SunLink™ Server Administration Guide

Beta Draft

A printable PDF version of this document is available on the `doc` *folder located on the product CD.*

Please
Recycle

Adobe PostScript™

Contents

Tables

Introduction to SunLink Server Administration

The SunLink™ Server 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 SunLink Server program administrator.

About Your New Server

SunLink Server 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, or mixed-client environment.

As a server within a LAN, a Sun computer with SunLink Server software installed provides file, print, authentication, 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, SunLink Server software works like a native NT server in network "neighborhoods" that include systems running Windows NT Server, Windows NT Workstation, Windows 95, Windows 98, and Windows for Workgroups (Windows 3.11).

SunLink Server features are those of Windows NT Server 4.0. This ensures compatibility with Microsoft networking features and desktop environments while also taking advantage of the Solaris operating environment's abilities to function simultaneously as a file, print, and communications server.

SunLink Server networking services are functionally equivalent to those offered by Windows NT Server. Among these services:

■ Windows NT PDC and BDC functionality

1. SunLink Server software incorporates AT&T's Advanced Server for UNIX Systems.

- Microsoft Remote Procedure Calls (RPCs)
- NT Directory Services (NTDS)
- NT Registry
- Microsoft-compatible file Access Control Lists (ACLs)

In addition, SunLink Server 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, multi-user 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 SunLink Server software is the Solaris operating environment. A SunLink Server system 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 SunLink Server computer on the network, users of Windows-based client computers won't notice that their network services are being provided by a Solaris, rather than Windows NT, server. Their 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 administration tasks that you ordinarily perform. But the presence of the SunLink Server computer in your Windows NT network does mean that you have one additional role that is not the same as Windows NT administration: SunLink Server administration.

The difference between administration of the SunLink Server computer on your network and the Windows NT network services *provided by* the SunLink Server computer is both critical and occasionally subtle.

For example, a native Windows NT server can be set up as a Windows Internet Naming Service (WINS) database server that resolves client computers' IP addresses to their host names. 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 SunLink Server computer 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 Windows NT and SunLink Server administrative duties:

- **Windows NT network administration** – Modifying the parameters of the WINS database—assigning a different name to an IP address, for example

- **SunLink Server computer administration** – Managing the integrity of the WINS database by compacting it

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

Similar to the WINS server example, you will find new administrative duties here that are closely related to, but importantly different from, many of your ordinary Windows NT administration tasks. This guide covers all of them; conversely, this guide *does not provide instructions for any Windows NT network administration tasks*.

NT Administration Tools Overview for Experienced Solaris System Administrators

You may be an experienced administrator of a Microsoft Windows or 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 next, "The SunLink Server Manager or Command Line: Your Choice" on page 19.

For administrators of a Solaris network, however, this section is a summary of the NT administration tools that make it possible to carry out your NT network responsibilities. Becoming familiar with the functions of these tools will help you discern the difference between an NT network administration task and a SunLink Server administration task.

Nearly all NT network administration tasks are carried out by way of several graphical user interface (GUI) tools. A SunLink Server computer can operate and be administered regardless of whether Windows NT is running on the network. However, client-based network administrative tools running on Windows NT Workstation and Windows 95 client computers enable remote administration of the NT services provided by a SunLink Server system.

To perform NT network administration tasks on a SunLink Server computer from a Windows NT computer, you install Windows NT administrative tools. And, to administer NT tasks on a SunLink Server computer from a Windows 95 client computer, you install Windows NT Server Tools.

Remote administration is supported for all network functions. Both Windows NT Administrative Tools and Windows NT Server Tools program groups are available in the SunLink Server installation package.

All of the GUI-based tools for NT network administration feature on-line help.

Among the most important and most commonly used NT administration tools, and the common administrative tasks associated with them, are the following. (Depending on which program group you use and which 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

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 will be established for them by the NT server at logon. This environment and various other user attributes are maintained by way of the *User Manager for Domains* tool.

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.

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 creation, deletion, alteration, naming, and disabling
- Creating and modify a path to the user's profile
- Creating logon scripts for users and specify 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

Server Manager

NT network resources—such as 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. Shares and other server-based resources are managed and administered 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 NT Directory Replicator service
- Specifying path names for logon scripts (script file names are specified by way of User Manager for Domains)
- Setting up and managing import and export computers
- 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) that requires user notification. 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 NT tool called *Event Viewer*, you can troubleshoot various hardware and software problems, and monitor NT security events. You also can archive logs in various file formats.

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

- Traps and displays 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 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 SunLink Server computers, 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 and Windows 95, 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 NT or SunLink Server computer on the network. These are called *roaming* user profiles.

As an administrative 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 NT tools available to many administrators include *WINS Manager*, *Registry Editor* (Regedit32), *Disk Administrator*, *Performance Monitor*, and a *Backup* utility. Detailed information about these and the previously described NT tools, as well as instructions for using them, are included in the tools' on-line help and your NT network documentation.

The SunLink Server Manager or 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 administration tasks directly on your Solaris system-based SunLink Server computer.

Suiting your background and preferences, SunLink Server administration provides a clear choice of methods: by way of a graphical user interface or the Solaris command line. This guide provides instructions on how to accomplish any administrative task on a SunLink Server computer by either method.

SunLink Server Manager GUI Tool

Fitting comfortably within a Windows NT and Windows environment, in which most routine and complex tasks are accomplished by way of GUI-based tools, is the SunLink Server GUI-based administration tool, SunLink Server Manager, shown below.
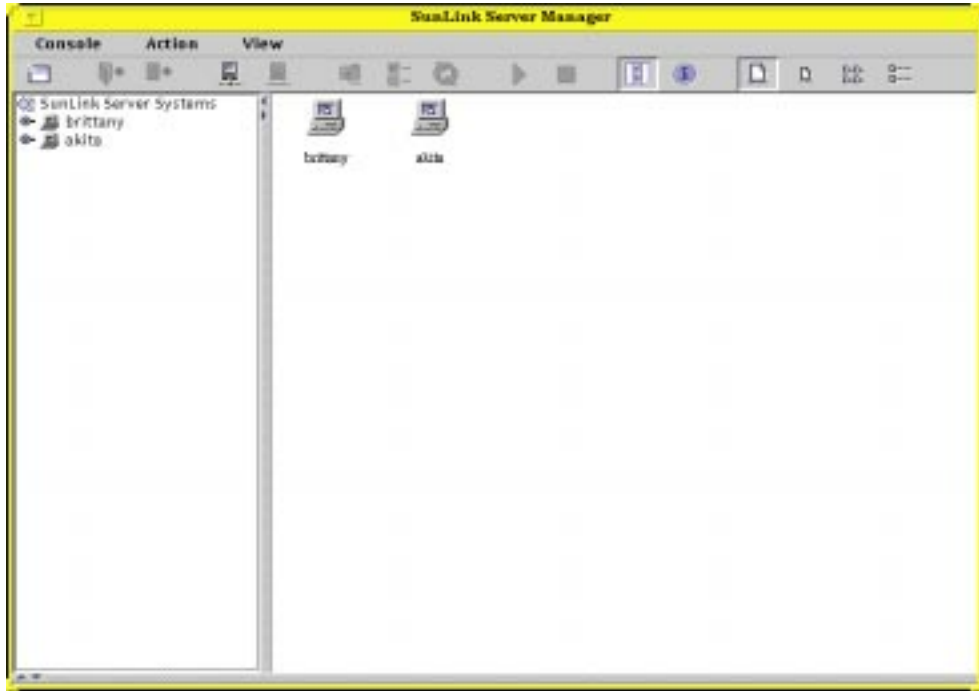
All Administration Duties Covered

You can manage all aspects of SunLink Server administration, which is distinct from Windows NT network administration, by way of SunLink Server Manager—a distributed client-server application based on Sun's Java™ programming language. You install the server portion of SunLink Server Manager on the SunLink Server computer, and the client portion on a Solaris, Windows NT 4.0, or Windows 95 client.

Among the most common and most important administration tasks and concerns for which SunLink Server Manager is useful:

■ **Logon and logoff** – To administer a SunLink Server computer from a remote client, you must have special user permissions (known as *root* in the Solaris and UNIX world). SunLink Server Manager enables you to do this.

- **Server startup and shutdown** – The SunLink Server software includes a set of Solaris server processes that enables the computer to act as a Windows NT network server. SunLink Server Manager alerts you when you are attempting a task that requires shutdown of the SunLink Server program, informs you about whether the server is running, and enables you to start and stop the program without having to invoke any special Solaris commands.

- **Domain Configuration** – SunLink Server Manager covers all SunLink Server domain configuration tasks, including naming the server and the domain, and specifying it as a PDC or a BDC.

- **Policy configuration** – SunLink Server Manager enables you to change various server policy parameters that are special to the SunLink Server computer, and provides context to help you understand the ramifications of policy changes that you put into effect.

- **Event management** – The SunLink Server Manager's Events view, much like the Windows NT Event Viewer tool, enables you to check a variety of events related to SunLink Server operations.

- **Database management** – SunLink Server Manager enables you to manage and maintain the integrity of various Windows NT-related databases that are stored on your SunLink Server computer—backing up and restoring them, for example. (Altering the content of these databases is a Windows NT administrative function, and not a SunLink Server administration function.) Among the databases that you can manage with SunLink Server Manager are the Access Control List (ACL), Registry, and Securities Account Manager (SAM).

- **NetBIOS** – Using SunLink Server Manager, you can set NetBIOS policies, including configuring the service as a WINS proxy.

- **User Account Migration** – With this feature of SunLink Server Manager, you are able to maintain a consistent identity for each user on your network who has both Solaris and Windows NT accounts.

- **Printing** – SunLink Server Manager includes a wizard that enables you to set up a Solaris printer, the first step toward setting up print services on a SunLink Server network.

- **On-line Help** – Detailed instructions for all tasks covered by SunLink Server Manager are available.

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 prompt you can type in 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 SunLink Server administration, see Chapter 2. That chapter also provides general explanations of the use of Solaris commands to administrators whose Solaris experience is limited.

A Note About the Format of This Guide

Because SunLink Server software offers both the SunLink Server Manager and the command line methods of administration, this guide will frequently give instructions on how to perform tasks by way of both methods, with the SunLink Server Manager method described first.

After SunLink Server Manager instructions appear for any given task, the equivalent command-line method appears.

CHAPTER **2**

Administering SunLink Server Software at the Command Prompt

This chapter describes how you can use SunLink Server commands, the Net commands, and `lanman.ini` file editing to administer your SunLink Server computer at the Solaris system console. It contains the following information:

- SunLink Server Commands – This section describes the Solaris system commands that you can use to administer your SunLink Server computer at its command prompt. (SunLink Server commands are installed in the `/opt/lanman/bin` and `/opt/lanman/sbin` directories. Exceptions are `euctosjis`, `lmshell`, and `sjistoeuc`, which are installed in the `/usr/bin` directory, and `makeclients`, which is installed with the `MSCLIENT` share.)

- Net Command – This section lists the Net commands that are available to administer your SunLink Server computer at its 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.

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

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

TABLE 2-1   Command Line Interface Tasks

Task...	...is on
How to Change a `lanman.ini` File Parameter	page 36
How to Administer a Local SunLink Server Computer	page 26
How to Administer a Remote SunLink Server Computer	page 26

About SunLink Server Commands

You can use Solaris system commands at the SunLink Server command prompt to perform several administrative tasks.

The following table lists the Solaris system commands that you can use. After making sure that your MANPATH variable is set to the proper value, you can find complete descriptions of each command by typing the following at the SunLink Server command prompt:

man *name of command*

The description lists the purpose and syntax of the command and provide comments and examples.

TABLE 2-2 Solaris Commands for SunLink Server Administration

SunLink Server Command	Description
acladm	Creates, checks, prunes, and removes the Access Control List (ACL) database.
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.)
blobadm	Displays statistical information, checks, and configures well-known or specified binary large object (BLOB) files.
delshmem	Deletes SunLink Server shared memory.
elfread	Displays event logs on the local SunLink Server computer at the Solaris system console.
euctosjis	Converts the coding of characters from Extended UNIX Code (EUC) to Shift-JIS (S-JIS) encoding.
joindomain	Moves a SunLink Server computer from one domain to another.
lmshare	Manipulates a SunLink Server share file without server intervention.
lmshell	Provides the "look and feel" of an MS-DOS shell at the SunLink Server 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 SunLink Server computer's shared memory.

TABLE 2-2   Solaris Commands for SunLink Server Administration

`mapuname`	Maps and unmaps SunLink Server user, global group, and local group names to and from Solaris system user names.
`netevent`	Sends administrative or user alerts, or printing alerts to users submitting print jobs.
`regcheck`	Manipulates the SunLink Server Registry to enumerate Registry keys, dump the contents of the Registry, or to check and repair Registry files.
`regconfig`	Queries or sets SunLink Server Registry key information.
`regload`	Creates a Registry file if one does not exist. Also reinitializes the Registry to system defaults.
`samcheck`	Checks or fixes the SAM database, or dumps the change log, built-in, account, or LSA databases.
`setdomainname`	Changes the domain name of the local SunLink Server computer.
`setservername`	Changes the name of the local SunLink Server computer.
`sjistoeuc`	Converts the coding of characters from Shift-JIS (S-JIS) to Extended UNIX Code (EUC) encoding.
`srvconfig`	Displays or modifies SunLink Server configuration information stored in the `lanman.ini` file.
`winsadm`	Configures the Windows Internet Name Service (WINS).

About the Net Command

You can perform many SunLink Server administrative tasks by using the Net command with any of its various options at the SunLink Server command prompt. Complete descriptions of the Net command options are in TABLE 2-4 on page 32.

The following sections summarize the Net command and its options that are available from the SunLink Server Solaris prompt, and describe syntax and usage conventions.

Administering Local and Remote Servers

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

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 SunLink Server command prompt.

However, to use the Net command to administer a remote SunLink Server computer, you must be logged in to the SunLink Server computer 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 work *only* at the SunLink Server command prompt of the server being administered.

▼ How to Administer a Local SunLink Server Computer

To administer a local SunLink Server computer using the Net command:

1. **Log in to the Solaris system that is running the SunLink Server software.**

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

   `net logon` *username password*

3. **Enter the appropriate Net command.**

   See a complete listing of Net command options in the section, "SunLink Server Net Command Options" on page 32.

Note – Remember to log off when you are finished administering the SunLink Server computer.

▼ How to Administer a Remote SunLink Server Computer

To perform server administration tasks using the Net command remotely, use the `net admin` command and the appropriate Net command for the task. (Note that Step 2 of the following procedure describes two ways of entering the `net admin` command.)

To enter a Net command remotely:

1. **Log in to the network as administrator or as a user with administrative privileges. (Operator privileges are not sufficient to perform this procedure.)**

2. **Enter the** `net admin` **command using one of the following methods:**

   - Enter 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.

   - Enter a `net admin` command followed by multiple Net commands. For example, to execute multiple Net commands on a 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 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.

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

Note – Net commands that take a domain or computer name as an option can be used 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`

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
```

You can also ask the SunLink Server computer to prompt you for your password, replacing the password with an asterisk (*) when you type the command.

Note – In the Solaris operating system, the asterisk (*) is a special character and must be preceded by a back slash (\ ).

For example, to use the same resource described above, type:

```
net logon jim \*
```

The SunLink Server software 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 SunLink Server software prompts you for it. Depending on the command that you type, the SunLink Server software also may 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 SunLink Server 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 SunLink Server prompts.

For example, if you use the `net logoff` command to log off the local area network with connections to remote shared resources intact, SunLink Server 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. For example, you are not prompted for confirmation when you type the following:

```
net logoff /yes
```

Using Abbreviations

The command reference pages in this chapter always use the full command names, command options, and service names. However, SunLink Server 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 SunLink

Server command, you must use an escape character (the back 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` on the Solaris system command prompt, you would type the following:

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

Some commonly used Solaris system special characters include the following: asterisk (`*`); semi-colon (`;`); pipe (`|`); square brackets (`[ ]`); parentheses [`( )`]; question mark (`?`); ampersand (`&`); caret (`^`); back 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 System Net Commands

The Solaris system uses a forward slash to separate names in a path. This is different from client computers, which use back 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 back slashes* – separate each element of the path with double back 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 single back slashes 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 computer operating systems, such as Windows 95 and Windows NT, use back slashes to separate names in paths. For example:

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

Understanding Command Syntax

Directions in man pages for using SunLink Server commands will be 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 slashes (/), back slashes (\), commas (,), double quotation marks (" "), equal signs (=), colons (:), semicolons (;), and asterisks (*) as they are shown.
- Replace the pound sign (#) with a number.
- At the Solaris system command prompt, you must type Net commands in *lowercase* letters.
- 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

On-line 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 SunLink Server system prompt:

TABLE 2-3   Help on Net Commands

Command	Descriptions
net help	Names of available Net commands.
net help *command*	Description, syntax and options for Net commands.
net *command* /help	Description, syntax and options for Net commands.
net *command* /?	Syntax only for Net commands.
net help *command* /*options*	Detailed description of the options of the command you selected.

SunLink Server Net Command Options

The following table includes descriptions of the SunLink Server Net command options that are available at the SunLink Server command prompt.

TABLE 2-4   SunLink Server Net Command Options

Command	Descriptions
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 an SunLink Server command or starts a command processor on a remote server.
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.

TABLE 2-4   SunLink Server Net Command Options

`net computer`	Displays or modifies the list of computer accounts in a domain. This command also can be entered as the following: `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 list of device names and controls shared printers. When used without options, this command displays the status of all shared printers at the specified server. When used with the *printername* option, this command displays only the status of the specified printer.
`net file`	Displays the names of all open shared files and the number of file locks, if any, on each file. This command also can be used to close shared files. When used without options, this command lists all of the open files at a server. This command also can be typed as `net files`.
`net group`	Adds, displays, or modifies global groups. This command also can be typed 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. This command also can be typed as `net localgroups`.
`net logoff`	Logs a user name off of the network.
`net logon`	Logs a user name in 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.

TABLE 2-4 SunLink Server Net Command Options

`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.
`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. This command also can be typed as `net sessions`.
`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.
`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 can be started are Alerter, Computer Browser, Directory Replicator, EventLog, Net Logon, Netrun, NvAlert, 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.

TABLE 2-4   SunLink Server Net Command Options

`net user`	Adds, modifies, or deletes user accounts or displays user account information.
`net version`	Displays version of network software currently running on the computer at which the command is issued.
`net view`	Displays 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 SunLink Server system configuration and performance. (Other configuration values are stored in the SunLink Server Registry, as well; see Appendix A.) The configuration values within the `lanman.ini` file are vital to the proper operation of the SunLink Server program, and editing this file is a task that should be performed *only by experienced administrators.*

When SunLink Server software is first installed, the `lanman.ini` file (`/etc/opt/lanman/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 SunLink Server 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.

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 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 into 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 `/`. If a path does not start with `/`, it is assumed to be relative to the `lanman` directory.
- If a numeric value begins with 0 it is octal; if it begins with X, it is hexadecimal; if it begins with a number 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
   ```

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

   The file is in the `/etc/opt/lanman` directory. 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 35.)

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

   For more information about the `srvconfig` command, type **man srvconfig** at the SunLink Server command prompt.

File Parameters

The following sections 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 2-5   {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 back 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 back 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.
clispooltime	The interval, in minutes, allowed for a job sent to a shared client printer to complete printing. If the printing has not finished by the end of this time, a warning message is sent to the server administrator. Values: 0 (no warning message) - unlimited; default: 20
country	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 (default—001)
dll_dir	The path to the directory containing message text files used by SunLink Server Solaris system commands. Default: `/opt/lanman/shares/asu/system32`
lang	Defines the character set that SunLink Server 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

TABLE 2-5   {Lmxserver} Section Parameters

Parameter	Description, Values, and Default Setting
listenqlen	Maximum number of client connection requests outstanding. If the server supports numerous clients that all attempt to connect to the server simultaneously, and some get refused, you should raise the value of this parameter. Only applicable if the listenname= parameter is being used. Values: 1 - unlimited; default: 3
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
lmgetmsg_path	Search order for message text files used by SunLink Server. 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.
mapaclblob	Configures whether to use memory-mapped file operations when accessing the SunLink Server Access Control List database. Values: yes, no; default: yes
mapchangelogblob	Configures whether to use memory-mapped file operations when accessing the SunLink Server Change Log database. Values: yes, no; default: no
maplsablob	Configures whether to use memory-mapped file operations when accessing the SunLink Server Local Security Authority database. Values: yes, no; default: no
mapregistryblob	Configures whether to use memory-mapped file operations when accessing the SunLink Server Security Accounts Manager database. Values: yes, no; default: no
mapsamblob	Configures whether to use memory-mapped file operations when accessing the SunLink Server 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

TABLE 2-5   {Lmxserver} Section Parameters

Parameter	Description, Values, and Default Setting
msgforward	Specifies if SunLink Server 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: (Vendor-specific)
nativeos	An additional field in the session setup request/response. Default: (Platform-dependent)
netaddonpath	The directory in which the SunLink Server program looks for dynamic libraries on startup. Dynamic libraries found in the directory are bound into the SunLink Server 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.)

TABLE 2-5 {Lmxserver} Section Parameters

Parameter	Description, Values, and Default Setting
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.
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 2-6 {Fsi} Section Parameters

Parameter	Description, Values, and Default Setting
fsaddonpath	The location of dynamic link libraries (DLL) 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

TABLE 2-6   {Fsi} Section Parameters

Parameter	Description, Values, and Default Setting
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 2-7   {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 2-8   {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 SunLink Server 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 SunLink Server command prompt. Values: any name of 1-15 characters; default: null
maxclients	Identifies the maximum number of simultaneous client sessions that the server must support. This number is set by default to a number that is equal to the SunLink Server user license installed on the server computer.
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`

TABLE 2-9   {Psi} section parameters

Parameter	Description, Values, and Default Setting
psaddonpath	The location of dynamic link libraries that support printer subsystems on the server. Values: A path up to a maximum of 256 characters; default: `/opt/lanman/lib/addon/psaddon`

Configuring and Managing SunLink Server Domains

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

Most tasks presented in this chapter can be accomplished in two ways: by using the SunLink Server Manager tool, and by typing commands at the SunLink Server system 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:

TABLE 3-1   Configuration and Management Tasks

Task...	...is on:
How to Start SunLink Server Manager	page 45
How to Log On, Using SunLink Server Manager	page 45
How to Log On from the Command Line	page 46
How to Log Off, Using SunLink Server Manager	page 47
How to Log Off, Using the Command Line	page 47
How to Start the SunLink Server Program	page 48
How to Stop the SunLink Server Program	page 49

TABLE 3-1   Configuration and Management Tasks

Task...	...is on:
How to Start SunLink Server from the Command Line	page 49
How to Stop SunLink Server from the Command Line	page 49
How to Start Individual Services	page 50
How to Stop Individual Services	page 50
How to Rename a Server or Domain	page 54
How to Move a Server to Another Domain	page 56
How to Change Computer Browsing Policy	page 69
How to Set up File Name Mapping	page 70
How to Edit NetBIOS Policy	page 71
How to Set Solaris File System Integration Policies	page 72
How to Use UPS Power Failure Notification	page 73
How to Edit User Account Mapping Policy	page 74
How to Authenticate SunLink Server Manager Users	page 75
How to Monitor Events	page 81
How to Monitor Events at the Command Prompt	page 82
How to View SunLink Server Status	page 83

About Logon and Logoff

To perform SunLink Server administration tasks, either from the SunLink Server console or from a remote client, you must be authorized by the server. Network resources are protected at several levels by different processes.

Some of your network 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 SunLink Server command prompt.

However, *remote* access to a SunLink Server computer 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 computer, it checks your user name and password against the computer directory database.

You can use SunLink Server Manager or the Solaris command line to log on to, or log off from, your SunLink Server system. Note that using the command line requires you first to log on to the Solaris system that hosts the SunLink Server program, and then to log on to the network with the `net` command.

▼ How to Start SunLink Server Manager

● **Do one of the following, depending on the computer you are using:**

  a. **Using a Windows system, select SunLink Server Manager from the "Programs" menu.**

  b. **Using a Solaris system, enter the following at the command prompt:**
     `/opt/lanman/sbin/slsmgr &`

▼ How to Log On, Using SunLink Server Manager

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

   a. **In the "Servers" list in the Navigation pane (left side) of SunLink Server Manager, click the name of any SunLink Server system; or**

   b. **Highlight a system name in the Results pane (right side) of SunLink Server Manager, and select "Log On..." from the Action menu.**

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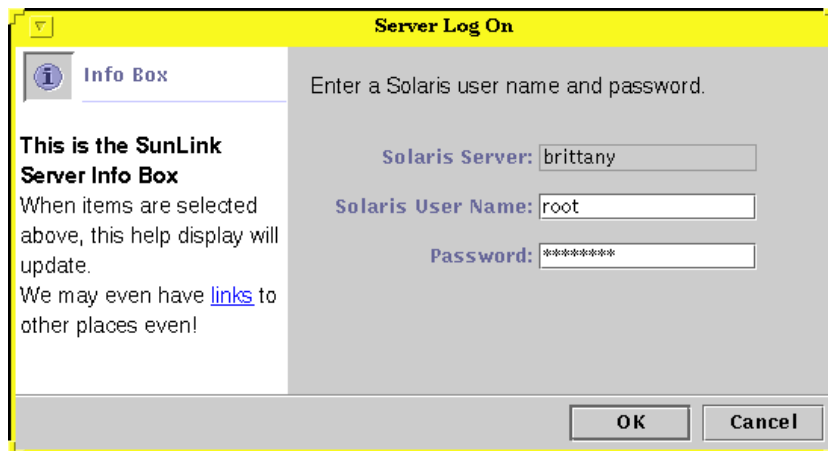
> **Note –** The Server Log On dialog box will also appear whenever you attempt to perform an administration task on a SunLink Server system to which you are not logged on. To make any changes, you must log on as root.

2. **In the boxes provided, type the user name `root` and root password.**

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

3. **Click OK.**

▼ How to Log On from the Command Line

1. **At the Solaris prompt of the system that hosts the SunLink Server program, enter the following command (note that the command ends with "in," not "on"):**

   ```
   system% login root
   Password:
   system#
   ```

2. **At the new system prompt, log on to the network as Administrator or as a user with administrative privileges by entering 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 administration tasks on any *remote* SunLink Server system, you must be logged on as a member of the Administrators group. Operator privileges are not sufficient for remote administration.

▼ How to Log Off, Using SunLink Server Manager

● **With the SunLink Server system name highlighted, select Log Off from the scrolldown list in the Action menu.**
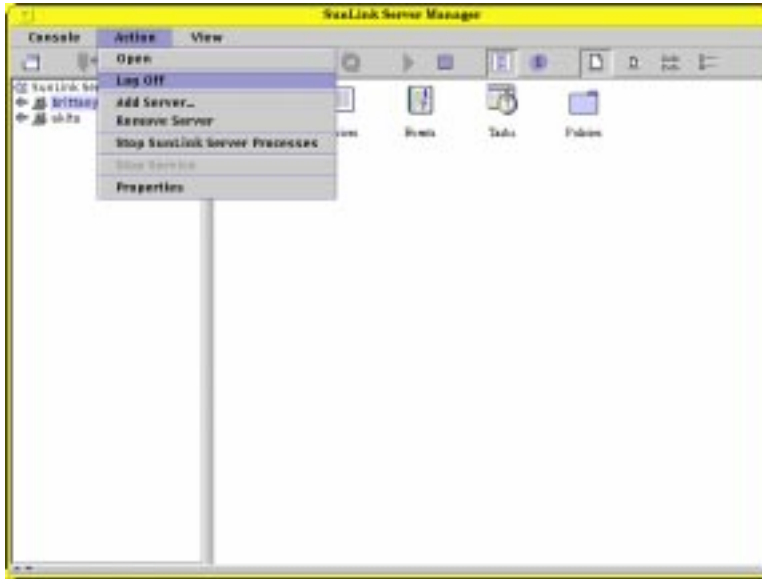
▼ How to Log Off, Using the Command Line

● **Enter the following command:**

system# **net logoff**

About Starting and Stopping Services

The SunLink Server program provides the following NT services:

- Alerter
- Computer browser
- Directory replication
- Event log
- Net logon
- Netrun
- WINS

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

In a native 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 service 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 SunLink Server software, only the Directory Replicator service logs on using a specific user account.)

To start and stop your SunLink Server program, as well as individual services that are specifically supplied by it, you use either SunLink Server Manager, the SunLink Server command line, or your Windows NT Server Manager.

▼ How to Start the SunLink Server Program

1. **Using SunLink Server Manager, log on to the system whose SunLink Server program you want to start.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, including starting the program, you must log on as root.

2. **With the name of the server highlighted, select "Start SunLink Server Processes."**

Note – SunLink Server Manager wizards for various administration tasks offer you the option of having the wizard itself shut down and start up SunLink Server processes. If you choose this option when using these wizards, you don't need to start up or shut down the processes manually.

▼ How to Stop the SunLink Server Program

1. **Using SunLink Server Manager, log on to the system whose SunLink Server program you want to start.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **With the name of the server highlighted, select "Stop SunLink Server Processes."**

> **Note –** SunLink Server Manager wizards for various administration tasks offer you the option of having the wizard itself shut down and start up SunLink Server processes. If you choose this option when using these wizards, you don't need to start up or shut down the processes manually.

▼ How to Start SunLink Server from the Command Line

1. **Log on to a SunLink Server computer.**

   For instructions, see "How to Log On from the Command Line" on page 46. To make any changes, you must log on as root.

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

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

▼ How to Stop SunLink Server from the Command Line

1. **Log on to a SunLink Server computer.**

   For instructions, see "How to Log On from the Command Line" on page 46. To make any changes, you must log on as root.

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

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

▼ How to Start Individual Services

1. **Using SunLink Server Manager, log on to the appropriate SunLink Server system.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **In the results pane, double-click "Services."**

   The Results pane changes, displaying a list of services and the current state of each.
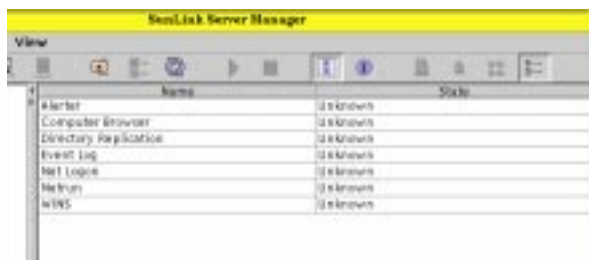
3. **Highlight the service that you want to start, then select "Start Service" from the Action menu.**
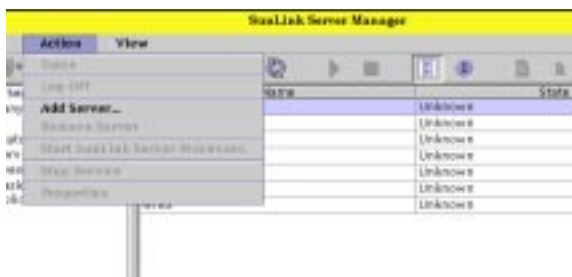
▼ How to Stop Individual Services

1. **Using SunLink Server Manager, log on to the system whose SunLink Server service you want to stop.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **In the results pane, double-click "Services."**

   The Results pane changes, displaying a list of services and the current state of each.
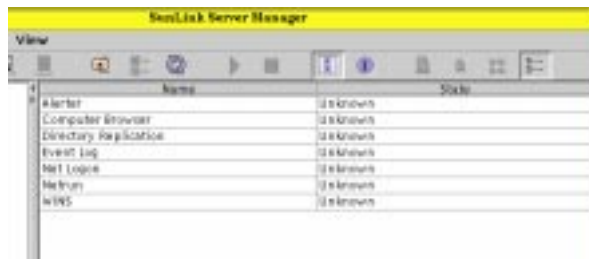
3. **Highlight the service that you want to stop, then select "Stop Service" from the Action menu.**

About Server 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 SunLink Server 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 SunLink Server system 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. If you were to configure a server as a primary domain controller in an existing domain, you'll wind up with *two* domains that have the same name, and neither would operate properly.

- **Backup domain controller (BDC)** – A BDC receives user account information from the primary domain controller and validates network logon requests. Using the 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.

When you installed your SunLink Server system, the installation program installed the system as a *primary* domain controller. As administrator, you can change the role of the server.

In addition to setting up the SunLink Server system as a PDC, the installation defaults specify:

- The server name is the host name of the Solaris system.
- The server domain name is *hostname*_dom.
- The default password for the Administrator account is password.

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 SunLink Server systems *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 primary domain controller; add, remove, and rename domain computers; and manage domain security, including account policy, audit policy, and trust relationships. (These Windows NT tools are also effective with the SunLink Server program.)

Adding, Renaming, Moving, and Removing SunLink Server Domain Computers

You created a new domain within your NT network when you installed the SunLink Server program and designated the system as a PDC. Other computers can be added to the domain.

Before a computer running SunLink Server, Windows NT Server, or Windows NT Workstation software can be a domain member and participate in domain security, it must be added to the domain. When a computer is added to a domain, the SunLink Server program creates a computer account for it. If the added computer is a BDC, it requests a copy of the domain directory database.

Adding a Domain Workstation or Server Computer

To add a computer 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 and servers to domains after installation.

To add a SunLink Server computer to a domain, you can use either SunLink Server Manager or the `joindomain` command. You must be a member of the Administrators or Account Operators group to reconfigure a SunLink Server computer to be a backup domain controller in an existing domain without reloading the server software. For this procedure to take effect, the primary domain controller must be running in the domain that is being joined.

Removing a Computer From a Domain

You can remove workstations, backup domain controllers, and member servers from a domain—but you cannot remove the primary domain controller until you promote a backup domain controller to a PDC.

When you remove a computer running Windows NT Workstation or Windows NT Server as a member server from a SunLink Server domain, use NT Server Manager to delete the computer's account from the directory database so that the computer cannot participate in domain security.

After a computer account has been removed from the domain, a user of the computer must move the computer to a new workgroup or domain using the Network option in Control Panel.

⚠ **Caution –** To remove a *native* Windows NT backup domain controller 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 backup domain controller that has been removed from a domain until you have reinstalled the operating system. A SunLink Server backup domain controller, however, does *not* need to be reinstalled.

Changing the Name of a Domain or Server

You can 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 the SunLink Server Manager tool or the `setdomainname` or setservername commands at the SunLink Server command line prompt. (For information about the commands, type `man setdomainname` or `man setservername` at the SunLink Server command prompt.)

Moving a Computer to a Different Domain

To change the domain to which a SunLink Server computer belongs, you use either the SunLink Server Manager tool or the `joindomain` command. (For information about the `joindomain` command, type `man joindomain` at the SunLink Server command prompt.)

To move a workstation or member server from one SunLink Server domain to another by way of the `joindomain` command, you must first remove the computer from the old domain and then add it to the new one. If you use the SunLink Server Manager tool, the removal is taken care of automatically.

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

▼ How to Rename a Server or Domain

1. **Using SunLink Server Manager, log on to the SunLink Server system whose domain name or server name you want to change.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **From the Action menu, select Properties.**

   An information window appears, listing the SunLink Server system's server name, the domain name, and the system's role in the domain—either PDC or BDC. If the system is a BDC, the name of the domain's PDC is also listed.

   Note – The SunLink Server Manager tool does not allow you to promote or demote the system to PDC or BDC within its *current* domain. You use the NT Server Manager tool for those tasks. If you are changing the system's domain, however, you may also designate its new role within the new domain. See the section, "How to Move a Server to Another Domain" on page 56.

   ---

3. **In the information window, click Change....**

   A Properties dialog box similar to the following appears.
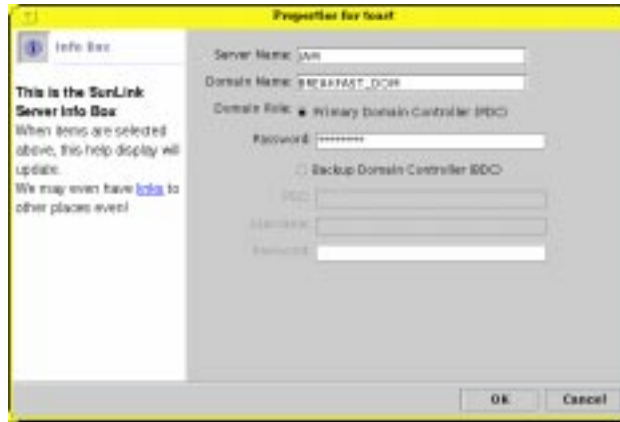
4. **In the appropriate text fields of the Properties dialog box, change the server name, the domain name, or both, according to the following guidelines:**

   ■ **Domain name** – To complete a change to the name of a SunLink Server domain, you must use this procedure on *every* SunLink Server computer 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. You must then reestablish existing trust relationships. While 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 and can contain any combination of the following characters:
   ```
   a-z A-Z 0-9 ~ ! # $ % ^ & _ ( ) . -
   ```

   ■ **Server name** – If you are changing the server name of a BDC, you must add the new computer account to the directory database before deleting the old computer account from the directory database by way of the NT Server Manager (see NT Server Manager's on-line help for instructions).

   Note that merely changing the name of the server does not permit you also to change its role.

5. **Enter the required PDC/BDC, user name, and password information into the appropriate text fields, according to the following guidelines:**

   ■ **Domain name** – When you change the name of the server's domain, you must indicate what role it will serve in the new domain: PDC or BDC. If PDC, click the button next to "Primary Domain Controller (PDC)" and furnish the *new* Administrator password. If BDC, click the button next to "Backup Domain Controller (BDC)," enter the name of the PDC in the new domain, and furnish the PDC's Administrator account user name and password.

■ **Server name** – If you are only changing the name of the server, enter the new name and leave all other text fields as is.

6. **Click "OK" to proceed, or click "Cancel" to abandon the procedure and leave the server name and domain name unchanged.**

If you continue the procedure by clicking "OK," the system will display an alert notifying you that the SunLink Server program must be restarted for the changes to become effective:

7. **Choose whether to have the SunLink Server Manager tool restart the program automatically and immediately ("Restart Now"), whether to restart it yourself at another time ("Restart Later"), or whether to cancel the entire operation.**

If you choose "Restart Now," the SunLink Server program will be stopped and then started automatically. If you choose "Restart Later," remember to stop and start the SunLink Server program for your name changes to take effect (see "How to Stop the SunLink Server Program" on page 49 and "How to Start the SunLink Server Program" on page 48 for instructions).

▼ How to Move a Server to Another Domain

1. **Using SunLink Server Manager, log on to the SunLink Server system whose domain name or server name you want to change.**

For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **From the Action menu, select Properties.**

An information window appears, listing the SunLink Server system's server name, the domain name, and the system's role in the domain—either PDC or BDC. If the system is a BDC, the name of the domain's PDC is also listed.

Note – The SunLink Server Manager tool does not allow you to promote or demote the system to PDC or BDC within its *current* domain. You use the NT Server Manager tool for those tasks. But by changing the system's domain name—and therefore assigning it to a new domain—you can also designate its new role within the new domain.

3. **In the information window, click Change....**

   A Properties dialog box similar to the following appears.
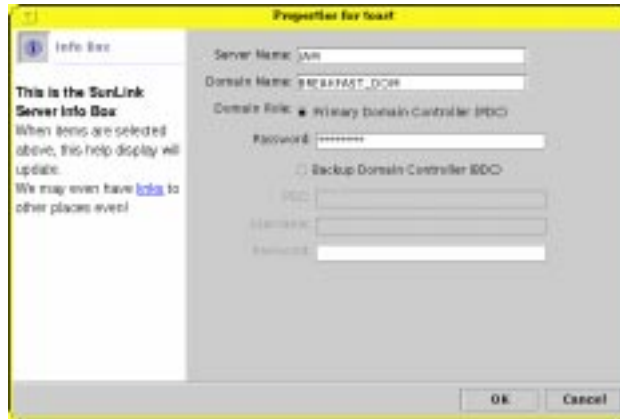
4. **In the appropriate text field of the Properties dialog box, change the server's domain name according to the following guidelines:**

   ■ By changing the domain name of the server, you are effectively reassigning it to the domain whose name you enter.

   ■ 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 and can contain any combination of the following characters:
   `a-z A-Z 0-9 ~ ! # $ % ^ & _ ( ). -`

5. **Enter the required PDC/BDC, user name, and password information into the appropriate text fields, according to the following guidelines:**

   ■ When you change the server's domain, you must indicate what role it will serve in its new domain: PDC or BDC.

     ■ **If PDC**, click the button next to "Primary Domain Controller (PDC)" and furnish the password. Note that you cannot assign more than one PDC to a single domain; you must demote the former PDC to a BDC when creating a new PDC.

- **If BDC**, click the button next to "Backup Domain Controller (BDC)," enter the name of the PDC that exists in the new domain, and furnish the PDC's Administrator account user name and password.

6. **Click "OK," or click "Cancel" to abandon the procedure and leave the domain name unchanged.**

   If you continue the procedure by clicking "OK," the system will display an alert notifying you that the SunLink Server program must be restarted for the changes to become effective:

7. **Choose whether to have the SunLink Server Manager tool restart the program automatically and immediately ("Restart Now"), whether to restart it yourself at another time ("Restart Later"), or whether to cancel the entire operation.**

   If you choose "Restart Now," the SunLink Server program will be stopped and then started automatically. If you choose "Restart Later," remember to stop and start the SunLink Server program for your domain name change to take effect (see "How to Stop the SunLink Server Program" on page 49 and "How to Start the SunLink Server Program" on page 48 for instructions).

About Managing Policies

You can define the following seven sets of SunLink Server policies:

- Computer browsing
- File name mapping
- NetBIOS
- Solaris file system security and permissions
- UPS power failure notification
- User account mapping
- SunLink Server Manager security

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

■ User password (account)
■ Audit
■ Trust relationships

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. Users of network client computers are viewing this list when they look at their Network Neighborhood. A *backup browser* also maintains a copy of the list, but is employed only in the event that the master browser fails.

Computer browsing policy in the SunLink Server program 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 is to be included in the system log.

File Name Mapping

On 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. And, while Windows NT Workstation and Windows NT Server users will see the long Solaris file name in a SunLink Server directory, users of client computers running Windows for Workgroups—which uses the MS-DOS 8.3 name convention—would not. To ensure access to all Solaris files by all users, the SunLink Server program provides *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.

Many Windows 3.1 and Windows for Workgroups users connecting to the file or directory over the network see the name in the 8.3 format; Windows NT Workstation and Windows NT Server users see the long name. (Note, however, that the SunLink

Server 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.)

SunLink Server name mapping also 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.

SunLink Server 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) is appended.
- The suffix (the characters following the tilde separator) is truncated to 3 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 name 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 server should support mixed-case file names should be considered carefully. Mixed-case support allows clients to have access to file names on Solaris systems that contain uppercase characters, but this feature has a negative impact on server performance.

It is inadvisable to switch frequently between 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 that are case-insensitively identical in the same directory. Although the Solaris system is case-sensitive, SunLink Server 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.

NetBIOS

NetBIOS is a session-layer interface used by applications to communicate. Its logical naming system permits computers' network interfaces to establish connections, and ensures reliable data transfer between computers once the connections exist.

Lana Numbers

LAN Adapter (Lana) numbers are part of the logical naming system established by NetBIOS. SunLink Server software assigns Lana numbers automatically to each network interface, choosing a number that is unique within the particular computer.

One NetBIOS LANA can be configured for each available network interface card. You should plan ahead to choose the particular network interfaces that you want to run NetBIOS LANAs.

WINS Servers

A Windows Internet Name Service (WINS) server is a machine that maintains a data base 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 93.

About WINS and NetBIOS Modes

By default, SunLink Server software brings up each network interface in Broadcast mode. 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 mode does not scale up well to large networks.

WINS servers use the NetBIOS Hybrid mode (h-mode). 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 mode. 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 entering 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 SunLink Server system running the WINS service, or another SunLink Server 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 SunLink Server 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-mode and h-mode NetBIOS nodes on the local subnet, and can cause unexpected name conflicts.

NetBIOS Scope

NetBIOS scope is a seldom-used feature that limits the computers that a particular network device can communicate with.

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 File System Security and Permissions

You can control the access that users have to files and directories on SunLink Server computers.

Directories and files can be secured by setting permissions on them. 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 SunLink Server 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 only to see it.

> **Note –** In the Solaris operating environment, Read permission is far more restrictive than the similarly named permission in the NT environment. In the NT environment, Read permission is advisory only—a user on an NT client machine would still be able to edit a nominally Read-only file. In the Solaris environment—the environment in which all SunLink Server 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 NT-style permissions, however. See "How to Set Solaris File System Integration Policies" on page 72 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 permissions to yourself only.
- **Group**—You can assign permissions for other users in your group to files and directories that you own. When your administrator creates your home directory, you are automatically assigned to the Solaris system group *other*, as are all others with home directories. This assignment enables you to share data easily with other network users, but prevents Solaris system users in different groups from reading or changing your files.
- **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 SunLink Server 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 SunLink Server 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 permission for an individual user does not override the access granted to the user through groups to which the user belongs.

Note – When you copy SunLink Server 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 they have been copied. 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.

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 SunLink Server 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 SunLink Server program enables you to regulate it.

File-locking is also an important security concern, particularly in your heterogeneous environment of NT and Solaris. While SunLink Server software accords the same file-locking security on network-based files and directories as NT does, locked files may still be accessible directly from a Solaris computer account. SunLink Server 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 NT and Solaris network client machines, you should change this setting to honor NT file-locking from Solaris accounts. See "How to Set Solaris File System Integration Policies" on page 72.

SunLink Server Manager Security

Another security consideration involves users' priviliges to administer the SunLink Server program by way of the SunLink Server Manager tool. You can choose settings that affect security on subsequent SunLink Server Manager sessions. Data Integrity 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 Authenticate SunLink Server Manager Users" on page 75.

UPS Power Failure Notification

You can send to all NT network users who are connected to a computer by using the "Send Message" command on the Computer menu in 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 SunLink Server Manager, you can warn users of server shutdown because of of power loss when the UPS service is available.

For alerts to be sent, the Alerter service must be running on the SunLink Server computer from which the alert is originated (see "How to Start Individual Services" on page 50). For client machines to receive the alerts, their Windows Messenger service must be running.

User Account Mapping

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

Having both SunLink Server 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 SunLink Server user account. Solaris system user accounts should be assigned to SunLink Server 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 SunLink Server user accounts ensures that Solaris system user accounts are created only when necessary. It also gives administrators complete control over the mapping of SunLink Server user accounts to Solaris system user accounts.

Solaris system user accounts can be created and assigned automatically to new SunLink Server user accounts by way of the SunLink Server Manager tool. See "How to Edit User Account Mapping Policy" on page 74. The Solaris system user account name that is assigned to the SunLink Server user account will be the same as or similar to the SunLink Server user account name. Differences can arise in cases of long, duplicate, or special character SunLink Server user account names.

If you were to map a SunLink Server user account to a non-existent Solaris system user account, or if the Solaris system account for a SunLink Server user is deleted, the SunLink Server user will not have access to any shared resources on the Solaris

system. To ensure that the SunLink Server 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 SunLink Server home directories with users' Solaris home directories.

User Account Management Utilities

SunLink Server software provides a pair of Solaris user account management utilities, called `passwd2sam` and `sam2passwd`.

passwd2sam

The `passwd2sam` user account management utility places user account information that is stored in a Solaris name service—such as FILES, NIS, and NIS+—into the SunLink Server Security Accounts Manager (SAM) database. If the SunLink Server system is configured as a BDC in an existing Windows NT domain, `passwd2sam` operations will transfer to the domain's PDC.

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

- It add Solaris user accounts into the SunLink Server Security Accounts Manager 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 delete Solaris user accounts from the SunLink Server Security Accounts Manager database. Solaris user accounts are deleted from the SunLink Server 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 SunLink Server 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 other user account management utility provided SunLink Server software is
sam2passwd. The sam2passwd user account management utility records SunLink
Server user accounts, writes out an /etc/passwd formatted file containing the
SunLink Server user accounts, and then adds the information to, or deletes it from, a
Solaris name service (FILES, NIS, NIS+).

The sam2passwd user account management utility supports two modes of
operation:

- It creates an /etc/passwd formatted output file containing non-privileged
  SunLink Server user accounts to add into a Solaris name service. This is the
  default mode of operation. If the SunLink Server system is configured as a BDC in
  an existing Windows NT domain, sam2passwd will create /etc/passwd
  formatted output files of the domain's PDC Security Accounts Manager database,
  for insertion into a Solaris name service.

- It finds SunLink Server user accounts that were created using sam2passwd and
  then subsequently deleted from the SunLink Server program, but that still linger
  in a Solaris name service.

You must format all input files to sam2passwd as /etc/passwd entries. See the
sam2passwd(1) man page for details on invocation options and arguments.

▼ How to Change Computer Browsing Policy

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server
   system whose browsing properties you want to change.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45.
   To make any changes, you must log on as root.

2. **Double-click Policies.**

3. **Double-click Computer Browsing.**

   The following screen appears:

4. **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.

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

   If you click OK to make any changes, SunLink 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 SunLink Server Manager, log on to, and then open, the SunLink Server system on which you want to set up or edit file name mapping policies.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Policies.**

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

   The following screen appears:

4. **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 are running Windows for Workgroups.

   - Check "Enable mapping to NT-style file systems" so that Solaris file names with characters that are invalid in NT are changed to "legal" characters.

   - Enter a new value in the "Suffix Separator" text field if you have reason to change the default; the separator is used to separate the main part of the file name from the file name's extension, such as "txt" or "doc."

   - Enter 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.

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

▼ How to Edit NetBIOS Policy

1. **TBS**

▼ How to Set Solaris File System Integration Policies

1. Using SunLink Server Manager, log on to and then open the SunLink Server system on which you want to set file system security and permissions policies.

For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. Double-click Policies.

3. Double-click Solaris File System Integration.

The following screen appears:
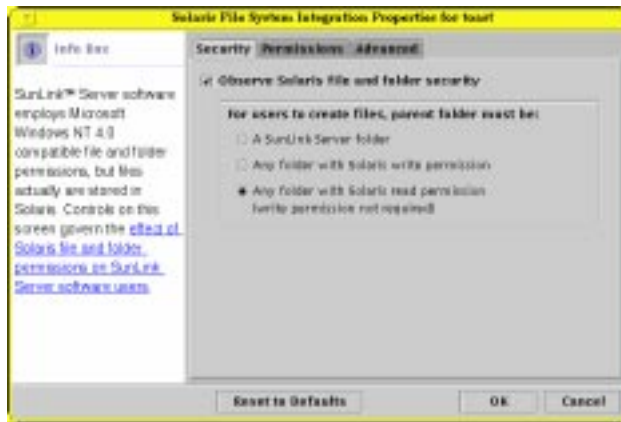
4. Set SunLink Server file creation policies according to the following guidelines, using the Security, Permissions, or Advanced tabs:

- Security – To establish policy for file creation within SunLink Server folders:

  - Least restrictive – Leave unchecked the "Observe Solaris file and folder security" option to set the least restrictive policies. With this option unchecked, SunLink Server software users can create files within SunLink Server folders even if the users have only Solaris "Read" permissions. Additionally, check "Any folder with Solaris read permission" if you want to enable SunLink Server software users with only Read permission to create files within SunLink Server folders that require Write permission.

  - Most restrictive – Check "Observe Solaris file and folder security" to create the most restrictive policy. Checking this option will require users to have Solaris "Write" permission to create a file within a SunLink Server folder. By checking this option, you also are presented two more options. Checking "A SunLink Server folder" requires that users have Solaris Write permission to create files within SunLink Server folders. Checking "Any folder with Solaris write

permission" eases the restriction by enabling SunLink Server software users to create files within SunLink Server folders regardless of permissions (in effect, it grants write permission to that 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.

- Advanced – To establish policies for ownership of NFS files (files created by way of the Solaris distributed file system), check the appropriate box to allow ownership by the file's creator or ownership by root. To cause SunLink Server software to observe NT file locking—thereby preventing users with Solaris accounts from accessing the locked files—check the box under File Locking. (Note that checking this box may slow down performance.)

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

▼ How to Use UPS Power Failure Notification

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server system from which you want to send a UPS power failure notice.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Policies.**

3. **Double-click UPS Power Failure Notification.**

   The following screen appears:

4. **Check "Send power failure messages."**

5. **Either select from the drop-down list, or type directly into the text field, the NetBIOS names of all the users or groups that you want to notify.**

   Select "All Users" if you want to send the message to everyone.

6. **Using the drop-down list, designate how often you want the notification to be repeated.**

7. **In the Message text field, type the message that you want to send.**

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

▼ How to Edit User Account Mapping Policy

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server system for which you want to establish or edit user account mapping policies.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Policies.**

3. **Double-click User Account Mapping.**

   The following screen appears:

4. **Establish or edit user account mapping policies according to the following guidelines:**
   - Check "Map new SunLink Server accounts to Solaris accounts" to create a Solaris account for a user simultaneously with the creation of his or her new SunLink Server account. If you have checked this option, you then have other options:
   - Choose the option of always creating a brand new Solaris account for the user, or using a Solaris account that exists for the user. Note that a Solaris account exists independently of both NT and SunLink Server systems.

- Choose whether to permit a user with a Solaris account to use that account independently of NT and SunLink Server software, by checking "Allow Solaris logons" or leaving it unchecked. If you choose to permit Solaris logons, use the "Solaris shell" text field to type in the name of the logon shell.

- Choose "Synchronize Home directories" for automatic synchronization of SunLink Server home directories with Solaris home directories.

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

▼ How to Authenticate SunLink Server Manager Users

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server system for which you want to establish SunLink Server Manager security policies.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Policies.**

3. **Double-click SunLink Server Manager Security.**

   The following screen appears:

4. **Check the box to require user authentication for SunLink Server Manager transactions and to invoke public key signatures to protect data that is passed between the server and clients.**

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

About Event Monitoring

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 every time you start the SunLink Server program. With an event log displayed by the SunLink Server Manager tool, you can troubleshoot various problems and monitor SunLink Server security events.

SunLink Server software records events in the following types of logs:

- The *system log* contains events logged by SunLink Server 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 SunLink Server program.

- The *security log* can contain valid and invalid logon attempts as well as events related to resource use, such as creating, opening, or deleting files or other objects.

- The *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.

SunLink 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:

Information	Meaning
Date	The date the event occurred.
Time	The time the event occurred.

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.
Computer	The name of the computer on which the event occurred.
Event ID	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 can be used by product support representatives to troubleshoot system problems.
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.
Type	A classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log. In SunLink Server Manager's normal list view, these are represented by symbols.
Category	A classification of the event by the event source. This information is used primarily in the security log.

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 SunLink Server Manager logs indicate the event types:

Event Type	Meaning
Error	Significant problems, such as a loss of data or loss of functions. For example, an Error event might be logged if a service was not loaded during SunLink Server startup.
Warning	Events that are not necessarily significant, but that indicate possible future problems. For example, a Warning event might be logged that 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 might 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 might be 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 might be logged as a Failure Audit event.

Additional Data

The data field contains binary data that can be displayed in bytes or words. 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.

Using SunLink 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 SunLink Server Manager.
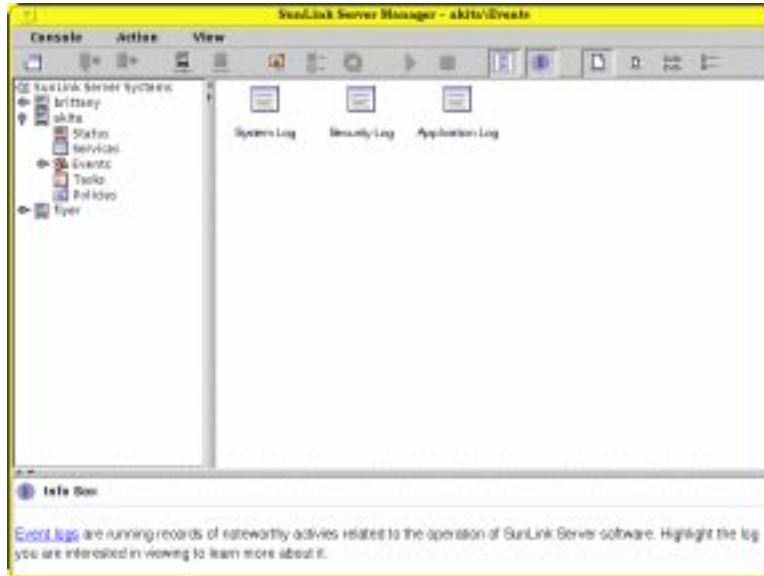
Selecting a Log

Double-click the appropriate log icon for event viewing. Although the logs for the local computer appear the first time you start SunLink Server Manager, you can choose to view the logs of any SunLink Server computer after you have logged on to it.

Refreshing the View

When you first open a log file, SunLink 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 the Refresh command from the View item on the menu bar.

Viewing Specific Logged Events

After you select a log to view in SunLink Server Manager, you can perform the following tasks:

- View descriptions and additional details that the event source logs.
- Sort events from oldest to newest or from newest to oldest.
- Filter events so that only events with specific characteristics are displayed.
- Search for events based on specific characteristics or event descriptions.

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 NT tools. You do not use SunLink Server Manager to set audit policy; therefore, this guide does not include 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 application software. If an 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:

- Archive logs in log format. The binary data associated with an event is discarded if you archive data in text or comma-delimited format.
- If a particular event seems related to system problems, try searching 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. This number can be used by product-support representatives to understand what occurred in the system.

Monitoring SunLink Server Security Events

You enable auditing from the NT User Manager for Domains Auditing Policy dialog box. Through auditing, you can track SunLink Server 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 NT User Manager for Domains tool.

The Audit policy determines the amount and type of security logging that SunLink Server 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 (accessed through Explorer) to specify which files are audited and what type of file access is audited for those files.

▼ How to Monitor Events

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server system whose event logs you want to view.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Events.**

The following screen appears:
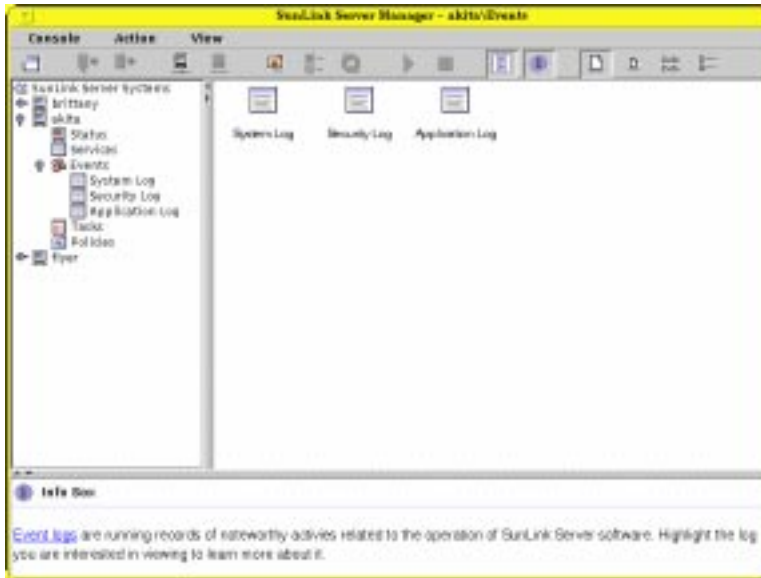
3. **Double-click the name of the log that you want to view.**

4. **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 76.

▼ How to Monitor Events at the Command Prompt

You can use the SunLink Server `elfread` command to read system, security and application logs. This command is especially useful when troubleshooting an SunLink Server system that has failed to start. (Events of this type typically are written to the system log.) The `elfread` command should be used as a backup to the SunLink Server Manager, which is the recommended method of viewing log files when the server is running.

● **At the SunLink Server command prompt, type the following:**

   `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 SunLink Server Status

1. **Using SunLink Server Manager, log on to, and then open, the SunLink Server system whose status you want to view.**

   For instructions, see "How to Log On, Using SunLink Server Manager" on page 45. To make any changes, you must log on as root.

2. **Double-click Status.**

   The following screen appears:
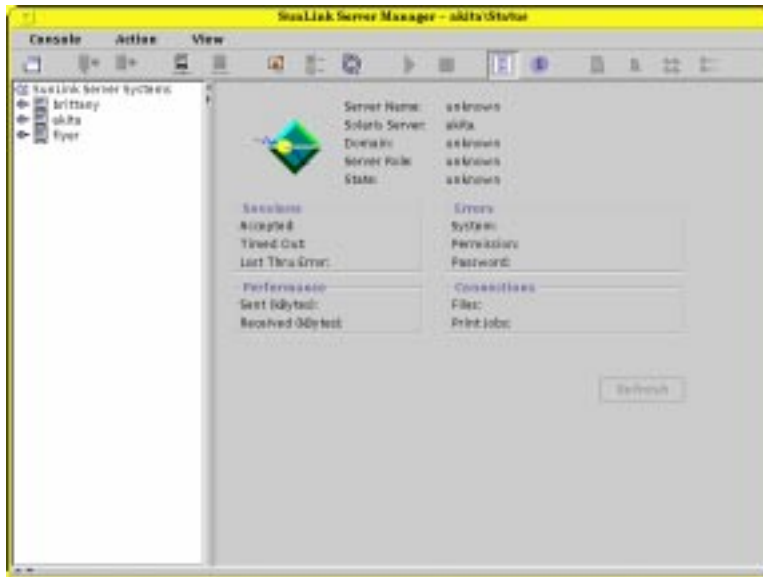
   The statistics displayed in the Status view are current, though not automatically updated. To update the view with the most recent statistics, choose Refresh from the View menu, or click the Refresh button.

Setting Up Printing Services

With a SunLink Server computer installed in your network, it won't matter whether Windows or Solaris clients send their jobs to the printers that it serves. The SunLink Server computer will recognize and process both types.

This chapter tells you how to set up a SunLink Server computer as a print server, and offers background information that will help you keep printing tasks running smoothly. The process for setting up a Solaris printer to work in the network comprises three groups of tasks:

■ Task 1 – Setting up the printer as a Solaris printer
■ Task 2 – Designating the printer as a SunLink Server shared printer
■ Task 3 – Making the new printer available to network clients

You need to perform the first two setup tasks only once per printer, and you use the SunLink Server Manager tool for the Solaris portion of the work. For the final two setup tasks, you use Windows tools. The final task, making the new printer available to clients, requires that each client machine user add the printer.

About SunLink Server Printing Services

SunLink Server printing offers the following features:

■ Clients can browse the network for available network printers. The browsing function is available from Network Neighborhood, the Add Printer Wizard, and from the Print Setup wizard of Windows NT and Windows 95 applications.

■ As an administrator, you can administer SunLink Server 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 and Windows 95 client computers to enable them to use a SunLink Server print server; this installation happens automatically because the driver is installed on the printer driver share.

If all printing clients are running Windows NT or Windows 95, it only is necessary to install printer driver files in one place — at the SunLink Server print server.

■ Clients can print to all networked printers that have their own direct Ethernet interface and have been configured as SunLink Server system printers.

SunLink Server Printing Terms

In SunLink Server terminology, a *shared printer queue* is the mechanism through which a collection of printer 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 serial or parallel port), to the network (via a network adapter card), or to a client computer on the network.

The Solaris operating system, which your SunLink Server computer runs, provides *LP Printer* functionality which mediates between the SunLink Server system, which sends clients' print requests to the LP service, and the print devices to which the LP service directs the requests. Users access printers 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 print share), when it will go, and various other aspects of the printing process.

In SunLink Server terminology, the shared printer queue is the software interface between the application and the print device. When you administer a SunLink Server 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 or PCL. 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 SunLink Server program supports all of the printer devices that are supported by the local spooling system. The *local spooling system* is the process that runs on the SunLink Server computer'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.

SunLink Server Network Printing

The SunLink Server program supports true network printing. When Windows NT and Windows 95 clients connect to a correctly configured SunLink Server print server, the printer driver is automatically installed on the client computer.

If you install a newer or different printer driver on a SunLink Server computer or a Windows NT or Windows 95 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.

Combining File and Print Services

When you use a SunLink Server computer for both file- and print-sharing, file operations have negligible impact on printers that are attached directly to the server; parallel and serial ports are always the greater bottlenecks. A dedicated print server may be desirable if a server is required to manage many frequently used printers.

The decision to combine print and file servers may depend on security concerns. While printers always should be available to users, you may want to restrict physical access to the servers by keeping them in secured rooms.

Setting Up SunLink Server Printing

Establishing a printer as a SunLink Server shared printer involves three groups of tasks:

- Configuring the printer as a Solaris printer
- Designating the printer as a shared SunLink Server printer
- Making the new printer available to individual clients

The groups of tasks are covered in the sections, "Task 1 of 3– How to Configure a Solaris Printer" on page 86, "Task 2 of 3 – How to Set Up the Solaris Printer as a SunLink Server Shared Printer" on page 91, and "Task 3 of 3 – How to Make the SunLink Server Printer Available to Windows Clients" on page 92.

This chapter presents steps for accomplishing each group of tasks by way of the SunLink Server Manager tool and the Solaris command line, with SunLink Server Manager steps presented first.

Note – Configuring a printer by way of the Solaris command line is recommended for experienced Solaris system administrators only. If you do not fit that description, you are advised to use the SunLink Server Manager method only.

▼ Task 1 of 3– How to Configure a Solaris Printer

1. **Using the SunLink Server Manager tool, log on to a SunLink Server computer.**

   In the following examples, the server "Basset" is a SunLink Server computer.

2. **Double-click "Tasks" in the Results Pane, and then double-click "Install Solaris Printer."**

   The opening screen of the Install Solaris Printer wizard appears, asking you to designate a name for the new printer.

3. **Type a name for the new printer into the provided field.**

   The name you choose will be its Solaris queue name. A printer name must be between one 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 onto Step 2 unless at least one character has been entered.

   The printer name you enter is checked against all existing Solaris printer names. If you enter the name of an existing printer, a screen similar to the following (with the actual name you chose inserted after "Printer") will appear asking for confirmation.

   (If you do not see the "Confirm Printer Configuration Change" screen, continue with Step 4.)

   If you intended to change the configuration of an existing printer, choose "OK." 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, "CANCEL." This will return the screen for naming the new printer, and you can enter a different name and proceed to the next step.

4. **Click "Next."**

   The following screen appears, requesting information about the printer's local or network status.

5. **Choose whether you are installing 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 SunLink Server network printer, it must be equipped with an Ethernet adaptor and be plugged directly into the network. A local SunLink Server printer must be plugged directly into the SunLink Server system.

Note – If you are running the 2.5.1 version of the Solaris operating environment, you must not attempt to set up the printer as a network printer, because it is not supported by the SunLink Server program. If you are running Solaris version 2.5.1, you can choose the "Local printer" option only.

Depending on which choice you make, complete one of the following two steps.

6. **If you chose "Network printer," skip this step and go on to Step 7. If you chose "Local printer," use the ensuing screen to indicate the correct port, then continue with Step 8.**

7. **If you chose "Network printer," use the ensuing screen to enter 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 chose in Step 3. If you have reason to identify the printer by a different name on the network, delete the default name and enter 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. The following tables may also be useful if you do not want to choose the generic driver. TABLE 4-1 lists common laser printer drivers.

TABLE 4-1 Common Laser Printer Drivers

If it is a...	Set it up as a...	Type this into the text field:
HPPCL (LaserJet) compatible	Hewlett-Packard LaserJet Plus	hplaserjet
35-font Plus font set or superset PostScript	Generic PostScript	(Use the default.)

10. **Click "Next."**

11. **Review and confirm the configuration choices that are summarized in the ensuing screen.**

    Make sure that your choices are accurately reflected. Click "Back" to change any of the configuration details that you want.

12. **Click "Finish."**

The following screen appears.
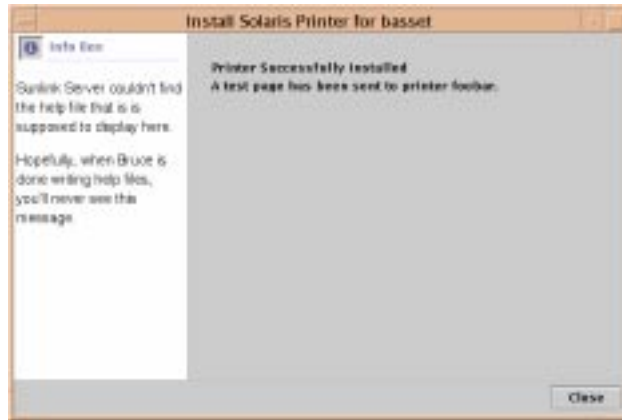
13. **Check test to be sure that the PostScript output is correctly printed.**

A test page is sent off to the printer after it has been properly installed. 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 has been 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).

Your Solaris printer is now set up as a SunLink Server printer available on your Windows NT or mixed network.

▼ Task 2 of 3 – How to Set Up the Solaris Printer as a SunLink Server Shared Printer

1. **From a Windows NT workstation, use Network Neighborhood to open the SunLink Server system that you are using as the Solaris print server.**

2. **Open the Printers folder.**

3. **Use the Add Printer wizard to add the SunLink Server (Solaris) printer.**

Note that to share a 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 SunLink Server Printer Available to Windows Clients

● **Use each Windows-based client's Add Printer wizard to add the SunLink Server shared printer.**

Implementing WINS and Maintaining Databases

This chapter provides detailed background information about the Windows Internet Name Service (WINS) that SunLink Server software incorporates, and considers important performance issues that can help you plan your network's implementation of WINS. Major sections dealing with such issues include:

- "About WINS and Its Function" on page 93
- "About Name Resolution Services" on page 94
- "About WINS Server Planning" on page 103

This chapter also describes how to maintain all databases—including WINS, the Access Control List (ACL), the NT Registry, the Securities Account Manager (SAM), the Binary Large Object (BLOB), and Share File—on a computer running the SunLink Server program. Major sections detailing these tasks include:

- "About Database Management" on page 119
- "Backing Up and Restoring the WINS Database" on page 119
- "Cleaning up the Databases" on page 120

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 SunLink Server systems is fully compatible with Microsoft WINS client implementations, including Microsoft TCP/IP-32 for Windows for Workgroups 3.11, Windows 98, Windows 95, Windows NT Workstation, Windows NT Server, and the Microsoft Network Client, Version 3.0.

SunLink Server WINS can replicate name databases with other SunLink Server WINS computers, and with WINS for Windows NT systems.

Note – You manage the NT functions of SunLink Server WINS by using the same Windows NT-based tool that you use to manage WINS for Windows NT. This allows both SunLink Server-based and Windows NT-based WINS servers to be managed from a single administrative tool on a single computer in the network. However, you use either the SunLink Server Manager tool or the SunLink Server command line to maintain the SunLink Server WINS database itself, as described in later sections of this chapter.

About Name Resolution Services

SunLink Server WINS with 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 SunLink Server or Windows NT setup.) To ensure that both names and IP addresses are unique, a computer using NetBIOS over TCP/IP registers its name and IP address on the network during system startup.

NetBIOS and DNS Computer Names

SunLink Server 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).

Fortunately, NetBIOS computer names are compatible with DNS host names, making interoperability possible between the two types of components. SunLink Server software combines the NetBIOS computer name with the DNS domain name to form the FQDN.

Note – In a SunLink Server 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:

- Windows Internet Name Service (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. (SunLink Server software does *not* use this method.)

- 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. Inthe SunLink Server 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 is the process used to register a unique name for each computer (node) on the network. A computer typically registers itself when it starts.

■ Resolution is 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 modes.

Defined within NetBT are modes that specify how network resources are identified and accessed. The NetBT modes supported by SunLink Server software are:

■ *b-node*, which uses broadcast messages to resolve names

■ *h-node*, which 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 DHCP users, the node type is assigned by the DHCP server. 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.

SunLink Server software can respond to b-node and h-node NetBT modes. (Windows NT supports all of the NetBT.)

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 SunLink Server 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 for Workgroups 3.11 uses a modified b-node system. 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

Windows networking clients (WINS-enabled Windows NT, Windows 98, Windows 95, or Windows for Workgroups 3.11 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 SunLink Server, 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.

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 automatically will be configured with WINS server information.

In a WINS and broadcast name resolution environment, a WINS-enabled client computer will behave in a different manner than a non-WINS-enabled client computer. These differences will be 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. During TCP/IP configuration, the client computer registers its name with the WINS server.

2. 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.

3. 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.

4. 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 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 95, 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 98, Windows 95, 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 remote access service servers that support PPP and/or SLIP connections, such as those that are available from CISCO, 3COM, and Bay Networks

Dial-up Windows 98, Windows 95, 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 98, Windows 95, and Windows NT computers that are configured to route TCP/IP and use WINS can access remotely their networks for services, including SunLink Server 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 can be supported per server varies according to usage patterns, data storage, and processing capabilities of the WINS server computer.

Planning for WINS server implementation on the network typically requires consideration of the issues presented in the following table.

TABLE 5-1   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, the location of routers on the network and the distribution of clients in each subnet should be considered 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 the following sections: "Planning for WINS Server Fault Tolerance" and "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 SunLink Server-based WINS client usually registers more NetBIOS names than other WINS-enabled clients. The name registration requests generated by a computer running under the SunLink Server 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. 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. The WINS database should be replicated 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 small 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 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 local-area-network 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 where many computers will go 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, one WINS server can be designated as the central server, and all other WINS servers can be configured 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.

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 5-2 WINS Server Time Interval Options

Configuration option	Description
Renewal Interval	Specifies how often a client reregisters its name. The default is six days.

TABLE 5-2   WINS Server Time Interval Options

Configuration option	Description
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.
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 5-3   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 SunLink Server WINS.)
Log Detailed Events	Specifies whether logging events is 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 5-3   WINS Server Advanced Configuration Options

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 propogating changes to all WINS servers. All released names are propogated 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.

A 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 check 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 serrver polls another server to get replicated information. This can begin when the WINS server is started, and is repeated based upon the configured update count or time interval, or by using WINS Manager to start immediate replication.

Replication alsi 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 to 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 5-4 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.

TABLE 5-4 Static NetBIOS Name-Mapping Types

Type option	Description
Domain	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 25 th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.
Internet group	Internet groups are user-defined groups that allow 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.

A WINS server can be configured to replicate only domain, Internet, and multihomed group to its replication partners. This is performed 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 and allow WINS clients to obtain.

TABLE 5-5 Basic WINS Server Statistics Descriptions

Statistic	Description
Server Start Time	The time when this WINS server was started.
Database Initialized	The last 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.

TABLE 5-5   Basic WINS Server Statistics Descriptions

Statistic	Description
Last Replication Times	The times at which the WINS database was last replicated
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 5-6   Detailed WINS Server Statistics Descriptions

Statistic	Description
Last Address Change	Indicates the time at which the last WINS database change was replicated.
Last Scavenging Times	Indicates the last times that the database was cleaned for specific types of entries.
Periodic	Indicates when the database was cleaned based on the renewal interval specified in **WINS Server Configuration (Local)**.
Admin Trigger	Indicates when the database was last cleaned because the administrator chose the **Initiate Scavenging** command.
Extinction	Indicates when the database was last cleaned based on the Extinction interval specified in the **WINS Server Configuration** dialog box

TABLE 5-6   Detailed WINS Server Statistics Descriptions

Statistic	Description
Verification	Indicates when the database was last cleaned based on the verify interval specified in **WINS Server Configuration**.
Unique Registrations	Indicates the number of name registration requests that have been accepted by this WINS server.
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. For information about groups, see "Managing Special Names" later in this chapter.
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 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 5-7   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 Extinct interval has expired	Marked *extinct*
Owned extinct names for which the Extinct timeout has expired	Deleted
Replicas of extinct names for which the Extinct 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 can be modified only through the 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 describes 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 subkey 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 default value of DoStaticDataInit to 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. This parameter can be set 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 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. SunLink Server Manager and various Solaris commands are the tools you use to maintain the databases; additionally, SunLink Server Manager enable you to schedule a routine for performing most database maintenance tasks automatically.

This following sections describe how to view, back up, restore, clean up, and compact the SunLink Server WINS database.

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 the Solaris command line on the SunLink Server computer to compact the database. See "How to Compact the WINS Database" on page 130.

Backing Up and Restoring the WINS Database

The following WINS server database files are stored in the `/opt/lanman/wins` directory. This directory was created when you installed the SunLink Server 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` and `wins.db` files in any manner.

You use the Solaris command line to back up and restore the database. You can also use the 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.

The local WINS database should be cleared periodically 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.

Database Maintenance Tasks

The following sections provided detailed instructions for scheduling and performing routine SunLink Server database maintenance tasks. You complete most of the tasks by using the SunLink Server Manager tool; however, some of the tasks require that you use the SunLink Server command line.

▼ How to Clean up SunLink Server Databases

1. **Using SunLink Server Manager, log on to and then open the SunLink Server computer on which you want to clean up one or more databases.**

2. **In the results pane, double-click "Tasks" and then double-click "Clean Up Databases."**

The resulting screen presents a list of databases to clean up.
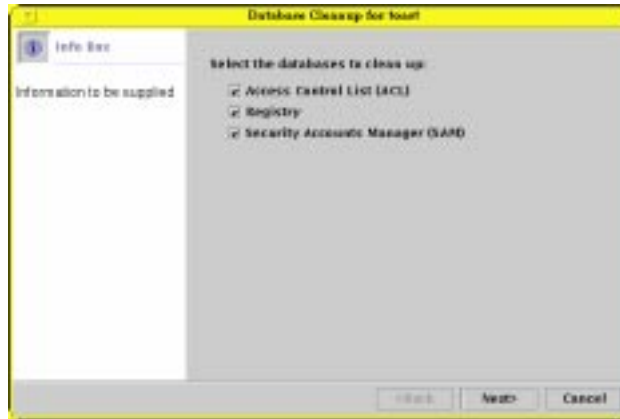
The Cleanup wizard performs the following tasks on the following databases:

- Checks, repairs, and prunes obsolete entries in the Access Control List (ACL), and synchronizes ACL information with the Solaris file system
- Checks and repairs the Registry
- Checks and repairs the Security Account Manager (SAM)
- Checks and compacts Binary Large Object and Share File systems

3. **Choose all of the databases that you want to clean up, then click Next.**

4. **Click Finish.**

The resulting screen follows the progress of the cleanup, indicating a completed task with a checkmark and a pending task with an arrow.
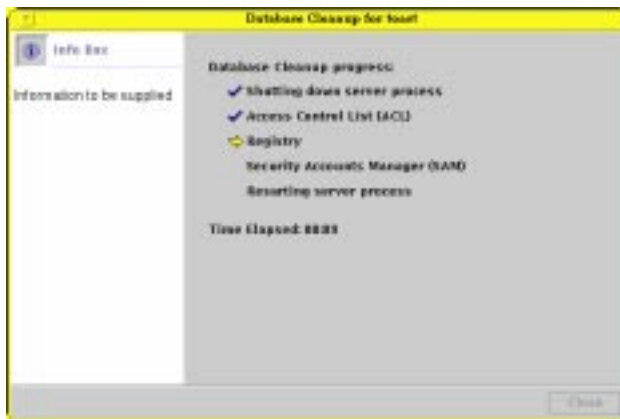
▼ How to Back up SunLink Server Databases

1. **Using SunLink Server Manager, log on to and then open the SunLink Server computer on which you want to back up one or more databases.**

2. **In the results pane, double-click "Tasks" and then double-click "Back Up and Restore Databases."**

   The resulting screen presents backup and restore options.

3. **Select "Back up one or more SunLink Server databases," and then click Next.**

   The resulting screen presents a list of databases that you can back up, and includes a text field in which you specify the path to your database backup file. Note that your backup file must be stored as a Solaris file in an existing directory on the SunLink Server system, rather than locally.
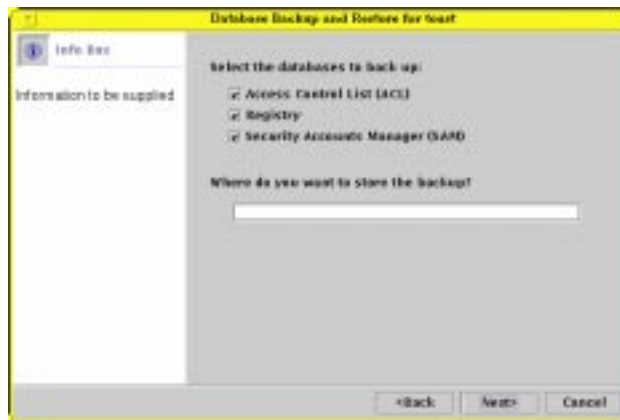
4. **Select all of the databases that you want to back up, specify the backup file's path name (either a directory or a device), and then click Next.**

The resulting screen enables you to specify how you want the Database Backup and Restore wizard to handle server shutdown and startup.
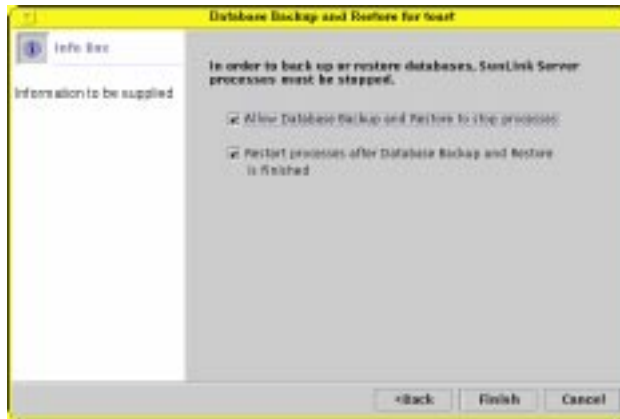
Note that the server *must* be shut down each time the wizard runs a maintenance task. If you do not choose the option to "Allow Database Backup and Restore to stop processes," you will be unable to continue the backup task. If you do choose to have the wizard automatically shut down the SunLink Server processes for maintenance, then you will also be able to specify that the wizard restarts the server after the tasks are completed.

5. **Choose how you want the Database Backup and Restore wizard to handle server shutdown and startup, then click Finish.**

The resulting screen follows the progress of the cleanup, indicating a completed task with a checkmark and a pending task with an arrow.
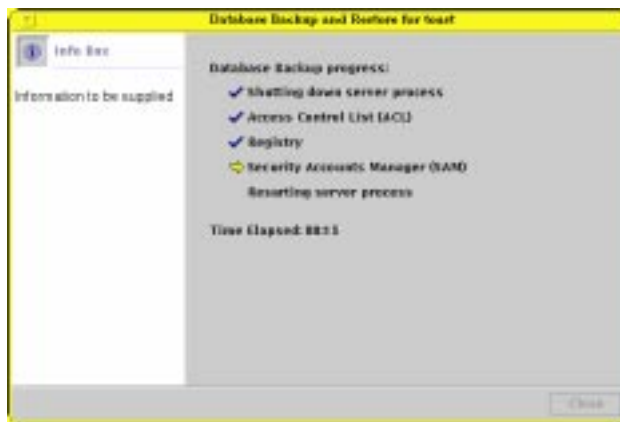
▼ How to Restore Backed-Up Databases

1. **Using SunLink Server Manager, log on to and then open the SunLink Server computer on which you want to restore one or more backed-up databases.**

2. **In the results pane, double-click "Tasks" and then double-click "Back Up and Restore Databases."**

   The resulting screen presents backup and restore options.

3. **Select "Restore one or more SunLink Server databases," and then click Next.**

   The resulting screen presents a text field in which you specify the path to the database backup file that you want to restore.
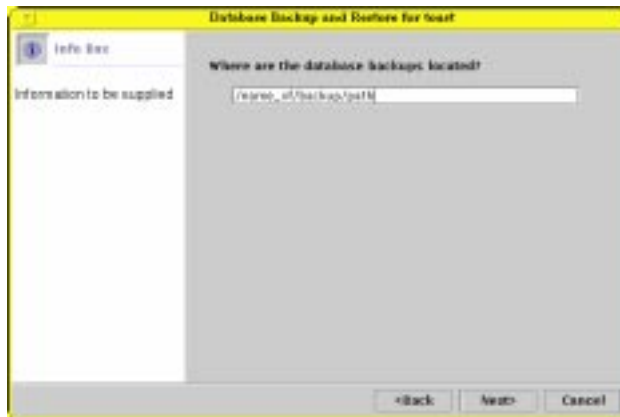
4. **Enter the path name of the backup file, and then click Next.**

   The resulting screen presents a list of databases that you can restore.

   Database Backup and Restore for toast

   Info Box

   Information to be supplied

   Select the databases to restore:

   - Access Control List (ACL)
   - Registry
   - Security Accounts Manager (SAM)

   <Back   Next>   Cancel
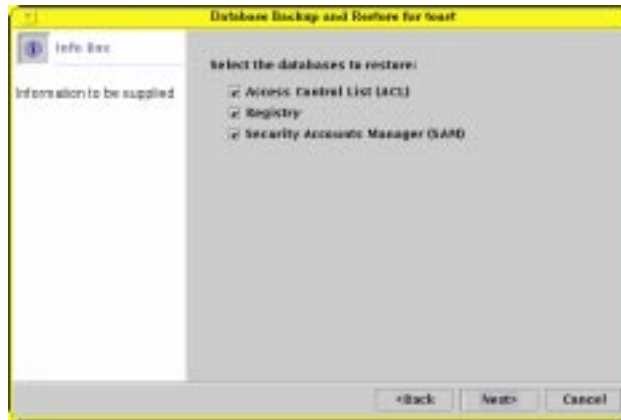
5. **Select all of the backed-up database files that you want to restore, and then click Next.**

   The resulting screen enables you to specify how you want the Database Backup and Restore wizard to handle server shutdown and startup.

   Database Backup and Restore for toast

   Info Box

   Information to be supplied

   In order to back up or restore databases, SunLink Server processes must be stopped.

   - Allow Database Backup and Restore to stop processes
   - Restart processes after Database Backup and Restore is finished

   <Back   Finish   Cancel
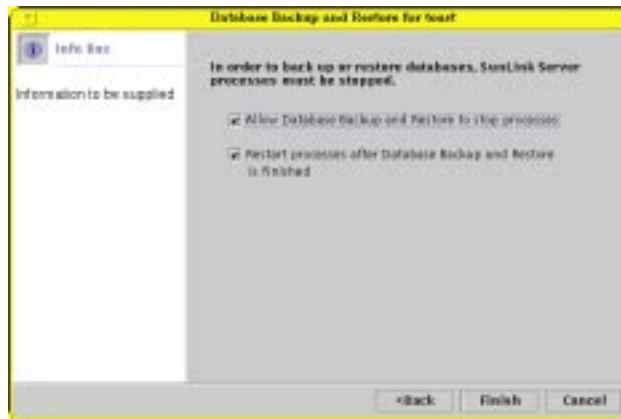
   Note that the server *must* be shut down each time the wizard runs a maintenance task. If you do not choose the option to "Allow Database Backup and Restore to stop processes," you will be unable to continue with database restoration. If you do choose to have the wizard automatically shut down the SunLink Server processes for maintenance, then you will also be able to specify that the wizard restarts the server after the tasks are completed.

6. **Choose how you want the Database Backup and Restore wizard to handle server shutdown and startup, then click Finish.**

   The resulting screen follows the progress of the cleanup, indicating a completed task with a checkmark and a pending task with an arrow.
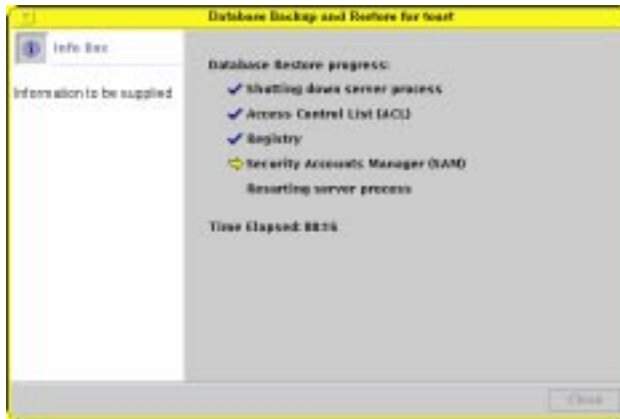
▼ How to Create an Automatic Schedule for Both Database Cleanup and Backup

1. **Using SunLink Server Manager, log on to and then open the SunLink Server computer on which you want to schedule maintenance tasks.**

2. **In the results pane, double-click "Tasks" and then double-click "Schedule Database Maintenance."**
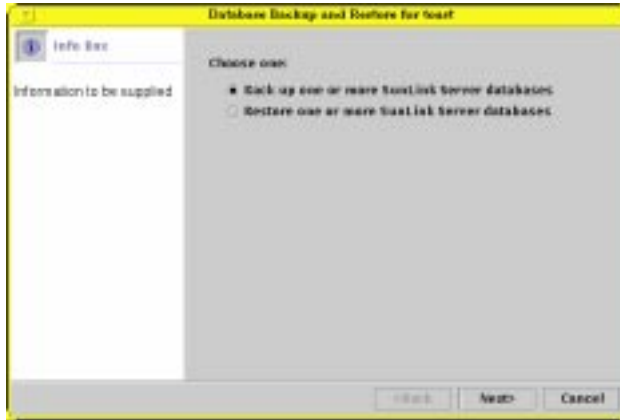
   The resulting screen presents both the cleanup and backup options:
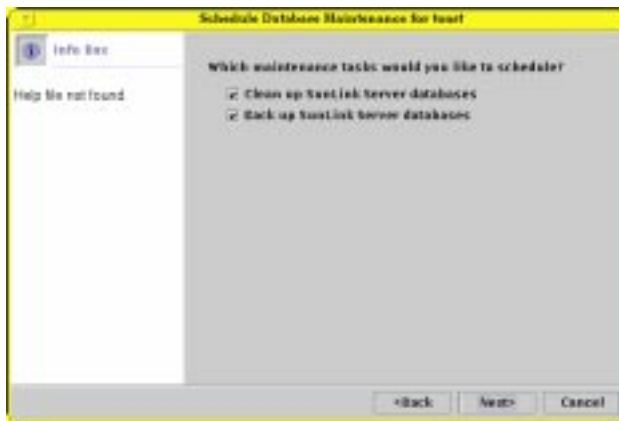
3. **Choose one or both both maintenance options (selected by default), then click Next.**

   (Depending on whether you chose one or both tasks, one of the following screens may not be displayed.)

   The resulting screen presents a list of databases to clean up automatically.
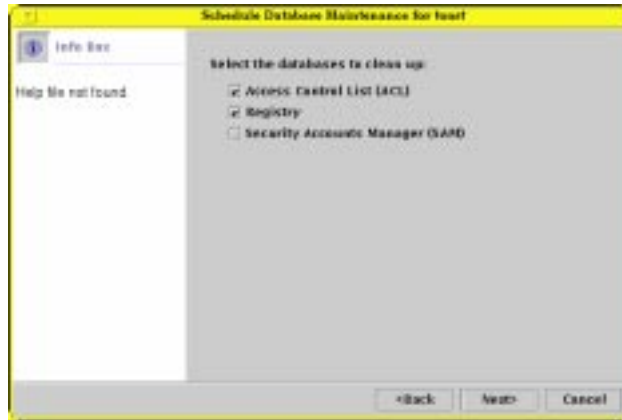
4. **Choose all of the databases that you want to clean up, then click Next.**

   The resulting screen presents a list of databases to back up automatically, and includes a text field in which you specify the path to your database backup file. Note that your backup file must be stored as a Solaris file in an existing directory on the SunLink Server system, rather than locally.
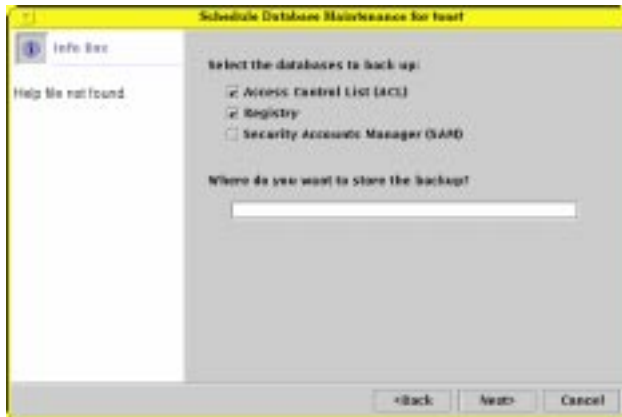
5. **Choose all of the databases that you want to back up, specify the backup file's path name, and then click Next.**

   The resulting screen enables you to specify how you want the Database Maintenance wizard to handle server shutdown and startup.
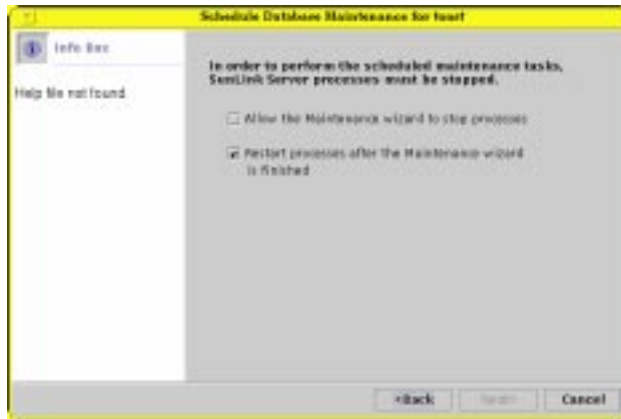
   Note that the server *must* be shut down each time the wizard runs a maintenance task. If you do not choose the option to "Allow the Maintenance wizard to stop processes," you will be unable to continue scheduling the maintenance tasks. If you do choose to have the Maintenance wizard automatically shut down the SunLink Server processes for maintenance, then you will also be able to specify that the wizard restarts the server after the tasks are completed.

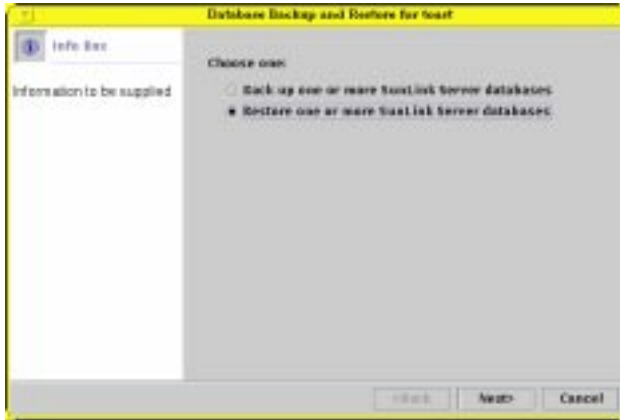6. **Choose how you want the Database Maintenance wizard to handle server shutdown and startup, then click Next.**

   The resulting screen enables you to specify the frequency of maintenance tasks: one time only, daily, weekly, or monthly. The default is weekly.
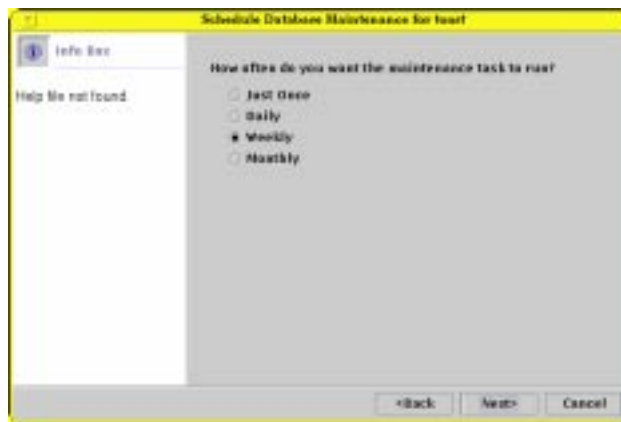
7. **Select how frequently you want the maintenance tasks to be run, then click Next.**

   The resulting screen enables you to choose times for the maintenance tasks with greater precision; the options will be different, depending on the frequency you chose:

   - **Just Once:** You choose a specific date and time
   - **Daily:** You choose a specific time of day
   - **Weekly:** You choose a specific day of the week and time of day
   - **Monthly:** You choose a specific date during the month and time of day

8. **Specify days, dates, and times, and then click Next.**

   The resulting screen presents a summary of your choices, and gives you another opportunity to amend them.
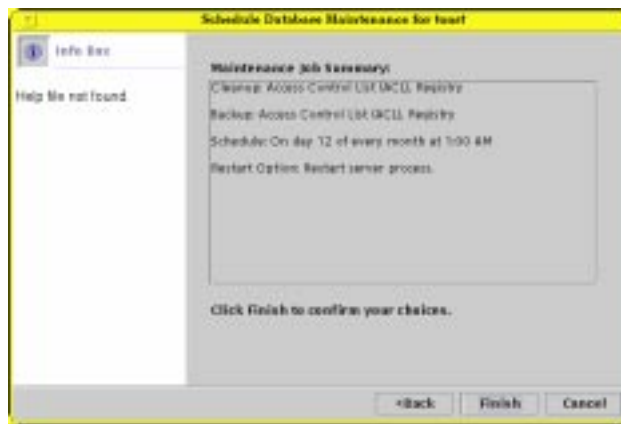
9. **Examine the Maintenance Job Summary, then click Finish to confirm your choices and activate the defined maintenance schedule, or Back to amend any of your choices.**

   After you have confirmed your choices and scheduled your maintenance tasks, a summary of the scheduled tasks will be presented to you each time you open the Maintenance Task wizard.

   Once you have scheduled your maintenance tasks, you can change the schedule—or delete it entirely—at any time. For details, see the next section, "How to View, Modify, or Delete Scheduled Database Maintenance Tasks" on page 129."

▼ How to View, Modify, or Delete Scheduled Database Maintenance Tasks

1. **Using SunLink Server Manager, log on as root to the SunLink Server computer on which you want to schedule maintenance tasks.**

2. **In the results pane, double-click "Tasks" and then double-click "Schedule Database Maintenance."**

The resulting screen presents a summary of the maintenance tasks that have been scheduled:
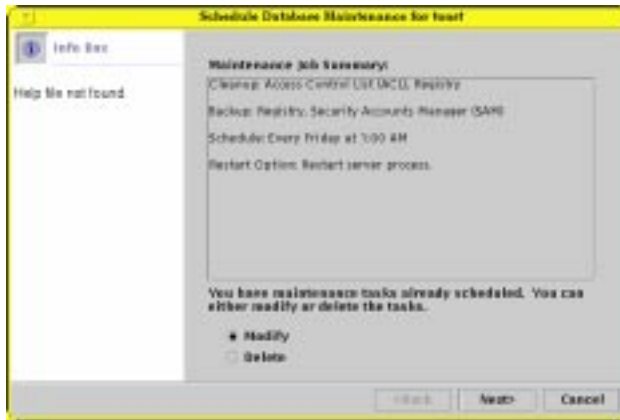
3. **Do *one* of the following:**
   - Select Modify, click Next, and then follow the procedures outlined in the previous section, "How to Create an Automatic Schedule for Both Database Cleanup and Backup" on page 126.
   - Select Delete, click Next, then continue with the following step, Step 4.

4. **Click Finish to confirm that you want to delete the specified maintenance task.**

▼ How to Compact the WINS Database

1. **Log on to the SunLink Server WINS computer as root.**

2. **Stop the WINS server by typing the following command:**

   ```
   net stop wins
   ```

3. **Compact the WINS database by typing the following command:**

   ```
   winsadm -c
   ```

4. **Start the WINS server by typing the following command:**

   ```
   net start wins
   ```

Troubleshooting

This chapter describes how to troubleshoot a computer running SunLink Server software. 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 SunLink Server systems involves gathering data about the problem and analyzing that data to determine the specific cause of the problem. The SunLink Server program includes a number of data-gathering tools. Additionally, more complex data-gathering tools may be available from your support personnel.

This chapter introduces the various tools that are provided with SunLink Server software and describes situations in which using them may be appropriate.

Administrators often can reduce the amount of time required to solve problems by observing the following guidelines:

- Be aware of and familiar with the tools and services that can be used for server troubleshooting.
- Configure the available server utilities to gather the necessary data as a general practice.
- Assess the status of the server at regular intervals.
- Follow a logical and comprehensive procedure when attempting to isolate a server problem.

There will be times when a particular problem requires more complex data-gathering than can be provided using the standard SunLink Server product package. 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.

SunLink Server Troubleshooting Tools

SunLink Server provides a variety of tools that can be used as troubleshooting aids. These tools can be arranged into the following three categories:

- Tools used for assessing the status of the server
- Tools used for automatic notification of the status of the server
- 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.

Tools for Assessing the Status of the Server

The SunLink Server program includes multiple tools that can be used to assess the operational status of the server at any given time. Frequent assessment of server status will improve your ability as a server administrator to notice a problem or trend quickly.

Periodic review of server status will provide a fairly stable basis for understanding how a normal problem-free server appears. Over time, information that deviates from the norm will be an indication that something has changed and warrants your attention.

Tools for assessing the status of the server include the following.

Event Logs

A number of events related to the daily operation of the server can be tracked using the SunLink Server Manager event logs (see Chapter 3). These events are maintained in one of three event logs: *system*, *security*, and *application*. Administrators should develop and implement an event logging policy and include a review of event logs as a regular part of troubleshooting activities.

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. This approach can be used to generate a standard operating profile of the server and can be used to predict trends in server usage.

Note – Event logs also can be viewed using the `elfread` command. For more information, type `man elfread` at the SunLink Server command prompt.

Server Status

SunLink Server 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.

Current Statistics

To view data about current server use, use the SunLink Server Manager Status view. This provides details about current client-server sessions and the resources being used by those sessions.

Cumulative Statistics

To view cumulative server usage data, you can also use the `net statistics` command at the SunLink Server 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 SunLink Server system:

TABLE 6-1   Cumulative Statistics Descriptions

Statistic	Description
Refreshed at	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	This does not apply to Solaris system servers.
Permission violations	Tells when a user attempts to access resources without the required permissions.
Password violations	The number of incorrect passwords that were tried.
Files accessed	The number of files that were used.

TABLE 6-1 Cumulative Statistics Descriptions

Statistic	Description
Comm devices accessed	Not supported on SunLink Server.
Print jobs spooled	The number of print jobs were spooled to printer queues on the server.
Times buffers exhausted	The number of shortages of big and request buffers. Always set to 0 for Solaris system servers.

▼ How to Display Session Information from an NT Workstation

Administrators can display and control sessions between clients and the server. This information can be used to gauge the workload on a particular server.

To display session information from a Windows NT Workstation computer or a Windows client computer using Server Manager:

1. **Start Server Manager.**

2. **Select the SunLink Server system about which you want to view session information.**

3. **Click on the USERS button.**

   You also can display session information using the `net session` command at the SunLink Server 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 Windows 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 computer or from a Windows client computer using Server Manager:

1. **Start Server Manager.**

2. **Select the SunLink Server system about which you want to view session information.**

3. **Click on the USERS button.**

4. **Highlight the user and select the Disconnect button.**

   You also can disconnect a user session by using the `net session` command at the SunLink Server command prompt.

▼ How to Close Open Resources from a 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. Administrators can close these files.

To close an open resource from a Windows NT computer or a Windows client computer using Server Manager:

1. **Start Server Manager.**

2. **Select the SunLink Server about which you want to view data.**

3. **Click on the IN USE button.**

4. **Highlight the open resource and select the Close Resource button.**

   You also can close an open resource by using the `net file` command at the SunLink Server command prompt.

Print Subsystem Event Logging

SunLink Server 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`

Remote Monitoring of Server

SunLink Server provides an SNMP-compliant monitoring service that can be used to monitor SunLink Server systems from remote locations.

If you are an administrator involved with a SunLink Server network that spans multiple locations, you may want to take advantage of this service.

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.

SunLink Server can be configured to notify specified users when a problem occurs. The Solaris system also can be configured to generate and notify the system administrator when problems occur. The following sections discuss these features.

Alerter Service

SunLink Server software includes an Alerter service which can be used 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 SunLink Server Registry.
- The number of bad access attempts exceeds a threshold set in the SunLink Server Registry.
- The number of bad password attempts exceeds a threshold set in the SunLink Server 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 SunLink Server Features

One of the benefits of SunLink Server is the availability of the inherent scripting features provided by the Solaris operating system. Combining these features with the data-gathering tools provided by SunLink Server, an administrator can create a powerful tool that can be used to assess the health of a SunLink Server system at any given time.

For example, using the Solaris system job scheduling feature (CRON), various data-gathering tools provided by SunLink Server, 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.

Tools for Debugging Server Problems

SunLink Server software includes Solaris system commands that can be used to troubleshoot server problems. These commands are executed at the SunLink Server command prompt. This section summarizes these commands and describes the roles they can play in troubleshooting a server.

For more information about each command, type man *command* at the SunLink Server command prompt.

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 SunLink Server 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.

SunLink Server 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     17726 1      0     12:03:36  0:00     lmx.alerter

root     17713 17461 0     12:03:32  0:00     lmx.srv -s 1

root     17722 17874 0     12:03:35  0:00     lmx.srv -s 2

root     17726 1      0     12:03:36  0:01     lmx.dmn

root     17728 1      0     12:03:36  0:01     lmx.browser

root     17744 1      0     12:03:28  0:00     lmx.ctrl
```

In this example, there are two `lmx.srv` server processes (17713 and 17722). The server may have nine clients with current sessions.

How does the administrator know to which `lmx.srv` process a client is connected? Executing the `lmstat -c` command at the server prompt usually provides the answer. 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 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. (The `-w` option is not valid on all operating systems.)

regconfig

The `regconfig` command is used to query or change SunLink Server 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.)

The `regconfig` command also can be used to reinitialize the SunLink Server Registry with system defaults.

For more information about the registry, see Appendix A.

regcheck

The `regcheck` command is used to check and repair the SunLink Server Registry file. This command checks only the internal structure of the SunLink Server 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 SAM database. You can use this command to determine whether the user accounts database has been corrupted and optionally, to fix it.

The `samcheck` command also can be used 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.)

The `lanman.ini` file contains several parameters that you can modify to change. Default settings are used for most of these parameters. However, a certain number 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.

acladm

The `acladm` command is used to check and repair problems found in the access control list.

Be sure to examine the options that are available with this command before executing it. Type the `man acladm` command at the SunLink Server command prompt.

Troubleshooting Procedures

SunLink Server 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 on the problem.

Isolating the Problem

The SunLink Server program runs on a Solaris system computer. The server depends upon a fully-functional NetBIOS network 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); and 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 SunLink Server to function in a network environment. Additionally, similar modules must be functioning on the machine which is attempting to use the file and print services of SunLink Server, such as a Windows NT Workstation computer or 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 servername on any network
```

Reviewing all of the modules involved in the end-to-end connection between a client and SunLink Server, 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 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 which 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.

Checking 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 the sanity of the network.

Step 1: Verify the Status of the Physical Network

The first item to check is the physical network. The majority of today's networking hardware provides status indicators that can be used to assess the state of the various network links (for example, 10-Base-T Hubs use LEDs). Always check these links for any signs of problems with the physical network such as excessive re-transmissions, Link Integrity mismatches, and jabber conditions.

Even in cases in which only a single client is affected, never assume that is it 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.

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. If however, 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 can be used to monitor the health of the physical network. It is worthwhile to check network traffic periodically with one of these devices 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 can be used 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 computer 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, or 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 SunLink Server.

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 SunLink Server software will not work. All SunLink Server 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, the next item to verify is the Solaris operating system on the computer hosting the SunLink Server program. The operating system provides a variety of log files and system checks that can be performed to verify proper operation. For information on these checks, see your Solaris system administrator documentation.

SunLink Server 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

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: Isolating Problems on the SunLink Server System

If you determine that all of the underlying software is functioning properly, then you should check SunLink Server system for problems. Problem isolation on the server 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 SunLink Server 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 Server Running?

It is worthwhile to verify that the server is actually running. You can do this easily by entering the following command at the system command prompt:

ps -ef | grep lmx

The system display should include the following (at a minimum):

```
root     3554      3452   Feb28    19:39 lmx.srv -s     1

root     3452      1      0        Feb28   5:03   lmx.ctrl

root     3568      1      0        Feb28   2:16   lmx.dmn
```

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 command prompt.

Are All of the 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 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 later in this chapter.

Are There Messages in the Error Logs?

Always check the error logs used by the server. You can view the system, security, and application logs from a client computer using Event Viewer, from the SunLink Server system using SunLink Server Manager, or at the system console 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/logs` directory.

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 SunLink Server Registry, then a core file is located somewhere on the system. The `CoreOk` value is in the following key:

```
SYSTEM\CurrentControlSet\Services\
        SunlinkServer\ProcessParameters
```

Go to the `root` directory, and execute the following command to search the file system for core files:

```
find . -name "core*" -print
```

Save any files that you may find. If the coreok parameter is set to no, then core files will not be created. You may want to set the `CoreOk` keyword to yes in order to capture core files which are useful for debugging purposes.

Are All of the Server Resources Properly Shared?

Some 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 are as follows:

ADMIN$

C$

D$

DOSUTIL

IPC$

LIB

NETLOGON

OS2UTIL

PRINTLOG

PRINT$

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 Server Be Contacted From the Console?

A simple test can be conducted to determine whether the server is communicating over the network. Issue the following command at the system console.

net view

The system displays the name of the 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

SunLink Server 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 Server Supporting a Maximum Number of 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 is indicated by the maxclients parameter in the server *lanman.ini* file. It can be displayed using the srvconfig - g maxclients command.

Has the SunLink Server 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 SunLink Server Registry, the you can use the `regload` command to reinitialize all registry values to their defaults.

Can the 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.

Troubleshooting a Shared Resource

If you can communicate with the server but cannot access a shared resource, check the following items:

1. Verify that the shared resource exists by using the `net view \\`*servername* 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.

   Verify that the resource can be used using either group membership or on a per-account basis for that particular user. Also, 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 being 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).

Solving Problems with Unknown File Systems

SunLink Server recognizes a subset of the Solaris system file systems. By default, the server knows only the following types of file systems:

■ `cdfs`
■ `nfs`
■ `s5`
■ `sfs`
■ `ufs`
■ `vxfs`

If you are using a file system other than those recognized by SunLink Server software, it 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, and press ENTER:**

   `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** *l*`anman.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 SunLink Server file system type you want to use.

3. **Stop and restart the server.**

   The SunLink Server program now will map the Solaris file system to the recognized file system you specified.

SunLink Server Registry

In the SunLink Server program, most configuration information is centrally stored in a single database called the Registry. Ordinarily, you use SunLink Server Manager to change Registry values by way of the graphical user interface. However, you may also use the Windows Registry Editor to change values by editing the Registry database manually.

This appendix provides the following information:

- Overview of the SunLink Server Registry structure.
- Description of Registry Editor.
- Descriptions of the SunLink Server Registry keys and values.

SunLink Server Registry Structure

The SunLink Server 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 SunLink Server Registry subtrees.

TABLE A-1   SunLink Server 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 SunLink Server Registry is stored in the `/var/opt/lanman/datafiles` directory on the SunLink Server computer.

Value Entries in the Registry Keys

Each registry key can contain data items called value entries. Keys are analogous to folders, and value entries are analogous to files with the folders.

A value entry has three parts: the name of the value, the data type of the value, and the value itself, which can be data of any length. The three parts of value entries always appear in the following order.

TABLE A-2   Registry Key Value Entries

Name	Data Type	Value
DependOnService:	REG_MULTI_SZ:	Tcpip Nbtsys Streams

Data types, such as `REG_SZ` or `REG_EXPAND_SZ`, describe the format of the data which can be up to 1 MB. Data types from 0 to 0x7fffffff are reserved for definition by the system, and applications are encouraged to 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-3   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-3   Registry Data Types

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 SunLink Server 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 SunLink Server. 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 SunLink Server Registry using the Windows NT Registry Editor, you must connect to SunLink Server 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 SunLink Server 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 95 Registry Editor to edit the SunLink Server 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.
- Click Auto Refresh from the Options menu to update the display continuously. You can also click one of the Refresh commands from the View menu to update the display of registry information when Auto Refresh is turned off.

The following table shows some keyboard methods for managing the display of data in each Registry Editor window.

TABLE A-4   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 SunLink Server Registry keys, including locations, that can be modified using SunLink Server Manager:

TABLE A-5   Registry Policies, Keys, and Locations

Policy	SunLink Server registry Key
Alerter Service	(SYSTEM\Current\ControlSet\Services\Alerter\Parameters) IncludeMessageHeader CountNotOnNetworkCache NotOnNetworkCacheTimeout
Computer Browser Service	(SYSTEM\CurrentControlSet\Services\Browser\Parameters) MasterUpdate BackupUpdate BackupRecovery MoreLog
Connected Clients	(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters) AutoDisconnect LogonQuery QueryDelay RelogonDelay
File Name Space Mapping	(SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters) NameSpaceMapping UniqueSuffixLength MixedCaseSupport TruncatedExtensions MappingSeparator
Netlogon Service	(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters) Scripts Pulse (PDC only) Update (BDC only) Randomize (BDC only) SSIPasswdAge (BDC only)
Server Announcement	(SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters) Hidden SrvAnnounce LmAnnounce
Solaris Account Mapping	(SYSTEM\CurrentControlSet\Services\AdvancedServer \FileServiceParameters) CreateUnixUser

Policy	SunLink Server registry Key

Solaris File System Integration	`(SYSTEM\CurrentControlSet\Services\AdvancedServer\`
	`    FileServiceParameters)`
	`IgnoreUnixPermissions`
	`UnixDirectoryCheck`
	`UnixFilePerms`
	`UnixDirectoryPerms`
	`UseUnixLocks`
	`RootOwnsFilesCreatedOnNFS`

UPS Service	`(SYSTEM\CurrentControlSet\Services\UPS\Parameters)`
	`IgnoreSIGPWR`
	`PowerFailAddress`
	`PowerFailMessage`
	`PowerMessageInterval`

Users Alerts	`(SYSTEM\CurrentControlSet\Services\AdvancedServer\`
	`    AlertParameters)`
	`AlertAdminOnLicenseOverFlow`
	`AlertUserOnLicenseOverFlow`
	`(SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
	`AccessAlert`
	`ErrorAlert`
	`LogonAlert`

Registry Keys and Values

This section describes the SunLink Server Registry keys that are changed during administration. You may want to modify these values directly using the SunLink Server Manager or a registry editor. You do not need to be concerned with every key in the SunLink Server Registry; only those keys that you may have reason to change are described. Note that you must stop and then restart the SunLink Server program for most changes to the Registry to take effect.

The SunLink Server 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`
- `\LanmanWorkstation`
- `\Netlogon`
- `\Netrun`

- `\Replicator`
- `\UPS`
- `\WINS`

SunLink Server Key Descriptions

The SunLink Server subkey of the SunLink Server Registry contains the following subkeys in the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
        \AdvancedServer
```

- `\AlertParameters`
- `\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 SunLink Server 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 was exceeded.

  Default: **0** (message will not be sent)

File Service Parameters Entries

The Registry path that contains entries for the SunLink Server file service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
   \AdvancedServer\FileServiceParameters
```

- AclCacheSize   REG_DWORD   0 - 100

  Specifies the number of entries in ACL cache which keeps track of the results or recent access checks performed on SunLink Server resources.

  Default: 6

- EAFilePrefix   REG_SZ   *Character string*

  Prefix used to name files containing extended attribute data. For example, by default, the extended attributes for file *foo* are stored in.ea@foo.

  Default: .ea@

- EnableSoftCompat   REG_DWORD   0, 1, or 2

  Specifies how SunLink Server handles file opens 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 SunLink Server will create an access control list for a newly-created directory if an explicit access control list was not provided by the client computer. If an access control list 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 or 1

  Determines whether the SunLink Server will create an access control list for a newly-created file if an explicit access control list was not provided by the client computer. If an access control list is not created, one will be inherited automatically from its parent directory whenever it is needed.

Default: 0 (will not create new access control list)

- ForceFileFlush   REG_DWORD   0 or 1

  Specifies whether to force a Solaris fsync(2) system call when an 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 SunLink Server users to write to or delete files for which they have sufficient SunLink Server 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 using the SunLink 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 using the SunLink 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*

  The maximum file size, in KBytes, that SunLink Server will allow a user to create on the server.

  Default: 20000

- 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: 0 (make all file names lowercase)

You can change the value of this key using the SunLink 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 8.3-style clients, such as MS-DOS, Windows 3.1, and Windows for Workgroups, 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 95, Windows NT, and OS/2, 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 the SunLink Server Manager.

- OplockTimeout   REG_DWORD   *1 - infinity*

The interval of time (in seconds) that the server waits for acknowledgment from a client of an "oplock" broken notification.

Default: 30

- ReadAheadCount   REG_DWORD   *0 (always read ahead) - infinity*

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 files on NFS are owned by root or user.

Default: 0 (use files owned by the user's Solaris system user ID)

You can change the value of this key using the SunLink Server Manager.

■ SyncAclFileOnWrite   REG_DWORD   *0 or 1*

Determines whether the server will force changes to the access control list (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 which originally were longer than 3 characters.   This feature can be used to distinguished longer file extensions from similar 3-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.)

You can change the value of this key using the SunLink Server Manager.

■ UniqueSuffixLength   REG_DWORD   *0 to 7*

Specifies the length of the alpha-numeric 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 may occur. They may 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 the SunLink Server Manager.

- UnixCloseCount   REG_DWORD   *1 - 20*

  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 SunLink Server 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 system 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 SunLink Server (as determined by checking group memberships of directory); and a value of 2 ignores Solaris system directory permissions.

  Default: 1

  You can change the value of this key using the SunLink Server Manager.

- UnixDirectoryPerms   REG_DWORD   *0 - 511*

  The Solaris system permissions for newly-created directories.

  Default: 509 (0775 octal)

  You can change the value of this key using the SunLink Server Manager.

- UnixFilePerms   REG_DWORD   *0 - 4095*

  The Solaris system permissions for newly-created files.

  Default: 1460 (02664 octal)

  You can change the value of this key using the SunLink Server Manager.

- UnixQuotas   REG_DWORD   *0 or 1*

  Specifies whether SunLink Server provides Solaris system disk quota support. This ensures that creating or writing to the file is performed under the Solaris system UID of the Solaris system user to which the SunLink Server 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 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 SunLink Server grants opportunistic locks to clients who request them on opens.

  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 the SunLink Server Manager.

- WriteBehind   REG_DWORD   *0 or 1*

  Specifies whether physical Solaris system writes are performed before or after the server responds to the client. If Solaris system writes are performed before the server responds to the client, then the server appears to be slower (because the response is delayed), but the server can report disk full errors to clients. If Solaris system writes are performed after the response is sent, disk full errors during write SMBs are not reported to the client.

  Default: 1 (enable write behind)

Net Administration Parameters Entries

The Registry path that contains entries for the SunLink Server Net Administration is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
   \AdvancedServer\NetAdminParameters
```

- NetAdminGroupName   REG_SZ   *Character string*

The Solaris system group name assigned to the net admin \\servername /c command.

Default: DOS----

- NetAdminPath   REG_SZ   *Character string up to 256 characters*

The Solaris system path used to find commands submitted by the net admin \\servername /c command.

Default: /var/opt/lanman/bin:/bin:/usr/bin

- NetAdminUserName   REG_SZ   *Character string*

The Solaris system user account name assigned to a process executed by net admin \\servername /c.

Default: lmxadmin

Parameters Entries

The Registry path that contains entries for the SunLink Server Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \AdvancedServer\Parameters
```

- CheckPrintQueueInMinutes   REG_DWORD   *1 - infinity*

The interval in minutes at which the server determines whether a printer queues should be started.

Default: 10 minutes

- DisableUpLevelPrinting   REG_DWORD   *0 or 1*

Specifies whether to disable or enable Windows NT-style printing.

Do not change this value from the default setting of 0. Doing so will disable all printing services.

Default: 0

- MaxDirectoryBufferSize   REG_DWORD   *1 - infinity*

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 SunLink Server will attempt to allocate these buffers using the GC memory allocator, one should consider increasing the SizeGcBufferPoolInKB key if one increases this value.

Default: 32768 bytes

- MaxIpcTryCount   REG_DWORD   *1 - infinity*

The number of read() system calls after which the server checks to see if 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: 20

- MaxMailslotReadTime   REG_DWORD   *1 - infinity*

The amount of time 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   *1024 - infinity*

The maximum amount of data that a client can exchange with the server.

Default: 4156 (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 SunLink Server program will use for processing Read Block Raw, Write Block Raw, Transaction, Transaction 2, or NT Transaction SMBs.

Default: 32768

MaxServiceWaitTime   REG_DWORD   *5 seconds - infinity*

Specifies the amount of time (in seconds) the server will wait for a service to respond when it changes the following statuses of the services: pause, continue, install, uninstall.

Default: 60

- NativeLM   REG_SZ   *Character string*

An additional field in the session setup request/response. This field is generated at run time.

Default: (Vendor-specific)

- 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 SunLink Server program has stopped.

  Default: 1 (send a message)

- SizeGcBufferPoolInKB   REG_DWORD   *1 - infinity*

  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 SunLink Server 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 length of time 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: 300 seconds (5 minutes)

- MaxVCPerProc   REG_DWORD   *0 - 101*

  The maximum number of virtual circuits that each lmx.srv process should be able to handle. This limit normally is calculated on the fly by SunLink Server 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: 0 (Use value of VCDistribution key)

- MaxVCs   REG_DWORD

  The maximum number of virtual circuits that can be established to a SunLink Server computer. This key permits administrators to manually override the sizing of shared memory. Do not change the value of this key.

- MinSmbWorkerTasks   REG_DWORD

  Determines how many SMBWORKER tasks are preallocated by lmx.srv processes on startup. Do not change the value of this key.

- MinVCPerProc   REG_DWORD

  The minimum number of virtual circuits that each lmx.srv process should be able to handle. This limit normally is calculated on the fly by SunLink Server 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: 0 (Use value of VCDistribution key)

- NumCIStructs   REG_DWORD

  Sizes the CLIENTINFO array in shared memory.

  Do not change the value of this key.

- NumCLIENT_SESSION   REG_DWORD   *5 - 128*

  Limits the 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: 5

- NumHashTables   REG_DWORD   *8 - infinity (powers of 2)*

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.

Do not change the value of this key.

Default: 128

- NumSERVER_SESSION   REG_DWORD   *5 - infinity*

Limits the 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: 100

- NumUStructs   REG_DWORD   *1 - infinity*

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.

Default: 1000

- SpareServerTime   REG_DWORD   *0 - infinity*

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 SunLink Server)

- 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 number 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: 1,2,12

20,2,20

35,2,24

50,3,28

85,4,28

100,5,32

130,6,36

180,8,42

250,9,44

350,10,50

500,10,60

750,10,80

1000,10,101

The following table describes the meaning of the default value:

TABLE A-6   `lmx.srv` Processes Default Value Meaning

Client Range	Min. Sessions per lmx.srv	Max. Sessions per lmx.srv
1-19	2	12
20-34	2	20
35-49	2	24
50-84	3	28
85-99	4	28
100-129	5	32
130-179	6	36
180-249	8	42
250-349	9	44
350-499	10	50
500-749	10	60
750-999	10	80
1000+	10	101

RPC Parameters Entries

The Registry path that contains entries for the SunLink Server RPC Parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
    \AdvancedServer\RpcParameters
```

- BrowserMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of open browser sessions that an lmx.srv process can support simultaneously.

  Default: 20

- EventlogMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of open event log sessions that an lmx.srv process can support simultaneously.

  Default: 20

- LsarpcMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of open LSA RPC sessions that an lmx.srv process can support simultaneously.

  Default: 20

- NetlogonMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of open Netlogon sessions that an lmx.srv process can support simultaneously.

  Default: 20

- SamrMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of SAM sessions that an lmx.srv process can support simultaneously.

  Default: 20

- SpoolssMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of print sessions that an lmx.srv process can support simultaneously.

  Default: 50

- SrvsvcMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of server sessions that an lmx.srv process can support simultaneously.

  Default: 20

- SvcctlMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of service control sessions that an lmx.srv process can support simultaneously.

  Default: 20

- WinregMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of Registry sessions that an lmx.srv process can support simultaneously.

  Default: 20

- WkssvcMaxCalls   REG_DWORD   *5 - infinity*

  The maximum number of workstation sessions that an lmx.srv process can support simultaneously.

  Default: 20

Share Parameters Entries

The Registry path that contains entries for the SunLink Server 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 SunLink Server should create a directory automatically if one does not exist.

  Default: 1 (create new directory)

- ShareCacheCount   REG_DWORD   *5 - infinity*

  The number of share names to store in the sharefile cache.

  Default: 40

- ShareReadCount   REG_DWORD   *1 - infinity*

  The number of share entries to read during sharefile operations. Setting this 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 SunLink Server 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 SunLink Server 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 SunLink Server 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 the SunLink Server Manager.

■ Exclude   REG_SZ   *Character string*

Specifies existing Solaris system user IDs excluded from being assigned to SunLink Server user accounts. If a SunLink Server 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 SunLink Server user account. This can be used to ensure that certain existing Solaris system user accounts never are assigned automatically to newly-created SunLink Server user accounts, even if the ForceUniqueUnixUserAccount key is set to 0.

Default: 0 - 100

■ ForceUniqueUnixUserAccount   REG_DWORD   *0 or 1*

Specifies whether to assign automatically an existing Solaris system user account to a newly-created SunLink Server 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 SunLink Server user accounts when they are created.

Default: 0 (A new SunLink Server 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.)

■ GroupUpdateTime   REG_DWORD   *0 - infinity*

The interval in seconds at which the server checks the Solaris system file */etc/ group* for changes.

Default: 3600 seconds (1 hour)

- NewUserShell   REG_SZ   *Character string*

  The login shell for new user accounts. The default prevents new users from logging into the Solaris system using a terminal emulator. To enable login, set this key to a real value, such as */bin/sh.*

  Default: /bin/false

- SyncUnixHomeDirectory   REG_DWORD   *0 or 1*

  Whenever the home directory of a SunLink Server user account changes, this key changes the home directory of the associated Solaris system user account to match the SunLink Server home directory.

  Default: 0 (do not synchronize home directories)

- UserComment   REG_SZ   *Character string*

  The comment to assign to all automatically-created Solaris system user accounts.

  Default: SunLink Server user

- UserRemark   REG_SZ   *0 to 48 characters*

  The comment string associated with the USERS shared directory.

  Default: Users Directory

Alerter Service Parameters

The Registry path that contains entries for the SunLink Server Alerter service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \Alerter\Parameters
```

- AlertNames   REG_MULTI_SZ   *List*

  A list of the 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 how long in seconds that non-running clients should remain in the server's cache of clients.

Default: 120 seconds (2 minutes)

Browser Service Parameters

You can use SunLink Server Manager to change the values of all of the following keys. The Registry path that contains entries for the SunLink Server Computer Browser service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \Browser\Parameters
```

■ BackupRecovery   REG_DWORD   *60 - infinity*

Specifies the period of time 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*

Indicates the interval in seconds at which the backup browser refreshes its browse lists with the master browser.

Default: 720 seconds (12 minutes)

■ 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)

EventLog Service 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 Account 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 to 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 to infinity*

Specifies the number of categories supported.

■ TypesSupported REG_DWORD *0 to infinity*

Specifies a bitmask of supported types.

Net Logon Service Parameters

The Registry path that contains entries for the SunLink Server Net Logon service is as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \Netlogon\Parameters

■ LogonQuery REG_DWORD *60 - infinity*

Specifies the interval, in seconds, at which the server checks if linked clients are still active.

Default: 900 (15 minutes)

■ 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 (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

- Randomize   REG_DWORD   *5 to 120*

Specifies the time period in seconds within which a backup domain controller randomizes its request to a PDC for updates after receiving an update notice. This keyword decreases the odds of servers in the same domain requesting an update from the primary domain controller at the same time.

Default: 30 seconds

- 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

- Scripts   REG_EXPAND_SZ

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

- SSIPasswdAge   REG_DWORD   *86400 (24 hours) - infinity*

Specifies the time, in seconds, at which a backup domain controller must change the password that it sends to the primary domain controller to verify its eligibility to receive user accounts database updates.

Values: 604800 (7 days)

- Update   REG_DWORD   *0 or 1*

If this value is set, 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

The Registry path that contains entries for the SunLink Server Netrun service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
   \Netrun\Parameters
```

- MaxRuns   REG_DWORD   *1 to 10*

  Sets the maximum number of netrun requests that can run simultaneously.

  Default: 3

- RunPath   REG_SZ   *Path up to 256 characters*

  Sets the path where programs accessible via the Netrun service are located. Only programs located in a runpath can be executed from a client or another server. Separate multiple path entries with colons (:).

  Default: \tmp

Replicator Service Entries

The Registry path that contains entries for the SunLink Server 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 computername; that is, do not include two backslashes (\\) at the beginning of the name.

  Default: (local domain name)

- ExportPath   REG_SZ or REG_EXPAND_SZ   *Pathname*

  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\shares\asu\repl\export

- GuardTime   REG_DWORD   *0 to one-half of Interval*

  Sets 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

- 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.

- ImportPath   REG_SZ or REG_EXPAND_SZ   *Pathname*

  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\shares\asu\repl\import

- Interval   REG_DWORD   *1 to 60*

  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.

  Default: 5

- MaxFilesInDirectory   REG_DWORD   *0 to infinity*

  Specifies the maximum number of files in an import directory that can be replicated.

  Default: 2000

- Pulse   REG_DWORD   *1 to 10*

  Specifies in minutes how often the export server repeats sending 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 receive the notice. The server waits the equivalent of (Pulse * Interval) minutes before sending each repeat notice.

  Default: 3

- Random   REG_DWORD   *1 to 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

- 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

- 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 SunLink Server Uninterrupted Power Source service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \UPS\Parameters
```

- IgnoreSIGPWR   REG_DWORD   *0 or 1*

Specifies whether UPS service will be enabled.

Default: 1 (disables UPS service)

You can change the value of this key using the SunLink Server Manager.

- PowerFailAddress   REG_SZ   *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 the SunLink Server Manager.

- PowerFailMessage   REG_SZ   *String up to 500 characters*

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."

- 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 would indicate to send the message one time only. The default is 1.