing Solaris printer names. If you type the name of an existing printer, a screen similar to the following (with the actual name you chose inserted after "A printer named") appears, asking for confirmation that you want to change its configuration.

If you do not see the Printer Name Exists screen, continue with Step 5.

- *If you intended to change the configuration of an existing printer*, choose Yes. At that point, the rest of the settings of the Install Solaris Printer wizard will default to the settings that the printer currently is using. In this manner, the Install Solaris Printer wizard can be used to change the configuration of an existing Solaris printer.
- *If you did not intend to change the configuration of an existing printer*, click the default choice, No. This will return the screen for naming the new printer, and you can type a different name and proceed to the next step.

The following screen appears, requesting information about the printer's local or network status.

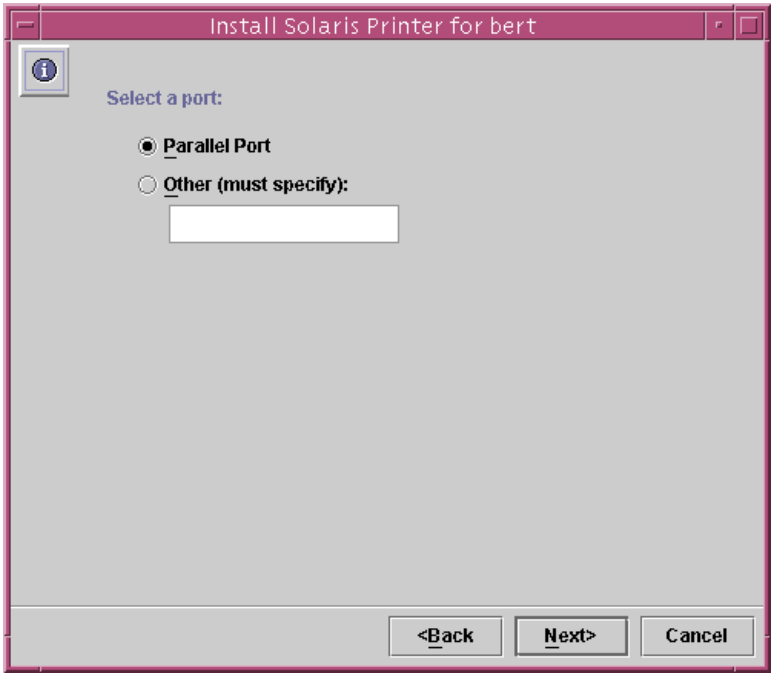


5. **Select whether to install the printer as a local printer or as a network printer, and then click Next.**

Note – If you intend to use this printer as a PC NetLink network printer, it must be equipped with an Ethernet adapter and be plugged directly into the network. A local PC NetLink printer must be plugged directly into the PC NetLink system.

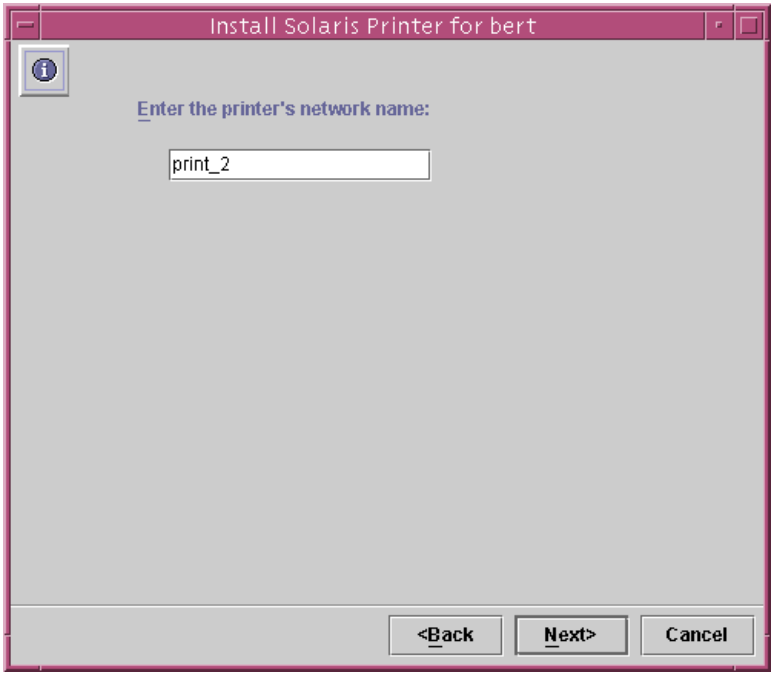
---

6. **Depending on which selection you made, do one of the following:**
   - *Network Printer* – Proceed to Step 7.
   - *Local Printer* – Use the ensuing screen to indicate the correct port, then click Next.



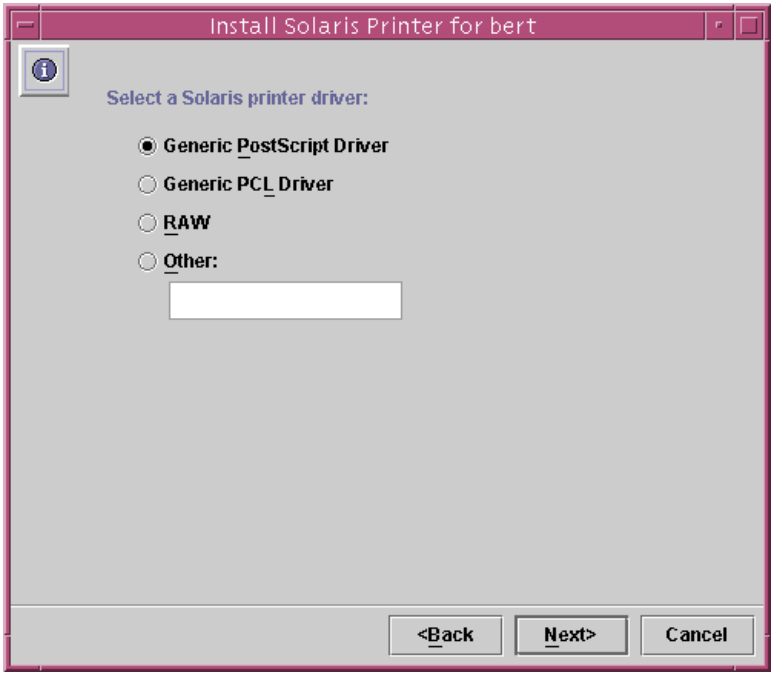
7. **If you selected Network Printer, use the ensuing screen to type the network name by which the printer is known, then continue with Step 8.**

   The name that is entered by default into the text field is the same name that you selected in Step 4. If you have reason to identify the printer by a different name on the network, delete the default name and type the new one.



8. **Click Next.**

   The following screen appears, requesting information about your Solaris printer driver.



9. **Designate a Solaris printer driver.**

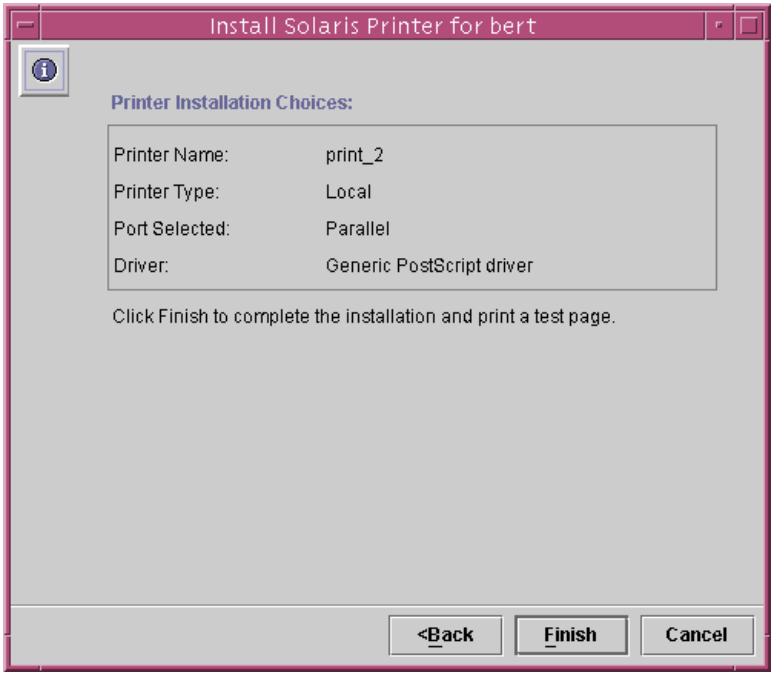
   The default choice is Generic PostScript Driver, which is suitable for most printers. If you are not sure which driver to choose, consult your printer manufacturer's documentation. Most major printer manufacturers have Web sites that list the drivers for their products.

   For a list of Solaris Ready printers, which have been verified by Sun Microsystems as compatible with the Solaris operating environment, see the following Web page:

   `http://www.sun.com/products-n-solutions/hw/peripherals/printers.html`

10. **Click Next.**

    A confirmation screen similar to the following appears.

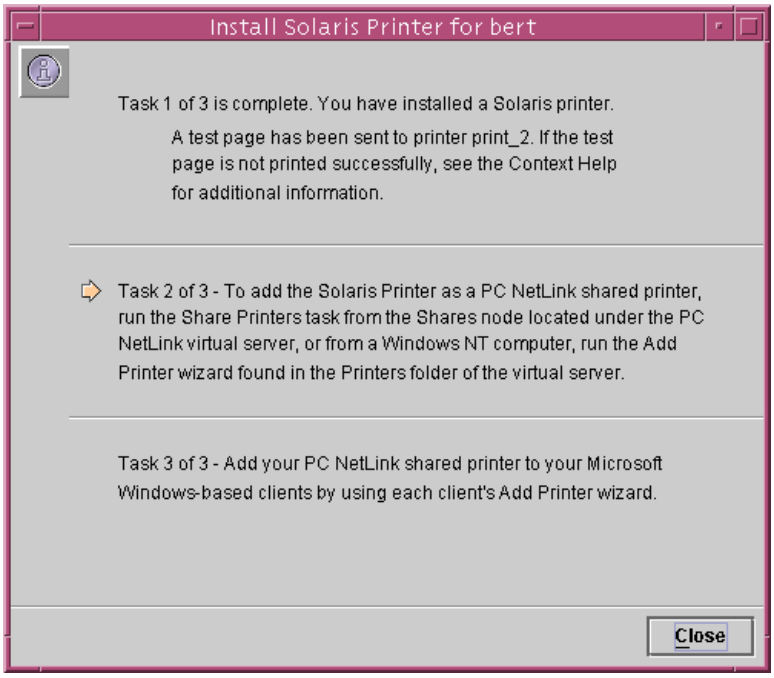


11. **Review and confirm the configuration choices.**

    Make sure that your choices are accurately reflected. Click Back to change any of the configuration details, Finish to cxonfirm your choices, or Cancel to halt the installation entirely and dismiss the window.

12. **Click Finish.**

    A screen similar to the following appears.



13. **Check the test page to be sure that the output is correctly printed.**

    If the Solaris driver you have chosen is either PostScript or PCL, a test page is sent to the printer after it has been properly installed. (No test page will be sent if you have chosen another type of driver.) If you detect a problem with the test page, it is possible that you have configured the printer incorrectly and you will have to begin the process again—paying particular attention to the printer driver that you have chosen.

    If your test page is printed successfully, you have a correctly installed Solaris printer. You can administer this printer from your Solaris command line using any of the standard Solaris printer commands (`lp`, `lpadmin`, `lpstat`, `cancel`, and so forth).

▼ Task 2a of 3 – How to Use PC NetLink Server Manager to Set Up the Solaris Printer as a PC NetLink Shared Printer

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host that has the printer installed.**
2. **In the Results pane, double-click the icon for the virtual server for which you want to set up the shared printer.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Click Shares.**
4. **Click Printer Shares.**
5. **Double-click the Add Printer Share icon.**
6. **In the screen that appears, type a name for your new printer share.**

   Allowable characters for a printer share name are alphanumeric characters, - (hyphen), and _ (underscore).
7. **In the next screen, in the left side select the Solaris printer or printers to be shared, then click Add.**
8. **Click Next.**
9. **In the next screen, specify how many users can access this printer share at a time.**
10. **Click Next to proceed with the configuration change, Back to make changes, or Cancel to abandon the procedure and leave the server configuration unchanged.**

    If you continue the procedure by clicking Next, the resulting screen summarizes the choices you have made.
11. **Click Finish to proceed with the name change, Back to make changes, or Cancel to abandon the procedure and leave the configuration unchanged.**

    The resulting screen informs you of the progress of the configuration change, marking pending activity with an arrow and completed activity with a check mark.

Note – When you use PC NetLink Server Manager to set up the PC NetLink shared printer, a Microsoft Windows printer driver is not installed. You can use Network Neighborhood to locate the printer share, open the Properties dialog box, and install a driver, or you can let Microsoft Windows users specify a driver when queried.

▼ Task 2b of 3 – How to Use Network Neighborhood to Set Up the Solaris Printer as a PC NetLink Shared Printer

Caution – You *must* complete the following procedure from a PC that has either Windows NT or Windows 2000 software installed. If you use a PC running Windows 98, the installation will fail.

1. **Use Network Neighborhood to open the PC NetLink system that you are using as the Solaris print server.**
2. **Open the Printers folder.**
3. **Use the Add Printer wizard to add the PC NetLink (Solaris) printer, paying particular attention to the following points that are specific to PC NetLink printers and may diverge from your usual Windows NT Add Printer routine:**
   - *Drivers for different operating systems* – As you use the Add Printer wizard, it presents you with a choice of installing drivers for various operating systems and asks you to choose from the list. *You do not need to make a selection unless you want to add a driver for an operating system in addition to the one that you are currently running*. The software detects the operating system that you are running and chooses it by default.
   - *Printer name* – As you use the Add Printer wizard, it prompts you to supply a printer name—with the name of the printer *driver* displayed as the default. *Do not type the same name that you chose for the printer in Task 1*. You must use a different name for the printer. You can use the default name or type in a name of your own.

Note – To share a Windows-hosted printer with network computers, you select the Sharing tab in the printer's Properties sheet, click Shared, and then provide a *share name.* The system displays by default the name of the shared printer queue.

After you have added the printer in this manner, it is available to your clients.

▼ Task 3 of 3 – How to Make the PC NetLink Printer Available to Microsoft Windows Clients

- **Use each Microsoft Windows-based client's Add Printer wizard to add the PC NetLink shared printer.**

Note – After you have successfully set up your Solaris printer, established it as a PC NetLink shared printer, and made it available to your Microsoft Windows clients, do not use the `net pause` command from your Solaris command line as a method to pause the print queue. That command is interpreted by PC NetLink software as a command to disable the printer rather than merely to pause the queue. Instead, to pause the queue by way of the command line, use the `net print /hold` command.

▼ How to Remove a PC NetLink Shared Printer

Removing a PC NetLink shared printer does not affect the printer's operation for Solaris print jobs.

1. **At each client, delete the PC NetLink printer from the local Printers folder.**
2. **Using Windows NT tools, delete the PC NetLink printer share.**

   Do one of the following:

   - In the Printer Shares Results pane, select the printer share and choose Delete Printer Share from the Action menu.
   - Using Network Neighborhood, browse to the Printers folder on the server, select the PC NetLink printer, then click Delete.

▼ How to Remove a Solaris Printer

1. **At each client, delete the PC NetLink printer from the local Printers folder.**
2. **Using Windows NT tools, delete the PC NetLink printer share.**

   Browse via Network Neighborhood to the Printers folder on the server, select the PC NetLink printer, then click Delete.

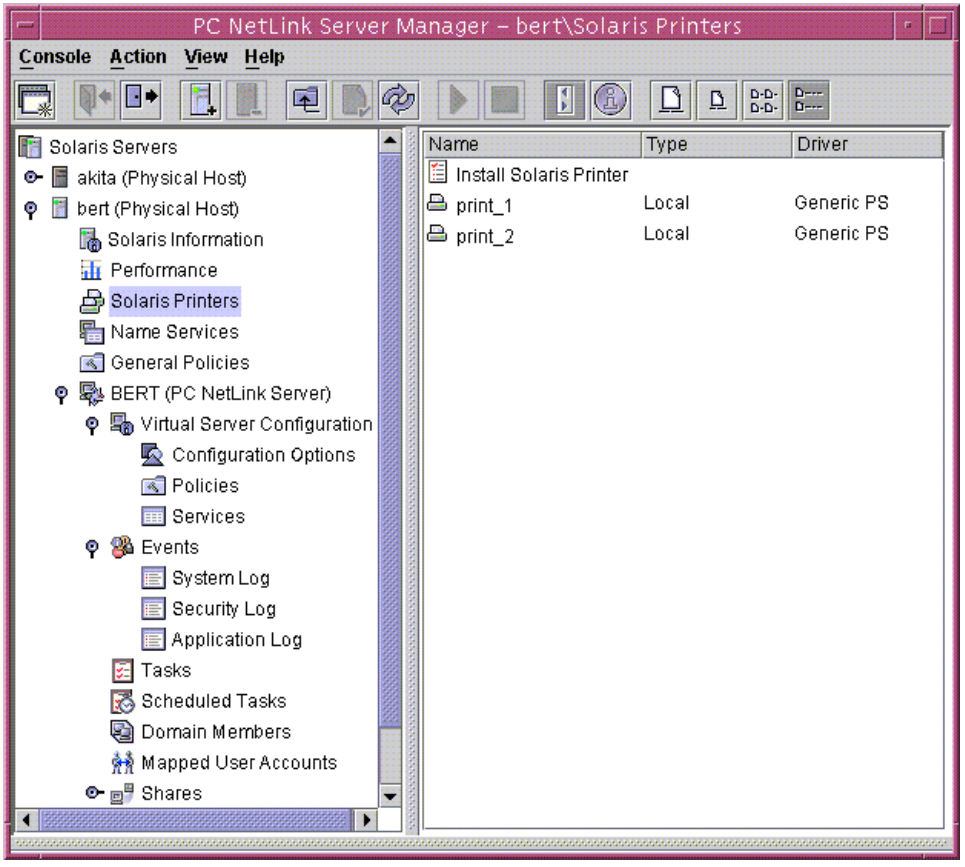
Note – You can also delete the printer share using PC NetLink Server Manager. See Step 2 of "How to Remove a PC NetLink Shared Printer" on page 208.

---

3. **In PC NetLink Server Manager, log on to the Solaris physical host that is the printer's print server.**

4. **Double-click Solaris Printers.**

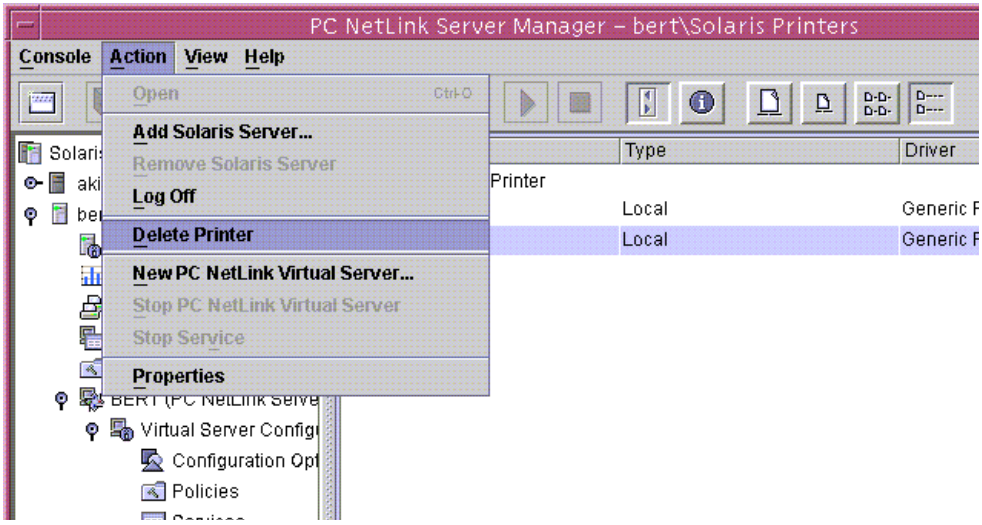
   A screen similar to the following appears, listing the installed printers.



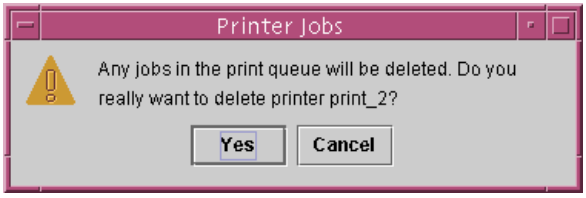
5. **Click to highlight the name of the printer that you want to delete.**

6. **From the Action menu, choose Delete Printer**

.



If there are print jobs queued, a warning similar to the following appears, alerting you that any print jobs currently in that printer's queue will be deleted.



7. **Click Yes to confirm deletion of the printer, or click Cancel.**

The printer is removed and deleted from the PC NetLink Server Manager list of Solaris Printers.

▼ How to Change Solaris Printer Properties

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host that is the printer's print server.**
2. **Double-click Solaris Printers in the Results pane.**
3. **Double-click the name of the printer whose properties you want to change.**

   The Printer Properties dialog appears, enabling you to change any of the following:

   - Solaris printer name – Allowable characters are alphanumeric characters, - (hyphen), and _ (underscore)
   - Printer type – Either local or network
   - Local printer port – Either parallel or "other"
   - Printer's network name
   - Printer driver – Generic PostScript, generic PCL, "raw," or other

4. **Click OK to save the properties changes, or click Cancel to quit without making changes.**

Note – You can also change some properties of Microsoft Windows printer shares using PC NetLink Server Manager.

CHAPTER 6

Implementing WINS and Maintaining Databases

This chapter provides detailed background information about the Windows Internet Name Service (WINS) that PC NetLink software incorporates, and considers important performance issues that can help you plan your network's implementation of WINS. Major sections in this chapter that deal with these issues include:

- WINS and its function
- Name resolution services
- WINS server planning

This chapter also describes how to maintain databases—including WINS, the Access Control List (ACL), the PC NetLink Registry, and the Security Accounts Manager (SAM)—on a server running the PC NetLink program.

The following tasks are covered in this chapter:

- "How to Clean Up PC NetLink Databases" on page 240
- "How to Back Up PC NetLink Databases" on page 248
- "How to Restore Backed-Up Databases" on page 254
- "How to Back Up the Complete Virtual Server Image" on page 258
- "How to Restore a Complete Virtual Server Image" on page 265
- "How to View, Modify, or Delete Scheduled Tasks" on page 268

Note – In a network that includes PC NetLink virtual servers, each virtual server is recognized by WINS as a unique client. When this chapter refers to a computer or client, this also includes any PC NetLink virtual servers in the network.

About WINS and Its Function

Windows Internet Name Service (WINS) is a database of available network resources and the computers that own them. This database is kept on a WINS server. A computer seeking such a resource "asks" the WINS server to look up the address of the machine that owns the resource. This speeds up network performance and reduces traffic when compared with the alternative "broadcast" scheme of identifying network resources.

WINS for PC NetLink systems is fully compatible with Microsoft WINS client implementations, including Microsoft TCP/IP-32 for Windows 98, Windows 2000, Windows NT Workstation, Windows NT Server, and the Microsoft Network Client Version 3.0.

PC NetLink WINS can replicate name databases with other PC NetLink WINS computers, and with WINS for Windows NT systems.

Note – You manage the NT functions of PC NetLink WINS and maintain it by using WINS Manager, the same Windows NT-based tool that you use to manage WINS for Windows NT. This allows both PC NetLink-based and Windows NT-based WINS servers to be managed from a single administration tool on a single computer in the network.

About Name Resolution Services

PC NetLink WINS with Transmission Control Protocol/Internet Protocol (TCP/IP) requires a unique IP address and computer name for each computer on the network. Although programs use IP addresses to connect computers, administrators use "friendly" names to connect them. As a result, TCP/IP internetworks require a *name resolution service* that converts computer names to IP addresses and IP addresses to computer names.

An *IP address* is the unique address by which all other TCP/IP devices on the internetwork recognize that computer. For TCP/IP and the Internet, the *computer name* is the globally known system name, plus a *Domain Name System* (DNS) domain name. (On the local network, the computer name is the name that was supplied either during PC NetLink or Windows NT setup.) To ensure that both names and IP addresses are unique, a computer using NetBIOS over TCP/IP (also known as NetBT) registers its name and IP address on the network during system startup.

NetBIOS and DNS Computer Names

PC NetLink networking components rely on a naming convention known as *NetBIOS*. In general, NetBIOS computer names consist of a single part.

In contrast, TCP/IP components rely on the DNS naming convention. DNS computer names consist of two parts: a *host name* and a *domain name*, which combined form the *fully qualified domain name* (FQDN).

Note – For a PC NetLink virtual server, the NetBIOS *computer name* in this case is the virtual server name, not the name of the physical host on which the virtual server runs.

Fortunately, NetBIOS computer names are compatible with DNS host names, making interoperability possible between the two types of components. PC NetLink software combines the NetBIOS computer name with the DNS domain name to form the FQDN.

Note – In a PC NetLink system, the NetBIOS computer name defaults to the same name as the DNS host name. You can change the default if you need unique names.

A computer can use one or more of the following methods to ensure accurate name resolution in TCP/IP internetworks:

- WINS

  A computer can use WINS if at least one WINS server is available that contains a dynamic database that maps computer names to IP addresses. WINS can be used in conjunction with *broadcast* name resolution for an internetwork where other name resolution methods are inadequate. As described in the following section, WINS is a NetBIOS over TCP/IP mode of operation.

- Broadcast name resolution

  A computer also can use broadcast name resolution, which is a NetBIOS over TCP/IP mode of operation defined in RFC 1001/1002 as *b-node*. This method relies on a computer making IP-level broadcasts to register its name by "announcing" it on the network. Each computer in the broadcast area is responsible for challenging attempts to register a duplicate name and for responding to name queries for its registered name.

- DNS name resolution

  The Domain Name System provides a way to look up name mappings when connecting a computer to foreign hosts using NetBIOS over TCP/IP or applications such as FTP. You can configure PC NetLink 2.0 software to use DNS.

- An `LMHOSTS` file to specify the NetBIOS computer name and IP address mappings, or a `HOSTS` file to specify the DNS name and IP address

  On a local computer, the `HOSTS` file (used by Windows Sockets applications to find TCP/IP host names) and `LMHOSTS` file (used by NetBIOS over TCP/IP to find Microsoft networking computer names) can be used to list known IP addresses mapped with corresponding computer names. `LMHOSTS` is used for name resolution for small-scale networks or remote subnets where WINS is not available.

NetBIOS Over TCP/IP (NetBT) Name Resolution

NetBIOS over TCP/IP (NetBT) is the session-layer network service that performs name-to-IP address mapping for name resolution. In the PC NetLink program, NetBT is implemented through WINS and broadcast name resolution. The two most important aspects of the related naming activities are registration and resolution:

- *Registration* – The process used to register a unique name for each computer (node) on the network. A computer typically registers itself when it starts.
- *Resolution* – The process used to determine the specific address for a computer name.

Note – RFCs 1001 and 1002 specify how NetBIOS should be implemented over TCP/IP and define the name resolution nodes.

Defined within NetBT are nodes that specify how network resources are identified and accessed. The NetBT nodes supported by PC NetLink software are:

- *b-node* – Uses broadcast messages to resolve names
- *h-node* – First uses another type of node for name queries and then b-node if the name service is unavailable or if the name is not registered in the database

---

Note – The RFCs refer to a NetBIOS Name Server (NBNS). WINS is an enhanced NBNS.

The two most common node types for Windows client computers are b-node and h-node.

For Dynamic Host Configuration Protocol (DHCP) users, the node type may be assigned by the DHCP server (depending on how the client has been configured). When WINS servers are in place on the network, NetBT resolves names on a client computer by communicating with the WINS server. When WINS servers are not in

place, NetBT uses b-node broadcast messages to resolve names. NetBT also can use `LMHOSTS` files for name resolution, depending on how TCP/IP is configured on a particular computer.

PC NetLink software can respond to b-node and h-node NetBT nodes.

B-Node (Broadcast Node)

The b-node mode uses broadcasts for name registration and resolution. For example, if `CLIENT_PC1` wants to communicate with `CLIENT_PC2`, it will broadcast to all machines that it is looking for `CLIENT_PC2` and then will wait a specified time for `CLIENT_PC2` to respond.

The b-node mode has two major problems:

- In a large environment, it loads the network with broadcasts.
- Typically, routers do not forward broadcasts, so computers that are on opposite sides of a router will never hear the requests.

H-Node (Hybrid Node)

The h-node mode solves the most significant problems associated with broadcast messages and with routed-environment operations. It is a combination of b-node and another node type that uses broadcast messages as a last effort. If the WINS server is down—making broadcast messages a necessity—the computer continues to poll the WINS server until it can be reached again. The h-node also can be configured to use the `LMHOSTS` file after broadcast name resolution fails.

No broadcast messages are generated if the WINS server is running, and computers can be on opposite sides of routers. If the WINS server is down, b-node is used, allowing computers on the same side of a router to continue to operate as usual.

Note – For Microsoft TCP/IP users who configure TCP/IP manually, h-node is used by default unless the user does not specify addresses for WINS servers when configuring TCP/IP.

Other Combinations

Another variation, known as *modified b-node*, is used in PC NetLink networks to allow messages to go across routers. The modified b-node does not use a WINS server. In this mode, b-node uses a list of computers and addresses stored in an `LMHOSTS` file. If a b-node attempt fails, the system looks in `LMHOSTS` to find a name

and then uses the associated address to cross the router. However, each computer must have this list, which creates an administrative burden in maintaining and distributing the list.

Windows NT uses this method if WINS servers are not used on the network. In Windows NT, some extensions have been added to this file to make it easier to manage—but modified b-node is not an ideal solution.

WINS and Broadcast Name Resolution

WINS provides a distributed database for registering and querying dynamic computer name-to-IP address mappings in a routed network environment. WINS solves the problems that occur with name resolution in complex internetworks.

WINS reduces the use of local broadcasts for name resolution and allows users to locate systems easily on remote networks. Additionally, when dynamic addressing through DHCP results in new IP addresses for computers that move between subnets, the changes are updated automatically in the WINS database. Neither the user nor the network administrator needs to make changes manually.

The following sections discuss how name resolution is provided by WINS and name query broadcast messages.

WINS in a Routed Environment

WINS consists of the following two components:

- The WINS server, which handles name queries and registrations
- Client software, which queries for computer name resolution

Microsoft Windows networking clients (WINS-enabled Windows NT, Windows 2000, or Windows 98 computers) can use WINS directly. Non-WINS computers on the internetwork that are b-node compatible (as described in RFCs 1001 and 1002) can access WINS through proxies (WINS-enabled computers that listen to name-query broadcasts and then respond for names that are not on the local subnet).

To allow browsing *without* WINS, the network administrator must ensure that the users' primary domain has PC NetLink, Windows NT Server, or Windows NT Workstation computers on both sides of the router to act as master browsers. These computers need correctly configured `LMHOSTS` files with entries for the domain controllers across the subnet.

To allow browsing *with* WINS, such strategies are not necessary because the WINS servers and proxies transparently provide the support necessary for browsing across routers where domains span the routers.

Note – If a client computer running Windows NT also is DHCP-enabled, and if the administrator specifies WINS server information as part of the DHCP options, the computer by default will be configured with WINS server information.

In a WINS and broadcast name resolution environment, a WINS-enabled client computer behaves in a different manner than a non-WINS-enabled client computer. These differences are apparent in the way these clients handle resolution, registration, release, and renewal, described in the next sections.

Name Resolution

With WINS servers in place on the internetwork, NetBIOS computer names are resolved using two basic methods depending on whether WINS resolution is available and enabled on the client computer. Regardless of which name resolution method is used, the process is not visible to the user after the system is configured.

- *If WINS is not enabled on the client* – The computer registers its name by sending name registration request packets (as broadcast messages) to the local subnet. To find a particular computer, the non-WINS computer sends name query request packets (as broadcast messages) on the local subnet. (This broadcast message cannot be passed on through IP routers.) If local name resolution fails, the local `LMHOSTS` file is consulted. These processes are followed whether the computer is a network server, a workstation, or another device.
- *If WINS is enabled on the client* – The computer first queries the WINS server. If this fails, it sends name registration and query requests (as broadcast messages) in the following series of steps:

1. A client's name query request is sent first to the WINS server. If the name is found in the WINS database, then the client can establish a session based on the address mapping received from the WINS server.
2. If the WINS server query is unsuccessful and if the client computer is configured as an h-node, the client computer sends name query request packets (as broadcast messages) in the same manner as a non-WINS-enabled computer.
3. Finally, if other methods fail, the local `LMHOSTS` file is checked. (Included in the search are any centralized `LMHOSTS` files referred to in `#INCLUDE` statements in the local file.)

WINS servers accept and respond to User Datagram Protocol (UDP) name queries. Any name-to-IP address mapping registered with a WINS server can be provided reliably as a response to a name query. However, a mapping in the database does not ensure that the related device is currently running, only that a computer claimed the particular IP address and that it currently is a valid mapping.

Name Registration

Name registration ensures that the NetBIOS computer name and IP address are unique for each device.

- *If WINS is enabled on the client* – The name registration request is sent directly to the WINS server to be added to the database. A WINS server accepts or rejects a computer name registration depending on the current contents of its database, as follows:
  - If the database contains a different address for that name, WINS challenges the current entry to determine whether that device still claims the name.
  - If another device is using that name, WINS rejects the new name registration request.
  - Otherwise, WINS accepts the entry and adds it to its local database together with a time stamp, an incremental unique version number, and other information.
- *If WINS is not enabled on the client* – For a non-WINS computer to register its name, a name registration request packet is broadcast to the local network stating its NetBIOS computer name and IP address. Any device on the network that previously claimed that name challenges the name registration (with a negative name registration response), resulting in an error for the computer attempting to register the duplicate name. If the name registration request remains unchallenged for a specific time period, the requesting computer adopts that name and address.

After a non-WINS computer claims a name, it must challenge duplicate name registration attempts (with a negative name registration response) and respond positively to name queries issued on its registered name (with a positive name query response). The positive name query response contains the IP address of the computer so that the two systems can establish a session.

Name Release

When a computer finishes using a particular name, it no longer challenges other registration requests for the name. This is referred to as *releasing* a name.

- *If WINS is enabled on the client* – Whenever a computer is shut down properly, it releases its name to the WINS server, which marks the related database entry as released. If the entry remains released for a certain period of time, the WINS server marks it as extinct, updates the version number, and notifies other WINS servers of the change.
  - If a name is marked released at a WINS server, and a new registration arrives using that name but a different address, the WINS server immediately can give that name to the requesting client because it knows that the old client no longer is using that name. This might happen, for example, when a DHCP-enabled laptop changes subnets.

- If the computer released its name during an orderly shutdown, the WINS server does not challenge the name when the computer is reconnected. If an orderly shutdown did not occur, the name registration with a new address causes the WINS server to challenge the registration. The challenge fails and the registration succeeds, because the computer no longer has the old address.

- *If WINS is not enabled on the client* – When a non-WINS computer releases a name, a broadcast is made to allow any systems on the network that might have cached the name to remove it. Upon receiving name query packets specifying the deleted name, computers simply ignore the request, allowing other computers on the network to acquire the released name.

Note – For non-WINS computers to be accessible from other subnets, their names must be added as static entries to the WINS database or in the `LMHOSTS` file(s) on the remote system(s) because they will respond only to name queries that originate on their local subnet.

Name Renewal

Client computers periodically are required to renew their NetBIOS name registrations with the WINS server. When a client computer first registers with a WINS server, the WINS server returns a message that indicates when the client will need to renew its registration, as follows:

- Default renewal interval for entries in the WINS database is six days.
- WINS clients register and refresh every three days.
- Primary and backup WINS servers should have the same renewal interval.
- An entry defined as static never expires.

If the entry is owned by the local WINS server, the name is released at the specified time unless the client has renewed it. If the entry is owned by another WINS server, the entry is revalidated at the specified time. If the entry does not exist in the database of the WINS server that owns the entry, it is removed from the local WINS database. A name renewal request is treated as a new name registration.

Caution – Incorrectly adjusting the renewal interval might adversely affect system and network performance.

WINS Proxy

A *WINS proxy* is a WINS-enabled computer that helps resolve name queries for non-WINS enabled computers in routed TCP/IP intranets. By default, non-WINS enabled computers are configured as b-node, which uses IP broadcasts for name queries. The WINS proxy computer listens on the local subnet for IP broadcast name queries.

When a non-WINS enabled computer sends an IP name query broadcast, the WINS proxy accepts the broadcast and checks its cache for the appropriate NetBIOS computer name-to-IP-address mapping. If the WINS proxy has the correct mapping in its cache, the WINS proxy sends this information to the non-WINS computer. If the name-to-IP-address mapping is not in cache, the WINS proxy queries a WINS server for the name-to-IP-address mapping.

If a WINS server is not available on the local subnet, the WINS proxy can query a WINS server across a router. The WINS proxy caches (stores in memory) computer name-to-IP-address mappings it receives from the WINS server. These mappings are used to respond to subsequent IP broadcast name queries from b-node computers on the local subnet.

The name-to-IP-address mappings that the WINS proxy receives from the WINS server are stored in the WINS proxy cache for a limited time. (By installation default, this value is six minutes. The minimum value is one minute.)

When the WINS proxy receives a response from the WINS server, it stores the mapping in its cache and responds to any subsequent name query broadcasts with the mapping received from the WINS server.

The role of the WINS proxy is similar to that of the `DHCP/BOOTP` relay agent, which forwards DHCP client requests across routers. Because the WINS server does not respond to broadcasts, a computer configured as a WINS proxy should be installed on subnets that include computers that use broadcasts for name resolution.

Note – To configure a Windows NT, Version 4.0, computer as a WINS proxy, you must manually edit that computer's Registry. The `EnableProxy` keyword must be set to 1 (`REG_DWORD`). This keyword is located in the following key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters`

WINS and Dial-Up TCP/IP Networking Clients

Dial-up TCP/IP networking clients provide remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users of dial-up TCP/IP networking on Windows 98, Windows 2000, or Windows NT computers can dial in to access their networks remotely for services such as file and printer sharing, electronic mail, scheduling, and database access.

Windows 2000, Windows 98, and Windows NT support routing TCP/IP traffic over dial-up TCP/IP connections through several different types of dial-up TCP/IP networking servers, including the following:

- UNIX system servers that support either of the industry-standard Point-to-Point Protocol (PPP) or serial line IP (SLIP) dial-up TCP/IP networking standards
- Windows NT remote access service (RAS) servers
- Third-party RAS servers that support PPP and/or SLIP connections, such as those that are available from CISCO, 3COM, and Bay Networks

Dial-up Windows 2000, Windows 98, and Windows NT computers that are configured to route TCP/IP also can be configured to use WINS servers. (For details, see your Microsoft documentation.)

Dial-up Windows 2000, Windows 98, and Windows NT computers that are configured to route TCP/IP and use WINS can access remotely their networks for services, including PC NetLink and Windows NT file and print sharing, electronic mail, scheduling, and database access.

About WINS Server Planning

The number of WINS servers that an enterprise requires is based on the number of WINS client connections per server and the network topology. The number of users that a server can support varies according to usage patterns, data storage, and processing capabilities of the WINS server computer.

Note – Although a Solaris physical host can have up to ten PC NetLink virtual servers configured on it, only one of the virtual servers on the host can act as a WINS server.

Planning for WINS server implementation on the network typically requires consideration of the issues presented in the following table.

TABLE 6-1 WINS Server Implementation Planning Issues

Planning Issue	Guideline
How many WINS servers are required to ensure distribution of name query and name registration loads throughout the network?	One WINS server can handle NetBIOS name resolution requests for 10,000 computers. However, consider the location of routers on the network and the distribution of clients in each subnet when deciding how many WINS servers are required. See the following sections: "Planning for WINS Client Network Traffic," "Planning for WINS Server Performance," and "Planning Replication Partners and Proxies."
Is the WAN bandwidth sufficient to support WINS server and WINS client name registration traffic?	See the next section, "Planning for WINS Client Network Traffic."
How many WINS servers are needed for disaster recovery, backup, and redundancy requirements?	See "Planning for WINS Server Performance."
How can a planned distribution of WINS servers throughout the network be validated before installation?	When planning a network configuration, a generally accepted approach is to consider the consequences of two simultaneous failures at different points on the network.

Planning for WINS Client Network Traffic

WINS clients generate the following types of network traffic:

- Name registration
- Name refresh
- Name release
- Name query

When a WINS-enabled client starts on the network, it sends a name registration request for the computer name, user name, domain name, and any additional Microsoft network client services running on the computer. In other words, when a WINS client starts on the network, it generates a minimum of three name registration requests and three entries in the WINS database.

A PC NetLink-based WINS client usually registers more NetBIOS names than other WINS-enabled clients. The name registration requests generated by a computer running under the PC NetLink program include the following:

- Server component
- Domain names
- Replicator service name
- Browser service name
- Additional network program and service names

WINS Client Traffic on Routed Networks

When planning for WINS client traffic on large routed networks, consider the effect of name query, registration, and response traffic routed between subnets.

Name requests and responses that occur at the daily startup of computers must pass through the traffic queues on the routers and may cause delays at peak times.

Daily Startup of WINS Clients

An active WINS client name registration in a WINS server database is replicated to all *pull partners* configured on that WINS server. (See "Configuring Replication Partners" on page 230 for an explanation of pull partners and *push partners*.) After some time, the active name registration is replicated to all WINS servers on the network.

When a WINS client is turned off at the end of the day, it releases the name. When the computer is started the next morning, the WINS client registers the name again with the WINS server and receives a new version ID. This new, active name registration entry is replicated to the WINS server's pull partners as on the previous day.

Therefore, the number of name registration entries that are replicated each day is roughly equivalent to the number of computers started each day times the number of NetBIOS names registered at each computer.

On large networks (50,000 or more computers), the biggest traffic load may be the name registration requests generated when WINS clients start on the network. Fortunately, the difference in time zones in large enterprise networks provides some distribution of this WINS client startup load.

Roving User

Name challenge traffic occurs when a user stops the computer and then moves and starts the computer on a different subnet with another primary WINS server.

Typically, the name registration request is answered with a Wait for Acknowledgment message (100 bytes), and the new WINS server, assuming the active entry was replicated, challenges the IP address that is currently in its database for this name (Name Query packet, 92 bytes).

When there is no reply, as can be expected in this case, the WINS server repeats the challenge two more times and then updates the name registration entry with the new IP address and a new version ID. The new version ID indicates that the entry must be replicated from its new "owning" WINS server to other WINS servers on the network.

Estimating WINS Client Traffic

You can estimate WINS client traffic based on the behavior of the WINS clients as described in the preceding sections.

However, when estimating WINS client traffic, you also must consider the network topology and the design or configuration of the routers in the network. In some cases it may not always be possible to predict the traffic load on a specific network router because the routers may be designed or configured to autonomously route traffic based on factors other than traffic load.

Planning for WINS Server Replication Across Wide Area Networks

The frequency of WINS database replication between WINS servers is a major planning issue. You should replicate the WINS database frequently enough that the down-time of any WINS server will not affect the reliability of the mapping information in the database of other WINS servers.

However, when planning WINS database replication frequency, you do not want the frequency to interfere with network throughput. This could occur if replication frequency is set to a short time interval.

Consider the network topology when planning for replication frequency. For example, if your network has multiple hubs connected by relatively slow wide area network (WAN) links, you can configure WINS database replication between WINS servers on the slow links to occur less frequently than replication on the local area network (LAN) or on fast WAN links. This reduces traffic across the slow link and reduces contention between replication traffic and WINS client name queries.

For example, WINS servers at a central LAN site may be configured to replicate every 15 minutes, while database replication between WINS servers in different WAN hubs might be scheduled for every 30 minutes, and replication between WINS servers on different continents might be scheduled to replicate twice a day.

Planning for WINS Server Performance

When planning for a large-scale power outage after which many computers will attempt to go back on line simultaneously, the conservative recommendation is that you plan to include one WINS server and a backup server for every 10,000 computers on the network. A WINS server typically can service 1,500 name registrations per minute and 4,500 queries per minute.

Two factors enhance WINS server performance. WINS server performance can be increased by almost 25 percent on a computer with two processors. WINS server name replication response time can be improved measurably by using a dedicated disk.

After you establish WINS servers on an intranet, you can adjust the time between a WINS client name registration and name renewal. This is referred to as the Renewal interval. Setting this interval to reduce the numbers of registrations can help tune server response time. (The Renewal interval is specified in the WINS Server Configuration dialog box.)

Planning Replication Partners and Proxies

Choosing whether to configure another WINS server as a push partner or pull partner depends on several facts, including the specific configuration of servers at your site, whether the partner is across a wide area network (WAN), and how important it is to distribute changes throughout the network.

You should install only one computer configured as a WINS proxy on each subnet. Configuring more than one WINS proxy per subnet can overload the WINS servers on the same subnet.

In one possible configuration, you can designate one WINS server as the central server, and all other WINS servers as both push partner and pull partner of this central server. Such a configuration ensures that the WINS database on each server contains addresses for every node on the WAN. (See the next section for definitions of push partner and pull partner.)

Another option is to set up a chain of WINS servers, where each server is both the push partner and pull partner with a nearby WINS server. In such a configuration, the two servers at the ends of the chain would be push and pull partners with each other. Other replication partners can be established for your site's needs.

Configuring WINS Servers and WINS Client Behavior

You should configure multiple WINS servers on your network to increase the availability and balance the load among servers. When using multiple servers, each WINS server should be configured with at least one other WINS server as its replication partner. You should have multiple WINS servers installed on your network for the following reasons:

- To distribute NetBIOS computer name query and registration processing load
- To provide WINS database redundancy, backup, and disaster recovery

Configuring a WINS server includes specifying information about when database entries are replicated between partners. A *pull partner* is a WINS server that pulls in replicas of database entries from its partner by requesting and then accepting replicas. A *push partner* is a WINS server that sends update notification messages to its partner when its WINS database has changed. When its partner responds to the notification with a replication request, the push partner sends a copy of its current WINS database to the partner.

For each WINS server, you must configure threshold intervals for triggering database replication, based on a specific time, a time period, or a certain number of new records. If you designate a specific time for replication, this occurs one time only. If a time period is specified, replication is repeated at that interval.

Use WINS Manager to configure WINS server management of WINS client mappings by using the configuration options in the WINS Server Configuration (Local) dialog box. The configuration options allow you to specify time intervals that govern WINS client behavior as described in the following table.

TABLE 6-2 WINS Server Time Interval Options

Configuration Option	Description
Renewal interval	Specifies how often a client reregisters its name. The default is six days.
Extinction interval	Specifies the interval between when an entry is marked as released and when it is marked as extinct. The default is dependent on the Renewal interval and, if the WINS server has replication partners, on the maximum replication time interval. The default is four days.

TABLE 6-2 WINS Server Time Interval Options *(Continued)*

Configuration Option	Description
Extinction timeout	Specifies the interval between when an entry is marked extinct and when the entry is finally scavenged from the database. The default is dependent on the Renewal interval and, if the WINS server has replication partners, on the maximum replication time interval. The default is six days.
Verify interval	Specifies the interval after which the WINS server must verify that old names it does not own are still active. The default is dependent on the Extinction interval. The minimum allowable value is 24 days.

The Extinction interval, Extinction timeout, and Verify interval are derived from the Renewal interval and the Partner Replication interval. The WINS server adjusts the values specified by the administrator to keep the inconsistency between a WINS server and its partners as small as possible.

You can change the following configuration parameters using the Advanced option in the WINS Server Configuration dialog box.

TABLE 6-3 WINS Server Advanced Configuration Options

Configuration Option	Description
Logging enabled	Specifies whether logging of database changes to `J50.log` files should be turned on. (This option is ignored in PC NetLink WINS.)
Log detailed events	Specifies whether logging events is in verbose mode. (This requires considerable computer resources and should be turned off if you are tuning for performance.)
Replicate only with partners	Specifies that replication occurs only with configured WINS pull or push partners. If this option is not checked, an administrator can ask a WINS server to pull or push from or to a non-listed WINS server partner. By default, this option is checked.
Backup on termination	Specifies that the database will be backed up automatically when WINS Manager is stopped except when the computer is stopped.

TABLE 6-3 WINS Server Advanced Configuration Options *(Continued)*

Configuration Option	Description
Migrate on/off	Specifies that static unique and multihomed records in the database are treated as dynamic when they conflict with a new registration or replica. This means that if they are no longer valid, they will be overwritten by the new registration or replica. By default, this option is not checked.
Starting version count	Specifies the highest version ID number for the database. Usually, you will not need to change this value unless the database becomes corrupted and needs to start fresh. In such a case, set this value to a number higher than appears as the version number counter for this WINS server on all the remote partners that earlier replicated the local WINS server's records. WINS may adjust the value you specify to a higher one to ensure that the database records are replicated quickly to the WINS servers. This value can be seen in the View Database dialog box in WINS Manager.
Database backup path	Specifies the directory where the WINS database backups will be stored. If you specify a backup path, WINS automatically performs a full backup of its database to this directory. WINS also uses this directory to perform an automatic restoration of the database in the event that the database is found to be corrupted when WINS is started. Do not specify a network directory.

Configuring Replication Partners

WINS servers communicate among themselves to replicate their databases fully, ensuring that a name registered with one WINS server is eventually replicated to all other WINS servers within the network. All mapping changes converge within the replication period for the entire WINS system, which is the maximum time for propagating changes to all WINS servers. All released names are propagated to all WINS servers after they become extinct, based on the interval specified in WINS Manager.

Use the Replication Partners command in WINS Manager to configure replication partners and replication partner properties. There are two types of replication partners: pull and push.

- A pull partner is a WINS server that pulls (requests) WINS database entries from its push partners. The pull partner pulls new WINS database entries by requesting entries with a higher version number than the last entry it received during the last replication from that push partner.

The pull partner can notify push partners that replication is needed by using either of the following methods: an arbitrary time interval, as configured by the WINS administrator, or immediate replication, initiated by the WINS administrator using WINS Manager.

- A push partner is a WINS server that sends a message to its pull partners that the WINS database has changed. When the pull partners respond to the message with a replication request, the push partner sends a copy of its new WINS database entries to the pull partners.

  The push partner notifies pull partners of replication requirements by using either of the following methods: an arbitrary number of WINS updates (update count), as configured by the WINS administrator, or immediate replication initiated by the WINS administrator by using WINS Manager.

  If you modify the update count using WINS Manager, you then can open the WINS Server Configuration dialog box and click the OK button. As a result, the new value will take effect immediately.

Choosing whether to configure another WINS server as a push partner or pull partner depends on several considerations, including the specific configuration of servers at your site, whether the partner is across a wide area network (WAN), and how important it is to propagate the changes.

Replication is triggered when a WINS server polls another server to get replicated information. This can begin when the WINS server is started, and is repeated based on the configured update count or time interval, or by using WINS Manager to start immediate replication.

Replication also is triggered when a WINS server reaches a threshold set by the administrator. This is an update count for registrations and changes. In this case, the server notifies its pull partners that it has reached this threshold, and the other servers can then decide to pull replicated information.

It is always a good idea for replication partners to be both push and pull partners of each other. The primary and backup WINS servers must be both push and pull partners with each other to ensure that the primary and backup databases are consistent.

Managing Static NetBIOS-to-IP Address Mappings

Static mappings are non-dynamic database entries of NetBIOS computer name-to-IP address mappings for computers on the network that are not WINS-enabled or for special groups of network devices.

Use the Static Mappings command on the Mappings menu in WINS Manager to view, add, edit, delete, import, or filter static mappings.

Once a static name-to-IP address mapping is entered into the WINS server database, it cannot be challenged or removed except by an administrator who must remove it manually using WINS Manager. All changes made to the WINS server database using WINS Manager take effect immediately.

Note – A DHCP-reserved (or static) IP address for a unique name in a multihomed computer overrides an obsolete WINS static mapping if the WINS server advanced configuration option Migration On/Off is checked On.

Static NetBIOS name mappings can be any of the types listed in the following table.

TABLE 6-4 Static NetBIOS Name-Mapping Types

Type Option	Description
Unique	A unique name that maps to a single IP address. Contrast with Multihomed type.
Group	Also referred to as a "Normal Group." When adding an entry to Group using WINS Manager, you must enter the computer name and IP address. However, the IP addresses of individual members of Group are not stored in the WINS database. Because member addresses are not stored, there is no limit to the number of members that can be added to a group. Broadcast name packets are used to communicate with group members. Contrast with Internet Group type.
Domain Group	A NetBIOS name-to-IP address mapping that has 0x1C as the 16th byte. A Domain Group stores up to a maximum of 25 addresses for members. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.

TABLE 6-4 Static NetBIOS Name-Mapping Types *(Continued)*

Type Option	Description
Internet Group	A user-defined group that enables you to classify resources such as printers for easy reference and browsing. The default 16th byte of an Internet Group name is set equal to 0x20. An Internet Group can store up to a maximum of 25 addresses for members. When you add an Internet Group, three unique records are added: • `InternetGroupName<0x20>` • `InternetGroupName<0x3>` • `InternetGroupName<0x0>` This is similar to the Domain Group. Internet Group members can be added as the result of dynamic group registrations. However, a dynamic member does not replace a static member that is added by using WINS Manager or by importing the `LMHOSTS` file. Contrast with Group type.
Multihomed	A unique name that can have more than one address. This is used for multihomed computers. The maximum number of addresses that can be registered as multihomed is 25. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration. Contrast with Unique type.

You can configure a WINS server to replicate only Domain, Internet, and Multihomed groups to its replication partners, by manually changing the Replication Type Registry parameter to a value of 1.

This procedure eliminates the replication of information (unique names) that is not needed outside the local domain, while allowing replication of special group information. When a group spans multiple domains that are serviced by other WINS servers, it is desirable to reduce replication traffic.

The following table describes basic WINS server statistics.

TABLE 6-5 Basic WINS Server Statistics Descriptions

Statistic	Description
Server Start Time	The time when this WINS server was started.
Database Initialized	The last time static mappings were imported into the WINS database.
Statistics Cleared	The time when statistics for the WINS server were last cleared with the Clear Statistics command from the View menu.
Last Replication Times	The times at which the WINS database was last replicated.

TABLE 6-5 Basic WINS Server Statistics Descriptions *(Continued)*

Statistic	Description
Periodic	The last time the WINS database was replicated based on the Replication interval specified in the Preferences dialog box.
Admin Trigger	The last time the WINS database was replicated because the administrator chose the Replicate Now button in the Replication Partners dialog box.
Net Update	The last time the WINS database was replicated as a result of a network request, which is a push notification message that requests propagation.
Total Queries Received	The number of name query request messages received by this WINS server. Successful indicates how many names were successfully matched in the database, and Failed indicates how many names this WINS server could not resolve.
Total Releases	The number of messages received that indicate a NetBIOS application has shut itself down. Successful indicates how many names were successfully released, and Failed indicates how many names this WINS server could not release.
Total Registrations	The number of messages received that indicate name registrations for clients.

You can display additional statistics by clicking Detailed Information on the Server menu. The following table describes these detailed information statistics.

TABLE 6-6 Detailed WINS Server Statistics Descriptions

Statistic	Description
Last Address Change	The time at which the last WINS database change was replicated
Last Scavenging Times	The last times that the database was cleaned for specific types of entries
Periodic	The time when the database was cleaned based on the Renewal interval specified in the WINS Server Configuration dialog box
Admin Trigger	The time when the database was last cleaned because the administrator chose the Initiate Scavenging command
Extinction	The time when the database was last cleaned based on the Extinction interval specified in the WINS Server Configuration dialog box
Verification	The time when the database was last cleaned based on the Verify interval specified in the WINS Server Configuration dialog box
Unique Registrations	The number of name registration requests that have been accepted by this WINS server

TABLE 6-6 Detailed WINS Server Statistics Descriptions *(Continued)*

Statistic	Description
Unique Conflicts	The number of conflicts encountered during registration of unique names owned by this WINS server
Unique Renewals	The number of renewals received for unique names
Group Registrations	The number of registration requests for groups that have been accepted by this WINS server
Group Conflicts	The number of conflicts encountered during registration of group names
Group Renewals	The number of renewals received for group names

Viewing WINS Server Status

WINS Manager allows you to view administrative and operational information about WINS servers. When you open WINS Manager, the title bar shows the IP address or computer name for the currently selected server, depending on whether you used the address or name to connect to the server. The right pane displays basic statistics about the selected WINS server.

Viewing the WINS Database

You can view actual dynamic and static mappings stored in the WINS database, based on the WINS server that owns the entries. Use WINS Manager to choose the Show Database command from the Mappings menu.

By default, the Show Database dialog box shows all mappings for the WINS database on the currently selected WINS server. You can select a Sort Order option to sort by IP address, computer name, time stamp for the mapping, version ID, or type. To view only a range of mappings, choose the Set Filter button.

This process, called *scavenging*, is done automatically over intervals defined by the relationship between the Renewal and Extinct intervals defined in the WINS Server Configuration (Local) dialog box. You can also clean the database manually.

To scavenge the WINS database, choose the Initiate Scavenging command from the Mappings menu. The following table describes the results of scavenging a WINS database.

TABLE 6-7 Effects of Scavenging WINS Database

State Before Scavenging	State After Scavenging
Owned active names for which the Renewal interval has expired	Marked *released*
Owned released name for which the Extinction interval has expired	Marked *extinct*
Owned extinct names for which the Extinction timeout has expired	Deleted
Replicas of extinct names for which the Extinction interval has expired	Deleted
Replicas of active names for which the Verify interval has expired	Revalidated
Replicas of extinct or deleted names	Deleted

Advanced Configuration Parameters for WINS

This section presents configuration parameters that affect the behavior of WINS and that you can modify only through the Windows NT Registry Editor. For some parameters, WINS can detect Registry changes immediately. For other parameters, you must restart WINS for the changes to take effect.

Caution – You can impair or disable WINS if you make incorrect changes in the Registry while using Registry Editor. Whenever possible, use WINS Manager to make configuration changes rather than using Registry Editor. If you make errors while changing values with Registry Editor, you will not be warned because the Registry Editor does not recognize semantic errors.

The following sections describe the value entries for WINS parameters that can only be set by adding an entry or changing values in Registry Editor.

Registry Parameters for WINS Servers

The Registry parameters for WINS servers are specified under the following key:
`..\SYSTEM\CurrentControlSet\Services\Wins\Parameters`

This lists all of the non-replication-related parameters needed to configure a WINS server. It also contains a `\Datafiles` subkey, which lists all the files that should be read by WINS to initialize or reinitialize its local database.

- DoStaticDataInit

  Data type = REG_DWORD
  Range = 0 or 1
  Default = 0 (false—that is, the WINS server does not initialize its database)

  If this parameter is set to a non-zero value, the WINS server will initialize its database with records listed in one or more files listed under the \Datafiles subkey. The initialization is done at process invocation and whenever a change is made to one or more values of the \Parameters or \Datafiles keys (unless the change is to modify the value of DoStaticDataInit to its default, 0).

The following parameters in this subkey can be set using the options available in the WINS Server Configuration dialog box:

- BackupDirPath
- DoBackupOnTerm
- LogDetailedEvents
- LoggingOn
- MigrateOn
- RefreshInterval
- RplOnlyWCnfPnrs
- TombstoneInterval (Extinction interval)
- TombstoneTimeout (Extinction timeout)
- VerifyInterval

Also, the \Wins\Parameters\Datafiles key lists one or more files that the WINS server should read to initialize or reinitialize its local database with static records. If the full path of the file is not listed, the directory of execution for the WINS server is assumed to contain the data file. The parameters can have any names (for example, DF1 or DF2). Their data types must be REG_EXPAND_SZ or REG_SZ.

Registry Parameters for Replication Partners

The \Wins\Partners key has two subkeys, \Pull and \Push, under which are subkeys for the IP addresses of all push and pull partners, respectively, of the WINS server.

Parameters for Push Partners

A push partner, listed under the \Partners\Pull key, is one from which a WINS server pulls replicas and from which it can expect update notification messages. The following parameter appears under the IP address for a specific push partner. You can set this parameter only by changing the value in the Registry:

- MemberPrec

Data type = REG_DWORD
Range = 0 or 1
Default = None

Specifies the order of precedence for this WINS partner, with 0 indicating low precedence and 1 indicating high precedence. Notice that dynamically registered names are always high precedence. When a 1C name is pulled from this WINS partner, the addresses contained in it are given this precedence level. The value can be 0 (low) or 1 (high). Set this value to 1 if this WINS server is serving a geographic location that is nearby.

The following parameters appear under this subkey and can be set in the WINS Server Configuration dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Pull

- InitTimeReplication
- CommRetryCount

The following parameters appear under this subkey and can be set using the Preferences dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners
\Pull*IP Address*

- SpTime (Start Time for pull partner default configuration)
- TimeInterval (Replication interval)

For SpTime, WINS replicates at the set time if it is in the future for that day. After that, it replicates every number of seconds specified by TimeInterval. If SpTime is in the past for that day, WINS replicates every number of seconds specified by TimeInterval, starting from the current time (if InitTimeReplication is set to 1).

Parameters for Pull Partners

A pull partner of a WINS server, listed under the \Partners\Push key, is one from which it can expect pull requests to pull replicas and to which it sends update notification messages. The following parameters appear under this subkey and can be set using the options available in the WINS Server Configuration (Local) dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Push

- InitTimeReplication
- RplOnAddressChg

The following parameter appears under this subkey and can be set using the options available in the Preferences dialog box:

..\SYSTEM\CurrentControlSet\Services\
Wins\Partners\Push*IP Address*

- UpdateCount

About Database Management

All databases need to be backed up and cleaned periodically. PC NetLink Server Manager and various Solaris commands are the tools you use to maintain the databases; additionally, PC NetLink Server Manager enables you to schedule a routine for performing most database maintenance tasks automatically.

The following sections describe how to view, back up, restore, clean up, and compact the PC NetLink databases.

Compacting the WINS Database

There is no built-in limit to the number of records that a WINS server can replicate or store. The size of the database is dependent on the number of WINS clients on the network. The WINS database grows over time as a result of clients starting and stopping on the network.

The size of the WINS database is not directly proportional to the number of active client entries. Over time, as some WINS client entries become obsolete and are deleted, there remains some unused space.

To recover space and improve performance, you use PC NetLink Server Manager or the Solaris command line on the PC NetLink server to compact the database.

Backing Up and Restoring the WINS Database

You use PC NetLink Server Manager, the Solaris command line, or the Windows NT tool, WINS Manager, to back up and restore the WINS database. The following WINS server database files are stored in the `/var/opt/lanman/wins` directory. This directory was created when you installed the PC NetLink program.

- `schema.db` – This file is used by WINS to hold information about the structure of its database.
- `wins.db` – This is the WINS database file.

Caution – Do not remove or tamper with the `schema.db` or `wins.db` files in any manner.

You can also use the Windows NT tool, WINS Manager, to examine the current database backup path and to establish a new one.

Cleaning Up the Databases

Cleaning up (also known as "scavenging") the WINS database is an administrative task related to backing up the database. Like any database, the WINS server database of address mappings needs to be cleaned periodically.

You should periodically clear the local WINS database of released entries and old entries that were registered at another WINS server and replicated to the local WINS server, but for some reason did not get removed from the local WINS database. Use PC NetLink Server Manager for database cleanup.

Database Maintenance Tasks

The following sections provide detailed instructions for scheduling and performing routine PC NetLink database maintenance tasks. You complete the tasks by using PC NetLink Server Manager. You cannot restore backups created using PC NetLink Version 1.2.

Note – If you are connected to a Solaris server that is running PC NetLink 1.2, some screens that include PC NetLink 2.0 features will not appear.

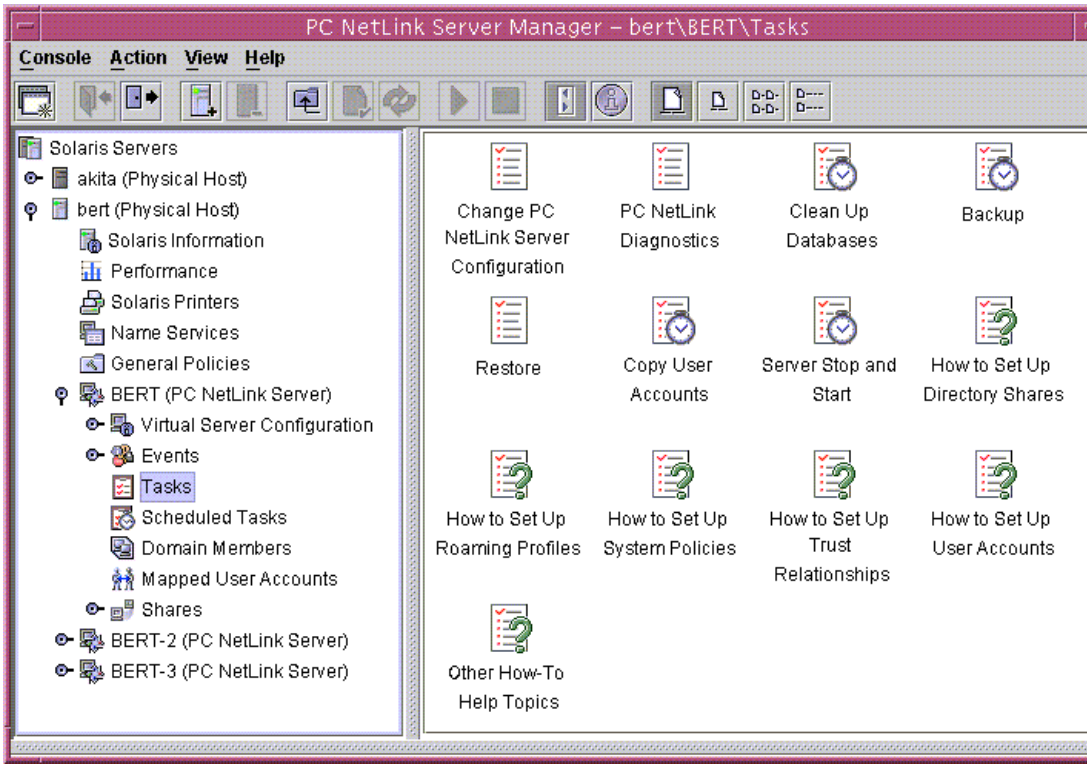
▼ How to Clean Up PC NetLink Databases

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server on which you want to clean up one or more databases.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

3. **Double-click Tasks.**

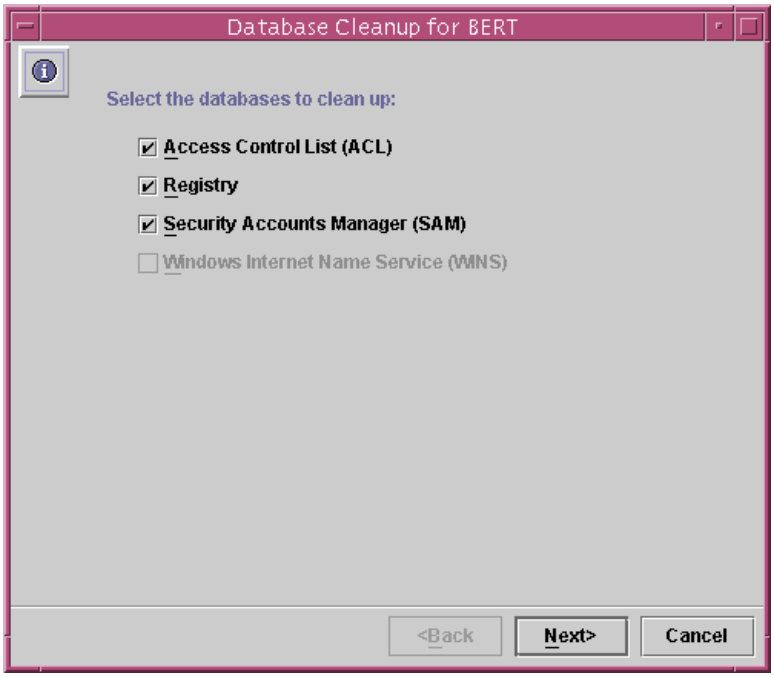
   A screen similar to the following appears.



Note that some of the tasks—including Clean Up Databases and Backup—are marked with a clock face. This indicates that these are tasks that you can run immediately, or automatically on a periodic schedule that you create.

4. **Double-click Clean Up Databases.**

   The resulting screen presents a list of databases to clean up. Note that the WINS option is greyed-out if you are not using the service.

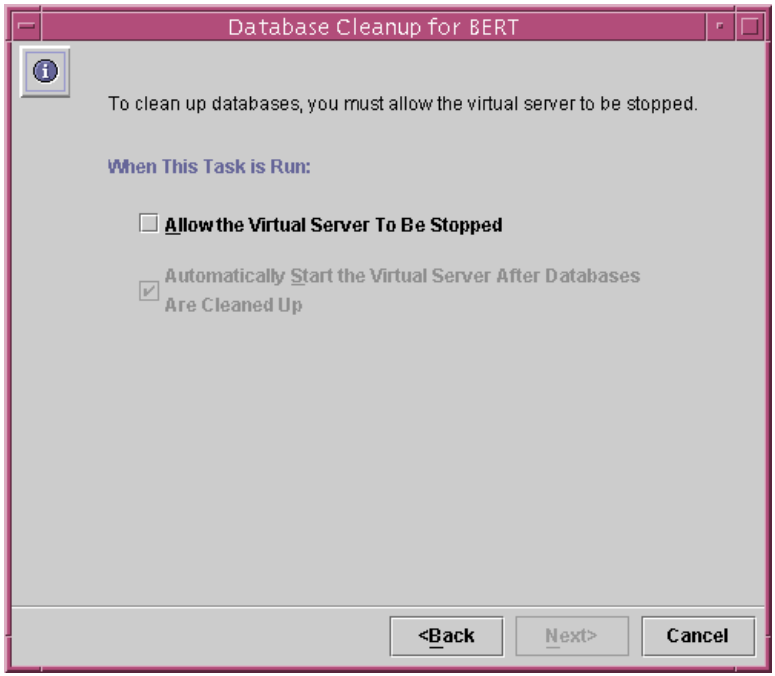


The Cleanup wizard performs the following tasks on the following databases:

- Checks, repairs, and prunes obsolete entries in the Access Control List (ACL) database
- Checks and repairs the Registry
- Checks and repairs the Security Accounts Manager (SAM)
- Checks and removes obsolete entries from the WINS database

5. **Select all of the databases that you want to clean up, and then click Next.**

   The following screen appears.

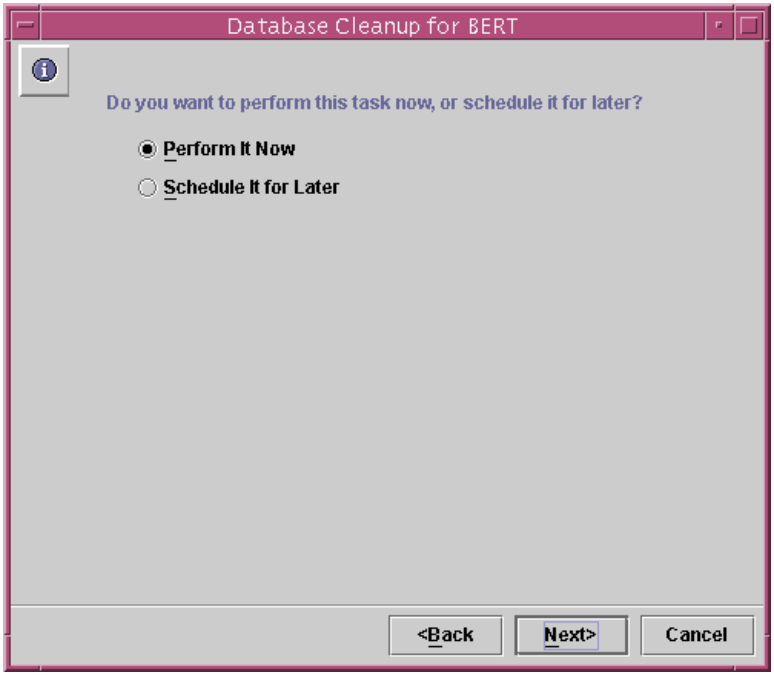


6. **Select Allow the Virtual Server To Be Stopped.**

   You must select this option to proceed. After you have chosen this, you have the option of permitting the system to restart the server automatically after the completion of the task. If you uncheck this option, which is selected by default, you must restart the server manually to complete the task.

7. **Click Next.**

   If you continue the procedure by clicking Next, the resulting screen prompts you for scheduling information.



8. **Select Perform It Now or Schedule It for Later, and then click Next.**

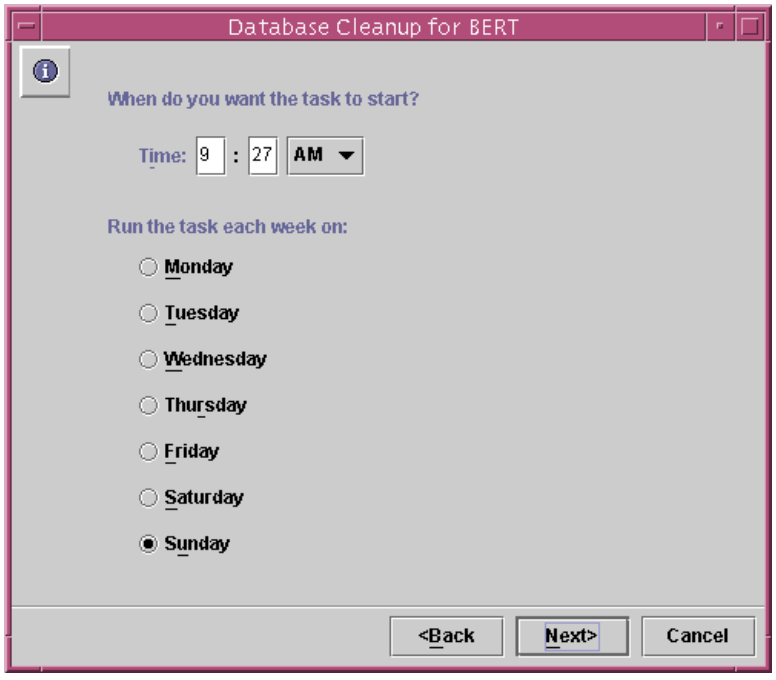
Note – Scheduled tasks are not supported in a high availability (HA) environment.

---

9. **Depending on the selection you made, do one of the following:**
   - *Perform It Now* – Skip to Step 14.
   - *Schedule It for Later* – Continue with Step 10.

10. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

    A screen similar to the following appears.



    The example shows the choices you must make when scheduling the task to be run weekly. Depending on your selection, you must furnish the following information about when you want the task to be run:

    - *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date
    - *Daily* – The time of day
    - *Weekly* – The time of day and the name of the day
    - *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only

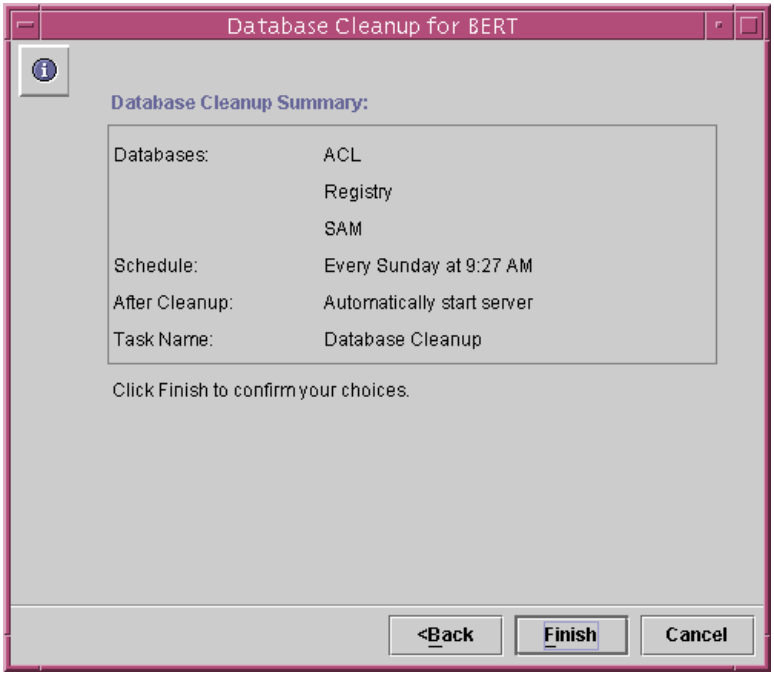
11. **Click Next.**

12. **In the text field of the resulting screen, type a name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

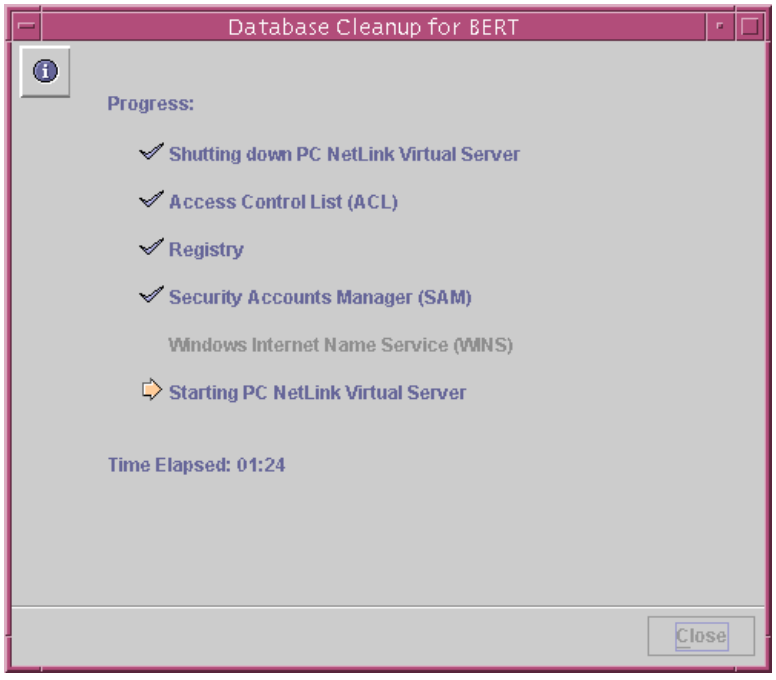
13. **Click Next.**

A summary screen similar to the following appears.



14. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



15. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

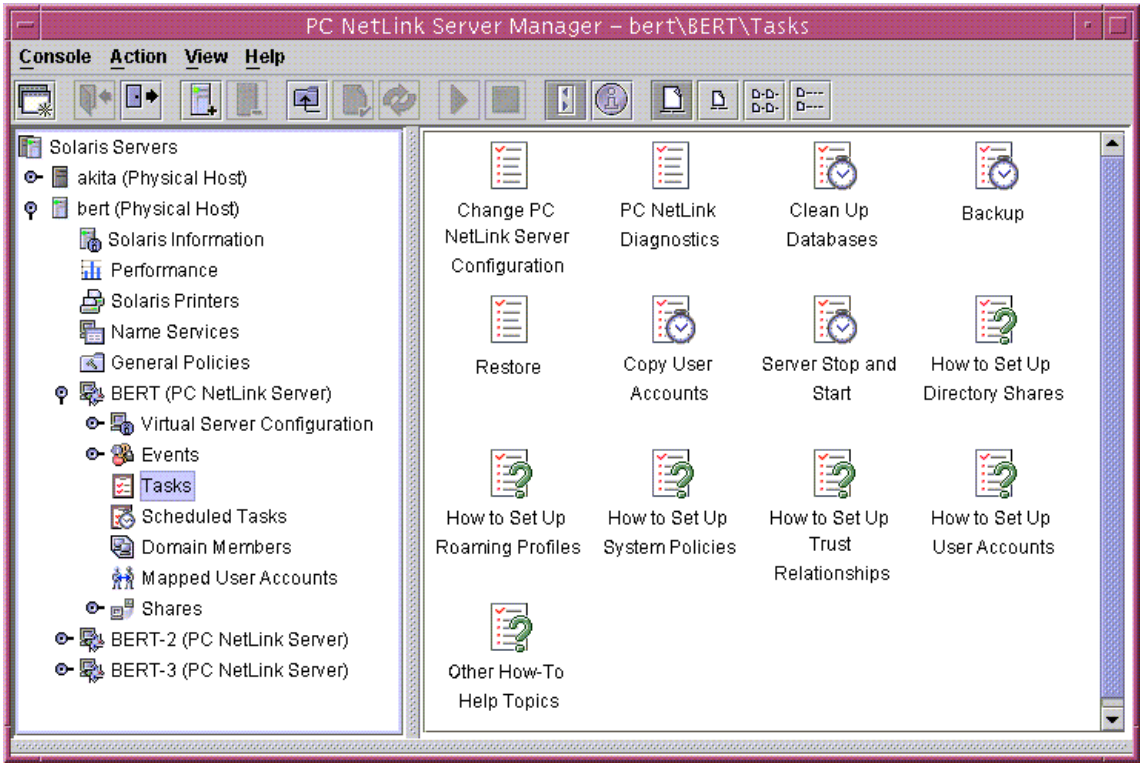
Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

▼ How to Back Up PC NetLink Databases

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server on which you want to back up one or more databases.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Tasks.**

   A screen similar to the following appears.



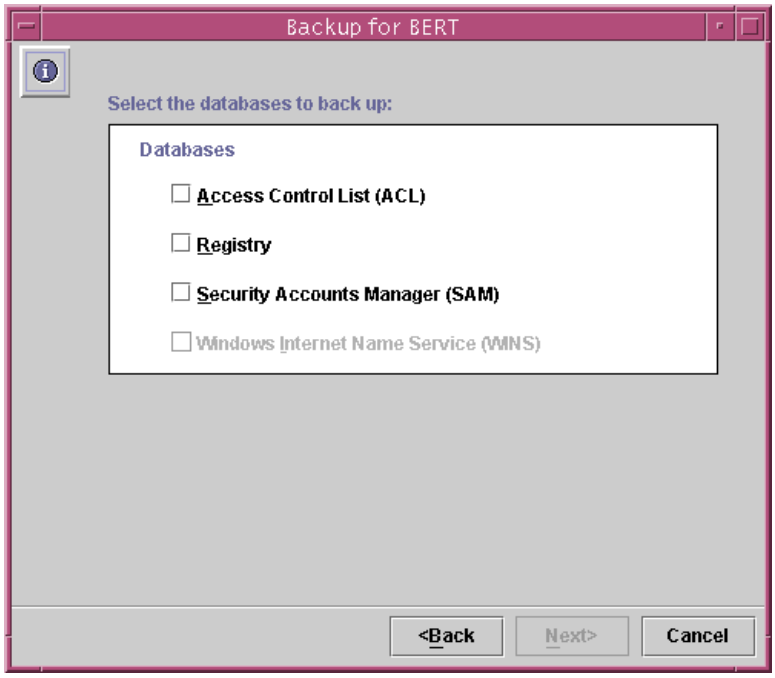
Note that some of the tasks—including Clean Up Databases and Backup—are marked with a clock face. This indicates that these are tasks that you can run automatically on a periodic schedule that you create.

4. **Double-click Backup.**

   A screen appears with two radio buttons for the type of backup to perform: Complete Server Image or Databases Only.

5. **Click the Databases Only radio button, and then click Next.**

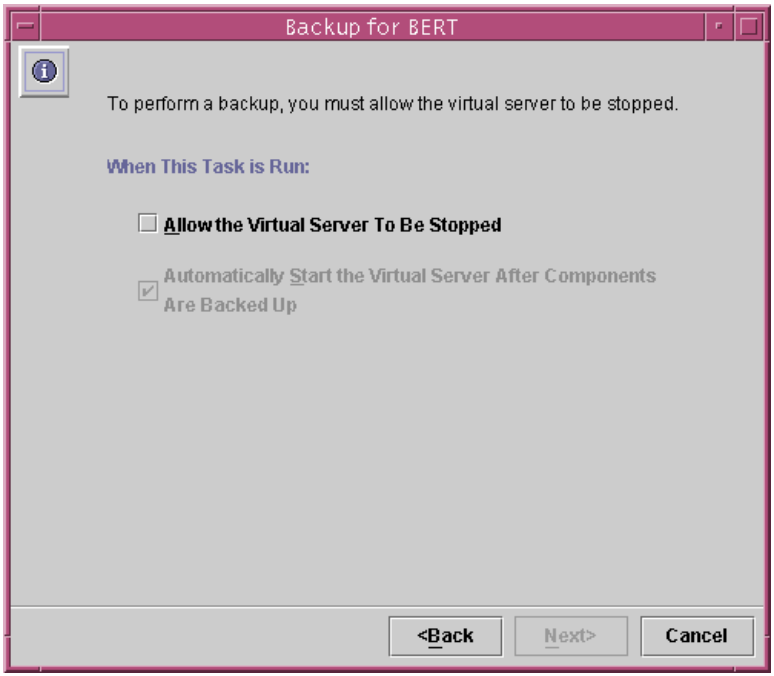
   The resulting screen presents a list of databases to back up. Note that the WINS option is greyed-out if you are not using the service.



6. **Select all of the databases that you want to back up.**

7. **Click Next.**

   A screen similar to the following appears.



8. **Select Allow the Virtual Server To Be Stopped.**

   You must select this option to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the task. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the task.

9. **Click Next.**

   If you continue the procedure by clicking Next, the resulting screen prompts you for scheduling information.

10. **Select Perform It Now or Schedule It for Later, and then click Next.**

Note – Scheduled tasks are not supported in a high availability (HA) environment.

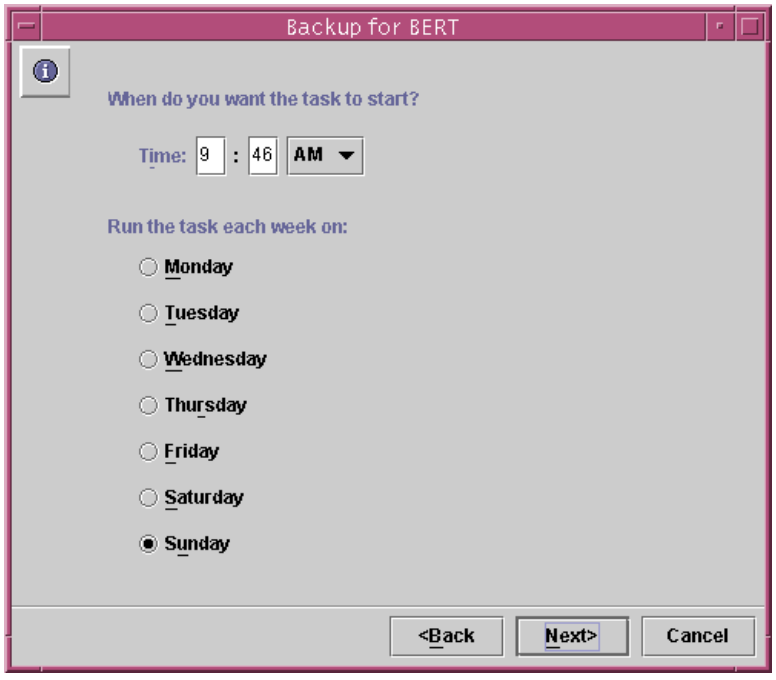
---

11. **Depending on the choice you made, do one of the following:**

    - *Perform It Now* – Skip to Step 17.
    - *Schedule It for Later* – Continue with Step 12.

12. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

    A screen similar to the following appears.



    The example shows the choices you must make when scheduling the task to be run weekly. Depending on your selection, you must furnish the following information about when you want the task to be run:

    - *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date
    - *Daily* – The time of day
    - *Weekly* – The time of day and the name of the day
    - *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only

13. **Click Next.**

    A screen appears that prompts for a path name for the backup files.

14. **In the text field under "Save the backup as" accept the default location, browse for a different location, or type the full path name to a new location.**

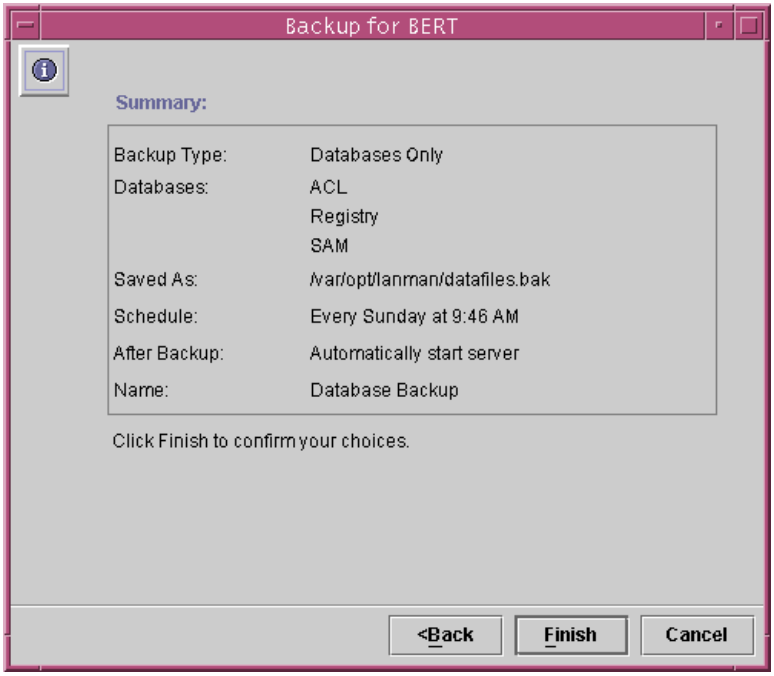
    You must store your backup file as a Solaris file in an existing directory on the PC NetLink system, rather than locally. If you specify a path to a nonexistent directory, a dialog box asks whether you want the wizard to create the directory for you.

15. **In the second text field, type a descriptive name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

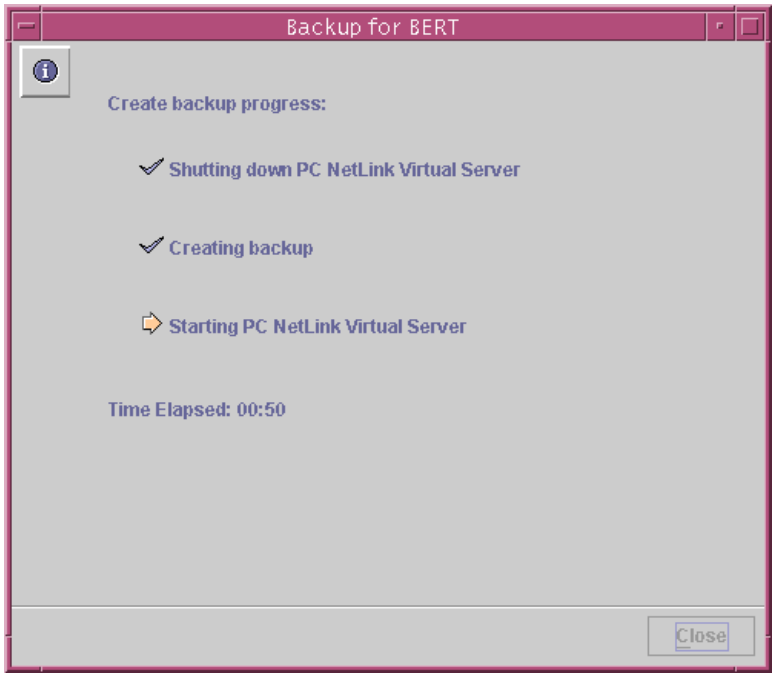
16. **Click Next.**

    A summary screen similar to the following appears.



17. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



18. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

▼ How to Restore Backed-Up Databases

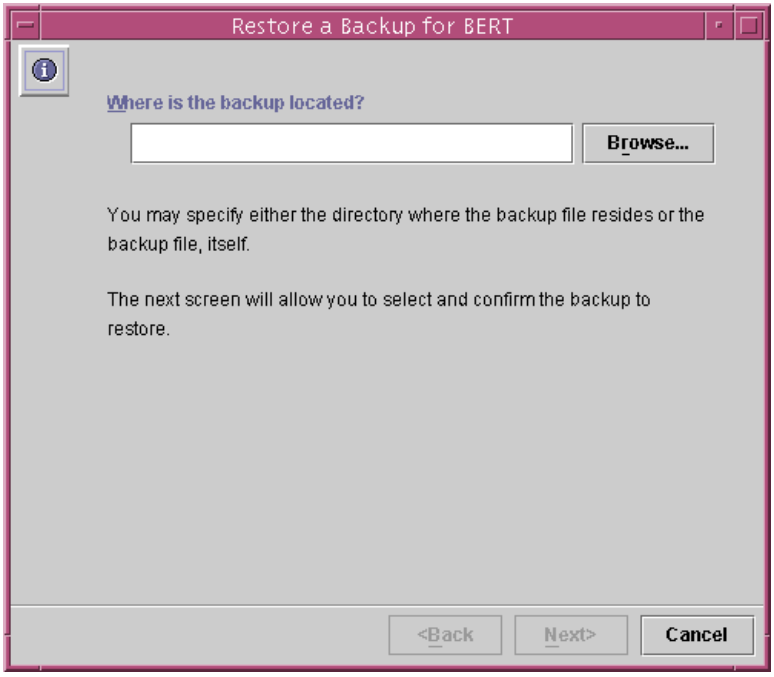
Note – If you are connected to a Solaris server that is running PC NetLink 1.2, some screens that include PC NetLink 2.0 features will not appear.

---

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server to which you want to restore one or more databases.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Tasks.**
4. **Double-click Restore.**

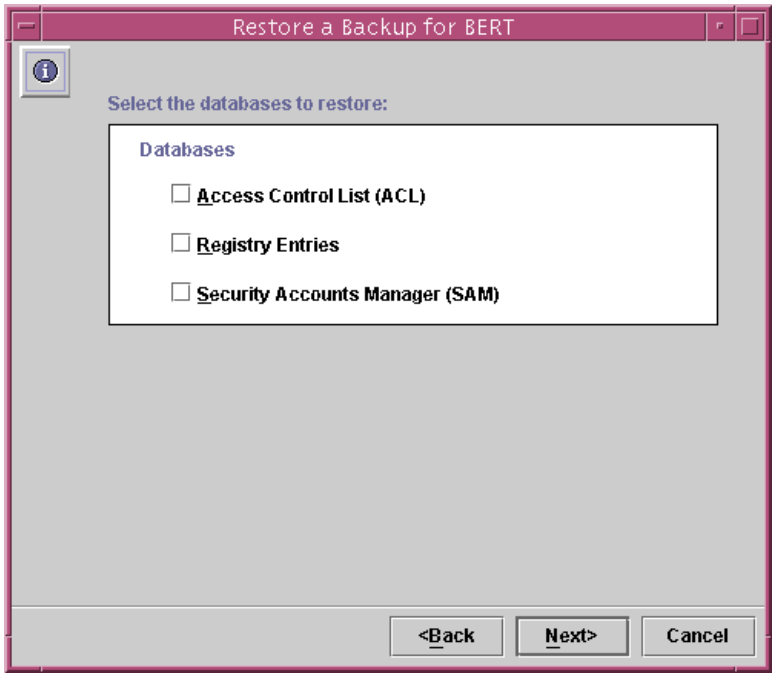
   A screen similar to the following appears.



5. **Type the path name of the backup file (or browse for it), and then click Next.**

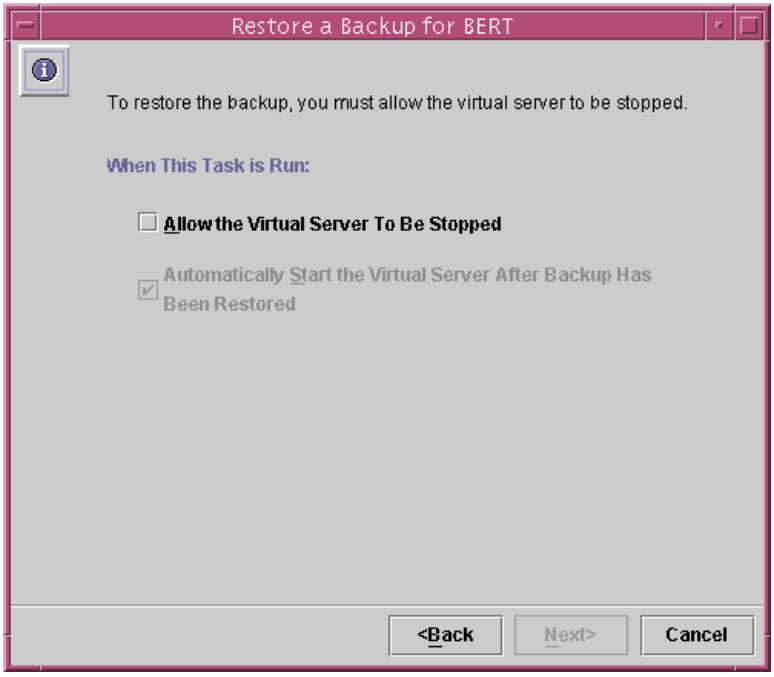
   The resulting screen presents a list of databases in the location you specified that you can restore, along with a description and type for each.

6. **Select the database file or files that you want to restore, and then click Next.**
   A screen similar to the following appears.



7. **Select which database backups to restore, and then click Next.**

   A screen similar to the following appears.

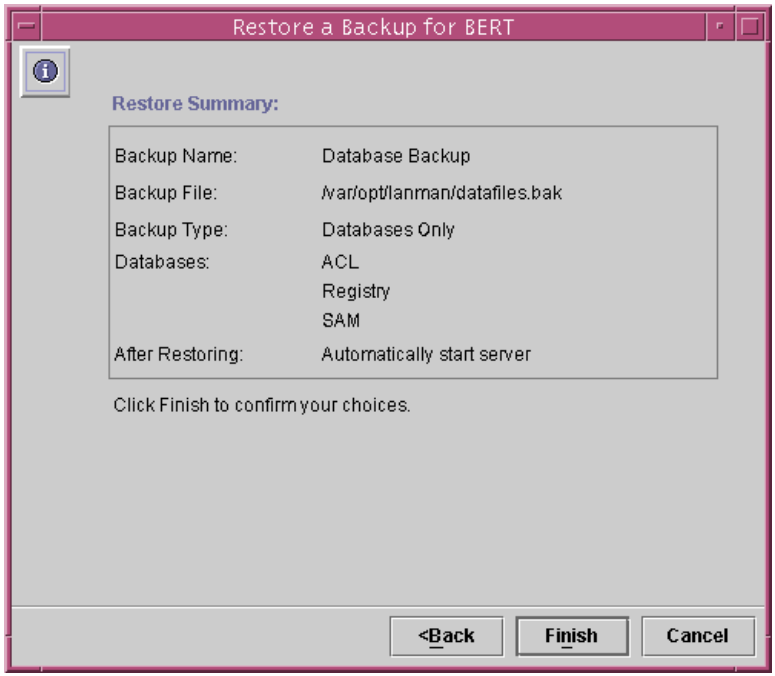


8. **Select Allow the Virtual Server To Be Stopped.**

   You must select this option to proceed. After you have chosen this, you have the option of permitting the system to restart the server automatically after the completion of the task. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the task.

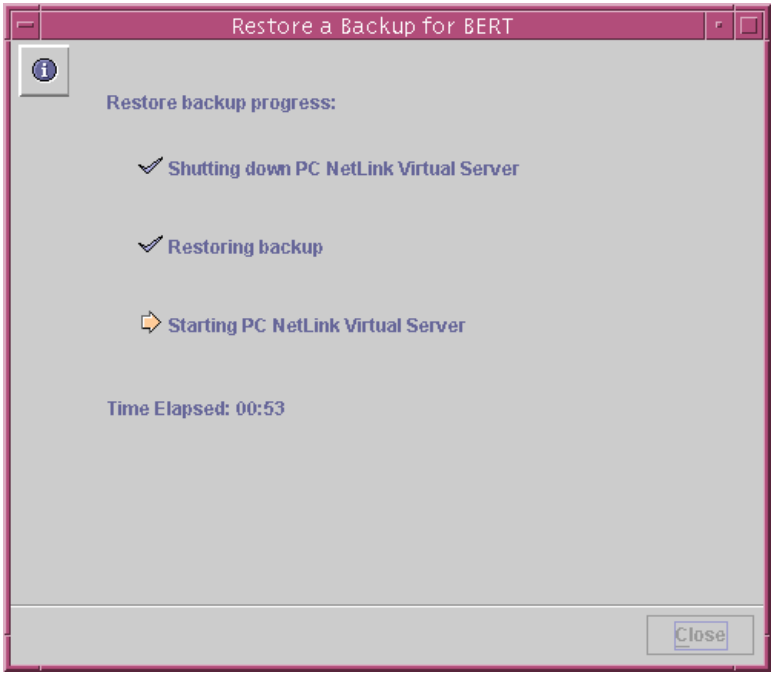
9. **Click Next.**

   A screen similar to the following appears.



10. **Confirm your choices, then click Finish to initiate the database restoration, Back to correct your choices, or Cancel to dismiss the window and leave the task unperformed.**

    The resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



11. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

▼ How to Back Up the Complete Virtual Server Image

A complete virtual server image includes a backup of all PC NetLink databases as well as all the information needed to fully reconstruct the virtual server. You can restore a complete virtual server image to the virtual server from which it was

created *only*. Restoring a complete virtual server image backup results in restoration of the instance state exactly as it was when backed up; any changes made since that time, including any scheduled tasks created after the backup, will be lost.

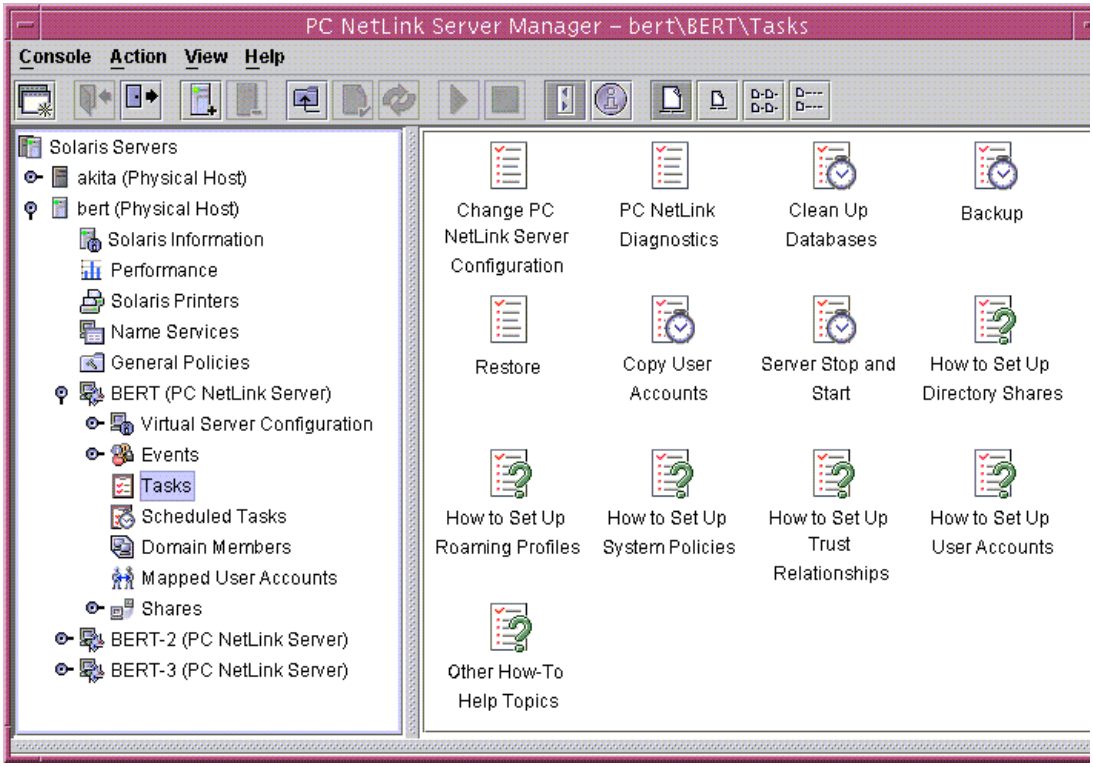
Note – You cannot back up a complete virtual server image for a server that is running PC NetLink Version 1.2 software.

---

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server that you want to back up.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Tasks.**

   A screen similar to the following appears.



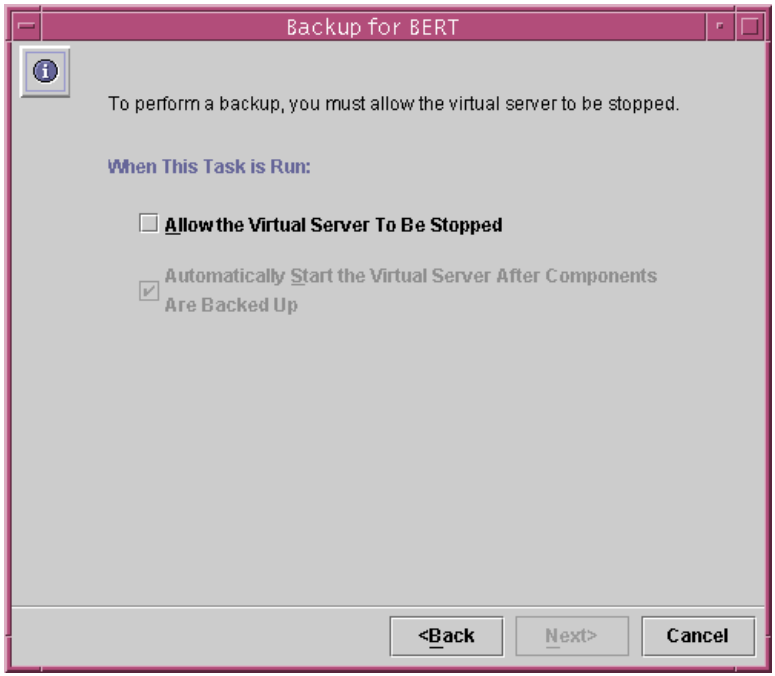
Note that some of the tasks—including Clean Up Databases and Backup—are marked with a clock face. This indicates that these are tasks that you can run automatically on a periodic schedule that you create.

4. **Double-click Backup.**

   A screen appears with two radio buttons for the type of backup to perform: Complete Server Image or Databases Only.

5. **Select Complete Server Image, and then click Next.**

   The following screen appears.



6. **Select Allow the Virtual Server To Be Stopped.**

   You must select this option to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the task. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the task.

7. **Click Next.**

   If you continue the procedure by clicking Next, the resulting screen prompts you for scheduling information.

8. **Select Perform It Now or Schedule It for Later, and then click Next.**

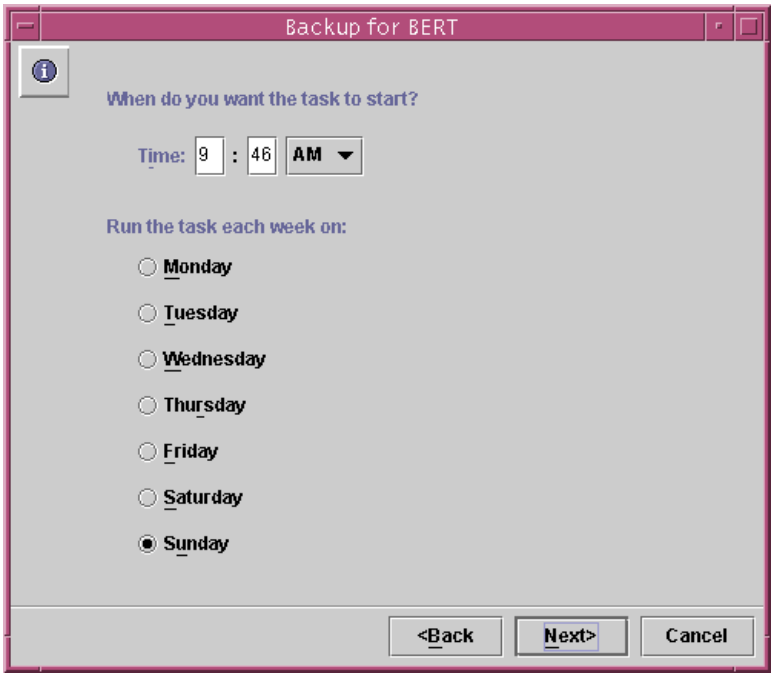
Note – Scheduled tasks are not supported in a high availabilty (HA) environment.

---

9. **Depending on the choice you made, do one of the following:**
   - *Perform It Now* – Skip to Step 11.
   - *Schedule It for Later* – Continue with Step 10.

10. **Select whether to run the task once, daily, weekly, or monthly, and then click Next.**

    A screen similar to the following appears.



    The example shows the choices you must make when scheduling the task to be run weekly. Depending on your selection, you must furnish the following information about when you want the task to be run:

    - *Just Once* – The time of day (noon is regarded as 12 PM and midnight is regarded as 12 AM in this wizard) and the specfic date
    - *Daily* – The time of day
    - *Weekly* – The time of day and the name of the day
    - *Monthly* – The time of day and the date of the month; note that if you select the 29th of the month, the task will be performed in February during "leap" years only, and if you select the 31st day of the month, the task will be performed during 31-day months only.

11. **Click Next.**

    A screen appears that prompts for a path name for the backup files.

12. **In the text field under "Save the backup as" accept the default location, browse for a different location, or type the full path name to a new location, and then click Next.**

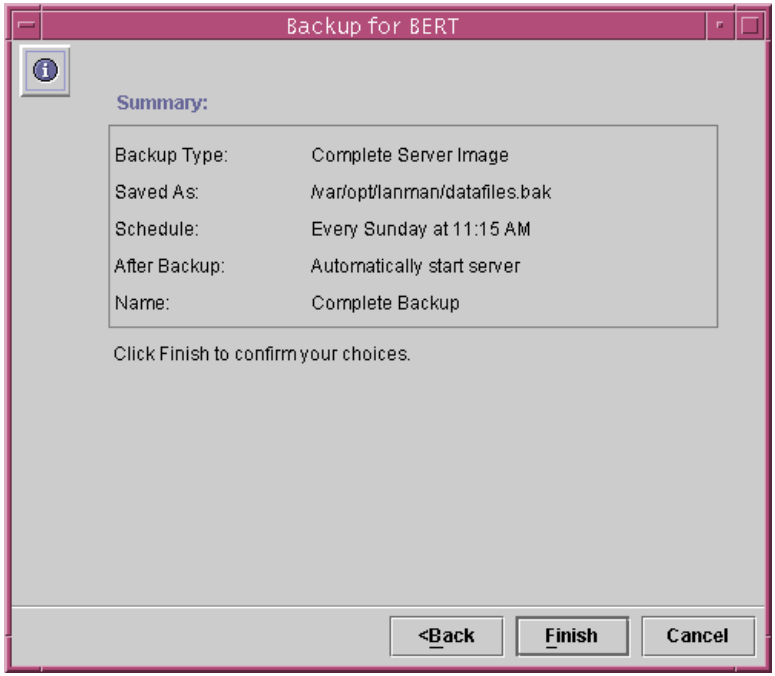
    You must store your backup file as a Solaris file in an existing directory on the PC NetLink system, rather than locally. If you specify a path to a nonexistent directory, a dialog box asks whether you want the wizard to create the directory for you.

13. **In the second text field, type a descriptive name for the task or accept the default.**

    The name *must* be unique; it must not be shared with any other task.

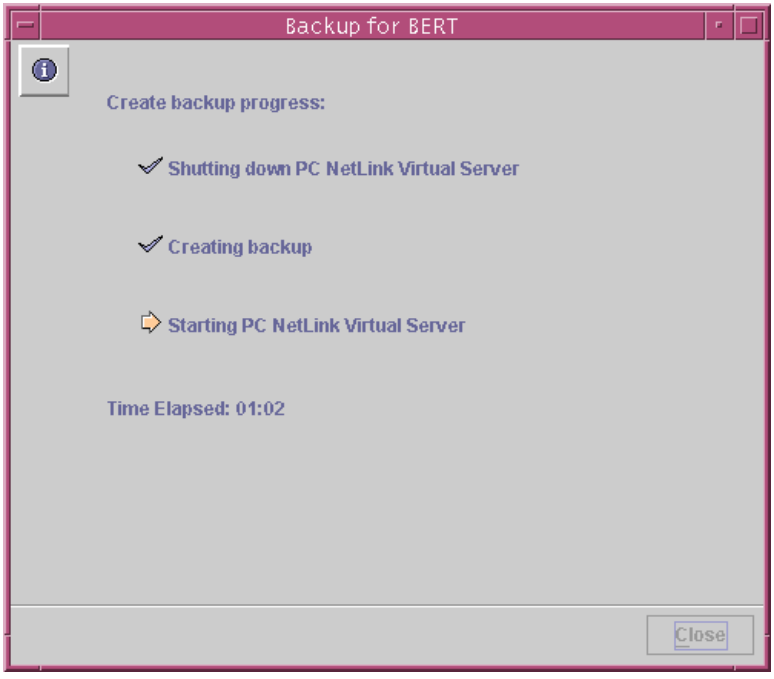
14. **Click Next.**

    A summary screen similar to the following appears.



15. **Confirm your choices, then click Finish to schedule the task (or perform it immediately if you chose Perform It Now), Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    If you elected to begin the task immediately, the resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



16. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will not become effective only after you restart the server.

Note – For instructions to view, modify, or delete a scheduled task, see "How to View, Modify, or Delete Scheduled Tasks" on page 268.

▼ How to Restore a Complete Virtual Server Image

A complete virtual server image includes a backup of all PC NetLink databases as well as all the the information needed to fully reconstruct the virtual server. You can restore a complete virtual server image to the virtual server from which it was created *only*. Restoring a complete virtual server image backup results in restoration of the instance state exactly as it was when backed up; any changes made since that time, including any scheduled tasks created after the backup, will be lost.

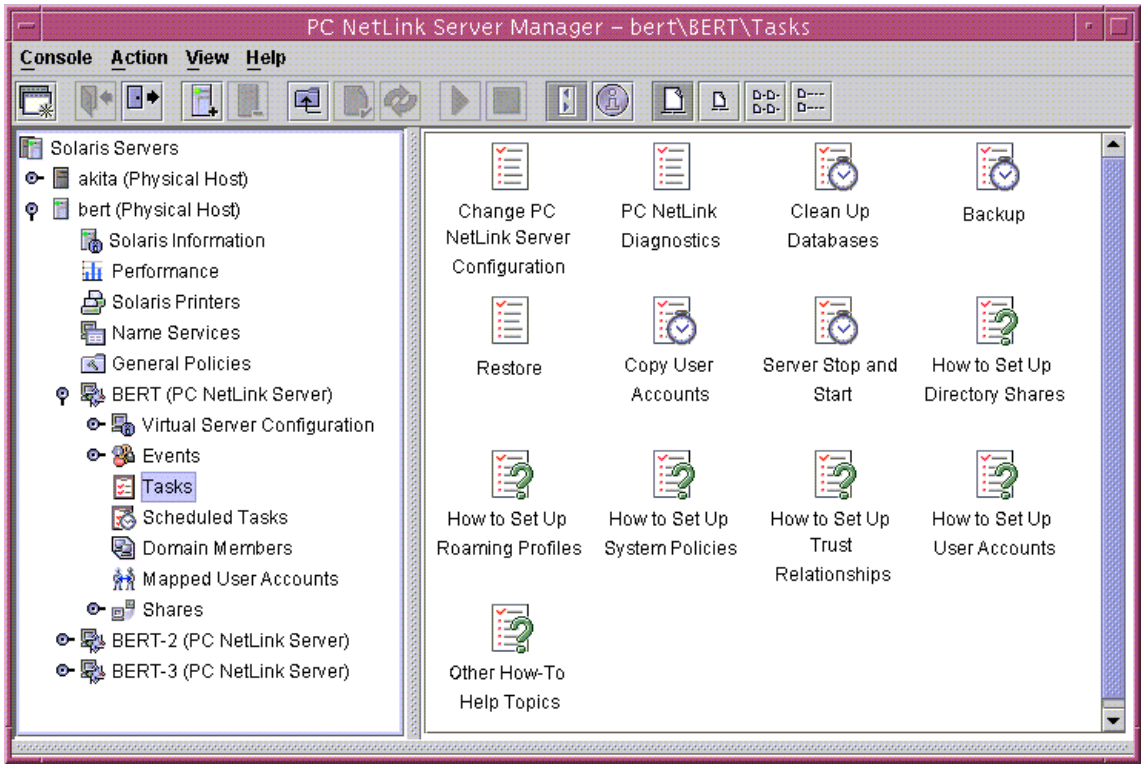
Note – You cannot back up or restore a complete virtual server image for a server that is running PC NetLink Version 1.2 software.

---

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server that you want to restore the complete server image.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Tasks.**

   A screen similar to the following appears.



4. **Double-click Restore.**

5. **In the window that appears, type the backup directory location or file name (or click Browse to locate it), and then click OK.**

6. **Click Next.**

   If you typed a file name in the last step, the file is selected in the file list. If you typed a directory path or browsed to a directory, all the backup files in that directory are listed and the first is selected. If desired, use the Show in List menu to filter the list of files by choosing complete backups.

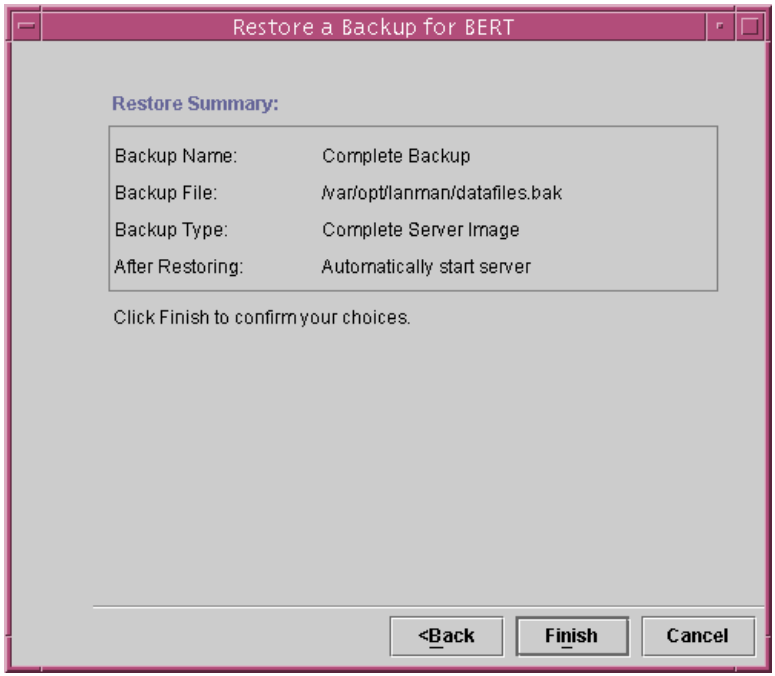
7. **Select the backup file to restore, and then click Next.**

8. **Select Allow the Virtual Server To Be Stopped.**

   You must select this option to proceed. After you have selected this, you have the option of permitting the system to restart the server automatically after the completion of the task. If you choose to uncheck this option, which is selected by default, you must restart the server manually to complete the task.

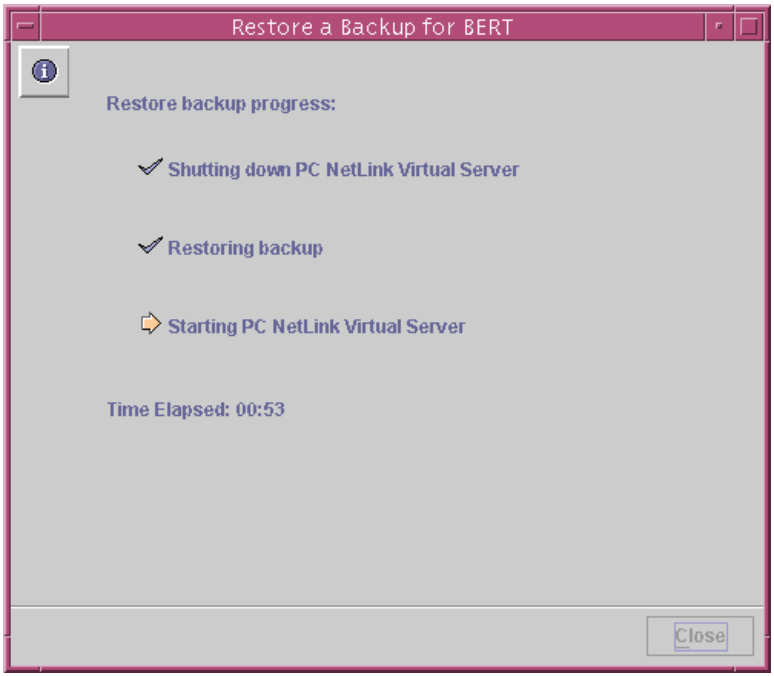
9. **Click Next.**

   A summary screen similar to the following appears.



10. **Confirm your choices, then click Finish to perform the task, Back to correct your choices, or Cancel to dismiss the window and leave the task unscheduled and unperformed.**

    The resulting screen informs you of the progress of the task, marking pending activity with an arrow and completed activity with a check mark.



11. **(Optional) If you did *not* choose to have the PC NetLink server restarted automatically, restart it by following the instructions in "How to Start a PC NetLink Virtual Server Using PC NetLink Server Manager" on page 46 or "How to Start a PC NetLink Virtual Server From the Command Line" on page 49.**

    Any changes you made will become effective only after you restart the server.

▼ How to View, Modify, or Delete Scheduled Tasks

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the virtual server for which you want to work with scheduled tasks.**
2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.
3. **Double-click Scheduled Tasks.**

   Any tasks that you have previously scheduled are listed, along with the frequency of the task, the date and time that the task will run next, and the status of the most recent run.

4. **Depending on whether you want to view, modify, or delete the scheduled task, do one of the following:**
   - *View or modify the scheduled task* – Double-click the name of the scheduled task, then use the resulting dialog box to view settings or make changes, then click Cancel or OK.
   - *Delete the scheduled task* – With the name of the task that you want to delete highlighted, choose Delete Scheduled Task from the Action menu.

CHAPTER 7

Troubleshooting

This chapter describes how to troubleshoot PC NetLink virtual servers and the Solaris physical hosts on which they run. It identifies the various tools that are available to you for use in the troubleshooting process and provides a high-level approach to use whenever troubleshooting is required.

Troubleshooting PC NetLink systems involves gathering data about the problem and analyzing that data to determine the specific cause of the problem. The PC NetLink program includes a number of data-gathering tools. Additionally, more complex data-gathering tools may be available from your support personnel.

This chapter includes instructions for the following tasks:

- "How to Access the Diagnostics Wizard" on page 273
- "How to Display Session Information From a Microsoft Windows NT Computer" on page 281
- "How to Close Sessions From a Microsoft Windows NT Computer" on page 282
- "How to Close Open Resources From a Microsoft Windows Computer" on page 282
- "How to Check the Network" on page 289
- "How to Troubleshoot a Shared Resource" on page 295
- "How to Solve Problems With Unknown File Systems" on page 296

There will be times when a particular problem requires more complex data-gathering than the standard PC NetLink product package provides. In these situations, special debugging versions of the software may be needed to gather more detailed data about the problem. This type of data-gathering may require the assistance of a technical support person to help with instructions on how to use the tools involved.

About PC NetLink Troubleshooting Tools

PC NetLink software provides a variety of tools that you can use as troubleshooting aids. These tools can be arranged into the following four categories:

- Diagnostics wizard
- Tools used for assessing the status of the server
- Tools used for automatic notification of the status of the virtual server and physical host
- Tools used for debugging specific server problems

The following sections summarize the tools found in each category and briefly describe the use of each in a troubleshooting context.

Diagnostics Wizard

The Diagnostics wizard runs a series of scripts to assess the status of the server. The scripts run by the Diagnostics wizard coincide with tests you can perform manually, described elsewhere in this chapter.

TABLE 7-1 Scripts Run by the Diagnostics Wizard

Diagnostics Wizard Test	Command-Line Tool/Script	See Section
Server machine accessible?	`ping`	"`ping`" on page 286
NetBIOS daemon running?	`ps -eaf | grep nbdaemon`	"Isolating the Problem" on page 288
PC NetLink processes running?	`ps -eaf | grep lmx`	"Is the Virtual Server Running?" on page 291

TABLE 7-1 Scripts Run by the Diagnostics Wizard *(Continued)*

Diagnostics Wizard Test	Command-Line Tool/Script	See Section
Verified PC NetLink connectivity?	`net start`	"Are All of the Virtual Server Services Running?" on page 292
Shares exported?	`net share`	"Are All of the Virtual Server Resources Properly Shared?" on page 293
User accounts accessible?	`net user`	"`samcheck`" on page 287

If a particular test fails, the Diagnostics wizard describes possible problems and their solutions. However, if all of the tests performed by the Diagnostics wizard are completed successfully, yet you still are experiencing problems with your server, you must perform more in-depth diagnostic techniques to isolate and solve the problem. See "Troubleshooting Procedures" on page 288 for more information.

▼ How to Access the Diagnostics Wizard

1. **Using PC NetLink Server Manager, log on as root to the Solaris physical host for the PC NetLink virtual server on which you want to perform diagnostic tests.**

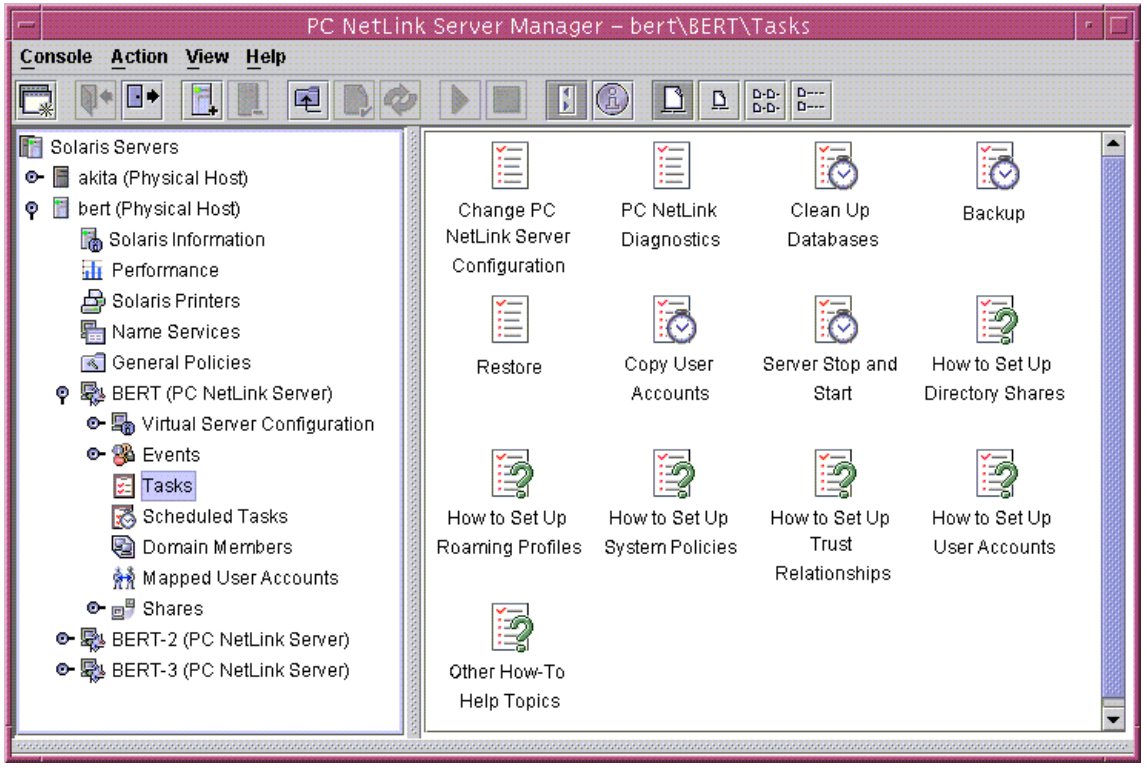
   For instructions, see "How to Log On to a Solaris Server Using PC NetLink Server Manager" on page 42.

2. **In the Results pane, double-click the icon that represents the virtual server.**

   The Results pane changes, displaying a list of seven administrative categories.

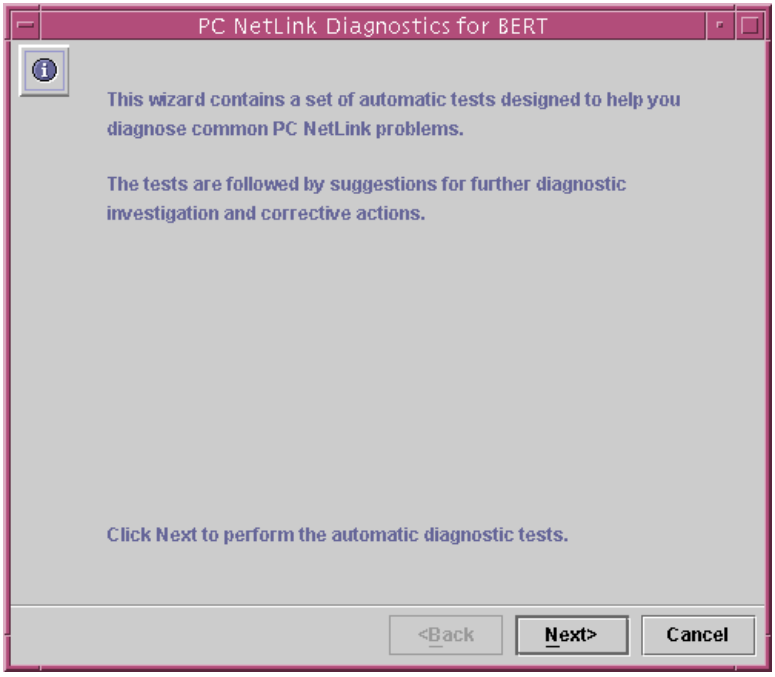
3. **Double-click Tasks.**

   A screen similar to the following appears.



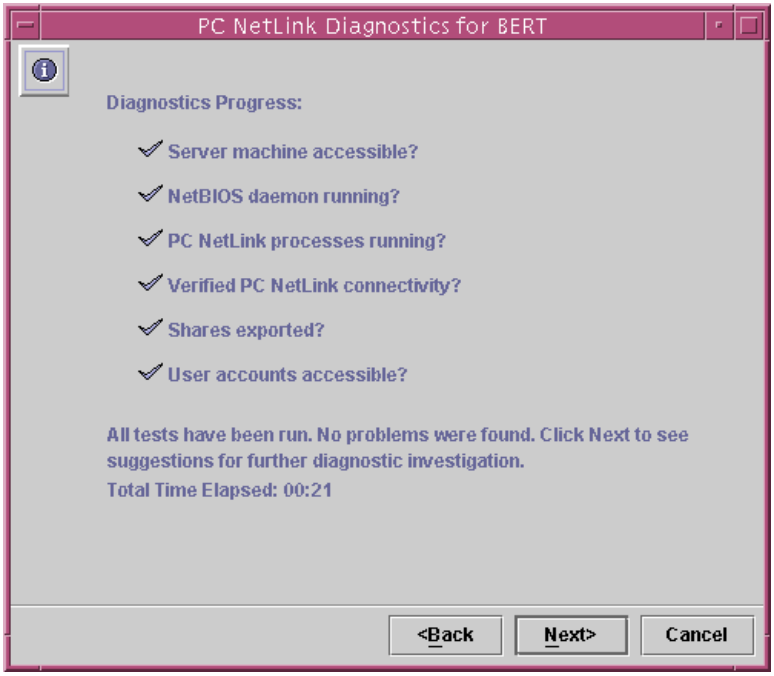
4. **Double-click PC NetLink Diagnostics.**

   The PC NetLink Diagnostics wizard appears.

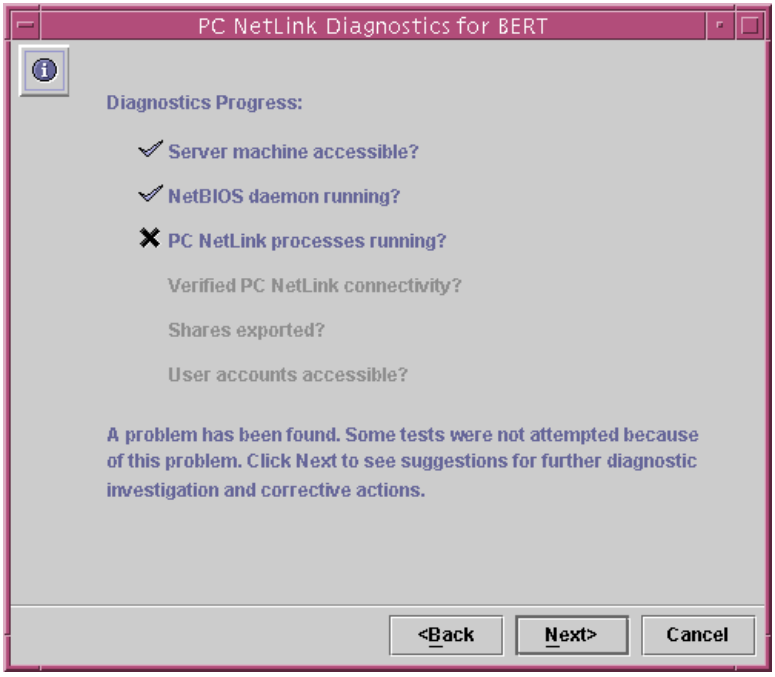


5. **Click Next to start the diagnostics process.**

   The Diagnostics wizard checks off each test as it is being performed. Click Cancel at any time to cancel the Diagnostics wizard before it is finished.

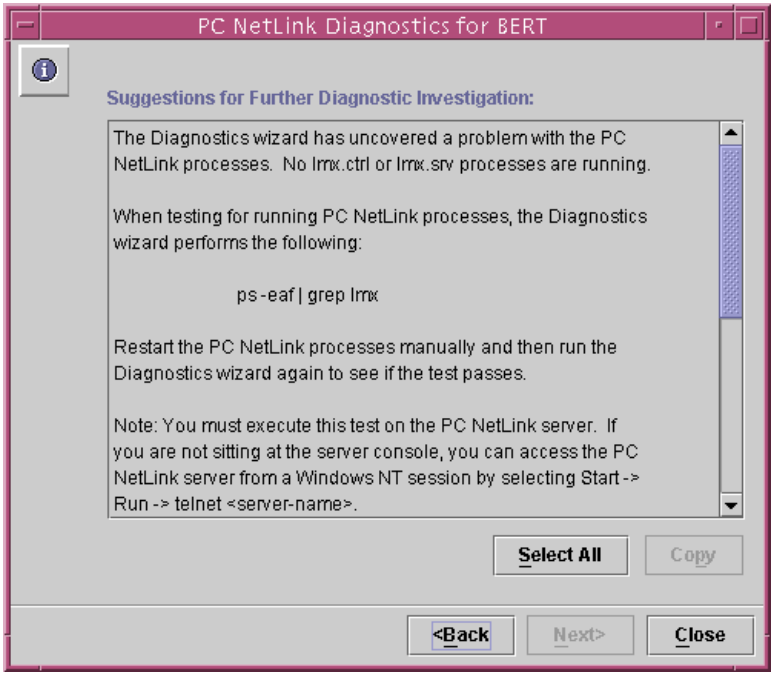


If any of the tests fail, the Diagnostics wizard indicates a failed test.



6. **Click Next.**

   A screen similar to the following appears.



The screen displays tips for further diagnosis and correction of the fault. Follow the steps indicated in the Diagnostics wizard Context Help pane, and run the Diagnostics wizard again to see if the fault was corrected.

Note – You can keep the Diagnostics wizard open while performing other tasks.

Other PC NetLink Diagnostic Tools

In addition to the Diagnostics wizard, there are a number of tools and utilities you can use for further diagnostic tests.

Event Logs

You can track a number of events related to the daily operation of the server by using the PC NetLink Server Manager event logs (in Chapter 3, see "About Event Monitoring" on page 163). These events are maintained in one of three event logs: System log, Security log, and Application log. Administrators should develop and implement an event logging policy and include a review of event logs as a regular part of troubleshooting activities. These events are *NT events*, which you can also see in the NT Event Viewer.

Administrators will find it particularly useful to characterize the typical use of the server by manipulating event log data using a spreadsheet or word processing program. You can use this approach to generate a standard operating profile of the server and to predict trends in server usage.

Note – You can also view event logs by using the `elfread` command. For more information, type `man elfread` at the Solaris command prompt.

Server Status

PC NetLink software maintains detailed statistics about its current usage as well as cumulative usage over a particular period of time. It is always helpful to review these statistics on a regular basis as well as when a server problem is encountered.

Performance Monitoring

The Performance Tuning interface of PC NetLink Server Manager (see "How to Tune PC NetLink for Optimum Performance" on page 112) lets you make some simple adjustments. You can also diagnose problems by drilling down and viewing ongoing performance data presented in PC NetLink Server Manager, and adjust performance thresholds that, when exceeded, generate alarms (see "How to Monitor Physical Host Performance" on page 156).

Server Information

To view data about current server use, open Solaris Information and PC NetLink Information views in PC NetLink Server Manager (see "How to View or Change PC NetLink Virtual Server Configuration Options" on page 171).

Solaris Information

- Server name
- Solaris operating environment version
- Last time the system was rebooted
- Ccurrent date and time on the server
- Name of the *current* user
- Hardware description
- System's processor type
- Amount of random access memory
- Total (not including swap) space on disks
- Swap space
- DNS domain name
- Internet Protocol (IP) address of the system
- Ethernet address of the system
- Name service currently in use
- Name service domain name
- Name of the name service server

PC NetLink Information

- PC NetLink server name
- PC NetLink server IP address
- PC NetLink server's domain name
- PC NetLink server's role
- Name of the domain PDC, if the server is a BDC or member server
- PC NetLink software version number
- Data files location (directory path on the physical host)
- Server instance number
- State of the server (stopped or running)
- Date and time that the server was last started (if running)
- High availability information is shown if the server is configured for high availability

Cumulative Statistics

To view cumulative server usage data, you can use the `net statistics` command at the Solaris command prompt. This command provides cumulative totals for a variety of server activities. Administrators who review the server statistics provided by using this command on a regular basis will find it easier to recognize and address changes in server operation.

The following statistics are maintained for the PC NetLink system, and are available by way of the `net statistics` command.

TABLE 7-2 Cumulative Statistics Descriptions

Statistic	Description
Statistics since	Tells when this set of statistics began (either at the last server startup or the last time the statistics were cleared).
Sessions accepted	Tells how many times users connected to the server.
Sessions timed-out	Tells how many user sessions were closed because of inactivity.
Sessions errored-out	Tells how many user sessions ended because of error.
Kilobytes sent	Tells how many Kbytes of data the server transmitted.
Kilobytes received	Tells how many Kbytes of data the server received.
Mean response time (msec)	Tells the average response time for processing remote server requests. This always will be 0 for Solaris system servers.
System errors	Does not apply to Solaris system servers.
Permission violations	Tells when a user attempts to access resources without the required permissions.
Password violations	Tells the number of incorrect passwords that were tried.
Files accessed	Tells the number of files that were used.
Comm devices accessed	Not supported in the PC NetLink program.
Print jobs spooled	Tells the number of print jobs that were spooled to printer queues on the server.
Times buffers exhausted	Tells the number of shortages of big and request buffers. Always set to 0 for Solaris system servers.

▼ How to Display Session Information From a Microsoft Windows NT Computer

An administrator can display session information and control sessions between clients and the server. You can use this information to gauge the workload on a particular server.

To display session information from a Windows NT Workstation computer or a Windows client computer using the NT tool Server Manager:

1. **Start Server Manager.**

2. **Double-click the PC NetLink system whose session information you want to view.**
3. **Click the Users button.**

   You also can display session information using the `net session` command at the Solaris command prompt.

Note – You may see sessions displayed that do not show user names. The sessions are a result of administrative activity and should not be deleted.

▼ How to Close Sessions From a Microsoft Windows NT Computer

An administrator can disconnect a user from the server at any time. Closing a user session does not prevent the user from reconnecting.

To disconnect a user session from a Windows NT Workstation or from a Windows client computer using the NT tool Server Manager:

1. **Start Server Manager.**
2. **Double-click the PC NetLink system whose session information you want to view.**
3. **Click the Users button.**
4. **Highlight the user and click the Disconnect button.**

   You also can disconnect a user session by using the `net session` command at the Solaris command prompt.

▼ How to Close Open Resources From a Microsoft Windows Computer

When a user uses a shared file, the file is open. Sometimes a file will be left open, perhaps even with a lock on it, because of an application program error or some other problem. Such files will remain open and unavailable to other users. An administrator can close these files.

To close an open resource from a Windows NT Workstation or a Windows client computer using the NT tool Server Manager:

1. **Start Server Manager.**
2. **Double-click the PC NetLink system whose resource you want to close.**

3. **Click the In Use button.**
4. **Highlight the open resource and click the Close Resource button.**

   You also can close an open resource by using the `net file` command at the Solaris command prompt.

Print Subsystem Event Logs

PC NetLink software maintains a separate print log for each printer share and each Solaris system printer it uses. These log files record any message generated because of a printer fault or print job error.

An administrator should check these log files periodically to determine whether any such errors are occurring. The logs can be accessed from a client computer by linking to the `PRINTLOG` shared resource.

The logs also can be accessed from the server. They are in the following directory: `/opt/lanman/shares/printlog`

Tools Providing Automatic Status on the Server

Quick response time is critical when dealing with server problems. Being aware of a problem at the time it occurs can decrease greatly the effect that the problem may have on the server user community.

You can configure PC NetLink software to notify specified users when a problem occurs. You can also configure the Solaris system to generate and notify you when problems occur. The following sections discuss these features.

Alerter Service

PC NetLink software includes an Alerter service that you can use to notify specified users of the occurrence of a particular event. An administrator should use this service in order to make server problems known immediately. Prompt action to resolve server problems often can minimize their effect. The following examples illustrate situations that could generate alerts:

- The number of server errors exceeds a threshold set in the PC NetLink Registry.

- The number of bad access attempts exceeds a threshold set in the PC NetLink Registry.
- The number of bad password attempts exceeds a threshold set in the PC NetLink Registry.
- Errors were encountered during start of the Net Logon service.
- A printer is malfunctioning.
- A print request has been deleted or completed.

Solaris System and PC NetLink Features

One of the benefits of PC NetLink software is the availability of the inherent scripting features provided by the Solaris operating system. Combining these features with the data-gathering tools provided by PC NetLink software, an administrator can create a powerful tool that can be used to assess the health of a PC NetLink system at any given time.

For example, using the Solaris system job scheduling feature (`CRON`), various data-gathering tools provided by PC NetLink, and some of the standard Solaris system commands for checking file system integrity and free space, administrators can write scripts that perform various system and server checks and then send the results to Solaris system administrators at regular intervals.

Command-Line Diagnostics and Repair Tools

In addition to the Diagnostics wizard, there are a number of command-line diagnostics and repair tools available in the `/opt/lanman/sbin` directory. These are described below.

`acladm`

The `acladm` command is used to check and repair problems found in the Access Control List (ACL).

Be sure to examine the options that are available with this command before executing it. Type the `man acladm` command at the Solaris command prompt.

blobadm

The `blobadm` command is useful for testing and fixing the binary structure of blob files, such as the Security Accounts Manager (SAM) database, ACL, and Registry. Before invoking `blobadm`, try less invasive fixes such as `acladm`, `regcheck`, and `samcheck`. Be sure to examine the options that are available with this command before executing it. For more information on `blobadm`, type `man blobadm` at the Solaris command prompt.

Caution – Serious damage to your files could result if `blobadm` is used incorrectly. Be sure to read the man page carefully before using `blobadm`.

lmshell

The `lmshell` command is useful for emulating an MS-DOS client session when you do not have access to an actual MS-DOS client. This command is especially useful when troubleshooting a connectivity problem between a client and server. Using the `lmshell` command, you can mimic a client logon and resource linking by executing the `net logon` and `net use` commands in `lmshell` at the Solaris command prompt.

lmstat

The `lmstat` command interrogates the server's shared memory image to gather a variety of data about the current state of the server. This command is especially useful when you want to determine which server process a client session is on.

PC NetLink software is composed of a set of cooperative processes. When the server is running, enter the following command:

```
ps -ef | grep lmx
```

Executing this command generates a display similar to the following:

```
root 18741      1   0 09:57:04 ?          0:00 lmx.browser -I 1
root 18670      1   0 09:57:04 ?         0:00 lmx.srv -I 1 -s 1
root 18680      1   0 09:57:04 ?         0:00 lmx.srv -I 2 -s 2
root 18737      1   0 09:57:04 ?          0:00 lmx.alerter -I 1
root 18581      1   0 09:56:26 ?          0:01 lmx.ctrl -I 1
root 18733      1   0 09:57:04 ?          0:00 lmx.dmn -I 1
```

In this example, there are two `lmx.srv` server processes (18670 and 18680). The server may have nine clients with current sessions.

The administrator can find out to which `lmx.srv` process a client is connected by executing the `lmstat -c` command at the server prompt. The system displays output similar to the following:

```
Clients:
BANANA.SERVE~X (nwnum=0, vcnum=0) on 17713
ORANGE (nwnum=0, vcnum=0) on 17713
PEAR (nwnum=0, vcnum=0) on 17722
```

Notice that each client name has an associated process ID number. This is the process ID of the `lmx.srv` process that currently is serving that client. The `vcnum` value specifies whether this is the client computer's first virtual connection (VC) or an additional one.

Being able to determine the process ID of the `lmx.srv` process that is serving a client is particularly useful when using `lmstat -w` or the Solaris system `truss( )` command. Both commands require a process ID as part of their startup arguments.

ping

The `ping` command is useful for determining if the server is accessible. To run `ping`, type the following at the Solaris command prompt:

`ping` *server–name*

If you are unable to ping the server successfully, something is wrong with the server connection to the network, such as the following:

- The server is down.
- There is a broken network connection.
- There is a hardware or driver configuration problem on the server.

If you are unable to ping any host successfully, there is something wrong with your own connection to the network.

regconfig

The `regconfig` command is used to query or change PC NetLink Registry key information. You can use this command to change any value in the Registry. (You also can use the Windows NT Registry Editor to change key values.)

You can also use the `regconfig` command to reinitialize the PC NetLink Registry with system defaults.

For more information about the Registry, see Appendix A, "PC NetLink Registry" on page 299.

regcheck

The `regcheck` command is used to check and repair the PC NetLink Registry file. This command checks only the internal structure of the PC NetLink Registry file; it does not check the validity of any data that may be stored in it.

If the internal structure of the Registry file is found to be invalid, use the `regcheck` command to make the necessary repairs.

samcheck

The `samcheck` command is used to check, dump, and fix the Security Accounts Manager (SAM) database. You can use this command to determine whether the user accounts database has been corrupted and optionally, to fix it.

You can also use the `samcheck` command to output the contents of the user accounts database to `stdout` in human-readable format.

srvconfig

The `srvconfig` command is used to display the current default settings of all the server parameters in the `lanman.ini` file. (It also is a good way to check the location and spelling of any parameter you want to modify.) In addition, the `srvconfig` command lists other parameters not contained in the file `lanman.ini`.

The `lanman.ini` file contains several configuration parameters that you can modify. Default settings are used for most of these parameters. However, some of them can be changed, overriding the default values set at server installation.

To display the default settings of the `lanman.ini` file, use the following command:

```
srvconfig -p | more
```

This command generates a listing of all of the parameters in the `lanman.ini` file and their default settings.

Troubleshooting Procedures

PC NetLink troubleshooting involves using a systematic approach to isolate the problem and then gathering detailed data in order to identify the specific module causing the problem. The following sections provide simple procedures that you can use to isolate a server problem. It then offers some suggestions on how to gather additional information about the problem.

Isolating the Problem

A PC NetLink virtual server runs on a Solaris physical host. Virtual servers depend upon a fully functional NetBIOS running on the physical host to perform its file- and print-serving functions.

A NetBIOS network typically includes the following components:

- An application that provides a NetBIOS protocol interface
- An application that provides a network transport protocol interface, such as TCP/IP (although some transport implementations include NetBIOS within a common module)
- An application that provides drivers for the network adapter interface (which also may be part of the transport module)

Every NetBIOS network component must be configured and operational in order for PC NetLink software to function in a network environment. Additionally, similar modules must be functioning on the machine that is attempting to use the file and print services of the PC NetLink program, such as a Windows NT Workstation computer or Microsoft Windows client computer.

When a NetBIOS network is not available, the system typically displays the following message when you start the server:

`unable to post` *server-name* `on any network`

Reviewing all of the modules involved in the end-to-end connection between a client and PC NetLink, it is easy to see that isolating a problem is the first step for problem solving in a client-server networking environment.

Before assuming that the problem is with the virtual server, you must ensure that other networking software is functioning properly. This is particularly true with new installations in which the opportunity for a transport or physical network problem is the greatest.

It is fruitless to perform an exhaustive check of every layer of software for a problem that affects only a single client or user. Experience will help you to determine when to use a comprehensive problem isolation procedure or a server-specific problem isolation procedure. The following sections offer guidelines on how to perform both procedures. Use the one that best fits your current problem description.

▼ How to Check the Network

Before assuming that the server is the cause of all network problems, it is worthwhile to perform checks to verify the sanity of the network. This is particularly important when all or a very large portion of server users are reporting a problem at the same time.

Use the following steps to verify that the network is functioning properly.

Step 1: Verify the Status of the Physical Network

The first item to check is the physical network.

- Check hardware LEDs for connection problems. Most networking hardware provides status indicators that you can use to assess the state of the various network links (for example, network routers, hubs, and interface cards use LEDs). Always check these links for any signs of problems with the physical network such as excessive retransmissions, link integrity mismatches, and jabber conditions.
- Check cable connections. Even in cases in which only a single client is affected, never assume that it is not a bad cable connection. For a single client it is easy to check to determine whether the problem occurs regardless of which server the client tries to use.
- Check the client's network configuration. If a client cannot "see" anything on a network that is otherwise functioning without incident, then it is safe to assume that the problem is related to that client's network configuration. However, if that same client can see other nodes on the network but cannot connect to a particular server, then the network path to that server, the server itself, or the account being used by that client are likely candidates for trouble.

There are several third-party products available that you can use to monitor the health of the physical network. It is worthwhile to check network traffic periodically with one of these products to see whether there are problems occurring with the physical network.

Step 2: Verify the Transport Protocol Status

If the physical network appears to be functioning properly, the next step is to determine whether the various computers on the network can "see" each other from the perspective of a transport protocol. Most transport protocol applications include a connectivity test tool that you can use to verify connectivity at the transport level between a client and the server over the network.

If you cannot reach a server machine from a particular client with the `ping` command, then neither will that client be able to connect to the server.

If you cannot ping a server from several client computers, then one of the following conditions may be present:

- The server is not running.
- The transport protocol is not running.
- There is a configuration problem that is disrupting network connectivity.

Review the recommendations in your transport protocol software documentation. If appropriate, continue with the procedures described later in this section on assessing the status of the NetBIOS protocol and PC NetLink software.

Step 3: Verify the NetBIOS Protocol Status

Check the NetBIOS protocol layer. Most NetBIOS modules provide test tools that test the connectivity between NetBIOS names over the network.

Connectivity between nodes using TCP/IP may be available, but if connectivity between NetBIOS names is not working, then PC NetLink software will not work. All PC NetLink communications are based on NetBIOS name sessions. Use the test tools provided with your protocol software to verify NetBIOS level connectivity. If you find a problem, isolate it according to the information provided with the NetBIOS protocol documentation.

Step 4: Verify Solaris System Functionality

If all of the network connectivity modules check out properly, check the Solaris operating environment on the computer hosting the PC NetLink program. The operating system provides a variety of log files that you can consult and system checks that you can perform to verify proper operation. For information on these checks, see your Solaris system administrator documentation.

PC NetLink software is particularly sensitive to the following system problems:

- Insufficient disk space in critical file systems such as `root` (`/`) or `/var`
- Insufficient system memory causing excessive swapping
- CPU bound conditions

- Unbalanced disk loads
- Improperly tuned kernel parameters such as maximum number of open files

Check the performance views available in PC NetLink Server Manager (see "How to Tune PC NetLink for Optimum Performance" on page 112 and "How to Investigate Performance Alarms" on page 162).

Operating system problems usually will affect all or most client computers connected to the server. Do not spend much time on this step if you are troubleshooting an individual client problem.

Step 5: Isolate Problems on the PC NetLink System

If you determine that all of the underlying software is functioning properly, then you should check the Solaris physical host for problems. Problem isolation on the physical host often is dependent on the type of problem reported by the user community.

If only a single user is experiencing a problem, then you can narrow your focus quickly to the operations that this user is attempting to perform.

If a group of users is experiencing problems but many other users are not, then you should look for a common thread among the users with problems. For example:

- Are they on the same hub?
- Are they using the same applications or printers?
- Are they on the same `lmx.srv` process?
- Are they members of the same PC NetLink group?

If all users of a server are experiencing a problem, then you should start with more basic assessments of the state of the server. These are described in the following sections.

Is the Virtual Server Running?

It is worthwhile to verify that the virtual server is actually running. You can do this easily by entering the following command at the Solaris command prompt:

```
ps -ef | grep lmx
```

The system display should include the following (at a minimum):

```
root 18680      1   0 09:57:04 ?          0:00 lmx.srv -I 2 -s 2
root 18581      1   0 09:56:26 ?          0:01 lmx.ctrl -I 1
root 18733      1   0 09:57:04 ?          0:00 lmx.dmn -I 1
```

The system display includes the virtual server instance number for each of the `lmx` processes.

This display indicates that the three required server processes are in fact running, the daemon (`lmx.dmn`), the control process (`lmx.ctrl`), and at least one worker process (`lmx.srv`). You also may see other processes, such as `lmx.browser` and `lmx.alerter`.

Additional multiple worker processes, each with a unique number displayed at the end of the line, may be displayed. The server spawns new worker processes based on the number of clients supported by the server. As more client sessions are started, more `lmx.srv` processes may be started, each with a unique process ID and number. This is normal.

If the server is not running, use the `net start server` command at the Solaris command prompt.

Are All of the Virtual Server Services Running?

If one of the required server processes is not running, determine whether all of the server services started properly. A situation can occur when several server processes are running but you still cannot use the server because a particular service did not start. This is especially true for the Net Logon service. To check which services are running, enter the following command at the Solaris command prompt:

```
net start
```

The system displays a list of the services that currently are active on the server.

It is critical that the Net Logon and Server services are displayed. If they are not shown, then the server has a problem. Often the Net Logon service will not start because of a problem with the server name, domain name, or domain configuration.

Check the error logs for problems as described in the next section.

Are You Unable to Access PC NetLink Server Manager?

If the server seems to be running properly, and all of the PC NetLink tools are running properly, yet you are unable to start PC NetLink Server Manager, there is probably something wrong with your Java installation. Perform the following (as root) to restart the PC NetLink Server Manager:

```
/etc/init.d/slsadmin restart
```

If you are still unable to start the PC NetLink Server Manager, try reinstalling the software, as described in the *Solaris PC NetLink 2.0 Installation Guide*.

Are There Messages in the Error Logs?

You can view the System, Security, and Application logs from a client computer using Event Viewer, from a client computer using PC NetLink Server Manager, or at the Solaris command prompt using the `elfread` command. You also can view the logs in the `PRINTLOG` share area if there is a printing-related problem. For problems related to server startup, you can check the `lmxstart.log` located in the `/var/opt/lanman/`*number*`/logs` directory, where *number* is the instance number.

If there are entries in any of these logs, save them for future reference. Never discard or overwrite error messages since they may indicate the cause of the problem. These logs may have to be supplied to support personnel at a later date.

The following message is particularly indicative of a server problem:

```
A server process has unexpectedly terminated
```

This message indicates that a server process has encountered an unexpected error. Depending on how your server is configured, there may be a core file located on your system.

If the value of the `CoreOk` keyword is set to 1 (yes) in the PC NetLink Registry, then core files are placed in the directory `/var/opt/lanman/`*number*`/debug`, where *number* is the instance number. The `CoreOk` value is in the following key:

```
SYSTEM\CurrentControlSet\Services\
    AdvancedServer\ProcessParameters
```

Save any core files that you may find. If the `CoreOk` parameter is set to 0 (no), then core files will not be created. You may want to set the `CoreOk` keyword to 1 (yes) in order to capture core files, which are useful for debugging purposes.

Are All of the Virtual Server Resources Properly Shared?

Some virtual server resources are shared automatically every time the server is started. These resources are used in the background by clients while performing other server activities.

The list of resources shared by default includes:

- `ADMIN$`
- `ADMINDOC`
- `C$`
- `D$`
- `IPC$`
- `MSCLIENT`
- `NETLOGON`
- `PRINTLOG`

- PRINT$
- TOOLS
- USERS

The resources followed by a dollar sign ($) are special resources required for server administration and communication. (An additional special resource — REPL$ — is available when the Directory Replicator service is running.)

Never attempt to delete or re-share these resources. If any of these resources are absent, the server will not function properly. If you detect that one of these resources is missing, stop and restart the server to determine whether they are shared at server startup. If they are not displayed, contact your service representative.

The remaining resources are default resources typically used by clients during logon (NETLOGON), to connect to home directories (USERS), and to access utilities or error logs (DOSUTIL, OS2UTIL, PRINTLOG). These items may be deliberately absent from your server. However, if you did not unshare them, then a problem with the server caused them to be removed.

Can the Virtual Server Be Contacted From the Console?

You can conduct a simple test to determine whether the virtual server is communicating over the network. Issue the following command at the system console:

```
net view
```

The system displays the name of the virtual server and other servers operating in the same domain. If your server name is displayed, execute the same command, adding the server name:

```
net view \\asutrial
```

The system displays a list of shared resources *similar* to the following:

```
Shared resources at \\asutrial
PC NetLink Systems
Sharename    Type Used as       Comment
-------------------------------------------------------------
DOSUTIL      Disk               DOS Utilities
LIB          Disk               Programming Aids
NETLOGON     Disk               Logon Scripts Directory
OS2UTIL      Disk               OS/2 Utilities
PRINTLOG     Disk               LP Printer Messages
USERS         Disk               User Directory
```

Other entries may be displayed if you added shared resources to your server.

If either of these commands fails consistently, then there is a problem with broadcast communications over the network. If these commands succeed, you can use the tests in the next section.

Is the Virtual Server Attempting to Support Too Many Users?

When a connectivity problem occurs, ensure that your server has not exceeded the maximum number of clients that it is configured to support. This number may be indicated by the `maxclients` parameter in the server `lanman.ini` file. It can be displayed using the `srvconfig -g maxclients` command.

Has the PC NetLink Registry Been Corrupted?

Execute the `regcheck -C` command to determine whether the internal format of the Registry file has been corrupted. If this command detects corruption, execute the `regcheck -R` command to repair the Registry file.

If invalid values have been entered in the PC NetLink Registry, then you can use the `regload` command to reinitialize all Registry values to their defaults.

Can the Virtual Server Be Contacted From a Client?

Attempt to log on to the server from a client computer. If the logon is successful, link a virtual drive ID to a shared resource. Then, view the contents of the linked drive.

If you have problems with these steps, isolate each problem using the following procedure.

▼ How to Troubleshoot a Shared Resource

If you can communicate with the virtual server but cannot access a shared resource, do the following:

1. **Verify that the shared resource exists by using the `net view` *server–name* command.**

   If the shared resource name is not displayed, then it does not exist. In that event, you must re-share the resource.

2. **Link to the shared resource while logged in as Administrator.**

   If this fails and the resource exists, then the resource may be shared incorrectly. Delete and re-share the resource. If this succeeds, then proceed to the next step.

3. **If the resource is a disk resource, check both levels of permissions associated with the shared resource.**

   First check the share permissions using Server Manager. Then check the permissions on the shared directory using Windows Explorer at an administrative client, or use the PC NetLink command `net perms` to find the permission. Verify that the resource can be used using either group membership or on a per-account basis for that particular user. Verify that the access permissions on the resource allow the desired action to be performed (for example, the user has read-only permission but is attempting to edit a file). Also, verify that the maximum user limit for a particular shared resource is not exceeded.

4. **On the shared resource, check the file attributes and the Solaris system access permissions.**

   If necessary, use the Properties menu in Windows Explorer. Use the `udir` command to display Solaris system permissions (user, owner, group).

▼ How to Solve Problems With Unknown File Systems

The PC NetLink program recognizes only the following types of file systems:

- `cdfs`
- `nfs`
- `s5`
- `sfs`
- `ufs`
- `vxfs`

File systems other than those listed above will be treated as an s5 file system. If you want *all* of your unknown file systems to be treated as a type other than s5, set the `fsnosupport` parameter in the [`fsi`] section of the `lanman.ini` file to the name of a recognized file system. Then, stop and restart the server.

If you want to set each unknown file system individually to a specific known file system, follow these steps:

1. **At the Solaris system prompt, type the following command, replacing** *pathname* **with the actual name of the path to the unknown file system:**

   `df -n` *pathname*

   The system displays the mount point and file system type as specified by the Solaris operating system.

2. **Set the `fsmap` parameter in the [`fsi`] section of the `lanman.ini` file as follows:**

`unknown:s5,sfs:vxfs,`*unixfilesystem:filesystem, ...*

Replace *unixfilesystem* with the name of the file system type returned in Step 1. Replace *filesystem* with the name of the PC NetLink file system type you want to use.

3. **Stop and restart the server.**

   The PC NetLink program now will map the Solaris file system to the recognized file system you specified.

APPENDIX **A**

PC NetLink Registry

In the PC NetLink program, most configuration information is centrally stored in a single database called the Registry. Ordinarily, you use PC NetLink Server Manager to change Registry values by way of the graphical user interface. However, you may also use the Windows Registry Editor or the PC NetLink `regconfig` command to change values by editing the Registry database manually. (For an explanation of `regconfig` usage, as root type `/opt/lanman/sbin/regconfig` on a PC NetLink server command line.)

This appendix provides the following information:

- Overview of the PC NetLink Registry structure
- Description of Registry Editor
- Descriptions of the PC NetLink Registry keys and values

PC NetLink Registry Structure

The PC NetLink Registry is a database organized in an hierarchical structure. It is composed of subtrees and their keys, and value entries. A key also can contain additional subkeys.

The following table identifies and defines the PC NetLink Registry subtrees.

TABLE A-1 PC NetLink Registry Subtrees

Root Key Name	Description
HKEY_LOCAL_MACHINE	Contains information about the local computer system, including hardware and operating system data such as bus type, system memory, device drivers, and startup control data.
HKEY_USERS	Contains all actively loaded user profiles and the default profile. Users who are accessing a server remotely do not have profiles under this key on the server; their profiles are loaded into the Registry on their own computers.

The PC NetLink Registry is stored in the `/var/opt/lanman/datafiles` directory on the PC NetLink server.

Each Registry key can contain data items called value entries. Keys are analogous to folders, and value entries are analogous to files within the folders.

A value entry has three parts, which always appear in the following order: the name of the value, the data type of the value, and the value itself, which can be data of any length.

Data types, such as `REG_SZ` or `REG_EXPAND_SZ`, describe the format of the data, which can be up to 1 Mbyte. Data types from 0 to 0x7fffffff are reserved for definition by the system, and applications should not use these types. Data types from 0x80000000 to 0xffffffff are reserved for use by applications.

The following table lists and defines the data types currently used by the system.

TABLE A-2 Registry Data Types

Data Type	Description
REG_BINARY	Binary data. For example: `Component Information : REG_BINARY : 00 00 00...`
REG_DWORD	Data represented by a number that is 4 bytes long. Many keys for device drivers and services are this type and can be displayed in Registry Editor in binary, hexadecimal, or decimal format. For example, entries for service error controls are this type: `ErrorControl : REG_DWORD : 0x1`

TABLE A-2 Registry Data Types *(Continued)*

Data Type	Description
REG_EXPAND_SZ	An expandable data string, which is text that contains a variable to be replaced when called by an application. For example, for the following value, the string %*SystemRoot*% will be replaced by the actual location of the directory containing the PC NetLink system files: `File : REG_EXPAND_SZ : %`*SystemRoot*`%\file.exe`
REG_MULTI_SZ	A multiple string. Values that contain lists or multiple values in human readable text are usually this type. Entries are separated by NULL characters. `AlertNames : REG_MULTI_SZ : Administrator tom`
REG_SZ	A sequence of characters representing human readable text. For example, a component's description is usually this type: `DisplayName : REG_SZ : Alerter`

Using Registry Editor

You can use the Registry Editor to view Registry entries for the various components in PC NetLink. You can also use Registry Editor to modify or add Registry entries.

The Registry Editor application, Regedt32.exe, does not appear in any default folders. It is installed automatically in the %*SystemRoot*%`\system32` folder on Windows NT systems. Click Run on the Start menu or switch to a command prompt and type `regedt32`.

Connecting to a Remote Registry

To edit the PC NetLink Registry using the Windows NT Registry Editor, you must connect to the PC NetLink system from the Registry Editor of a remote Windows NT computer. To do so, use the Select Computer command in the Registry menu of the Registry Editor.

Connecting to the PC NetLink Registry remotely will result in the display of the `HKEY_USERS` and `HKEY_LOCAL_MACHINE` subtrees.

For more information about connecting to a remote Registry, see your Registry Editor Help.

Caution – Using the Windows 98 Registry Editor to edit the PC NetLink Registry remotely is *not* recommended.

Viewing the Registry

Registry Editor displays the subtrees of the Registry. The hierarchical structure that appears in Registry Editor is similar to the hierarchical directory structures of Windows NT Explorer.

Your ability to make changes to the Registry using Registry Editor depends on your access permissions. Generally, you can make the same kinds of changes using Registry Editor as your permissions allow for other administrative tools.

Registry Editor Commands

You can use the mouse or commands to manipulate the windows and panes in the Registry Editor in the same way as in the Windows NT Explorer. For example:

- Double-click a key name to expand or collapse an entry. Or click commands from the View and Tree menus to control the display of a selected key and its data.
- Use the mouse or arrow keys to move the vertical split bar in each window to control the size of the left and right panes.
- Click Tile or Cascade from the Window menu to arrange the Registry Editor windows.

The following table shows some keyboard methods for managing the display of data in each Registry Editor window.

TABLE A-3 Keyboard Commands for Managing Registry Editor Data Display

Procedure	Keyboard Action
Expand one level of a selected Registry key.	Press Enter.
Expand all of the levels of the predefined handle in the active Registry window.	Press CTRL + *
Expand a branch of a selected Registry key.	Press the numeric keypad asterisk (*) key.
Collapse a branch of a selected Registry key.	Press Enter or - on the numeric keypad.

The following table lists the policies and their associated PC NetLink Registry keys, including locations, that can be modified using the Windows NT Registry Editor or,

in some cases, PC NetLink Server Manager.

TABLE A-4 Registry Policies, Keys, and Locations

Policy	PC NetLink Registry Key
PC NetLink Alert Service	(SYSTEM\CurrentControlSet\Services\AdvancedServer\Alert Parameters) AlertAdminOnLicenseOverflow AlertUserOnLicenseOverflow
PC NetLink File Service	(SYSTEM\CurrentControlSet\Services\AdvancedServer \FileServiceParameters) AclCacheSize DosAttributeStorage EADirName EnableSoftCompat EnableSoftFileExtensions ForceDirectoryAcl ForceFileAcl ForceFileFlush IgnoreUnixPermissions MappingSeparator MaxEASize MaxFileSizeInKB MemoryMapFiles MixedCaseSupport NameSpaceMapping OpLockTimeout ReadAheadCount ReportNTFS RootOwnsFilesCreatedOnNFS SyncAclFileOnWrite TruncatedExtensions UniqueSuffixLength UnixCloseCount UnixDirectoryCheck UnixDirectoryPerms UnixFilePerms UnixQuotas UseEAs UseNfsLocks UseOplocks UseUnixLocks

TABLE A-4 Registry Policies, Keys, and Locations *(Continued)*

Policy	PC NetLink Registry Key
PC NetLink Net Administration	(SYSTEM\CurrentControlSet\Services\AdvancedServer \NetAdminParameters) NetAdminGroupName NetAdminPath NetAdminUserName
PC NetLink Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer \Parameters) BigEndianLuidCompatibilityMode CheckPrintQueueInMinutes DeletedPrintJobTimeOnQ MaxDirectoryBufferSize MaxIpcTryCount MaxMailslotReadTime MaxMessageSize MaxPrintQueueNameLength MaxRawSize MaxServiceWaitTime NativeLM NativeOS SendByeMNessage SizeGcBufferPoolInKB
PC NetLink Process Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer \ProcessParameters) CoreOK KeepSpareServer LockNapInMSec MaxLockTimeInSeconds MaxVCPerProc MaxVCs MinSmbWorkerTasks MinVCPerProc NumCIStructs NumCLIENT_SESSION NumUStructs SpareServerTime StopOnCore VCDistribution

TABLE A-4 Registry Policies, Keys, and Locations *(Continued)*

Policy	PC NetLink Registry Key
PC NetLink RPC Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer\RPCParameters) BrowserMaxCalls EventLogMaxCalls LsarpcMaxCalls NetlogonMaxCalls SamrMaxCalls SpoolssMaxCalls SrvsvcMaxCalls SvcctlMaxCalls WinregMaxCalls WkssvcMaxCalls
PC NetLink Share Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer\ShareParameters) KeepAdministrativeShares MakeUnixDirectoriesOnShare ShareReadCount
PC NetLink User Service Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer\UserServiceParameters) CreateUnixUser Exclude ForceUniqueUnixUserAccount MaxUnixUID MinUnixUID NewUserShell ShareUnixHomeDirectories SyncUnixHomeDirectory UnixHomeDirectoryRemark UserComment UserRemark
PC NetLink Directory Synchroniza-tion Parameters	(SYSTEM\CurrentControlSet\Services\AdvancedServer\DirectorySyncParameters) NetLinkPwdSyncDaemon SyncPasswordsToSolaris
Alerter Service	(SYSTEM\CurrentControlSet\Services\Alerter\Parameters) AlertNames CountNotOnNetworkCache IncludeMessageHeader NotOnNetworkCacheTimeout

TABLE A-4 Registry Policies, Keys, and Locations *(Continued)*

Policy	PC NetLink Registry Key
Computer Browser Service	(SYSTEM\CurrentControlSet\Services\Browser\Parameters) BackupRecovery BackupUpdate IsDomainMaster MaintainServerList MasterUpdate MoreLog WinsServer
EventLog Service	(SYSTEM\CurrentControlSet\Services\EventLog*log-file)* File MaxSize Retention Sources EventMessageFile CategoryMessageFile CategoryCount TypesSupported
Net Logon Service	(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters) DisablePasswordChange LogonQuery MaximumPasswordAge Pulse QueryDelay Randomize RefusePasswordChange RelogonDelay Scripts Update
Netrun Service	(SYSTEM\CurrentControlSet\Services\Netrun\Parameters) MaxRuns RunPath

TABLE A-4 Registry Policies, Keys, and Locations *(Continued)*

Policy	PC NetLink Registry Key
Replicator Service	(SYSTEM\CurrentControlSet\Services\Replicator \Parameters) ExportList ExportPath GuardTime ImportList ImportPath Interval MaxFilesDirectory Pulse Random Replicate TryUser UnixDirectoryGroup UnixDirectoryOwner UnixFileGroup UnixFileOwner
UPS Service	(SYSTEM\CurrentControlSet\Services\UPS\Parameters) IgnoreSIGPWR PowerFailAddress PowerFailMessage PowerMessageInterval
Local Security	(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Lsa) LmCompatibilityLevel Notification Packages RestrictAnonymous
LAN Manager Service	(SYSTEM\CurrentControlSet\Services\LanmanServer \Parameters) AccessAlert AutoDisconnect EnableSecuritySignature ErrorAlert Hidden LmAnnounce LogonAlert NullSessionShares RequireSecuritySignature SrvAnnounce SrvComment UserPath

Registry Keys and Values

This section describes the PC NetLink Registry keys that are changed during administration. You do not need to be concerned with every key in the PC NetLink Registry; *only those keys that you may have reason to change are described*. Note that you must stop and then restart the PC NetLink program for most changes to the Registry to take effect.

The PC NetLink Registry keys described in this section are defined in subkeys located in the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

- `\AdvancedServer`
- `\Alerter`
- `\Browser`
- `\EventLog`
- `\LanmanServer`
- `\Netlogon`
- `\Netrun`
- `\Replicator`
- `\UPS`
- `\WINS`

PC NetLink Key Descriptions

The PC NetLink subkey of the PC NetLink Registry contains the following subkeys in the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer
```

- `\AlertParameters`
- `\DirectorySyncParameters`
- `\FileServiceParameters`
- `\NetAdminParameters`
- `\Parameters`
- `\ProcessParameters`
- `\RpcParameters`
- `\ShareParameters`
- `\UserServiceParameters`

The following sections describe the entries contained within those subkeys.

Alert Parameters Entries

The Registry path that contains entries for the PC NetLink Alerter service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\AlertParameters
```

- `AlertAdminOnLicenseOverflow` `REG_DWORD` 0 or 1

  Specifies whether the server sends an administrative alert message when the maximum allowable number of clients is exceeded.

  Default: 0 (message will not be sent)

- `AlertUserOnLicenseOverflow` `REG_DWORD` 0 or 1

  Specifies whether the server sends a message to a client that tried to link but failed when the maximum allowable number of clients is exceeded.

  Default: 0 (message will not be sent)

File Service Parameters Entries

The Registry path that contains entries for the PC NetLink File service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\FileServiceParameters
```

- `AclCacheSize` `REG_DWORD` 0 - 100

  Specifies the maximum number of entries in the ACL cache used to keep track of the results of recent access checks performed on PC NetLink resources. There is a separate cache for each client.

  Default: 6

- `DosAttributeStorage` `REG_DWORD` 0 - 3

  This entry supports alternate mechanisms for storing DOS attributes of a file or directory. By default, DOS file attributes (hidden, system, archive, and read-only) are stored in the UNIX GID (group ID) field of a file or directory. Whenever a DOS attribute is set, a corresponding "DOS" group is assigned to the file. The "DOS" groups, which are created when PC NetLink is installed, include groups such as "DOS-a--", which is assigned to a file when the archive bit is set. However, this default mechanism prevents the normal use of the GID field by UNIX applications.

  If the value of this entry is set to 0, DOS attributes are not stored, leaving the GID field for use by UNIX applications. The attribute set returned for files includes "archive."

If the value of this entry is set to 1, DOS attributes are stored using DOS group ID properties.

If the value of this entry is set to 2, DOS attributes are stored using a mechanism used by SAMBA---storing the attributes in UNIX "mode" bits. The "archive" attribute is stored in the "user execute" bit, the "system" attribute is stored in the "group execute" bit, and the "hidden" attribute is stored in the "other execute" bit.

If the value of this entry is set to 3, DOS attributes are stored in a POSIX ACL assigned to the user `lanman`.

Default: 1

- `EADirName` `REG_SZ` *Character string*

  Specifies the directory to use for files containing extended attribute data. The directory name must begin with a dot (.), must end with a colon (:) , and can contain a maximum of five additional alphanumeric characters.

  Default: `.LMX:`

  The extended attributes for a file are stored in the `.LMX:` directory at the same level in the directory hierarchy where the file exists. For example, extended attributes for the file `foo` are stored in `.LMX:foo`. The extended attributes for a directory are stored in the directory itself. For example, extended attributes for the directory `foo` are stored in `/foo/.LMX:/.:`

- `EnableSoftCompat` `REG_DWORD` 0, 1, or 2

  Specifies how PC NetLink handles file opening in read-only compatibility mode. Use 0 to keep the compatibility mode; 1 to translate to Read-Only/DenyWrite mode for files with special extensions (for example, .EXE, .COM, and .BAT) specified by the value of the `EnableSoftFileExtensions` key; and 2 to translate to Read-Only/DenyWrite mode for all file opens.

  Default: 1 (translate files with special extensions to Read-Only/DenyWrite)

- `EnableSoftFileExtensions` `REG_MULTI_SZ` *List*

  Specifies the file extensions for which the compatibility mode will be translated to Read-Only/DenyWrite if the value of the `EnableSoftCompat` key is set to 1.

  Default: `bat com exe dll cmd`

- `ForceDirectoryAcl` `REG_DWORD` 0 or 1

  Determines whether the PC NetLink program will create an Access Control List (ACL) for a newly created directory if an explicit ACL was not provided by the client computer. If an ACL is not created, one will be inherited automatically from its parent directory whenever it is needed.

  Default: 1 (create new Access Control List)

- `ForceFileAcl` `REG_DWORD` 0 - 3

  Determines whether PC NetLink will create an Access Control List (ACL) for a newly created file if an explicit ACL was not provided by the client computer. If an ACL is not created, one will be inherited automatically from its parent directory whenever it is needed. Registry values force the following behavior:

  - 0 (the default): Do not create a new ACL
  - 1: Create an ACL for each newly created file
  - 2: Do not create an ACL for regular files unless the owner of the parent is different from the owner of the file
  - 3: Do not create an ACL for regular files, but if the owner is being changed, change the UNIX owner

- `ForceFileFlush` `REG_DWORD` 0 or 1

  Specifies whether to force a Solaris `fsync(2)` system call when a server message block (SMB) flush request is received. Not forcing `fsync(2)` system calls can improve file server performance; files will be flushed automatically to disk by the Solaris `fsflush` daemon periodically, regardless of the setting of this key.

  Default: 0 (will not force `fsync` system call)

- `IgnoreUnixPermissions` `REG_DWORD` 0 or 1

  Gives users the option to bypass Solaris system permissions when working with files and directories. For example, enabling this option would allow PC NetLink users to write to or delete files for which they have sufficient PC NetLink permissions even though only Solaris system Read permissions had been granted to those files.

  Default: 0 (enforce Solaris system permissions)

  You can change the value of this key by using the Solaris File System Integration policy wizard in PC NetLink Server Manager.

- `MappingSeparator` `REG_SZ` *Character string* up to 7 characters

  Specifies the string that will be appended to the file name before its unique suffix to indicate that the name is mapped. This value matters only in Solaris system to Windows NT file name mapping. The default is a tilde (~), the same as in Solaris system to 8.3 mapping, but it is possible to set it to enable the client to easily identify files containing characters illegal in Windows NT. By default, a file named `my?` will be mapped to `my_~xyz`. When the value of this key is set to `~slm~`, the name will be mapped to `my_~slm~xyz`. If an invalid parameter is placed in the Registry, the `MappingSeparator` will be replaced by the default value.

  Default: ~

You can change the value of this key by using the File Name Mapping policy wizard in PC NetLink Server Manager.

- `MaxEASize` `REG_DWORD` 1 - infinity

  Specifies the buffer size in bytes that is allocated for extended attributes.

  Default: 4096

- `MaxFileSizeInKB` `REG_DWORD` 100 - infinity

  Specifies the maximum file size, in Kbytes, that the PC NetLink program will allow a user to create on the server.

  Default: 2097152

- `MemoryMapFiles` `REG_DWORD` 0 or 1

  Specifies whether the server uses the Solaris system `mmap` system call to memory map file data into the server's address space for efficiency. File mapping is attempted only for read-only files.

  Default: 1 (memory map read-only files)

- `MixedCaseSupport` `REG_DWORD` 0 or 1

  Specifies whether mixed-case support is enabled on the server. Mixed-case support allows clients to access file names containing uppercase characters on the Solaris system. Enabling mixed-case support may negatively affect the server's performance.

  Default: 1 (enables mixed case)

  You can change the value of this key using PC NetLink Server Manager.

- `NameSpaceMapping` `REG_DWORD` 0, 1, 2, or 3

  Specifies the type of file name space mapping enabled on the server.

  A value of 0 indicates that there is no name space mapping enabled.

  A value of 1 specifies that only Solaris system to 8.3 mapping is enabled. This allows applications that require 8.3-style names to access files with long file names and file names containing characters that are invalid in DOS (+ , ; = [ ] ? " \ < > * | : . [space]).

  A value of 2 specifies that only Solaris system to Windows NT mapping is enabled. This allows Windows NT-style clients, such as Windows 98, Windows 2000, and Windows NT to access files with file names containing characters that are illegal in Windows NT (? " \ < > * | :).

  A value of 3 specifies that both Solaris system to 8.3 and Solaris system to Windows NT mappings are enabled.

Default: 3

You can change the value of this key using PC NetLink Server Manager.

- `OplockTimeout` `REG_DWORD` 1 - infinity

  Specifies the time in seconds that the server waits for acknowledgment from a client of an "oplock broken" notification.

  Default: 30 seconds

- `ReadAheadCount` `REG_DWORD` 0 (always read ahead) - infinity

  Specifies the number of sequential file accesses by a client that the server must detect before it begins reading ahead.

  Default: 2

- `ReportNTFS` `REG_DWORD` 0 or 1

  Specifies whether to report share Solaris system volumes as NTFS or actual Solaris file system type.

  Default: 1 (report as NTFS)

- `RootOwnsFilesCreatedOnNFS` `REG_DWORD` 0 or 1

  Specifies whether the Solaris superuser, root, owns all files created within the Solaris file system.

  Default: 0 (root does not own)

- `SyncAclFileOnWrite` `REG_DWORD` 0 or 1

  Determines whether the server will force changes to the ACL file to be written to disk using an `fsync(2)` system call or whether the server will permit the operating system to write the changes to disk normally.

  Default: 0 (write ACL changes to disk normally)

- `TruncatedExtensions` `REG_DWORD` 0 or 1

  Specifies whether to replace the last character of the file extension of a mapped file name with a tilde (~). This key applies to file extensions that originally were longer than three characters. This feature can be used to distinguish longer file extensions from similar three-character extensions that were unchanged. For example, enabling this feature prevents a file named *file1.document* from being mapped to a file named *file~xyz.doc*, which could cause some clients to consider this file a Microsoft Word file. (This key affects only Solaris system to 8.3 file mapping.)

  Default: 1 (do not replace last character with a tilde)

- `UniqueSuffixLength` `REG_DWORD` 0 - 7

  Specifies the length of the alphanumeric suffix appended to the file name to guarantee the mapping uniqueness. The longer the suffix, the higher the probability that the mapped name is unique. If the mapped name is not unique within a directory, name collisions can occur. They can cause the client to be denied access to the file it needs, or the client may get access to a different file than the one it requested.

  It is not advisable to set `UniqueSuffixLength` to a value less than 3, unless the preservation of a longer file name prefix outweighs possible name collision problems.

  Default: 3

  You can change the value of this key using PC NetLink Server Manager.

- `UnixCloseCount` `REG_DWORD` 1 - 20

  Specifies the number of least recently accessed open files that the server closes transparently to avoid reaching the Solaris system's per-process limit. The server uses a technique called file descriptor multiplexing to allow clients to open far more files than the per-process limits would normally allow.

  Default: 5

- `UnixDirectoryCheck` `REG_DWORD` 0, 1, or 2

  Specifies whether the PC NetLink program will allow clients to write to Solaris system directories that do not have Write permissions. Microsoft client software treats the Read-only attribute as advisory and does not limit the behavior of directories. In contrast, the Solaris operating environment treats Read-only permissions as mandatory and prohibits users from writing in directories for which they do not have Write permission.

  A value of 0 allows writing only to directories with Write permissions; a value of 1 allows writing to directories belonging to or created by the PC NetLink program (as determined by checking group memberships of directory); and a value of 2 ignores Solaris directory permissions.

  Default: 1

  You can change the value of this key using PC NetLink Server Manager.

- `UnixDirectoryPerms` `REG_DWORD` 0 - 511

  Specifies the Solaris system permissions for newly created directories.

  Default: 509 (0775 octal)

  You can change the value of this key using PC NetLink Server Manager.

- `UnixFilePerms` `REG_DWORD` 0 - 4095

  Specifies the Solaris system permissions for newly created files.

  Default: 436 (664 octal)

  You can change the value of this key using PC NetLink Server Manager.

- `UnixQuotas` `REG_DWORD` 0 or 1

  Specifies whether the PC NetLink program provides Solaris system disk quota support. This ensures that creating or writing to the file is performed under the Solaris system user ID (UID) of the Solaris system user to which the PC NetLink user is mapped. Each action counts toward that user's quota; an error message is sent to the client when the quota is exceeded. Two quotas are supported: i-node and block quotas for UFS and NFS file systems. This is true to the extent of the ability of these file systems to support Solaris system quotas.

  Default: 0 (no support for disk quotas)

- `UseEAs` `REG_DWORD` 0 or 1

  Specifies support for OS/2 extended attributes.

  Default: 0 (no support for OS/2 extended attributes)

- `UseNfsLocks` `REG_DWORD` 0 or 1

  Specifies whether the server tries to set Solaris system record locks in files as requested by clients. Record locks may not work on NFS files on a server running NFS. If the value of the `UseUnixLocks` key is 0, this feature has no effect on the server.

  Default: 0 (do not set locks)

- `UseOplocks` `REG_DWORD` 0 or 1

  Specifies whether PC NetLink grants opportunistic locks to clients who request them on opening a file.

  Default: 1 (use opportunistic locks)

- `UseUnixLocks` `REG_DWORD` 0 or 1

  Specifies whether record locks created by clients are reflected in the Solaris file system.

  Default: 0 (locks are not reflected in Solaris file system)

  You can change the value of this key using PC NetLink Server Manager.

Net Administration Parameters Entries

The Registry path that contains entries for the PC NetLink Net Administration is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\NetAdminParameters
```

- `NetAdminGroupName` `REG_SZ` *Character string*

  Specifies the Solaris system group name assigned to the `net admin \\`*server–name* `/c` command.

  Default: `DOS----`

- `NetAdminPath` `REG_SZ` *Character string* up to 256 characters

  Specifies the Solaris system path used to find commands submitted by the `net admin \\`*server–name* `/c` command.

  Default: `/opt/lanman/bin:/usr/bin`

- `NetAdminUserName` `REG_SZ` *Character string*

  Specifies the Solaris system user account name assigned to a process executed by the `net admin \\`*server–name* `/c` command.

  Default: `lmxadmin`

Parameters Entries

The Registry path that contains entries for the PC NetLink Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\Parameters
```

- `BigEndianLuidCompatibilityMode` `REG_DWORD` 0 or 1

  This entry fixes a problem with the order of the high and low 32-bit parts of the 64-bit locally unique identifier (LUID). Setting the value to 1 causes remote procedure calls used by User Manager for Domains to return the LUID in both orders.

  Default: 1

- `CheckPrintQueueInMinutes` `REG_DWORD` 1 - infinity

  Specifies the interval in minutes at which the server determines whether a printer queue should be started.

  Default: 10 minutes

- `DeletedPrintJobTimeOnQ` `REG_DWORD` 0 - 1000

  Specifies the interval in seconds that a deleted print job is left on the print queue. If the value is 0, deleted print jobs are not left on the queue.

  Default: 180 seconds

- `MaxDirectoryBufferSize` `REG_DWORD` 1 - infinity

  Specifies the maximum size of a buffer that the server will use for a `getdents(2)` system call to read the contents of a Solaris system directory. Because PC NetLink will attempt to allocate these buffers using the GC memory allocator, you should consider increasing the `SizeGcBufferPoolInKB` key if you increase this value.

  Default: 32768 bytes

- `MaxIpcTryCount` `REG_DWORD` 1 - infinity

  Specifies the number of `read()` system calls after which the server checks whether other work could be done by the server. There is a considerable amount of interprocess communication (IPC) between server processes. The server uses the `read` system call to receive IPC messages, but `read` does not always return the entire message. This key ensures that the server does not keep trying to get an IPC message at the expense of other activities the process could perform.

  Default: 50

- `MaxMailslotReadTime` `REG_DWORD` 1 - infinity

  Specifies the interval in seconds to wait for a local mailslot application to read a class 1 mailslot. A value specified here keeps the server from waiting indefinitely for a message to be delivered.

  Default: 90 seconds

- `MaxMessageSize` `REG_DWORD` 32768 - infinity

  The maximum amount of data that a client can exchange with the server.

  Default: 4356 bytes

- `MaxPrintQueueNameLength` `REG_DWORD` 1 - 255 characters

  Provides dynamic control of the allowable length of the name of a printer queue. LP subsystem commands currently allow class names to be as large as 255 characters, but jobs sent to these classes cannot be controlled and many of the Solaris system commands to manipulate these jobs result in a fatal error. This key is used by printer queue functions to restrict access to queues based on the length of the queue name.

  Default: 14

- `MaxRawSize` `REG_DWORD` 8192 bytes - infinity

  Specifies the maximum size in bytes of the raw send or receive buffers that the PC NetLink program will use for processing Read Block Raw, Write Block Raw, Transaction, Transaction 2, or NT Transaction SMBs.

  Default: 65535 bytes

- `MaxServiceWaitTime` `REG_DWORD` 5 seconds - infinity

  Specifies the interval in seconds that the server will wait for a service to respond when it changes the following statuses of the services: pause, continue, install, uninstall.

  Default: 60 seconds

- `NativeLM` `REG_SZ` *Character string*

  Specifies an additional field in the session setup request/response. This field is generated at run time.

  Default: (Solaris PC NetLink)

- `NativeOS` `REG_SZ` *Character string*

  An additional field in the session setup request/response. This field is generated at run time.

  Default: (platform-dependent)

- `SendByeMessage` `REG_DWORD` 0 or 1

  Specifies whether the server sends a message to every client in the domain in the event that it is going to stop for any reason other than a normal shutdown. The message states that the PC NetLink program has stopped.

  Default: 1 (send a message)

- `SizeGcBufferPoolInKB` `REG_DWORD` 1 - infinity

  Specifies the buffer size in Kbytes allocated for each server process for client files.

  Default: 200 Kbytes

Process Parameters Entries

The Registry path that contains entries for the PC NetLink Process Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\ProcessParameters
```

- `CoreOk` `REG_DWORD` 0 or 1

  Specifies whether the server can create a core dump file on disastrous failures.

  Default: 0 (do not create core file)

- `KeepSpareServer` `REG_DWORD` 0 or 1

  Specifies whether the server should have a spare `lmx.srv` process available for another client. New client connections are likely to be quicker if this key is enabled.

  Default: 1 (start `lmx.srv` process)

- `LockNapInMSec` `REG_DWORD` 1 - infinity

  Specifies the interval in milliseconds that the server sleeps when shared memory lock contention occurs. The server retries busy locks at intervals specified in this key until the length of time specified in the value of the `MaxLockTimeInSeconds` key elapses.

  Default: 10 milliseconds

- `MaxLockTimeInSeconds` `REG_DWORD` 5 - infinity

  The maximum interval in seconds that a server process waits for a shared memory lock to become available.

  Default: 30 seconds

- `MaxVCPerProc` `REG_DWORD` 0 - 101

  Specifies the maximum number of virtual circuits that each `lmx.srv` process should be able to handle. This limit normally is calculated contemporaneously by PC NetLink software using the value of the `VCDistribution` Registry key and the value of the `maxclients` parameter in the `lanman.ini` file. If the value of this key is non-zero, its value is used instead of the calculated value.

  Default: 100 (if set to 0, use value of `VCDistribution` key)

  You can change the value of this key using PC NetLink Server Manager.

- `MaxVCs` `REG_DWORD` 1 - infinity

  Specifies the maximum number of virtual circuits that can be established to a PC NetLink server. This key permits administrators to manually override the sizing of shared memory.

  Default: 1

  Do not change the value of this key.

- `MinSmbWorkerTasks` `REG_DWORD` 0 - 100

  Determines how many `SMBWORKER` tasks are preallocated by `lmx.srv` processes on startup.

  Default: 3

  Do not change the value of this key.

- `MinVCPerProc` `REG_DWORD` 0 - infinity

  Specifies the minimum number of virtual circuits that each `lmx.srv` process should be able to handle. This limit normally is calculated contemporaneously by PC NetLink using the value of the `VCDistribution` Registry key and the value of the `maxclients` parameter in the `lanman.ini` file. If this value is non-zero, its value is used instead of the calculated value.

  Default: 10 (if set to 0, use value of `VCDistribution` key)

  You can change the value of this key using PC NetLink Server Manager.

- `NumCIStructs` `REG_DWORD` 0 - infinity

  Sizes the `CLIENTINFO` array in shared memory.

  Default: 3

  Do not change the value of this key.

- `NumCLIENT_SESSION` `REG_DWORD` 5 - 128

  Specifies the maximum number of trust relationships that a server can maintain with other domains. This figure should be at least one greater than the number of domains trusted by the server's domain.

  Default: 10

- `NumHashTables` `REG_DWORD` 8 - infinity (powers of 2)

  Specifies the number of buckets for the hash table in shared memory to keep track of the various modes that clients have used to open files and set record locks.

  Default: 128

  Do not change the value of this key.

- `NumSERVER_SESSION` `REG_DWORD` 5 - infinity

  Specifies the maximum number of servers and Windows NT clients that can authenticate with the server. This figure should be large because it limits the number of Windows NT clients that can contact the server. On a primary domain controller, it must be at least the number of servers and Windows NT clients in the domain.

  Default: 1000

- `NumUStructs` `REG_DWORD` 1 - infinity

  Specifies the number of structures allocated in shared memory to handle record lock and open file records. The sum of open files and record locks cannot exceed the value of this key. If you set this parameter larger than the default, you may also need to increase the setting for Solaris shared memory.

  Default: 15000

- `SpareServerTime` `REG_DWORD` 0 - infinity

  Specifies the interval in seconds that a spare `lmx.srv` process is allowed to run without serving a client before being terminated.

  Default: 120 seconds (2 minutes)

- `StopOnCore` `REG_DWORD` 0 or 1

  Specifies whether the `lmx.ctrl` process is to stop if it finds that an `lmx.srv` process has terminated unexpectedly.

  Default: 0 (do not stop PC NetLink)

- `VCDistribution` `REG_MULTI_SZ` *List*

  Specifies the distribution of virtual circuits or sessions over `lmx.srv` processes. The architecture of the server allows multiple sessions to be served by each `lmx.srv` process on the Solaris system. The server must decide if a new session should be handed off to an existing `lmx.srv` process or if a new process should be started. This key specifies the distribution of sessions over the `lmx.srv` processes.

  Values are entered in sets of three integers separated by commas, each set of three numbers on a new line. In each set, the first number specifies the number of clients; the second is the minimum number of virtual circuits each `lmx.srv` process should support; the third is the maximum number of virtual circuits each process should support.

  Default: 1,5,50

  500,6,65

  700,8,80

  1000,10,100

The following table describes the meaning of the default values.

TABLE A-5 `lmx.srv` Processes Default Value Meaning

Value of `maxclients`[1]	Min. Sessions per `lmx.srv`[2]	Max. Sessions per `lmx.srv`[3]
1-499	5	50
500-699	6	65
700-999	8	80
1000 and above	10	100

1. This column refers to `lanman.ini maxclients` settings.
2. This column describes the internal default value assigned to the Registry parameter `MinVCPerProc.`
3. This column describes the internal default value assigned to the Registry parameter `MaxVCPerProc`.

RPC Parameters Entries

The Registry path that contains entries for the PC NetLink remote procedure call (RPC) Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\RPCParameters
```

- `BrowserMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of open browser RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `EventlogMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of open event log RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `LsarpcMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of open `LSA RPC` sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `NetlogonMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of open NetLogon RPC sessions that an `lmx.srv` process can support simultaneously.

Default: 60

- `SamrMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of Security Accounts Manager (SAM) RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `SpoolssMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of print RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 200

- `SrvsvcMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of server RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `SvcctlMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of service control RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `WinregMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of Registry RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

- `WkssvcMaxCalls` `REG_DWORD` 5 - infinity

  Specifies the maximum number of workstation RPC sessions that an `lmx.srv` process can support simultaneously.

  Default: 60

Share Parameters Entries

The Registry path that contains entries for the PC NetLink Share Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\ShareParameters
```

- `KeepAdministrativeShares` `REG_DWORD` 0 or 1

  Specifies whether administrators are prevented from removing the `ADMIN$` and `IPC$` shared resources.

  Default: 1 (prevented from removing shared resources)

- `MakeUnixDirectoriesOnShare` `REG_DWORD` 0 or 1

  When creating a new share using Server Manager, specifies whether PC NetLink software should create a directory automatically if one does not exist.

  Default: 1 (create new directory)

- `ShareReadCount` `REG_DWORD` 1 - infinity

  Specifies the number of share entries to read during sharefile operations. A value greater than 1 causes the server to read ahead `SHAREENTRY` structures from the sharefile.

  Default: 10

User Service Parameters Entries

The Registry path that contains entries for the PC NetLink User Service Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\UserServiceParameters
```

- `CreateUnixUser` `REG_DWORD` 0 or 1

  Automatically creates and assigns a similarly named Solaris system user account to every new PC NetLink user account created in the domain in which the server is a member. The value of this key must be set to 1 on every server on which Solaris system accounts are to be created. Note that new PC NetLink users are assigned to the Solaris system `lmworld` account.

  Default: 0 (do not create Solaris system user account)

  You can change the value of this key using PC NetLink Server Manager.

- `Exclude` `REG_SZ` *Character string*

  Specifies existing Solaris system user IDs excluded from being assigned to PC NetLink user accounts. If a PC NetLink user account is created whose name matches an existing Solaris system user account whose ID is contained in the exclude list, a new Solaris system user account will be generated automatically and assigned to the PC NetLink user account. This can be used to ensure that

certain existing Solaris system user accounts never are assigned automatically to newly created PC NetLink user accounts, even if the `ForceUniqueUnixUserAccount` key is set to 0.

Default: 0 - 100 user IDs

- `ForceUniqueUnixUserAccount` `REG_DWORD` 0 or 1

  Specifies whether to assign automatically an existing Solaris system user account to a newly created PC NetLink user account. If you select 1, then the system does not assign existing Solaris system user accounts. Instead, new Solaris system user accounts are generated automatically and assigned to PC NetLink user accounts when they are created.

  Default: 0 (A new PC NetLink user account can be assigned automatically to an existing Solaris system user account with an equal or similar name, provided that the Solaris system user account is not specified in the exclude list.)

  You can change the value of this key using PC NetLink Server Manager.

- `MaxUnixUID` `REG_DWORD` 0 - 2147483647

  If the entry `CreateUnixUser` is set to 1, the `MaxUnixUID` entry specifies the maximum limit for the value of the UNIX user ID (UID) that will be assigned to the UNIX account created by PC NetLink.

  Default: 2147483647

- `MinUnixUID` `REG_DWORD` 0 - 1073741823

  If the entry `CreateUnixUser` is set to 1, the `MinUnixUID` entry specifies the minimum limit for the value of the UNIX user ID (UID) that will be assigned to the UNIX account created by PC NetLink.

  Default: 1073741823

- `NewUserShell` `REG_SZ` *Character string*

  Specifies the login shell for new user accounts. The default prevents new users from logging in to the Solaris system using a terminal emulator. To enable login, set this key to a real value, such as `/bin/sh`.

  Default: `/bin/false`

  You can change the value of this key using PC NetLink Server Manager.

- `ShareUnixHomeDirectories` `REG_DWORD` 0 or 1

  If set to 1, this entry causes a user's UNIX home directory to be shared dynamically when that user logs in. The dynamic share is named as the name of the NT user account. It requires that the NT user account has been mapped to a UNIX account. The share is visible only on sessions that have been authenticated

by that user. If a user's home directory is mounted by the automounter, this feature will cause the user's UNIX home directory to be automounted when it is mapped by a client.

Default: 0 (do not share UNIX home directories)

- `SyncUnixHomeDirectory` `REG_DWORD` 0 or 1

  Whenever the home directory of a PC NetLink user account changes, this key changes the home directory of the associated Solaris system user account to match the PC NetLink home directory.

  Default: 0 (do not synchronize home directories)

  You can change the value of this key using PC NetLink Server Manager.

- `UnixHomeDirectoryRemark` `REG_SZ` 0 - 48 characters

  Specifies the Remark string that is displayed by Server Manager in the share list.

  Default: Dynamic Home Directory

- `UserComment` `REG_SZ` *Character string*

  Specifies the comment to assign to all automatically created Solaris system user accounts.

  Default: Solaris™ PC NetLink user

- `UserRemark` `REG_SZ` *Character string* up to 48 characters

  The comment string associated with the `USERS` shared directory.

  Default: Users Directory

Directory Synchronization Entries

The Registry path that contains entries for Directory Synchronization parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\DirectorySyncParameters
```

- `SyncPasswordsToSolaris` `REG_DWORD` 0, 1, or 2

  Enables bidirectional password synchronization between the Solaris name service and the NT Domain Services. If this entry is set to 1, the password synchronization daemons will listen for password change requests from NT password synchronization filters and from Solaris PAM modules.

  If the value of this parameter is set to 2, NT user accounts will be mapped to UNIX accounts only if the passwords are synchronized. This permits the administrator to assign a standard password to all new NT user accounts. The

NT user will not be able to access directories and files belonging to the mapped UNIX user until the NT user synchronizes the NT password to the UNIX password, demonstrating knowledge of the UNIX user's password.

Default: 0 (password synchronization disabled)

- `NetLinkPwdSyncDaemon` `REG_SZ` *Character string*

  This entry is used if `SyncPasswordsToSolaris` is enabled. It specifies the IP address of the PC NetLink system that is running the password synchronization daemon.

  The format of the IP address is `XXX.XXX.XXX.XXX`.

  Default: None

Alerter Service Parameters Entries

The Registry path that contains entries for the PC NetLink Alerter service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Alerter
\Parameters
```

- `AlertNames` `REG_MULTI_SZ` *List*

  Specifies a list of user accounts and computer names that should receive administrative alerts.

  Default: None

- `CountNotOnNetworkCache` `REG_DWORD` 0 - infinity

  Specifies the number of non-running cached clients to which the Alerter service should not send messages. When the Alerter service tries to send a popup message to a client, NetBIOS name resolution can cause unwanted delays if the client is not on the network. To circumvent this problem, the Alerter service caches the names of clients that are not running and does not send alerts to these clients.

  Default: 10

- `IncludeMessageHeader` `REG_DWORD` 0 or 1

  Specifies whether the Alerter service should add four lines of header information to messages (sender, recipient, subject, and date).

  Default: 0 (do not include headers)

- `NotOnNetworkCacheTimeout` `REG_DWORD` 0 - infinity

  Specifies the interval in seconds that non-running clients should remain in the server's cache of clients.

  Default: 120 seconds (2 minutes)

Browser Service Parameters Entries

You can use PC NetLink Server Manager to change the values of all of the following keys. The Registry path that contains entries for the PC NetLink Computer Browser service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser
\Parameters
```

- `BackupRecovery` `REG_DWORD` 60 - infinity

  Specifies the interval in seconds that must elapse before a server that has ceased being a backup browser can become a backup browser again.

  Default: 1800 seconds (30 minutes)

- `BackupUpdate` `REG_DWORD` 60 - infinity

  Specifies the interval in seconds at which the backup browser refreshes its browse lists with the master browser.

  Default: 720 seconds (12 minutes)

- `IsDomainmaster` `REG_SZ` 0 or 1

  Setting this parameter to 1 (Yes) gives the browser a greater chance of winning the master browser election.

  Default: 0 (No)

- `MaintainServerList` `REG_SZ` 0 or 1

  Setting this parameter to 0 (No) makes the browser less likely to become a master browser, backup browser, or potential backup.

  Default: 1 (Yes)

- `MasterUpdate` `REG_DWORD` 60 - infinity

  Indicates the interval in seconds at which the master browser ages its browse lists and updates its lists with the domain master browser.

  Default: 720 seconds (12 minutes)

- `MoreLog` `REG_DWORD` 0 or 1

  Indicates whether the Computer Browser service should record additional system log entries for events such as election packets that the Computer Browser service receives and the role of the browser server (master or backup).

  Default: 0 (do not record additional entries)

- `WinsServer` `REG_SZ` *Character string*

  This entry is used to assist the Browser mechanism in finding systems in other domains. The value of this entry is the IP address of the WINS server in the form 100.200.300.400. If this entry is set, the Browser will send queries to the WINS server as it builds its list of domains.

  Default: None

EventLog Service Parameters Entries

The subkey for EventLog contains at least three subkeys for the three types of logs: Application, Security, and System. These *logfile* subkeys contain subkeys that define the locations of the related event message files and the supported types of events, as follows:

- *Application* – Perflib, Perfmon, Replicator, RemoteBoot
- *Security* – LSA, SC Manager, Security, Security Accounts Manager, Spooler
- *System* – Alerter, Browser, EventLog, NetLogon, Print, Rdr, SAM, Server, Service Control Manager, Srv, Wins, Workstation

Each of the three *logfile* subkeys for the EventLog service can contain the value entries described in this section. The Registry path for these entries is the following, where *logfile* is System, Application, or Security.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\`*logfile*

These entries are described for informational purposes only. This information is usually maintained by Event Viewer.

- `File` `REG_EXPAND_SZ` *Path* and *file name*

  Specifies the fully qualified path name of the file for this log.

  Default: %*SystemRoot*%`\var\opt\lanman\logs\`*filename*

- `MaxSize` `REG_DWORD` Multiples of 64 Kbytes

  Specifies the maximum size of the log file. This value can be set using the Event Viewer.

Default: 524288 (512 Kbytes)

- `Retention` `REG_DWORD` 0 - infinity

  Specifies in seconds that records newer than this value will not be overwritten. This is what causes a log full event. This value can be set using the Event Viewer.

  Default: 604800 seconds (7 days)

- `Sources` `REG_MULTI_SZ` *List*

  Specifies the applications, services, or groups of applications that write events to this log. Each source may be a subkey of the *logfile* subkey. (The `appsources`, `secsources`, and `syssources` keys also are in the `lanman.ini` file.)

  Default: (varies according to log file)

The subkeys under a *logfile* subkey are created by the applications that write events in the related event log. These subkeys contain information specific to the source of an event under the following types of value entries.

- `EventMessageFile` `REG_EXPAND_SZ` *Character string*

  Specifies the path and file name for the event identifier text message file.

- `CategoryMessageFile` `REG_EXPAND_SZ` *Character string*

  Specifies the path and file name for the category text message file. The category and event identifier message strings may be in the same file.

- `CategoryCount` `REG_DWORD` 0 - infinity

  Specifies the number of categories supported.

- `TypesSupported` `REG_DWORD` 0 - infinity

  Specifies a bitmask of supported types.

Net Logon Service Parameters Entries

The Registry path that contains entries for the PC NetLink Net Logon service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon
\Parameters
```

- `DisablePasswordChange` `REG_DWORD` 0 or 1

  Setting this entry to 1 on an NT workstation or member server prevents it from attempting to change its machine account password. By default, machine account passwords are changed every seven days.

  Default: 0 (passwords are changed automatically)

- `LogonQuery` `REG_DWORD` 60 - infinity

  Specifies the interval in seconds at which the server checks if linked clients are still active.

  Default: 900 seconds (15 minutes)

- `MaximumPasswordAge` `REG_DWORD` 1 - 1000000

  Specifies the frequency in days with which an NT workstation, member server, or backup domain controller will attempt to change its machine account password. By default, machine account passwords are changed every seven days.

  Default: 7 days (passwords are changed every seven days)

- `Pulse` `REG_DWORD` 60 - 3600 (1 hour)

  Specifies the interval in seconds for sending update notices when no updates are occurring to the master user accounts database. This keyword applies only to a primary domain controller and is ignored by other servers.

  Default: 300 seconds (5 minutes)

- `QueryDelay` `REG_DWORD` 1 - infinity

  Specifies the interval in seconds that a client can wait before responding to the server's inquiry about whether it is active.

  Default: 2 seconds

- `Randomize` `REG_DWORD` 5 to 120

  Specifies the interval in seconds within which a backup domain controller randomizes its request to a primary domain controller for updates after receiving an update notice. This keyword reduces the chance that backup domain controllers in the same domain will simultaneously request an update.

  Default: 30 seconds

- `RefusePasswordChange` `REG_DWORD` 0 or 1

  Setting this entry to 1 on domain controllers causes them to refuse machine account password changes from NT workstations or member servers. By default, an NT system that is a member of a domain will attempt to change its machine account password every seven days. Setting this entry to 1 will eliminate the replication traffic that results from synchronizing these password changes to the backup domain controllers.

  Setting this entry to 1 on the domain controllers is an alternative to setting the `DisablePasswordChange` parameter on member servers and workstations. The `RefusePasswordChange` entry should be set on all backup domain controllers and then on the primary domain controller.

  Default: 0 (do not refuse machine account password changes)

- `RelogonDelay` `REG_DWORD` 1 - infinity

  Specifies the interval in seconds that a client can wait before logging back on to the server after the server has been stopped and restarted.

  Default: 2 seconds

- `Scripts` `REG_EXPAND_SZ` *Path name*

  Specifies the location of the logon scripts directory.

  Default on primary domain controller:
  %SystemRoot%`\var\opt\lanman\shares\asu\repl\export\scripts`

  Default on backup domain controller:
  %SystemRoot%`\var\opt\lanman\shares\asu\repl\import\scripts`

- `Update` `REG_DWORD` 0 or 1

  If this value is set to 1, the server synchronizes the user accounts database with the primary domain controller every time it starts. This keyword applies only to a backup domain controller and is ignored by the primary domain controller. Note that full synchronization is a very time-consuming operation.

  Default: 0 (do not synchronize)

Netrun Service Parameters Entries

The Registry path that contains entries for the PC NetLink Netrun service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netrun
\Parameters
```

- `MaxRuns` `REG_DWORD` 1 - 10

  Specifies the maximum number of Netrun requests that can run simultaneously.

  Default: 3

- `RunPath` `REG_SZ` *Path name* up to 256 characters

  Specifies the path for programs accessible via the Netrun service. Only programs located in a run path can be executed from a client or another server. Separate multiple path entries with colons (`:`).

  Default: `\tmp`

Directory Replicator Service Parameters Entries

The Registry path that contains entries for the PC NetLink Directory Replicator service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Replicator
\Parameters
```

- `ExportList` `REG_SZ` *Character string*

  Lists an unlimited number of servers or domains that receive notices when the export directory is updated. These servers subsequently replicate from the export server. If no value is specified, the export server sends a notice to its domain. Separate multiple names with a semicolon (`;`). This value is ignored if the value of the Replicate key is `2` (Import).

  Do not use the UNC name when you specify a computer name; that is, do not include two backslashes (\\) at the beginning of the name.

  Default: *local-domain-name*

- `ExportPath` `REG_SZ` or `REG_EXPAND_SZ` *Path*

  Specifies the export path. All files to be replicated must be in a subdirectory of the export directory. This value is ignored if the value of the Replicate key is set to `2` (Import).

  Default: `C:\var\opt\lanman\repl\export`

- `GuardTime` `REG_DWORD` 0 to one-half of *Interval*

  Specifies the number of minutes an export directory must be stable (no changes to any files) before import servers can replicate its files.

  This option applies only to directories with tree integrity.

  Default: 2 minutes

- `ImportList` `REG_SZ` *Character string*

  Lists an unlimited number of servers or domains from which files and directories are to be replicated. If no value is specified, files and directories will be replicated from the server's domain. Separate multiple names with a semicolon (`;`). This value is ignored if the value of the Replicate key is `1` (Export).

  Do not use the UNC name when you specify a computer name; that is, do not include two backslashes (\\) at the beginning of the name.

  Default: none

- `ImportPath` `REG_SZ or REG_EXPAND_SZ` *Path name*

  Specifies the path on the import server to receive replicas from the export servers. This value is ignored if the value of the Replicate key is `1` (Export).

Default: `C:\var\opt\lanman\repl\import`

- `Interval` `REG_DWORD` At least twice as large as `GuardTime` value

  Specifies how often in minutes an export server checks the replicated directories for changes. Used in conjunction with the `Pulse` key. Ignored on import servers. The value of `Interval` must be at least twice as large as the value of `GuardTime`. Otherwise, the Replicator service will not start.

  Default: 5 minutes

- `MaxFilesInDirectory` `REG_DWORD` 0 - infinity

  Specifies the maximum number of files in an import directory that can be replicated.

  Default: 2000

- `Pulse` `REG_DWORD` 1 - 10

  Specifies how often in minutes the export server repeats the last update notice. These repeat notices are sent even when no changes have occurred, so that import servers that missed the original update notice can get the notice. The server waits the equivalent of (`Pulse` * `Interval`) minutes before sending each repeat notice.

  Default: 3 minutes

- `Random` `REG_DWORD` 1 - 120

  Specifies the maximum time in seconds that the import servers can wait before requesting an update. An import server uses the export server's value of `Random` to generate a random number of seconds (from 0 to the value of `Random`). The import server waits this long after receiving an update notice before requesting the replica from the export server. This prevents the export server from being overloaded by simultaneous update requests.

  Default: 60 seconds

- `Replicate` `REG_DWORD` 1, 2, or 3

  Specifies the Replicator action, according to the following:

  1 = Export – The server maintains a master tree to be replicated.

  2 = Import – The server receives update notices from the export server.

  3 = Both – The server is to export and import directories or files.

  Default: Varies with role of server

- `TryUser` `REG_DWORD` 0 or 1

  Specifies whether the import server should try to update directories when a user name is logged on locally.

Default: 0 (do not try to update)

- `UnixDirectoryGroup` `REG_SZ` *Character string*

  Specifies the Solaris system group account name for replicated directories.

  Default: `DOS----`

- `UnixDirectoryOwner` `REG_SZ` *Character string*

  Specifies the Solaris system user account name for replicated directories.

  Default: `lmxadmin`

- `UnixFileGroup` `REG_SZ` *Character string*

  Specifies the Solaris system group account name for replicated files.

  Default: `DOS----`

- `UnixFileOwner` `REG_SZ` *Character string*

  Specifies the Solaris system user account name for replicated files.

  Default: `lmxadmin`

UPS Service Parameters Entries

The Registry path that contains entries for the PC NetLink Uninterruptible Power Supply (UPS) service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UPS
\Parameters
```

- `IgnoreSIGPWR` `REG_DWORD` 0 or 1

  Specifies whether the UPS service will be enabled.

  Default: 1 (disables the UPS service)

  You can change the value of this key using PC NetLink Server Manager.

- `PowerFailAddress` `REG_SZ` *Character string* up to 15 characters

  Specifies the NetBIOS name to which the server sends a message when it receives a `SIGPWR` signal.

  Default: * (all users)

  You can change the value of this key using PC NetLink Server Manager.

- `PowerFailMessage` `REG_SZ` *Character string* up to 500 characters

  Specifies the text of the message to be sent by the server when it receives a `SIGPWR` signal.

  Default: The system has experienced a power failure. Please close all applications and files and log off immediately.

  You can change the value of this key using PC NetLink Server Manager.

- `PowerMessageInterval` `REG_DWORD` 0 - infinity

  Specifies the interval in minutes at which the server repeats the message sent when it receives a `SIGPWR` signal. A value of 0 indicates that the message should be sent one time only.

  Default: 1 minute

  You can change the value of this key using PC NetLink Server Manager.

Local Security Parameters Entries

The Registry path that contains entries for Local Security parameters is as follows:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

- `LMCompatibilityLevel` `REG_DWORD` 0 - 5

  Specifies the authentication mechanism that is negotiated between the client and server.

  Default: 0

- `Notification Packages` `REG_MULTI_SZ` *Character strings*

  This entry may contain a list of strings that are the names of password change filter libraries. For example, to configure the Windows NT "strong password" policy, add the library name `libpassfilt.so` in this entry. To configure password synchronization, add the name of the password synchronization filter, `libsyncfilt.so`. Note that the name of the password synchronization filter should be added at the end of the list of password filters (see `SyncPasswordsToSolaris` on page 326).

  Default: None

- `RestrictAnonymous` `REG_DWORD` 0 or 1

  Set this entry to 1 to prevent unauthenticated (anonymous) sessions from querying user and share information.

  Default: 0

Lanman Server Parameters Entries

The Registry path that contains entries for the LAN Manager service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanmanServer\Parameters
```

- `AccessAlert` `REG_DWORD` 0 - infinity

  Specifies the number of resource access violations that can occur before the server sends an alert to the `alertnames` list.

  Default: 5

- `AutoDisconnect` `REG_DWORD` 0 - 3600 (60 hours)

  Specifies the interval in minutes that the server waits before dropping the virtual circuit to an inactive client.

  Default: 0 (no automatic disconnect)

- `EnableSecuritySignature` `REG_DWORD` 0 or 1

  Enables integrity checking on SMB packets. A message digest (hash) is created from the contents of each SMB packet and is appended to the packet by the sender. The receiver of the packet will verify that the contents it has received generates the same digest as the one appended by the sender. Setting this entry to 1 may degrade performance. This mechanism is used only if both sender and receiver have been configured to use it. Otherwise, packets are sent and received on the session without integrity checking.

  Default: 0 (integrity checking is disabled)

- `ErrorAlert` `REG_DWORD` 0 - infinity

  Specifies the number of errors that can occur before the server sends an alert to the `alertnames` list.

  Default: 5

- `Hidden` `REG_DWORD` 0 or 1

  Specifies whether the server is hidden on the network. If the server is not hidden, it announces its presence set in the `SrvAnnounce` and `LmAnnounce` keys.

  Default: 0 (the server is visible)

- `LmAnnounce` `REG_DWORD` 0 or 1

  Specifies whether a server should announce itself with the old LAN Manager-type announcement in addition to the new Windows NT-type announcement. This key has an effect only if the value of the `Hidden` key is 0.

  Default: 0 (use only Windows NT-type announcement)

- `LogonAlert` `REG_DWORD` 0 - infinity

  Specifies the number of logon violations that can occur before the server sends an alert to the `alertnames` list.

  Default: 5

- `NullSessionShares` `REG_MULTI_SZ` *Character strings*

  Specifies a list of share names to which null sessions can connect. A null session is an unauthenticated or anonymous session.

  Default: None

- `RequireSecuritySignature` `REG_DWORD` 0 or 1

  If this entry is set to 1, the system requires integrity checking on SMB packets, and will not communicate with systems that have not been configured to use this feature. A message digest (hash) is created from the contents of each SMB packet and is appended to the packet by the sender. The receiver of the packet will verify that the contents it has received generates the same digest as the one appended by the sender. Setting this entry to 1 may degrade performance. This mechanism is used only if both sender and receiver have been configured to use it. Otherwise, packets are sent and received on the session without integrity checking.

  Default: 0 (integrity checking is disabled)

- `SrvAnnounce` `REG_DWORD` 1 - infinity

  Specifies the interval in seconds at which the server announces its presence to the network. This key has an effect only if the value of the `Hidden` key is 0.

  Default: 180 seconds (3 minutes)

- `SrvComment` `REG_DWORD` *String* up to 48 characters

  Specifies the descriptive comment that the server sends when it announces its presence to the network.

  Default: Vendor-specific

- `UserPath` `REG_SZ` *Path*

  Specifies the UNIX system directory on the server to be used as a default parent directory for home directories for new user accounts.

  Default: `C:\export\lanman\`*number* (where *number* is the virtual server instance number)

APPENDIX **B**

Performing Common Windows NT Administrative Tasks

This appendix provides instructions for accomplishing many basic Windows NT/PC NetLink administrative tasks that are not covered elsewhere in this book. Intended mainly for the experienced Solaris administrator who performs tasks via the command line and has little Windows NT experience, this appendix focuses on interoperability issues rather than purely Windows NT administration.

This appendix does not provide background information about the Microsoft Windows or Windows NT environments. Many third-party books, as well as documentation from Microsoft, are available for that purpose.

The tasks included in this appendix are:

- "How to Join a Domain as a BDC When the PDC Is on a Different Subnet" on page 340
- "How to Add `LMHOST` Functionality to a PC NetLink Server Running as a BDC" on page 341
- "How to Set Up Directory Replication Between Servers on Different Domains" on page 342
- "How to Set Up Windows NT Alerts and Security Auditing" on page 347

PC NetLink Server Manager "How to" Help

PC NetLink Server Manager also offers complete instructions for performing a variety of Windows NT/PC NetLink interoperability tasks. Double-click Tasks and then double-click any of the "How to" icons (illustrated with a question mark) to find the instructions.

Topics covered are:

- How to Set Up File Shares
- How to Set Up Roaming Profiles
- How to Set Up System Policies
- How to Set Up Trust Relationships
- How to Set Up User Accounts

Available by double-clicking "Other How-To Help Topics" are:

- How to Enforce Solaris Disk Quotas in a PC NetLink Environment
- How to Create Solaris Home Directory Access From Client PCs
- How to Configure Printer Pooling
- How to Set Up Directory Replication
- How to Migrate a Windows NT Server to a PC NetLink Server

Common Windows NT Administrative Tasks

This section provides information about performing common Windows NT administrative tasks.

▼ How to Join a Domain as a BDC When the PDC Is on a Different Subnet

When you need to have your PC NetLink server become a backup domain controller (BDC) to a primary domain controller (PDC) in a different subnet, the PC NetLink server must resolve the NetBIOS name of the PDC. There are two ways to do this, depending on whether a WINS server exists in the PDC's domain.

If a WINS Server Exists

If a WINS server exists in the PDC's domain, and if the PDC is already registered in this WINS server, then you must register the PC NetLink server in this same WINS server. In this way, the PC NetLink server can resolve the PDC's NetBIOS name.

Do the following to register the PC NetLink server in the WINS database:

1. **Restart the PC NetLink server by typing the following commands:**

```
# winsconf -p IP-address-of-WINS-server
# net stop server
# net start server
```

2. **Use the `joindomain` command to join the PC NetLink server to the domain.**

If a WINS Server Does Not Exist

If a WINS server does not exist in the PDC's domain, do the following to resolve the NetBIOS name:

1. **Type the following commands:**

```
# cd /opt/SUNWlznb/sbin
# ./nbns_adm -a -N PDC-name -A IP-address -P TCP
```

2. **Use the `joindomain` command to join the PC NetLink server to the domain.**

▼ How to Add `LMHOST` Functionality to a PC NetLink Server Running as a BDC

This section tells you how to add `LMHOST` functionality to a PC NetLink BDC server by creating and activating a `fnbnsusr.info` file.

1. **Do either of the following:**

   a. **Create a `fnbnsusr.info` file.**

   PC NetLink software has a feature similar to `LMHOST`, configured in `/var/opt/SUNWlznb/fnbnsusr.info`.

   This file has the following format:

   PDC-name fill_character last_character ip_address name_type protocol_type

   Note the following restrictions:

   - The fill character is always `0x20`.
   - The last character should be `0x20` if referring to a server.
   - `0x1B` is used for a BDC, and so on.

- The name type is either unique or group.
- Protocol type is always `TCP`.

b. Create a `lmhosts` file in `/var/opt/SUNWlznb`.

2. Activate the changes, as root, by typing the following command:

```
# /opt/SUNWlznb/sbin/nbnsName.add
```

3. As root, type the following command to verify that the NetBIOS name is being resolved correctly:

```
# nbutil -f PDC-name
```

This function will not work correctly unless you have added the NetBIOS name of the PC NetLink BDC server in the `LMHOST` file of the Windows NT-based PDC server. This will take care of some of the `net` commands (issued from the PC NetLink BDC) needed to contact the PDC server. See Chapter 2, "PC NetLink Administration at the Solaris Command Line" on page 13, for additional information about using commands.

▼ How to Set Up Directory Replication Between Servers on Different Domains

A server can play the following roles in directory replication:

- Export server
- Import server
- Both export server and import server

You have to configure the server according to the role it will play. You have to place the files to be replicated on the export server in subdirectories under `C:\Winnt\System32\Repl\Export` on Windows NT servers or on `C:\var\opt\lanman\repl\export` on PC NetLink systems.

Each time you add or modify a file in these subdirectories, the export server sends an update message to the import servers. The Replicator service on the import servers then logs on to the export server as a service and retrieves the files. The replicated files are placed in the same subdirectories' names under `C:\Winnt\System32\Repl\Import` on Windows NT systems or `C:\var\opt\lanman\repl\import` on Solaris PC NetLink systems.

To achieve directory replication between servers on different domains, a trust relationship has to be defined between the two domains. The user who runs the Replicator service on the import domain has to be added to Replicator Local Group of the export server and also has to be able to perform the "Log on as a Service" operation on the export server.

Configuring the Import Server

To configure the import server, log on as Administrator and do the following:

1. **Open the User Manager tool and create a new user, `repladmin`, adding it to the following groups:**
   - Domain Users
   - Backup Operators
   - Replicator
2. **Assign a password to the `repladmin` account, setting the password to Never expire and not to be Changed on Next Logon; also, no machine restrictions should be set.**
3. **Still using the User Manager tool, add the export server's domain as a Trusting Domain:**
   a. **From the Policies menu, choose Trust Relationship.**
   b. **Click the Add button to the right of Trusting Domains. You should see a new window, in which you type the name of the Trusting (Export) Domain, password, and password confirmation.**

Note – Password and Confirm Password are used only at the time the trust relationship is set. You can leave them blank. The value you use for Password and Confirm Password is used in Step 3b of the "Configuring the Export Server" section below, so note them for later use.

---

   c. **Click OK.**
4. **In the Server Manager tool, select the import server and then, from the Computer menu, choose Services.**
   a. **Select the Directory Replicator service and click the Startup button.**
   b. **Select Startup Type as Automatic.**
   c. **On the Logon As option, select This Account and type the name of the user account; such as:** *Import_Domain_Name*`\repladmin`

d. Type the password of the `repladmin` user in the Password and Confirm Password boxes.

e. Close these dialog boxes.

If the operation is successful, this will add `repladmin` to the Replicator Local Group on the import domain and will grant `repladmin` the "Log on as a Service" right on the import domain.

f. Restart the Directory Replicator service by clicking the Start button.

5. Still using PC NetLink Server Manager, double-click the import server icon.

a. Click the Replication button to open a dialog box.

b. Select the Import Directories option.

c. In the From Path field, type the path to which you want to import the subdirectories.

In most cases, you should be able to use the default path of `C:\Winnt\system32\Repl\Import` on Windows NT, or `C:\var\opt\lanman\repl\import` on Solaris PC NetLink servers.

d. Click the Add button below the Import Directories and type or select the export domain name or export server name.

e. Click OK to close the Add window.

f. Click OK to close all windows.

Note – It is very important to verify that the directory into which you are importing files has the correct Solaris permissions; otherwise, it will not work. To do this, type the following commands at the Solaris system prompt:

```
# chmod 777 dirtoexport
# chown lmxadmin dirtoexport
# chgrp DOS---- dirtoexport
```

It is much easier if the system administrator creates the directories to be exported from a client mapped to the share. Then they have a true Solaris PC NetLink directory.

Configuring the Export Server

To configure the export server, log on to it as Administrator and follow these steps:

1. **In the User Manager tool, create a new user, `repladmin`, and add it to following groups:**
   - Domain Users
   - Backup Operators
   - Replicator
2. **Assign a password to the `repladmin` account, setting the password to Never Expire and not to be Changed on Next Logon.**
3. **Still using the User Manager tool, add the Import Server's domain as a Trusted Domain:**
   a. **From the Policies menu, choose Trust Relationship.**
   b. **Click the Add button to the right of Trusted Domains. You should see a new window, in which you type the name of the Trusted (import) Domain and password. Type the password that you typed when you configured the Trusting Domain in Step 3b in "Configuring the Import Server" above.**
   c. **Click OK.**
4. **In the User Manager tool on the export domain, add the `repladmin` account from the import domain to the Replicator Local Group.**
   a. **Double-click on the Replicator group from the Group list at the bottom of the window.**
   b. **Click the Add button.**
   c. **In List Names From, select the import domain name.**
   d. **Double-click the `repladmin` user account.**
   e. **Click OK to close the Add window.**
   f. **Click OK to close the Group window.**
5. **From the User Manager pull-down menu, choose Policies and then User Rights.**
   a. **Select Show Advanced User Rights.**
   b. **From the Rights options list, select Log on as a Service.**
   c. **Click the Add button, then from the new window that appears, select the Replicator group.**
   d. **Click the Add button.**

e. **Click OK to close the User Rights window.**

6. **In Server Manager, select the export server and then, from the Computer menu, choose Services.**

   a. **Choose Startup from the Directory Replicator service menu.**

   b. **Select Startup Type as Automatic.**

   c. **On the Logon As option, select This Account and type the name of the user account; such as:** *Export-Domain-Name*`\repladmin`

   d. **Type the password of the `repladmin` user in the Password and Confirm Password boxes.**

   e. **Close these dialog boxes.**

      If the operation is successful, this will add `repladmin` to the Replicator Local Group on the export domain and will grant `repladmin` the Log on as a Service right on the export domain.

   f. **Click the Start button to restart the Directory Replicator service.**

7. **Still using Server Manager, double-click on the export server.**

   a. **Click the Replication button to open a dialog box.**

   b. **Select the Export Directories option.**

   c. **In the From Path field, type the export path name.**

      In most cases, you can use the default path of `C:\Winnt\System32\Repl\Export` on Windows NT or `C:\var\opt\lanman\repl\export` on PC NetLink systems.

   d. **Click OK to close these dialog boxes.**

8. **Use Server Manager to make sure that the Replicator service was started on both servers.**

   Replication will start soon.

   If you want to establish a two-way replication (both servers acting as import and export server), you have to establish a two-way trust relationship between the two domains. The `repladmin` users of both domains have to be added to the Replicator Local Group in each domain, and the Replicator Local Group has to be able to “Log on as a Service” in each domain.

▼ How to Set Up Windows NT Alerts and Security Auditing

Two of the most useful administrative features available to a PC NetLink server are the Windows NT Alerter service and the Auditing service. These are native Windows NT services, not unlike the PC NetLink Server Manager Performance Alert policy.

You set up the Windows NT Alerter service by way of Windows NT Server Manager to notify you (or any Windows NT-connected machine that you specify) whenever specific events occur. You set a threshold value, and the Alerter service generates an alert whenever the actual value exceeds or falls below the threshold. You can set alerts to be triggered, for example, based on the number of server sessions or on a specified throughput level. You can have the alerts stored in a dedicated log or even sent immediately and directly to your machine.

Auditing is a key security service that you can use, for example, to monitor who is accessing files or directories on a PC NetLink server. Almost any action performed by a user can be audited. This service is not enabled by default under Windows NT.

Setting Up Alerts

1. **Use PC NetLink Server Manager to make sure the Alerter service is running on the PC NetLink server.**

   See Chapter 3, "Configuring and Managing PC NetLink Software" on page 37.

2. **On a Windows NT server, start Performance Monitor.**

   Click the Start button, and then choose Programs, then Administrative Tools, then Performance Monitor.

3. **In Performance Monitor, choose View and then Alerts.**

4. **In the Alerts sheet, choose Edit and then Add to Alerts.**

   Use the following guidelines:

   - *Computer* – Choose the PC NetLink server
   - *Counter* – Pick one; for example, Bytes Total/sec. (For details about the Counter, click Explain.)
   - *Alert If* – Set the over/under value.

Saving Alerts

- **From the File menu, choose Save Alert Settings.**

Using Saved Settings

- **From the File menu, choose Open.**

Setting Up Security Auditing

Note – The following instructions assume that the user has sufficient privileges to manage auditing and edit the Security log.

---

1. **In Network Neighborhood, highlight a PC NetLink file or folder.**
2. **Under Properties, choose Security and then Auditing.**
3. **In the File Auditing sheet, choose Add, and then pick an option; for example, Everyone.**
4. **Select an event to audit; for example, Read, Write.**

   View audited events in the Security log.

Viewing the Security Log

1. **In Windows NT Event Viewer, choose Log, then Computer, and select the PC NetLink server.**
2. **Choose the Security log.**

Index

A

account operators group, 18, 39
account passwords
  initial synchronization, 188
accounts
  mapping for password synchronization, 180
ACL (Access Control List)
  ability to back up, 11
  `acladm` command, 284
  `AclCacheSize` Registry parameter, 309
  and database cleanup, 242
  `blobadm` command, 285
  `DosAttributeStorage` Registry parameter, 309
  `ForceDirectoryAcl` Registry parameter, 310
  `ForceFileAcl` Registry parameter, 311
  improved database scalability, 1
  managing data, 106
  `SyncAclFileOnWrite` Registry parameter, 313
adding computers to domain, 173
adding computers to domain, described, 65
administration, remote, 5
Administrators group, 19
alarms, configuring, 153
alarms, investigating, 162
Application log, 163

B

backup
  complete server image, 258
  databases, 258
  described, 239
  WINS database, 239
b-node (Broadcast node), 139
broadcast name resolution, 215
  and WINS, 218

C

cleaning up databases, 240
  and ACLs (Access Control Lists), 242
  WINS, 240
command line administration
  described, 13
  Show Commands feature, 14
compacting WINS database, 239
complete server image backup, 258
computer browsing policy
  changing, 109
  defined, 98
computer names
  NetBIOS and DNS, 215
copying user accounts
  described, 108
  from PC NetLink to Solaris, 128
  from Solaris to PC NetLink, 121
  utilities, described, 134 to 137

D

databases
backing up, 258
backing up and restoring, described, 239
cleaning up, 240
compacting WINS, 239
maintenance tasks, 240
management, 239
restoring, 254
scheduled tasks, 268
deleting computers from domain, described, 175
dial-up TCP/IP and WINS, 223
directory share, deleting, 97
DNS, 214
DNS (Domain Name System)
computer names, 215
name resolution, 215
names, 215
resolution, 215
domain controllers
BDC (backup domain controller), 63
member server, 63
PDC (primary domain controller), 63
Domain Name System (DNS)
names, 215
resolution, 215
domain names
changing, described, 66
domains
adding computers, 173
adding computers, described, 65
changing names, described, 66
changing server role, 91
configuration and management, described, 62
creating virtual server, 66
creating virtual server IP address, 66
creating virtual server, described, 64
defined, 62
deleting directory share, 97
deleting members, 175
deleting virtual server, 74
managing, 64
moving computer to different, described, 66
moving virtual server to another, 80, 173, 175
promoting server, 89
removing computers, described, 65
renaming virtual server, 75

E

enabling password synchronization, 188
error codes
from the password synchronization logfile, 192
event monitoring
Application log, using, 163
described, 163
interpreting, 164
PC NetLink Server Manager, using, 168
Security log, using, 163
System log, using, 163
using PC NetLink Server Manager, 166
Events
using logs for troubleshooting, 167
events
description, 164
header, 164
interpreting, 164
monitoring using command line, 169
security, monitoring, 167
types, 165
using logs to troubleshoot, 167

F

file name mapping policy
defined, 99
mixed-case support, 100
rules, 100
setting up, 111

H

h-node (Hybrid node), 139, 217

I

installing and starting the server agent, 184
IP (Internet Protocol) address
DNS server, 151
member server, 63
required for domain controller, unique, 63
virtual server, creating for, 66
WINS server, 139

L

`lanman.ini` file
  changing a parameter, 30
  parameter description, 30
  `srvconfig` command, 29
  syntax, 29
`lanman.ini` file parameters (tables), 31 to 35
`ldif2sam` utility, 135
`ldifmerge` utility, 135
`ldifmerge` utility, using, 137
`LMHOSTS` file, name resolution, 216
local physical host, administering, 18, 19
log
  Application, 163
  event description, 164
  event header, 164
  event types, 165
  Security, 163
  System, 163
  using event logs for troubleshooting, 167
logoff
  described, 39
  from the command line, 45
  using PC NetLink Server Manager, 45
logon
  described, 39
  from the command line, 44
  privileges, 39
  root, 39
  Solaris, 39
  using PC NetLink Server Manager, 42
  Windows NT, 39

M

mapping existing user accounts, 120
mapping user accounts, 119
member server, IP address, 63
modified b-node, 217

N

name registration, and WINS, 220
name release, and WINS, 220
name renewal, and WINS, 221
name resolution
  broadcast, 215
  broadcast and WINS (Windows Internet Name Service), 218
  DNS, 215
  DNS (Domain Name System), 215
  `LMHOSTS` file, 216
  NetBIOS over TCP/IP (NetBT), 216
  WINS, 215, 219
name resolution services, described, 214
name server agent
  installing, 178
  troubleshooting, 190
name services
  for password synchronization, 180
names
  DNS, 215
names, DNS, 215
`net` command usage
  abbreviations, 23
  confirmation, 22
  getting help with, 25
  path names, 24
  special characters, 23
  typing path names at client computers, 24
  typing path names with, 24
`net` commands
  described, 18
  local server, administering with, 19
  `net session`, 282
  `net view`, 295
  options (table), 26 to 28
  remote server, administering with, 19
  servers, administering with, 18
NetBIOS, 138
  computer names, 215
  defined, 138
  Lana numbers, 139
  managing static address mappings, 231
  nodes, 139
  scope, 140
  WINS proxy, 139
  WINS server, 138
NetBT, 214
networks
  adding domain computers, described, 65
  security, 62

nodes
b-node (Broadcast), 139, 217
h-node (Hybrid), 139, 217
modified b-node, 217

O

operator groups
account, 18, 39
print, 18, 39
server, 18, 39

P

PAM module, 178
installing and configuring, 185
sample files, 185
troubleshooting, 191
`passwd2sam` utility, 135
password changes
from Solaris to Windows NT, 179
from Windows NT to Solaris, 178
password daemon, 178
common configuration problems, 189
configuring, 186
IP address, 191
location, 186
troubleshooting, 190
password filter
configuring on a Windows NT PDC, 183
installing, 178
password filters
configuring on a Windows NT PDC, 181
using multiple password filters, 182, 183
password synchronization
about, 177
common configuration problems, 189
configuring a Windows NT PDC, 181
configuring the password daemon, 186
configuring the password filter on a Solaris PDC, 181
configuring the password filter on a Windows NT PDC, 183
enabling using PC NetLink Server Manager, 187
enabling using the command line, 188
enabling using the PC NetLink Server Manager, 187
how it works, 178
in multi-instance environments, 182, 183
in User Accounts Properties dialog box, 120
installing and configuring components, 178
installing and starting the server agent, 184
installing the PAM module, 185
logfiles, 192
manual synchronization, 191
name server agent, 178
name services, 180
PAM module, 178
password changes, 178
password daemon, 178
password filter, 178
requirements for account mappings, 180
sample PAM module files, 185
setting up, 181
suitable environments, 180
synchronizing passwords for the first time, 188
system requirements, 180
troubleshooting, 189
unsupported features, 192
using multiple password filters, 182
PC NetLink commands
`acladm`, 284
described, 16
`elfread`, 279, 293
how to use on Windows client, 21
`ldif2sam`, 16
list of (table), 16
`lmshell`, 285
`lmstat`, 285
man pages, 16
quick reference (table), 16 to 18
`regcheck`, 287, 295
`regconfig`, 286
`regload`, 295
`sam2passwd`, 17
`samcheck`, 287
special characters, 23
`srvconfig`, 287, 295
syntax, 24
PC NetLink commands usage
paging through screens, 21
specifying a virtual server, 21
using abbreviations, 23
using command confirmation, 22
using passwords with, 22

PC NetLink Server Manager
adding a server to, 41
enabling password synchronization, 187
features, 10
log off, using to, 45
log on, using to, 42, 44, 45
memory, controlling amount used, 40
overview, 9
security, 140
services, 46
start server, using to, 46
starting, 39, 40
stop server, using to, 47
PC NetLink services
configuring startup, 60
starting individually, 56
stopping individually, 58
PC NetLink setup
suitability for password synchronization, 180
performance
monitoring physical host, 156
WINS server, 227
performance monitoring and alarms, described, 141
performance monitoring, configuring, 153
performance tuning
client workload, 102
described, 101
processes and virtual circuits, 101
physical host information, monitoring, 170
physical host, local, administering, 18, 19
physical host, remote, administering, 18, 19
policies
browsing, described, 98
described, 98
file name mapping
mixed-case support, 100
rules, 100
file ownership, 105
list of, 98
managing, described, 98
NetBIOS, 138
Lana (LAN Adapter) numbers, 139
scope, 140
WINS and NetBIOS nodes, 139
WINS servers, 138
PC NetLink Server Manager security, 140
performance monitoring and alarms, configuring, 153
performance tuning, 101
client workload, 102
processes and virtual circuits, 101
UPS power failure notification, 107
user account mapping, 107
`/etc/passwd` files, 107
passwd2sam, 135
`passwd2sam`, 134, `135`
tools, 134 to 137
print operators group, 18, 39
printing
described, 195
network, 197
PC NetLink terms, 196
local spooling system, 197
LP printer, 196
network-interface print device, 197
print server, 197
printer, 196
printer driver, 197
shared printer queue, 196
spooling, 197
setting up, 197
Solaris printer
configuration, 198
removing, 208
setting up as shared printer, 206
proxy, WINS, 222
pull partner and WINS server, 238
push partner and WINS server, 237

R

Registry
connecting to remote, 301
editor
commands, 302
using, 301
keys and values, 308, 336
Alert parameters, 309
Alerter service parameters, 327
Browser service parameters, 328
Eventlog service parameters, 329, 330
File service parameters, 309, 310, 311, 312, 313, 314, 315

Net Administration parameters, 316
Net Logon service parameters, 330, 332
Netrun service parameters, 332
PC NetLink parameters, 316 to 318
PC NetLink subkey, 308
Process parameters, 318, 322
Replicator service parameters, 333, 335
replicator service parameters, 236
RPC parameters, 322, 324
UPS service parameters, 335, 336
user service parameters, 324, 326
WINS parameters, 236
policies, 303, 308
structure, 299, 301
remote administration, 5
remote physical host, administering, 18, 19
removing computers from domain, described, 65
replication partners, configuring WINS, 230
replication planning, 227
replication planning and WINS server, 226
restore
WINS database, 239
restoring
databases, 254
routed environment, use of WINS in, 218
roving user and WINS server, 225

S

`sam2ldif` utility, 135
`sam2passwd` utility, 135, 136
sample files
for the PAM module, 185
scheduled tasks
complete virtual server image backup, 258
copying user accounts, 108
from PC NetLink to Solaris, 128
from Solaris to PC NetLink, 121
database backup, 248
database cleanup, 240
deleting, 268
modifying, 268
viewing, 268
virtual server restart, stop, or start, 50
security events, monitoring, 167
Security log, 163
server
starting using command line, 49
starting using PC NetLink Server Manager, 46
stopping using command line, 49
stopping using PC NetLink Server Manager, 47
server agent
installing and starting for password synchronization, 184
server operators group, 18, 39
services
configuring startup for, 60
listed, 46
starting and stopping, 46
`setdomainname` command, 66
setup
for password synchronization, 181
Show Commands tool
described, 14
using, 14
Solaris client
installing the PAM module, 185
Solaris file system
ownership of files and directories, 105
security, 102
Solaris physical host information, monitoring, 170
Solaris printer, setting up as shared printer, 207
static address mappings, managing NetBIOS, 231
synchronizing passwords
in User Accounts Properties dialog box, 120
System log, 163

T

troubleshooting
assessing status of server
`elfread` command, 279
Event Viewer, 279
open resources, 282
Server Manager, 279, 281, 282, 296
session information, 281
UNIX system scripting feature, 284
viewing events, 279
checking the network, 289
debugging tools
`acladm` command, 284
`lmstat` command, 285

regcheck command, 287
regconfig command, 286
samcheck command, 287
srvconfig command, 287
examining the logfile, 192
isolating problems
maximum number of users, 295
Registry corrupted, 295
resources shared properly, 293
server contacted from client, 295
server contacted from console, 294
server running, 291
services running, 292
manual synchronization, 191
name server agent, 190
NetBIOS protocol status, 290
PAM module, 191
password daemon, 190
password synchronization, 189
physical network, 289
problems on the server, 291
procedures
checking the network, 289
isolating the problem, 291
shared resource, 295
transport protocol, 290
UNIX system functionality, 290
verifying the correct setup, 189
trusted domain accounts, 181

U

udir command, 296
UPS (uninterruptible power supply) power failure notification, described, 107
user account mapping policy, editing, 118
user accounts, mapping, 119
existing, 120

V

virtual server
creating, 64, 66
creating IP address for, 66
deleting, 74
moving to another domain, 80, 173, 175
options, viewing or changing, 171
renaming, 75
scheduling restart, stop, or start, 50
virtual servers
setting up password synchronization, 182, 183

W

WANS (wide area networks) and WINS, 226
Windows NT administration tools
described, 4
Event Viewer, 6
Server Manager, 6
System Policy Editor, 7
User Manager for Domains, 5
User Profile Editor, 7
WINS (Windows Internet Name Service)
advanced configuration, 236
and broadcast name resolution, 218
and dial-up TCP/IP, 223
and NetBIOS nodes, 139
described, 214
in a routed environment, 218
name registration, 220
name release, 220
name renewal, 221
name resolution, 215, 219
DNS (Domain Name System), 214
methods, 215
NetBT, 214
NetBIOS, 215
policy, configuring, 141
proxy, 139, 222
roving user, 225
server
client network traffic, 224
configuring, 228
defined, 138
performance, 227
planning, 223
pull partner, 238
push partner, 237
Registry parameters, 236
replication partner Registry parameters, 236
replication partners, configuring, 230
replication planning, 226, 227
viewing database, 235

viewing status, 235
wide area networks, 226
WINS database
backing up, 239
cleaning up, 240
compacting, 239
management, 239, 240
name resolution services, described, 214
restoring, 239