

Advanced Server/9000 Administrator's Guide

HP Systems Networking

Edition 2



J2716-90017

HP 9000 Networking

E1097

Printed in: U.S.A.

© Copyright 1997, Hewlett-Packard Company.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Copyright Notices. ©copyright 1983-97 Hewlett-Packard Company, all rights reserved. ©copyright 1985-97 Microsoft Corporation, all rights reserved. ©copyright 1985-97 AT&T, all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Trademark Notices UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Windows, Windows NT, and Windows for Workgroups are trademarks of Microsoft Corporation in the U.S.A and other countries.

MS-DOS and Microsoft are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard's Advanced Server/9000 is based on AT&T's Advanced Server for UNIX Systems.

Contents

1. Administering Advanced Server at the Command Prompt

Advanced Server Commands	13
Net Command	16
Administering Local and Remote Servers.	16
Understanding Command Syntax	21
Getting Help on Net Commands	22
Running net logon before Running net Commands	23
Advanced Server Net Commands	23
Mapping AS/U Users to HP-UX Users.	27
Using mapuname Across Subnets and Domains	29
Making Backups	35

2. Handling Files

Pathname Formats and Use of Forward and Back Slash	38
File Formats.	39
File Attributes	40
Configure keepunixgroups to Retain UNIX GIDs or DOS Attributes . .	41
AS/U and HP-UX File Access Permissions.	43
Permissions when HP-UX User is Not File Owner	45
Advanced Server/9000 File Interlocking	46
Managing Files between HP-UX and DOS Clients	47
Displaying Filenames in the HP-UX System Format.	48
Using the udir Command on Local Client Drives.	50
Renaming HP-UX System Files.	50
Using the uren Command to Move Files.	51
Changing HP-UX System Permissions for AS/U Files.	51
Handling Incompatible File Formats	52

Contents

Using ud to Convert between DOS and HP-UX	53
Guidelines for Using the ud Command	53
Piping and Redirecting Converted Files	54
Configuring Reported Disk Space	56
3. Printing	
AS/U Spooler Service	58
AS/U Support of Native lp Spooler.	58
AS/U Support of OpenSpool/UX Spooler	59
AS/U Support of HPDPS Spooler	60
4. Using CD ROMs	
Using CD ROMs	64
5. Operating with NFS	
Using NFS Mounted Resources with Advanced Server/9000	66
Multiple AS/U Server Access to NFS Files	68
Configuring for NIS Interoperability	69
6. Logging and Tuning	
Event Logging.	72
Viewing a Log Archived in Log File Format	73
Tuning.	74
Configuring NetBIOS Memory Usage	74
Batch Oplocks Performance	75
Detecting and Reporting File Write Failure	76
Guidelines for Tuning HP-UX Kernel Parameters.	77

Contents

7. AS/U in a Subnetted Domain

WINS Client Support	81
Windows NT 4.0 Client Interoperability.....	82
Enabling WINS Client Support	82
Disabling WINS Client Support	83
Using the Autoconfig Utility	83
Name Resolution in Subnetted Domains without WINS	85
Manually Configuring NetBIOS Names.....	86
Advanced Server/9000 Access	86
Non Advanced Server/9000 Access	87
Administering the NetBIOS Name Cache	89

8. Troubleshooting

Advanced Server Troubleshooting Tools	95
Tools for Assessing the Status of the Server.....	95
Tools Providing Automatic Status on the Server	99
Tools for Debugging Server Problems	100
Troubleshooting Procedures	103
Isolating the Problem.....	103
Checking the Network	104
Troubleshooting a Shared Resource	110
Differences Between System Access Permissions	112
UNIX System Access Permissions.....	113
Solving Browsing Problems.....	117
Solving Printing Problems	118
NetBIOS Troubleshooting Tools and Hints	120

Contents

9. Software Availability in Native Languages

European Character Support	126
Japanese Character Support	128

A. Advanced Server Registry

Advanced Server Registry Structure	133
Value Entries in the Registry Keys	133
Using Registry Editor	135
Connecting to a Remote Registry	135
Viewing the Registry	135
Using AS/U Administrator	137
Registry Keys and Values	140
Advanced Server Key Descriptions	141
Alert Parameters Entries	141
File Service Parameters Entries	142
Net Administration Parameters Entries	148
Parameters Entries	148
Process Parameters Entries	151
RPC Parameters Entries	155
Share Parameters Entries	156
User Service Parameters Entries	157
Alerter Service Parameters	159
Browser Service Parameters	160
EventLog Service Entries	161
Lanman Server Parameters	162
Net Logon Service Parameters	164
Replicator Service Entries	166

Contents

B. Lanman.ini File

File Syntax.....	171
File Parameters.....	173
[Server] Section Parameters.....	173
[Workstation] Section Parameters.....	174
[Lmxserver] Section Parameters.....	174
[Fsi] Section Parameters.....	181
[Hpparms] Section Parameters.....	182
[Psi] Section Parameters.....	182
[Spooler] Section Parameters.....	182
Lanman.ini File Parameter Mapping to Registry Keys.....	187
[Server] Section Parameter Mappings to Registry Keys.....	187
[Workstation] Section Parameter Mappings to Registry Keys.....	188
[Uidrules] Section Parameter Mappings to Registry Keys.....	189
[Netlogon] Section Parameter Mappings to Registry Keys.....	189
[Lmxserver] Section Parameter Mappings to Registry Keys.....	190
[Replicator] Section Parameter Mappings to Registry Keys.....	197
[Fsi] Section Parameter Mappings to Registry Keys.....	198
[Psi] Section Parameter Mappings to Registry Keys.....	198
[Version] Section Parameter Mapping to Registry Key.....	199
[Browser] Section Parameter Mappings to Registry Keys.....	199

Contents

Preface

Advanced Server Administration describes a variety of configuration tasks that will help you to get Advanced Server for UNIX Systems operational. It also describes various tools that you can use to administer and troubleshoot Advanced Server.

Before installing or upgrading Advanced Server/9000, you should read *Advanced Server/9000 Concepts and Planning Guide* and *Advanced Server/9000 Installation Guide*. You also should be familiar with the HP-UX operating system.

This guide contains the following information:

Chapter 1, "Administering Advanced Server at the Command Prompt," lists and describes the UNIX system and Net commands that you can use to administer Advanced Server.

Chapter 2, "Handling Files," describes correct file syntax, conversion between HP-UX and DOS, and permissions.

Chapter 3, "Printing," describes use of the lp and hpdps spoolers in AS/U.

Chapter 4, "Using CD ROMS," describes how to use the pfs_mounts command to integrate CD ROMS into the AS/U enterprise.

Chapter 5, "Operating with NFS," describes how to use NFS with AS/U.

Chapter 6, "Logging and Tuning," describes event logging, and NetBIOS, kernel, and WAN extensions tuning.

Chapter 7, "AS/U in a Subnetted Domain" describes how to configure AS/U NetBIOS to make use of WINS or name caches to operate in routed environments.

Chapter 8, "Troubleshooting," provides a high-level approach to resolving server problems and identifies the various tools available for this purpose.

Chapter 9, "Software Availability in Native Languages," describes use of AS/U with European and Japanese character sets.

Appendix A, "Advanced Server Registry," summarizes the Registry structure, describes the AS/U Administrator, and lists Advanced Server Registry keys and values.

Appendix B, "Lanman.ini File," lists and defines the parameters in the lanman.ini file. It also shows how parameters from earlier versions of the lanman.ini file are mapped to Advanced Server Registry keys.

1 **Administering Advanced
Server at the Command Prompt**

You can use Windows NT Server Tools or Windows NT Administrative Tools to administer AS/U. If you do not use those graphic user interfaces, you can use **net** commands from the HP-UX command prompt.

The AS/U server based executables are in the directory **/opt/asu/lanman/bin**. If you are using the executables frequently, you may want to set the HP-UX path for *root* or the user who will be administering AS/U to include **/opt/asu/lanman/bin**.

This chapter describes how you can use Advanced Server commands and the Net command to administer Advanced Server at the UNIX system console. It contains the following information:

- **Advanced Server Commands** — describes the UNIX system commands that you can use to administer Advanced Server at the command prompt. Advanced Server commands are installed in the **/opt/asu/lanman/bin** directory.

AS/U permits you to access UNIX files and directories based on your secondary group memberships.

- **Net Command** — lists the **net** commands that are available to administer Advanced Server at the command prompt.

Advanced Server Commands

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

The following table lists the UNIX system commands that administrators can use with Advanced Server. Complete descriptions of each command can be found by typing the following at the Advanced Server command prompt:

```
man name of command
```

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

Advanced 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 there also exists UNIX system and MS-DOS at commands.)
blobadm	Displays statistical information, checks, and configures well-known or specified BLOB files.
delshmem	Deletes Advanced Server shared memory.
elfread	Used to view event logs on the local Advanced Server computer at the UNIX system console.

Administering Advanced Server at the Command Prompt
Advanced Server Commands

Advanced Server Command	Description
joindomain	Used to move an Advanced Server from one domain to another. It is an interactive command and takes no arguments. Only use joindomain to change the role of the server if you are also changing its domain. If you wish to promote or demote the server's role, use Server Manager.
lmshare	Manipulates Advanced Server share information without server intervention.
lmshell	Provides the “look and feel” of an MS-DOS shell at the Advanced Server command prompt. Allows users to log on and link to other servers on the network, and to run a subset of DOS commands.
lmstat	Displays statistical information retrieved from the Advanced Server's shared memory.
mapuname	Maps and unmaps Advanced Server user, global group, and local group names to and from UNIX system user names.
netevent	Used to send administrative or user alerts, or to send printing alerts to users submitting print jobs.
regcheck	Manipulates the Advanced Server Registry to enumerate Registry keys, dump the contents of the Registry, or to check and repair Registry files.
regconfig	Used to query or set Advanced Server Registry key information.
regload	Used to create a registry file if one does not exist. Also used to reinitialize registry to system defaults.

Advanced Server Command	Description
samcheck	Used to check or fix the SAM database, or to dump the change log, built-in, account, or LSA databases.
setdomainname	Used to change the domain name of the local Advanced Server. It is an interactive command but also accepts command line arguments.
setservername	Used to change the name of the local Advanced Server.
srvconfig	Used to display or modify Advanced Server configuration information stored in the lanman.ini file.
ud	Converts text files between MS-DOS, UNIX system, and Macintosh file formats.

Net Command

Although we recommend that you use the programs available through Windows NT Administrative Tools and Windows NT Server Tools to administer Advanced Server, the Net command-line interface also can be used. Refer to the *Advanced Server/9000 Quick Installation Guide* for details on which computers to install the Windows NT Administrative Tools and Windows NT Server Tools on.

You are automatically granted the Administrator privilege if you run **net** commands as root even if you are logged in to AS/U as a non-administrative user. This is so you can perform administrative actions (like stopping the server) without having to log in as an administrative user.

The following sections summarize the **net** commands that are available in Advanced Server and describes 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 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 Advanced Server command prompt.

However, to use the **net** command to administer a remote Advanced Server, you must be logged on to Advanced Server as an Administrator with full administrative privilege. If you have different operators responsible for parts of your network and you do not want to assign them full administrative privilege, then they must work only at the Advanced Server command prompt of the server being administered.

Administering a Local Advanced Server

To administer a local Advanced Server using the Net command

1. Log on to the UNIX system hosting the Advanced Server.

2. At the UNIX system prompt, log on 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. For example, to display a list of the server's shared resources, type `net share`.

NOTE

Remember to log off when you are finished administering Advanced Server.

Administering a Remote Advanced Server

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

To enter a Net command remotely

1. Log on 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 wish 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 executes on the server that you specify. For example, at the prompt, type:

Administering Advanced Server at the Command Prompt

Net Command

```
[\\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 which 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 UNIX 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 the user name `jim` with the password `kahuna` on the network, you would type:

```
net logon jim kahuna
```

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

NOTE

In the UNIX 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 Advanced Server 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 Advanced Server prompts you for it. Depending on the command that you type, the Advanced Server 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 Advanced Server reads one of these options, it does not pause to display the corresponding prompt. Instead, Advanced Server 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 Advanced 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, Advanced Server 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, Advanced Server recognizes abbreviations.

Net Command

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 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 UNIX system command prompt typing a name with a special character in an Advanced 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 quotes.

For example, to log on with the user name marksp and the password mrkt&dev on the UNIX system command prompt, you could type the following:

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

Some commonly used UNIX 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 UNIX special characters that you may encounter. For more information on special characters, consult your UNIX system documentation.

Typing Path Names With UNIX System Net Commands

The UNIX system uses a forward slash to separate names in a path. This is different from client computers, which use back slashes. Always precede path names with c: when using the Net command.

When typing path names at a UNIX 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 quotes** — separate each element of the path with single back slashes and surround the whole path in single quotes, 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 quotes. For example, to change the comment for the domain guests group, you could 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, Windows NT, and MS-DOS use back slashes to separate names in paths. For example,

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

Understanding Command Syntax

The commands that are used in Advanced Server 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.

Net Command

- 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 quotes (" "), equal signs (=), colons (:), semicolons (;), and asterisks (*) as they are shown.
- Replace the pound sign (#) with a number.
- At the UNIX system command prompt, you must type Net commands in lower- case letters.
- When you finish typing a command, press ENTER. 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, type one of the following commands at the Advanced Server system prompt:

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.

Running net logon before Running net Commands

For most administrative operations, you should perform `net logon` as an administrator before running the `net` commands. This is especially important when running the `net` commands as root. Running `net` commands as root grants you administrative privileges and bypasses password checks. This allows you to run commands without logging on first. For most `net` commands, it is not a problem if this is done. `net trust`, however, relies on the current user's password when establishing the trust relationship. If you run `net trust` as root without first logging on, a null password is used, and the trust relationship cannot be authenticated when it is later used.

Advanced Server Net Commands

The Advanced Server `net` commands described in the following table are supported at the Advanced Server command prompt.

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 logon user requirements.
net admin	Runs an Advanced Server command or starts a command processor on a remote server.
net auditing	Displays and modifies the auditing settings of a resource.

Administering Advanced Server at the Command Prompt
Net Command

<code>net browser</code>	Displays the list of domains that are visible from a local server or the list of computers that are active in a domain.
<code>net computer</code>	Displays or modifies the list of computer accounts in a domain. This command also can be entered as <code>net computers</code> .
<code>net config</code>	Displays the controllable services that are running.
<code>net config server</code>	Displays or changes settings for the Server service while it is running.
<code>net continue</code>	Reactivates suspended services when typed at a server, and reactivates paused shared printers when typed at a client computer.
<code>net device</code>	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 printer name option, this command displays only the status of the specified printer.
<code>net file</code>	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 <code>net files</code> .
<code>net group</code>	Adds, displays, or modifies global groups. This command also can be typed as <code>net groups</code> .
<code>net help</code>	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 on 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 UNIX system logon name.
net password	Changes the password for a user account on a server or in a domain.
net pause	Suspends services or printers at a server.
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 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 Command

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, Server, Spooler, and Time Source.
net statistics	Displays or clears the statistics log.
net status	Displays a server's computer name, configuration settings, and a list of shared resources.
net stop	Stops a network service.
net time	Synchronizes the client's clock with that of a server or domain, or displays the time for a server or domain.
net trust	Establishes and breaks trust relationships between domains, and lists trust information for a specified domain.
net user	Adds, modifies, or deletes user accounts or displays user account information.
net version	Displays 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

Mapping AS/U Users to HP-UX Users

Advanced Server/9000 user accounts are *not* related to HP-UX user accounts. Use the **mapuname** command to associate an Advanced Server/9000 user account to an HP-UX user account. The **mapuname** command *does* work across domains.

The following are the recommended steps to map AS/U users to HP-UX users:

1. Create the HP-UX user.
2. Create the AS/U user.
3. Use **mapuname** to map the AS/U user to the HP-UX user.

Run **mapuname** on the system where the HP-UX user being mapped to resides. The AS/U user may be in the local or in a trusted domain.

If the AS/U and HP-UX user accounts reside on separate Advanced Server/9000 servers, run **mapuname** on the server with the HP-UX user. Mapuname can map user accounts on:

- a single AS/U server, or
- between 2 AS/U servers within a domain, or
- between AS/U servers in separate domains, or
- between AS/U servers that reside on separate subnets.

Usage between domains requires an existing trust relationship. Usage over subnets requires WINS or NetBIOS name cache configuration.

See "Using mapuname Across Subnets and Domains" in the next section of this guide for setting up trusts and extended LAN configurations using **mapuname**. After using **mapuname**, for the user mapping to take effect, a user must establish a NEW session on the AS/U server.

NOTE

A session for a user may remain on the AS/U server for a period of time after the user has disconnected from the server. If the user logs back in while that session exists, they will re-use that session and **mapuname** mappings will not take effect. Use the **net session** command on the AS/U server to verify that a session for the user does not exist. Use **net session** with the **/delete** option to delete a user session. Use **net help session** on the AS/U server to get more information.

Mapping AS/U Users to HP-UX Users

To automatically map new Advanced Server user accounts to existing HP-UX system accounts set the following registry values:

```
CreateUnixUser=yes  
ForceUniqueUserAccount=no
```

When a new Advanced Server user account is created, if an existing HP-UX system account is found, the new AS/U user will be mapped to the HP-UX user account.

NOTE

If an existing HP-UX system user is not found at AS/U user creation time, an inactive HP-UX user will be created using the AS/U user account name. This HP-UX user will not have a password, homedir, or shell, and cannot be used as a logon. For this reason, automatic mapping of AS/U user accounts to HP-UX system user accounts (using the `CreateUnixUser` value) is not recommended. To activate this HP-UX user, modify the user via SAM. You *must* maintain the same user ID (uid).

Mapping to Non-Existent HP-UX System User Account

If an Advanced Server/9000 user is mapped to a non-existent HP-UX system user account, or if the HP-UX system account for an Advanced Server user is deleted, the Advanced Server user will not have access to any shared resources on the HP-UX system. To ensure that the Advanced Server user can continue to access the system, delete the account mapping or remap the user to another HP-UX system user account.

Using mapuname Across Subnets and Domains

This procedure guides you through configuring an Advanced Server/9000 installation where you map AS/U users to HP-UX users on remote systems that are in separate domains. With this procedure, you will be able to coordinate all of the components that are necessary to use mapuname over routers and between domains, which will simplify the task.

Configuration Scenarios

There are 5 different network layout scenarios that are applicable:

1. Inter-domain, remote subnets
2. Inter-domain, local subnet
3. Local domain, remote subnets
4. Local domain, local subnet
5. Local system

This procedure will address scenario 1. Scenarios 2 through 5 are increasingly simple, so once scenario 1 is understood, the others will be easily understood.

Strategy

This procedure will use the Master Accounts Domain model (MAD). There will be an Accounts domain, where all of the user accounts and security will be defined. There will also be a Resource domain, where information resources are kept. The users in the Accounts domain will access files in the Resource domain. They will have access to the Resource domain through a trust relationship. Using **mapuname** and **keepunixgroups=yes**, you will be able to create files on the Resource domain that will have the user and group attributes of local Resource system HP-UX users.

Components

Here is a list of the components and concepts that will be used in the procedure:

Domains	Account Domain	Resource Domain
Domain Names	Account.DOM	Resource.DOM
Server Name (PDCs)	Account.PDC	Resource.PDC

Administering Advanced Server at the Command Prompt
Using mapuname Across Subnets and Domains

Clients:

Computer Name	Acclinet
User Name	ASUser
LMHOST	entry on Acclinet

UNIX user	hpuxuser
UNIX group	hpuxgrp

AS/U Local Group	Localgrp
------------------	----------

Trusts	Trusted Domain	Trusting Domain
--------	----------------	-----------------

Shares	Sharename: resource
Share Directory	/home/lanman/resource
Permissions	for Localgrp on Resource share

HP-UX commands	mapuname
----------------	----------

lanman.ini	keepunixgroups=yes
------------	--------------------

Name Cache	Cache entries	Cache entries
------------	---------------	---------------

Mapuname Procedure

Pre-requisites

Account.DOM and Resource.DOM should be configured on separate subnets. In this example there will be only one server per domain: the PDCs are Account.PDC and Resource.PDC, respectively.

The NT client is a member of Account.DOM. The client computer name is Acclinet, with the user ASUser configured in the Account.DOM domain security database. Acclinet is on the local Account.DOM subnet.

On the Resource.PDC AS/U server, the HP-UX user hpuxuser is defined (in **/etc/passwd**). hpuxuser is a member of the hpuxgrp group (in **/etc/group**). The sub-directory **/home/lanman/resource** exists and is shared via the Resource share.

Server administration for this procedure is accomplished with the NT Server Tools. The administration of trusts and local groups (necessary for this configuration) can also be done with the AS/U command line **net** commands.

NOTE Ignore steps 2 and 7 in the following procedure if using WINS and all machines are using the same WINS database.

Step #1

Edit the Resource.PDC **lanman.ini** parm to retain HP-UX group ownership of files:

srvconfig -s hpparms,keepunixgroups=yes

The server must be stopped and re-started for this to take effect:

net stop server
net start server

Step #2

Each AS/U PDC and domain name must be added to the other's Name Cache. This allows the PDCs from the different domains to communicate over the router (the router segments the LAN). The PDCs need access to each other for the trust relationship that will be invoked later. Also, the domain names must be entered. On Account.PDC:

nbutil -a Resource.PDC -A 18.123.456.78 -V
nbutil -a Resource.DOM -A 18.123.456.78 -D

On Resource.PDC

nbutil -a Account.PDC -A 10.987.654.32 -V
nbutil -a Account.DOM -A 10.987.654.32 -D

To display the Name Cache contents, type:

nbutil -p

The Account.PDC Name Cache should look like this:

```
Cache has 4 entries
Name                    Type           Remote Address Life[sec]
-----
RESOURCE.PDC <20>    UNIQUE        18.123.456.78  -1
RESOURCE.PDC <00>    UNIQUE        18.123.456.78  -1
RESOURCE.DOM <1C>    GROUP         18.123.456.78  -1
RESOURCE.DOM <00>    GROUP         18.123.456.78  -1
```

Administering Advanced Server at the Command Prompt
Using mapuname Across Subnets and Domains

The Resource.PDC Name Cache should look like this:

Cache has 4 entries

Name	Type	Remote Address	Life [sec]
ACCOUNT.PDC <20>	UNIQUE	10.987.654.32	-1
ACCOUNT.PDC <00>	UNIQUE	10.987.654.32	-1
ACCOUNT.DOM <1C>	GROUP	10.987.654.32	-1
ACCOUNT.DOM <00>	GROUP	10.987.654.32	-1

Step #3

Now that the PDCs can communicate, a trust relationship can be created. The trust will be granted from Resource.DOM (the TRUSTING domain). This requires that Account.DOM (the TRUSTED domain) will permit the trust.

From the NT administrator for Account.DOM:

- click on Administrative Tools
- click on User Manager
- click on Policies
- click on Trust Relationships

Under "Permitted to Trust this Domain" Add Resource.DOM

From the NT administrator for Resource.DOM

- click on Administrative Tools
- click on User Manager
- click on Policies
- click on Trust Relationships

Under "Trusted Domains" add Account.DOM

The trust is now established between the 2 domains.

Step #4

The just-created trust does not have much use at this point because there are no users from Account.DOM that have permissions in Resource.DOM. In this step we will add a Local Group to Resource.DOM and add to it users from Account.DOM.

From the NT administrator for Resource.DOM

- click on Administrative Tools
- click on User Manager
- click on Users

click on New Local Group
add "Localgrp", enter a description, click on Add
under "List Names From" choose Account.DOM
From the "Names" list choose ASUser, click on Add
click on OK

The local group "Localgrp" is now created in the Resource.DOM with ASUser as a member of the group.

Step #5

Now localgrp must be given permission to access the Resource share subdirectory.

From the NT administrator for Resource.DOM

click on Main
click on File Manager
click on Disk
click on Connect Network Drive
in the Path box, enter "\\RESOURCE.PDC\RESOURCE", click OK
{the Resource share will be displayed}
click on Security
click on Permissions
click on Replace Permissions on Subdirectories
click on Add
click on localgrp
click on Add
in the Type of Access window choose "Full Control"
click on OK
click on OK

Step #6

On Resource.PDC, at the AS/U command line prompt, map the HP-UX user hpuxuser to the ASUser in the Account.DOM domain:

mapuname -a Account.DOM:ASUser hpuxuser

Check the mapping by typing at the HP-UX prompt:

mapuname

It should look like this:

```
Builtin:Backup Operators lmxadmin  
ACCOUNT.DOM:ASUserhpuxuser<*****mapping!!!!  
Builtin:Print Operators lmxadmin  
Builtin:Administrators lmxadmin
```

Administering Advanced Server at the Command Prompt
Using mapuname Across Subnets and Domains

```
:SYSTEM root
Builtin:Account Operators lmxadmin
account.dom:Domain Admins
account.dom:Guest lmxguest
account.dom:Domain Guests lmxguest
Builtin:Guests lmxguest
Builtin:Server Operators lmxadmin
account.dom:Administrator lmxadmin
```

Step #7

The client within the Account.DOM domain needs to have access to the Resource.PDC server where the Resource share is located, which is over a router on a remote subnet. To accomplish this, add the following line to the NT client **LMHOSTS** file:

18.123.456.78 Resource.PDC #PRE #DOM:Resource.DOM

Summary

- Step #1: Allow newly-created files to retain unix groups
- Step #2: Allow PDCs and Domains to communicate over router
- Step #3: Set up a trust between domains to allow inter-domain permissions
- Step #4: Create a local group and add the remote domain user to it
- Step #5: Give permissions to the local group
- Step #6: Map the remote AS/U user to the local HP-UX user
- Step #7: Add Resource IP address to client **LMHOSTS** file.

Test

On the NT client, log on to the Account.DOM as ASUuser. Under File Manager, connect the network drive to **\\resource.pdc\resource**. Minimize the File Manager, and use Notepad under Accessories to create a new file. Add some text, then save the file to the Network Drive **\\resource.pdc\resource**. On the HP-UX Resource.PDC server, list the file that you created, and observe that the owner and group are hpuxuser and hpuxgrp.

```
-rw-rw-r-- 1 hpuxuser hpuxgrp 27 Jun 28 14:12 testfile
```

Making Backups

It is recommended that you bring down the AS/U server when doing a full HP-UX backup in order to make sure the security database and directories are backed up. Integrity of a backup copy of AS/U Security Accounts Database can only be assured when AS/U is stopped while the backup is performed. It is recommended that you back up the subdirectories and files of the following directories:

/var/opt/asu/lanman
/etc/opt/asu/lanman

Administering Advanced Server at the Command Prompt
Making Backups

2 Handling Files

Pathname Formats and Use of Forward and Back Slash

HP-UX pathnames use a slash (/) to separate directories, subdirectories, and files. Clients indicate the same separation with a backslash (\).

The Advanced Server/9000 allows you to use the forward slash or backslash to specify pathnames of directories you want to share with the **net share** command or Server Manager. You must precede the pathname with the **c:** drive designation.

NOTE

In all cases, all system responses from the Advanced Server/9000 server are represented in DOS syntax. This is so that clients can request a listing of a server's shared resources and see them listed in the syntax with which they are most familiar.

File Formats

DOS text file format differs from the HP-UX file format. HP-UX text file lines are terminated by the line-feed character. Client text file lines are terminated by the two-character sequence: carriage return and line feed. Because of this difference in file formats, files created by the HP-UX system are missing necessary carriage returns when accessed by clients. Files created by clients have superfluous carriage returns when accessed by the HP-UX system.

In general, PC clients who use only the Advanced Server/9000 do not need to be concerned with this discrepancy in file formats. There are, however, two conditions under which the discrepancy can become an issue which you, as the Advanced Server/9000 administrator, may be asked to help resolve:

- You share an existing directory on the HP-UX system for your Advanced Server/9000 users. The files in such a directory are formatted to be read by the HP-UX system. They do not have the carriage return needed by the client file-formatting convention.
- A user logs on to the HP-UX system and creates or manipulates a directory or file which a client also uses .

NOTE

The Advanced Server/9000 provides the **ud** utility to convert files between HP-UX and DOS formats. For more information, refer to the section titled "Handling Incompatible File Formats" later in this chapter.

File Attributes

Client files have several attributes that are not available in HP-UX. These include the hidden, system, and archive attributes. The Advanced Server/9000 uses the group field of a file to represent these bits.

If the group of the file or directory is one of the eight special Advanced Server UNIX system groups `DOS----`, `DOS-a--`, `DOS--s-`, `DOS---h`, `DOS-as-`, `DOS--sh`, `DOS-a-h`, `DOS-ash`, or the HP-UX system group of `other -` then the group permissions apply. The Advanced Server/9000 makes use of the group field to indicate if a file is hidden (h), system (s), or archive (a). It uses these group names to identify the various combinations of attributes.

File and Directory Creation Using `keepunixgroups`

Whenever files or directories are created, they are created with the group ID being one of the Advanced Server/9000 groups. For directories, it is the group `DOS----`. Files have the `DOS-*` group that matches the attributes (hidden, system, or archive) that are specified by the client.

The `lanman.ini` parameter `keepunixgroups` allows retaining the UNIX group ID field instead of replacing it with the DOS attributes. Refer to the section “Configuring `keepunixgroups` to Retain UNIX GIDs or DOS Attributes” in this document for details.

NOTE

If `keepunixgroups` is set to `yes`, the UNIX group name will govern the ownership of the file and will not be one of the Advanced Server group names. Therefore, the DOS attributes “archive”, “system”, and “hidden” have no meaning and modifying those attributes has no effect on the attributes. Only the “read-only” attribute is significant.

When files or directories are created by the Advanced Server/9000, the permissions for owner and group are identical. By default, files are created `rw- owner`, `rw- group`, and `r-- other`, and directories are created `rwx owner`, `rwx group`, and `r-x other`. These defaults can be changed with the registry values `UnixDirectoryPerms` and `UnixFilePerms`.

Other DOS file attributes, such as read-only and directory, do have HP-UX equivalents. These are mapped into the HP-UX file system directly.

Configure keepunixgroups to Retain UNIX GIDs or DOS Attributes

The files created by Advanced Server/9000 may have their gid set to one of the DOS attributes (system, hidden, archive) or the gid in the password file.

The **lanman.ini** parameter **keepunixgroups** allows you to retain the UNIX group id field of a file or replace it with the DOS attributes of the file

AS/U administrators can choose to have UNIX group ids by invoking the following command: **srvconfig -s "hpparms,keepunixgroups=yes"**

By default **keepunixgroups** is set to **no**. The default behavior allows replacing UNIX group ids with DOS attributes.

AS/U honors the HP-UX setgid bit on a file or directory's parent directory when the keyword **[hpparms], keepunixgroups** is set to **yes**. This allows a group of users to access files and directories based on group memberships.

keepunixgroups may be used in conjunction with the **mapuname** command to obtain UNIX-like owner and group ids for files and directories.

Example: Entry in the **/etc/passwd** file **userA::500:1000:Unix User A:/home/userA:/sbin/sh**

Execute the **mapuname** command for the AS/U user USERA

```
mapuname -a hpntcxx_dom:USERA userA
```

If **keepunixgroups** is set to **yes**, then files created by USERA will be listed as follows:

```
rw-rw-r-- 1 userA 1000 50 Apr 26 10:10 fileA
```

If **keepunixgroups** is set to **no**, then files created by USERA will be listed as follows:

```
rw-rw-r-- 1 userA DOS-a-- 50 Apr 26 10:10 fileA
```

However, the group of a file is determined at the time the file is created. After the file has been created, modifying **keepunixgroups** will have no effect on the group id of a file.

Handling Files

Configure keepunixgroups to Retain UNIX GIDs or DOS Attributes

NOTE If `keepunixgroups` is set to `yes`, the DOS attributes “archive”, “system”, and “hidden” have no meaning. Hence modifying these attributes has no effect on the attributes. Only the “read-only” attribute is significant.

NOTE AS/U uses the `group` field (which contains the DOS attributes) to determine if a directory is an AS/U directory or a UNIX directory. It uses this information to enforce AS/U permissions or UNIX permissions. Another registry value **UnixDirectoryCheck** exists to determine what level of permission needs to be enforced. If **keepunixgroups** is set to **yes**, then **UnixDirectoryCheck** should be set to **2** in order for AS/U to treat a directory as an AS/U directory rather than a UNIX directory. Please refer to configuration of the **UnixDirectoryCheck** parameter for more information.

AS/U and HP-UX File Access Permissions

Advanced Server/9000 client permissions are checked before HP-UX file permissions. If a user's access is restricted because of the Advanced Server/9000 access control list, then access is denied without regard to the HP-UX file permissions.

When an Advanced Server/9000 user attempts to access a file or directory, the access must be allowed by *two* sets of permissions: Advanced Server/9000 permissions created through the File Manager, and HP-UX system file and directory permissions.

When an Advanced Server/9000 user attempts to access a file, the set of HP-UX system permissions that are applied is governed by the following rules:

- If the Advanced Server/9000 user has not been mapped to an HP-UX system user account, then the HP-UX user and group default are the Advanced Server/9000 user `lmworld` and one of the special Advanced Server/9000 HP-UX system groups. Permissions are set by using Advanced Server/9000 apply.
- If the Advanced Server/9000 user has been mapped to an HP -UX system user account using the **mapuname** command, and that HP-UX system user account is the same as the HP-UX system owner of the file or directory, then the owner permissions apply.
- If the Advanced Server/9000 user has been mapped to an HP -UX system user account and the HP-UX system user account belongs to the HP-UX system group of the file or directory, then the group permissions apply.
- If the group of the file or directory is one of the eight special Advanced Server/9000 HP-UX system groups--DOS---, DOS-a-, DOS--s-, DOS--h, DOS-as-, DOS--sh, DOS-a-h, DOS-ash--then the group permissions apply. (The Advanced Server/9000 makes use of the group field to indicate if a file is hidden (h), system (s), or archive (a). It uses these group names to identify the various combinations of attributes.)
- Otherwise, the permissions for Others apply.

Handling Files

AS/U and HP-UX File Access Permissions

For example, if a file named **proposal** has the HP-UX system permissions `rw-r--r--` with owner `fmd` and group `DOS-a--`, and the Advanced Server/9000 user `fred` is mapped to the HP-UX system user `fmd`, and the Advanced server permissions grant all users Read & Write permission, then the Advanced server user `fred` would be allowed to read and write the file. All other Advanced Server/9000 users who do not map to the HP-UX system user `fmd` would be limited to Read permission because the HP-UX system permissions allow only Read access for users other than the owner.

For more information on sharing and permissions, see "Managing Shared Resources and Resource Security" in the *Advanced Server/9000 Concepts and Planning Guide*.

Permissions when HP-UX User is Not File Owner

The Advanced Server/9000 controls the HP-UX owner and group of files created by Advanced Server/9000 users. When the HP-UX user is not the owner of the file or directory, access is granted based on the HP-UX file permission for `other`.

If an HP-UX system user wants to allow Advanced Server/9000 users to access a file created by that HP-UX system user but does not want to give permission to `other` (any user), the following command is used:

`chgrp DOS-a- file`

This will allow Advanced Server/9000 clients to access the file under the group permissions (assuming they also have access control list permissions).

To change all of the files and directories of a tree, use the following command:

`chgrp -R DOS---- directory`

Advanced Server/9000 File Interlocking

The Advanced Server/9000 supports shared file access with other servers running on the same HP-UX system when file interlocking is enabled. File interlocking will propagate client file range locks to HP-UX file system range locks. If other servers also respect HP-UX file range locks then files can be safely accessed by multiple servers. Advanced Server/9000 does *not* support the extended interlocking options that LAN Manager 1.x and LAN Manager 2.2 provide to support PacerShare servers.

Advanced Server/9000 employs the following registry value:
UseUnixLocks 0 or **1** (default is **0**, locks not reflected in UNIX file system)

NOTE

LAN Manager 1.x has interlock=exclusive and interlock=readonly modes to support the PacerShare product. LAN Manager 2.2 has a **unixlocks=access** mode to support PacerShare. Advanced Server/9000 does *not* have equivalent locking functionality.

Examples:

- In the following entry, no HP-UX locks are placed on files by Advanced Server/9000 servers.

UseUnixLocks 0

- In the following entry, F_WRLCK locks are placed on HP-UX files by Advanced Server/9000 servers on behalf of clients on ranges specified in LOCK calls by clients.

UseUnixLocks 1

Managing Files between HP-UX and DOS Clients

The Advanced Server/9000 runs as an application on the HP-UX operating system. The server computer may contain files that are accessible to HP-UX system users but are not accessible to clients. Conversely, files created on clients may not be accessible to HP-UX system users

This section contains information for making the files on your network accessible to users working in different environments. Some of the tools you will use to make files accessible are special commands available on the Advanced Server/9000. These commands enable you to do the following:

- List and rename HP-UX system files.
- Convert text files from DOS format to HP-UX system format and vice versa.
- Change the HP-UX system access permissions of files and subdirectories

To access these commands you must connect to the shared directory **DOSUTIL**. If you want to have access to this directory every time you start your PC, you may enter a **net use** command in a batch file, profile, or login script. You can run these commands from the DOS prompt of a DOS-based client. You cannot run them from the DOS prompt of an NT client.

In addition, you can use some of these special commands on your PC to execute HP-UX system commands on the server. The following table lists the special commands and the sections in which they are described.

Command	Section
<code>udir</code>	“Displaying Filenames in HP-UX System Format”
<code>uren</code>	“Renaming HP-UX System Files”
<code>uchmod</code>	“Changing HP-UX System Permissions for Advanced Server/9000 Files”
<code>ud</code>	“Using <code>ud</code> to Convert between DOS and HP-UX”

NOTE These commands may not work reliably under Windows for Workgroups 3.11.

Displaying Filenames in the HP-UX System Format

The `udir` command enables you to display the contents of a directory on the server. The format of the display is similar to that displayed by the HP-UX system `ls -l` command. The `udir` command is useful when you want to display files and directories that are valid to the HP-UX system but invalid to the DOS system or when you want to see the HP-UX system access permissions and ownership of files and directories.

To use the `udir` command, do the following:

1. Connect to the shared directory for example, **E:**, containing the `udir` command usually `\\server1\DOSUTIL` and set your `PATH` variable to that drive.
2. Connect to the shared directory whose contents you wish to display.
3. At the DOS prompt, type the following:
`udir pathname`
4. Press <**Return**>.

Replace *pathname* with the full path of the directory whose contents you wish to display.

The following is an example of a directory list in HP-UX system format:

```
DOS-PROMT H:\KHOA\TEST>udir h:\khoa\test
Volume in drive H: is TESTSRV
Directory of h:/khoa/test/*
UNIX-based server 'TESTSRV' in share area 'UXUSERS'

DOS Name      UNIX Name Owner Group Modes
.              . khoa katy rwxr-xr-x <DIR> 3-13-95 8:44a
..            .. khoa katy rwxrwxr-x <DIR> 3-13-95 8:43a
name_too_long khoa katy rw-r--r-- 27 3-13-95 8:43a
NET.DIR       net.dir khoa katy rwxr-xr-x <DIR> 3-13-95 8:43a
OK_FOR.DOS   ok_for.dos khoa katy r--r--r-- 6243 3-13-95 8:43a
ROOTFILE     rootfile root sys r--r--r-- 2191 3-13-95 8:44a
```

6 Files 203.98 Megabytes free

The following list describes each column on the screen:

1. **DOS Name**—DOS file and directory names. The entry “.” is an abbreviation for the current directory. The entry “..” is an abbreviation for the next higher level, or parent directory. These abbreviations have the same meaning in the DOS and HP-UX operating systems.
2. **UNIX name**—HP-UX system file and directory names. The file named **name.too.long** appears under this HP-UX system column only because this filename is invalid on the DOS file system. Filenames up to 1024 characters long can be displayed in this column.
3. **Owner**—The HP-UX system owner of the file or directory.
4. **Group**—The HP-UX system group to which the file or directory belongs.
5. **Modes**—HP-UX system access permissions for the file or directory.
6. **Size**—The size of the file, in bytes. Directories are identified by <DIR>.
7. **Date**—The date when the file or directory was most recently modified.
8. **Time**—The time when the file or directory was most recently modified.

Using the `udir` Command on Local Client Drives

If you use the **`udir`** command to list a physical disk drive on your client (for example, drive **A:**, **B:**, or **C:**), it provides a display similar to that of the DOS **`dir`** command. This display also includes an DOS access permissions column similar to that displayed by the HP-UX system **`ls -l`** command.

NOTE

When you enter the **`udir`** command, you can specify a single filename if you want to display one file only, or use the wildcard characters (`*` and `?`) to display multiple filenames.

The following is a sample **`udir`** display of directories and files on a client's local hard disk:

```
C:> udir
Directory of c:.
ansi.sys          rw--a      1651   5-09-92   11:05a
autoexec.bat     rw--a       145  11-08-92   8:00a
config.sys       rw--a       344  11-08-92   9:30a
landoc           rw--a      <DIR>    9-10-92   7:30a
dos3_2           rw---      <DIR>   10-10-92  11:08a
four1.scr        rw--a      8007  10-04-92   9:34a
ibmdos.com       r-hsa     28009   9-12-92   3:45p
lanman.scr       rw--a     1054  11-24-92   4:45p
report1.dft      rw--a     8128   9-02-92   5:30p
report2.dft      rw--a     9012  10-06-92   9:30a
old.scr          rw--a     2045   8-08-92   8:30p
list             rw--a     3206  11-08-92   4:04p
                12 Files      19.13 Megabytes free
C:>
```

Renaming HP-UX System Files

The **`uren`** command enables you to rename an HP-UX system file or directory. Specifically, you can use it to change HP-UX system filenames on the server that are invalid for the DOS system to filenames that are valid.

This command is useful if you created a file while logged in as an HP-UX system user and now want to access that file from an DOS client.

To rename an HP-UX system file, follow these steps at the DOS prompt on a client:

1. Connect to the shared directory on the server that contains the **`uren`** command (usually `\\server1\DOSUTIL`), and set your `PATH` variable to that drive.

2. Use the **cd** command to change to the directory that contains the file.
3. Type the following:
uren name1 name2
where: *name1* is the current HP-UX system filename.
and *name2* is the new filename. (Make sure that the new filename complies with the DOS filename conventions.)
4. Press <Return>.

Using the **uren** Command to Move Files

Because the **uren** command accepts full pathnames, you also can use it to move a file from one HP-UX system directory to another. For example, to move the file **budget** from the **report** subdirectory to the **memos** subdirectory, and to rename the moved file **1qbudget**, enter the following command:

```
uren \report\budget \memos\1qbudget
```

The **uren** command also enables you to move one or more files to another directory by entering the command in the following format:

```
uren name1 name2 ... directoryname
```

Replace *directoryname* with the name of the destination directory.

NOTE

You cannot use the DOS wildcard characters (* and ?) with the **uren** command. In addition, you cannot use the **uren** command to move a file from one drive to another.

Changing HP-UX System Permissions for AS/U Files

Because the Advanced Server/9000 runs on the HP-UX operating system, all Advanced Server/9000 files stored on the server are HP-UX system files with HP-UX system access permissions. The HP-UX system access permissions on an Advanced Server/9000 file will always agree with the Advanced Server/9000 access permissions unless the HP-UX system access permissions are explicitly changed. If HP-UX system access permissions are modified, they can prevent access to a file or directory even if Advanced Server/9000 access permissions grant access to the resource.

Handling Files

Managing Files between HP-UX and DOS Clients

The `uchmod` command enables you to change HP-UX system access permissions on a file to resolve access conflicts.

Use the `udir` command to display the current HP-UX system access permissions for a file.

Handling Incompatible File Formats

Different operating systems store files in different formats. For this reason, even if you can connect to a shared directory that contains a file you wish to use, you may not be able to open the file, or if you are able to open the file, it may be inappropriately formatted for your environment.

For example, suppose the following file was created with an HP-UX system text editor:

```
Dear Bob:
This letter is in response to your inquiry of February 25.
The information you requested is enclosed, along with other
materials that should help you evaluate our product line.
```

If you look at this file with the DOS `type` command, you would see the following:

```
Dear Bob:
  This letter is in response to your inquiry of February 25.
he information you requested is enclosed, along with other
terials that should help you evaluate our product line.
```

Similarly, if you had created the original file using an DOS editor and listed it with the HP-UX system `cat -v` command, you would see the following:

```
Dear Bob:^M
^M
This letter is in response to your inquiry of February 25.^M
The information you requested is enclosed, along with other^M
materials that should help you evaluate our product line.^M
^Z
```

This is because, in the HP-UX system, each line of text ends with a line-feed character. In the DOS system, however, each line of text ends with a carriage-return character, followed by a line-feed character.

If you need to convert text files from one operating system format to another, the Advanced Server/9000 provides a conversion utility, the `ud` command, which is described in the next section. The `ud` command can be used to translate a text file from DOS format to the HP-UX system format, or vice versa.

Using `ud` to Convert between DOS and HP-UX

The `ud` command converts a text file from DOS to HP-UX format or HP-UX to DOS. It is intended only for text files. Do not use this command on non-text data or executable files. The `ud` command is available in the **DOSUTIL** share or the HP-UX command prompt in **/opt/asu/lanman/bin**.

To convert a file, do the following:

1. Connect to the shared directory containing the `ud` command (usually `\\server1\DOSUTIL` and set your `PATH` variable to this drive.
2. At the DOS prompt, type the following:

```
ud [ option ] filename1 > filename2
```

Replace *option* with one of the three options discussed in the next section, or leave it blank to convert DOS to HP-UX and vice versa. Replace *filename1* with the name of the original file. Replace *filename2* with the name for the new, converted file. The filenames must be different from each other. For example, to convert an HP-UX file named **hpuxtext** to a DOS file named **systemt**, type the following:

```
ud -d hpuxtext > systemt
```

Press <Return>.

The `ud` command rewrites the file `hpuxtext` in DOS format and puts it in a file named `systemt`. The original `hpuxtext` file remains unchanged.

Guidelines for Using the `ud` Command

When you are not sure of the format of a text file, use the `ud` command with the `-d` or `-u` option to convert the file to the format you need. If the file is already in that format, the command output (`filename2`) will be identical to the original file.

If you do not enter a second filename, the file is converted and its text is displayed on your screen.

CAUTION

If you enter a second filename, be sure the filename is different from the first filename. If the filename is the same, the contents of the file that you want to convert will be deleted.

Options

The `ud` command has the following options:

- `-d` Converts a file to DOS format.
- `-u` Converts a file to HP-UX system format.
- `-m` Converts a file to Macintosh format.
- `-z` Affects the `^z` character. DOS files often have `^z` as the last byte in the file. When converting an HP-UX system file to DOS format, the `-z` parameter does not put `^z` at the end of the file. When converting an DOS file, the `-z` parameter forces `ud` to ignore any `^z` characters in the file. Without the `-z` parameter, the conversion stops when the first `^z` is encountered.

NOTE

If you use either `-d` or `-u` for a file that is already in the specified conversion format, the file remains unchanged and a new file is also created in the specified format.

Piping and Redirecting Converted Files

You can use the pipe operator (`|`) with the `ud` command to send a reformatted file to a program.

For example, to convert a file named **hpuxtext** from HP-UX system format to DOS format and display the converted file a screenful at a time, pipe the output of `ud` to the DOS `more` utility by entering the following command:

```
ud -d f:hpuxtext | more
```

Press `<Return>`.

In this example, drive F: is linked to the server directory that contains the **hpuxtext** file, and the `more` utility is in your path.

Piping is especially useful with DOS commands, such as `sort`, which use a carriage return to determine where each line ends in the file. Because files in HP-UX system format do not identify line ends by carriage returns, the files must be converted to DOS format for the `sort` command to operate properly. You can then pipe the converted text to the `sort` command. For example, type the following:

```
ud -d hpuxtext | sort
```

This example displays the sorted text on your screen. To store the results in a new file called **text.srt**, you can use the redirection character (>) as follows: `ud -d hpuxtext | sort > text.srt`

Configuring Reported Disk Space

Maximum disk space reported can be controlled by configuring the **maxdiskspacereported** parameter in the **hpparms** section of **lanman.ini** file. Prior to the addition of this parameter, when a disk on an Advanced Server 9000 machine had total disk space larger than 2 GB, AS/U reported to client machines that the total disk was 0 bytes and there were 0 bytes free. The parameter **maxdiskspacereported** has the default value of **0**; a maximum value of **4194303** (in KBytes). By setting the parameter **maxdiskspacereported** to a value between **0** and **4194303**, you instruct Advanced Server/9000 to report a maximum free disk of that value even though the actual free disk space could be larger. Advanced Server/9000 may report the disk space when a DOS, Windows 95, a Windows NT Workstation, or Windows for Workgroups client does a **dir** command in a shared directory. Example: suppose there is a directory on a UNIX system that has 937418 KB free disk space. Consider the following cases:

1. Set the parameter **maxdiskspacereported** to a value between **0** and **4194303**.
 - Set the parameter **maxdiskspacereported** to 500000. Restart AS/U.
 - Share a directory.
 - From a Window NT Workstation, access the shared directory, then do a **dir** command.
2. The output from the **dir** command will show only 500000 KB of free disk space while there is actually 937418 KB of free disk space.
3. Set the parameter **maxdiskspacereported** to **0** (default value).
 - Set the parameter **maxdiskspacereported** to **0**. Restart AS/U.
 - From a DOS client, access the shared directory, then do a **dir** command.

The output from the **dir** command will show 937418 KB of free disk space.

3 Printing

AS/U Spooler Service

The AS/U spooler service was designed with a limited administrator definable interface to the HP-UX spooler. In addition to the native HP-UX lp spoolers, the following HP-UX spoolers have been tested for co-existence with AS/U: OpenSpool/UX and HPDPS. The following subsections show the AS/U **lanman.ini** entries for the HP-UX native lp spooler, OpenSpool/UX spooler, and the HPDPS spooler:

AS/U Support of Native lp Spooler

Following are the lanman.ini entries for the AS/U spooler with their default values for operation with the HP-UX native lp spooler.

```
[spooler]
```

cancelcmd = LANG=C /usr/bin/cancel %s Fully qualified path to HP-UX command to cancel job-id %s.

cancelkey = **cancelled** Upon the canceling of a print job, the output (stdout) of the cancel command is checked for this entry. The cancel operation succeeds if this string is found.

lpcmd = LANG=C /usr/bin/lp -d%s Fully qualified path to HP-UX command to submit destination %s.

lpcopiesopt = -n%d HP-UX switch to be used with lpcmd to specify number of copies to print, where %d is number of copies.

lpkey = **request id is** %s Upon submittal of a job to print, the output (stdout) of the command is scanned for this string, where %s will be the position of the space delimited job-id returned by the HP-UX spooler.

lptitleopt = -t"%s" HP-UX switch to be used with lpcmd to specify the title of a print job, where %s is the title.

statjcmd = LANG=C /usr/bin/lpstat %s Fully qualified path to HP-UX command to check for the status of a job, given its job-id %s. Note that this job-id must be the same as that which was returned and scanned in by the entry lpkey.

statjkey = %[^\\n]-%[0-9] Upon execution of statjcmd, the output (stdout) of the command is scanned for this entry. The above fscanf(3S) regular expression searches for xxx-yyy, where yyy are digits.

statjpkey = \ on \ Upon execution of statjcmd, the output (stdout) of the command is scanned for this entry. Note that the \ characters serve to include spaces on both side of “on”. If this is found, the job is considered printing by the AS/U spooler.

statskey = - This entry specifies the delimiter which separates the printer name and job number in the job-id returned by the HP-UX spooler. This entry must reflect the delimiter in the entry statjkey. For example, the default works for the HP-UX lp spooler's designation lj3_2-726 for a print job.

statpcmd = LANG=C /usr/bin/lpstat -p%s Fully qualified path to HP-UX command to check for existence of the printer %s.

statpkey = **printer** Upon execution of the statpcmd, the output (stdout) of the command is scanned for this entry. If entry exists, the printer exists. Technically, the *cmd entries are used as the format for fprintf(3S) calls in the AS/U spooler. The *key entries are used as the format for fscanf(3S).

CAUTION

Incorrect information for these entries will almost certainly break the AS/U spooler! For example, the number of % selectors must never be greater than that which is given in the default.

AS/U Support of OpenSpool/UX Spooler

Following are the AS/U lanman.ini entries for the HP-UX OpenSpool/UX spooler:

```
[spooler]
cancelcmd=LANG=C /opt/openspool/runtime-sw/bin/npdel -v %s
cancelkey=deleted
lpkey=Print-request ID is %[^.]
statjcmd=LANG=C /opt/openspool/runtime-sw/bin/npshow %s
statjkey=%[^_\\n]_[0-9]
statjskey=_
lptitleopt=-\T"%s"
statpcmd=LANG=C /opt/openspool/runtime-sw/bin/npstat -q%s
statpkey=accepting
lpcopiesopt=-c%d
lpcmd=LANG=C /opt/openspool/runtime-sw/bin/np -q%s
```

Printing
AS/U Spooler Service

AS/U Support of HPDPS Spooler

AS/U supports HPDPS printers in one of two modes: LP emulation and native HPDPS.

AS/U and HPDPS in LP emulation mode:

AS/U supports HPDPS printers via the LP commands without changing the AS/U configuration. To use an HPDPS print destination under LP emulation with AS/U, simply add the printer to HPDPS, then add this printer to AS/U via the commands while the AS/U server is running:

```
net share asu_queue1=hpdps_lp1 /print
```

or alternatively:

```
net share asu_queue1 # net print asu_queue1 /route:hpdps_lp1
```

AS/U sees the printer hpdps_lp1 in exactly the same way as LP spooler printers in this mode.

AS/U and HPDPS in native mode:

AS/U may support HPDPS exclusively with the following settings in the [spooler] section of the **lanman.ini** file:

```
[spooler]
cancelcmd = LANG=C PD_CONFIRM_DELETE=no /opt/pd/bin/pdrm -r0 %s
cancelkey =
lpcmd = LANG=C /opt/pd/bin/pdpr -g -rbrief -Nnone -p%s
lpkey = %*s %s
lptitleopt = -t"%s"
statjcmd = LANG=C /opt/pd/bin/pdls -g %s
statjkey = %*s %[^:\n]:%[0-9]
statjpkey = processing
statjskey = :
statpcmd = LANG=C /opt/pd/bin/pdls -cprinter %s
statpkey = Printer
```

The AS/U server must be restarted after the above entries are changed. Note that the entries above *must* be entered *exactly*. Incorrect values for the [spooler] entries will prevent the AS/U server from functioning properly. HPDPS printers may now be added to AS/U in the usual manner:

```
# net share asu_queue1=hpdps_lp1 /print
```

or alternatively:

```
# net share asu_queue1  
# net print asu_queue1 /route:hpdps_lp1
```

In HPDPS native mode support, AS/U will not be able to print to any other spoolers' destinations (LP spooler, OpenSpool/UX, for example). LP emulation mode is suggested for systems with multiple spoolers whose printers are used by AS/U.

When AS/U is in HPDPS native mode, the print options must be valid HPDPS options. For example, AS/U queues with the options set by the command:

```
# net print asu_queue1 /parms:"types=-oduplex" /options
```

will cause the AS/U device to which the queue is routed to enter an error state since the HPDPS command to print does not understand **-oduplex**. The correct options must be specified for HPDPS:

```
# net print asu_queue1 /parms:"types=-xsides=2" /options
```

As with LP options, use a comma instead of a space in the /parms: "types=" parameter. For example, use:

```
# net print asu_queue1  
/parms:"types=-xsides=2,-xdocument-format=ps" /options
```

instead of:

```
# net print asu_queue1 /parms:"types=-xsides=2  
-xdocument-format=ps" /options
```

HPDPS and Remote HP-UX LP Printers:

The way AS/U routes HPDPS printers to remote HP-UX LP destinations is governed by HPDPS's support of the remote LP printers. Currently HPDPS printers routed to HP-UX remote LP printers will not send the **-tjob name (-tjob title** in HPDPS LP emulation) to the remote LP printers. Until this is fixed by HPDPS, remote LP printer destinations for HPDPS printers will not have the AS/U client's name on their jobs' banner pages.

The **-xprinter-pass-through=** options may be used to send extra LP options to remote LP printers from HPDPS native printers. For example, the LP emulation mode command for HPDPS printer rlp to a remote LP printer:

```
# lp -dhpdpdps_rlp1 -oraw pclfilename  
# lp -dhpdpdps_rlp2 -onb pclfilename
```

is equivalent to the HPDPS native command:

Printing
AS/U Spooler Service

```
# pdpr -phpdps_rlp1 -xprinter-pass-through=raw pclfilename  
# pdpr -phpdps_rlp2 -xprinter-pass-through=nb pclfilename
```

and if AS/U is in HPDPS native mode, the queue would be configured by:

```
# net print asu_queue1=hpdps_rlp1 /print  
# net print asu_queue1  
/parms:"types=-printer-pass-through=raw" /options  
# net print asu_queue2=hpdps_rlp2 /print  
# net print asu_queue2  
/parms:"types=-xprinter-pass-through=nb" /options
```

Printing with more than one remote LP option is not currently available via native HPDPS. Jobs sent from HPDPS to remote LP printers will be considered printed by HPDPS the moment they leave HPDPS, even if their remote LP printer destinations are disabled and queueing all incoming jobs.

4 **Using CD ROMs**

Using CD ROMs

The HP-UX 10.10 operating system and later releases include a set of pfs (portable file system) programs for use with CD-ROM file systems. The `pfs_mount` program includes filename-translation options to convert file and directory names from uppercase to lowercase and to suppress version numbers on filenames. These options can be used to allow PC client users access to CD-ROM files in mounted directories shared on the AS/U server.

Using the `pfs_mount` translation options eliminates the need to run the `cdrutil` utility to establish symbolic links to provide the necessary translation for each CD. The `cdrutil` utility is for use with systems that do not have the pfs programs. It is provided with AS/U in the `/opt/asu/lanman/bin` directory. Please refer to the pfs man pages for more information on usage. The following example shows how you might use the `pfs_mount` program with the AS/U server. It assumes that the pfs mount daemons and RPC server have already been started.

```
pfs_mount -x unix -t iso9660 -o ro /dev/dsk/c0t4d0 /cdrom
```

This command mounts the CD specifying lowercase filenames and version suppression (`-x unix`) as well as ISO9660 format and read-only. The device file may be different on your system. You must create the `/cdrom` subdirectory manually.

To enable PC client access, you would then share the `/cdrom` directory.

```
net share cdrom=c:/cdrom
```

5 **Operating with NFS**

Using NFS Mounted Resources with Advanced Server/9000

NFS mounted resources can be shared like any other local resources on the AS/U server. However, you should exercise caution when using NFS mounted resources with AS/U. Please note the following risks and recommendations:

- Read-only access to NFS mounts used with AS/U is strongly recommended to insure data integrity. AS/U will consider writes complete before they are actually written to the remote NFS server file system.
- Root access must be enabled across NFS mounts when NFS mounts are used as shares in AS/U. AS/U initially creates a file as root and then changes the ownership to the appropriate user.
- The special AS/U users (`lmxadmin`, `lmworld`, etc.) and groups (`DOS---`, etc.) must be configured on the system providing the NFS mounted resources. These will need to be created manually if AS/U is not installed on the system. AS/U may set the file ownership to one of these users or groups.
- Ensure that the uids and gids in the `/etc/passwd` files on all systems match. This is necessary to ensure that HP-UX access permissions are interpreted correctly.

CAUTION

The reliability of the AS/U server is only as good as the NFS mounts beneath it. If an NFS mount goes down, not only may data be lost, but any AS/U server process (`lmx.srv`) which is attempting to access the remote file system hangs. In such cases, all the clients associated with these processes may hang and new connection requests may fail. These `lmx.srv` processes will hang forever if the NFS mount is a hard mount. The `lmx.srv` process will eventually return if the NFS mount is a soft mount ; however, all client connections associated with the `lmx.srv` process may be dropped if the NFS timeout period (including retries and retransmissions) is longer than the session timeout parameter configured on the client for any clients associated with that `lmx.srv` process.

The **UseNfsLocks** and **RootOwnsFilesCreatedOnNFS** registry values are associated with NFS usage. The **UseNfsLocks** value is in effect only if **UseUnixLocks** is set to 1. It works as follows:

- **UseNfsLocks 1** The record locks on NFS files created by clients are reflected in the NFS file system. If this UNIX lock fails because the NFS lock manager is not running, then AS/U returns an error.
- **UseNfsLocks 0** The record locks created by clients on the NFS files are reflected in the NFS file system as in the previous case. But if this UNIX lock fails because the NFS lock manager is not running, then AS/U ignores that error and returns success status.

In most circumstances, the AS/U server will return an error if the lock request is not granted. The **RootOwnsFilesCreatedOnNFS** value is set to 1 by default and should not be changed.

Multiple AS/U Server Access to NFS Files

File sharing and locking on NFS mounts has special considerations with AS/U in the following environment.

1. An NFS file system is mounted by more than one AS/U server.
 2. A mounted file is accessed concurrently by more than one AS/U server on behalf of its clients.
- By default, the file record lock information from one AS/U server will not be propagated to the others across NFS, so two servers can own a lock on the same file at the same time. Set the registry value **UseUnixLocks** to **1** to coordinate these locks through the NFS file system.
 - By default, the opportunistic lock information for an open file on one AS/U server will not be propagated to the other across NFS. So an AS/U server can open a file even though the file is already opened with *oplock* by another AS/U server. To prevent this from happening, disable the *oplock* option on the server. This can be done by setting the registry value **UseOplocks** to **0**.

NOTE

The default settings for the **UseUnixLocks** and **UseOplocks** keywords are chosen to optimize performance. Make the suggested changes only if you need file locking information to be propagated across NFS mounts or to other HP-UX applications running on the AS/U server.

- The file open mode sharing information (like DENY_ALL, DENY_WRITE, DENY_READ etc.) for an open file on one AS/U server will not be propagated to the other servers across NFS. So more than one server may open the NFS mounted file with a sharing mode like DENY_WRITE (which should not be allowed). To prevent problems from occurring, applications need to explicitly lock files when updating them rather than relying on the file open mode information to prevent other readers or writers.

Configuring for NIS Interoperability

Advanced Server/9000 has been enhanced to install on systems that have NIS enabled. When Advanced Server/9000 is operating in an NIS environment, the registry value **CreateUnixUser** should not be used to create UNIX user accounts automatically on the server. When NIS is enabled, the **CreateUnixUser** parameter should be set to 0. The AS/U user should be mapped to a UNIX user using mapuname, and the UNIX user should be created using standard UNIX commands.

NOTE

The **lanman.ini** parameter [lmxserver] `stacksize` must be at least 40000 if NIS is used. The default value is 40000.

Operating with NFS
Configuring for NIS Interoperability

6 **Logging and Tuning**

Event Logging

Following are the supported ways you can view the Event Log:

- Use the Event Viewer Utility in Windows NT 4.0 or 3.51.
- Use the Event Viewer Utility in Windows 95.
- Type the **/opt/asu/lanman/bin/elfread** command at the HP-UX command prompt.

HP does *not* recommend viewing event logs from clients other than Windows NT or Windows 95.

Viewing a Log Archived in Log File Format

NOTE

This procedure will make the saved event log your current system log. Any new events will be logged to the end of the current log file not the previously active log file that was renamed to a temporary filename. You may want to save your active log before following these steps. After you are finished viewing the saved log, copy the active log file back to **sysevent.evt**.

To display an archived log file that was saved in log file format to a shared drive on the server:

1. From the HP-UX command line (logged in as root):
`cd /var/opt/asu/lanman/logs`
then:
`cp sysevent.evt temporary_filename`
2. Copy your archived event log from the shared directory where it resides to:
/var opt/asu/lanman/logs
and name it **sysevent.evt**.
3. You can then view it in the event viewer.

Event Logging is operational for most successful audit events. See the *Advanced Server/9000 Concepts and Planning Guide* for information on managing the audit policy. In some cases, failure events are not logged.

Tuning

AS/U server performance is sensitive to client usage levels. To improve performance from clients to AS/U servers, connections are established with the TCP No Delay option. This option removes a delay for certain SMB transactions.

The registry values and **lanman.ini** parameters are set to default levels that should be appropriate for the average installation. Tuning individual parameters for specific server usage can often improve performance. Two such parameters that are sensitive to tuning are the registry value **VCDistribution** and the **lanman.ini** parameter **maxclients**.

The default value for the registry value **LockNapInMSec** is based on benchmark tuning. The optimal value for a particular installation is workload-dependent and may require some experimentation to determine.

Configuring NetBIOS Memory Usage

The configurable kernel parameter **nrfc_nb** allows you to specify the maximum number of NetBIOS connections that will be in use on a system. This parameter is used to tune the amount of memory used by NetBIOS.

Acceptable Values:

Minimum: 100

Maximum: 2048

Default: 1024

The number of connections is closely bound to the system memory usage. More memory will be used when more connections are configured. Too little memory will prevent NetBIOS from operating properly. Therefore, unless it is needed, we do not recommend changing the default value. Increase the value if you receive either of the following NetBIOS warning messages on the console or syslog: the **rncb** warning message "Resource map low" or "No resource map available."

The value can be modified through SAM or by editing the **/stand/system** file on the system. An error will be returned if the value is outside the boundaries of the minimum and maximum values.

Batch Oplocks Performance

Batch oplocks, used by Windows NT, are implemented in this release. Unlike exclusive oplocks, which allowed a client to open a file for exclusive access, batch oplocks enable a client to repeatedly open and close a file without forcing a remote server to physically open and close it. A client can keep a file open until another client wants to modify it (for example, to move the file, delete the file, get file information, or set file information). This process more efficiently handles DOS, which traditionally forces batch files to be opened and closed each time a line is read.

Detecting and Reporting File Write Failure

AS/U currently performs physical file writes after sending the SMB response back to the client. While this produces the best performance, it prevents the server from correctly responding to out of disk space conditions. This means a client can write to a file and never know that the write failed because the HP-UX file system is out of space. AS/U allows detection and reporting of write failures.

The registry value **WriteBehind** controls whether the server issues the write system call before or after responding to the client. The default value for this parameter is **1** which matches the current AS/U behavior. If the value is **1**, the server sends an SMB response back to the client and then performs the physical file writes. If the value is **0**, the server issues the write system call and returns the appropriate message to the client based on the results of the write.

Choosing **1** provides the best performance while choosing **0** will ensure that the client receives write errors such as disk full.

Guidelines for Tuning HP-UX Kernel Parameters

The following guidelines are provided for tuning HP-UX kernel parameters for the Advanced Server/9000. For more information on changing kernel tuning parameters for HP-UX, refer to the *HP-UX System Administration Tasks* manual.

For determining HP-UX kernel tuning parameters values that use the number of `lmx.srv` processes in their calculations, use the largest number of processes that you may expect to exist on your system.

The number of `lmx.srv` processes that can exist simultaneously on your system is based on the number of active Advanced Server/9000 users and the registry value: **VCdistribution**.

- **maxfiles**: Soft Limit on Number of Files a Process May Open. This parameter should be at least as large as the number of active Advanced Server/9000 users.
- **nfile**: Max Number of Open Files. this parameter should reflect non-Advanced Server/9000 usage plus at least 10 times the number of `lmx.srv` processes plus 1.3 times the number of active clients:
 $nfile = non\text{-}Advanced\ Server/9000_usage + (10 * no_lmx.srv_procs.) + (1.3 * no_active_clients)$

This parameter should be increased if your usage of Advanced Server/9000 involves extensive file access by clients.

- **nflocks**: Maximum Number of File Locks. Advanced Server/9000 only puts HP-UX locks on files if the registry value **UseUnixLocks** is set to **1**.

If **UseUnixLocks** is set to **1**, set `nflocks` to the number of locks that are expected to be used simultaneously on the system.

- **ninode**: Maximum Number of Open Inodes. It is suggested that this parameter be set equal to **nfile**.
- **nproc**: Maximum Number of Processes. This parameter should reflect non-Advanced Server/9000 usage plus the number of `lmx.srv` processes plus 10:
 $nproc = non\text{-}Advanced\ Server/9000_usage + no_lmx.srv_procs. + 10$

Guidelines for Tuning HP-UX Kernel Parameters

- **semnu**: Number of Semaphore Undo Structures on the System. This parameter should reflect non-Advanced Server/9000 usage plus the number of `lmx.srv` processes on your system.

The following HP-UX kernel tuning parameter values are suggested for proper operation of the Advanced Server/9000. The default values for these parameters as shipped with HP-UX releases are usually adequate.

- **semmni**: Number of Semaphore Identifiers. This parameter should be increased by one (1) if your system is currently operating at this parameter's limit.
- **semmns**: Maximum Number of Semaphores. Increase this parameter by three (3) if your system is currently operating at this parameter's limit.
- **semume**: Semaphore Undo Entries per Process. Set this parameter to at least three (3) for Advanced Server/9000.
- **shmmax**: Maximum Shared Memory Segment (bytes). For Advanced Server/9000, this parameter should be at least five (5) megabytes. The system default is usually more than adequate.
- **shmmni**: Number of Shared Memory Identifiers. Increase this parameter by two (2) if your system is currently operating at this parameter's limit.
- **shmseg**: Shared Memory Segments per process. for Advanced Server/9000, this parameter must be set to at least two (2).

7

AS/U in a Subnetted Domain

Advanced Server/9000 uses an IP broadcast based method to send datagrams to entire domains and to resolve NetBIOS names to IP addresses. These IP broadcasts are usually not routable across subnets. Thus, if you using Advanced Server/9000 in multi-subnet domain

environments, you need a way to forward domain based datagrams (for example, netlogon requests) to clients and servers on different subnets. You also need a way to resolve the NetBIOS names to IP address of clients and servers on different subnets. Listed below are some approaches to solving this problem with AS/U.

- Use a Windows NT WINS server.
- Manually configure entries in a NetBIOS name cache.

WINS Client Support

AS/U NetBIOS is WINS compliant. AS/U provides WINS client functionality as well as the ability to contact primary and secondary WINS servers. AS/U NetBIOS also contains features to enhance interoperability with Windows NT 4.0 clients. See the “Windows NT 4.0 Client Interoperability” section in this chapter for more details.

With WINS client support, AS/U servers can use a Windows NT WINS server to perform NetBIOS name registration and name resolution. Name registration is how each networked computer acquires a unique name. When an AS/U server starts, it registers itself with the WINS server. Name resolution identifies the specific IP address linked to a computer name.

NOTE

The AS/U server can not act as the WINS server. The database of WINS information is contained in a Windows NT server.

Previous versions of NetBIOS for AS/U registered and resolved names by sending UDP broadcasts over a computer subnet. This limited the NetBIOS name services to a single subnet. The method, also known as B-Node NetBIOS, is the default method used when WINS client support is not enabled.

When WINS client support is enabled, a WINS client first attempts to do name registration and name resolution by contacting a WINS server directly via a UDP unicast. If a WINS server is unavailable and/or doesn't respond, NetBIOS will revert to using its default method of using broadcasts to do name registration and name resolution. This method of first contacting the WINS server and then broadcasting if a WINS server is unavailable is known as H-Node NetBIOS.

When a secondary (or backup) WINS server is present, the WINS client performs name registration as follows: 1) try to contact primary WINS server (if configured), 2) if no response, try to contact the secondary WINS server (if configured), and 3) if no response, try broadcast.

When a secondary (or backup) WINS server is present, the WINS client performs name resolution as follows: 1) try to contact primary WINS server (if configured), 2) if no response or if failed, try to contact the secondary WINS server (if configured), and 3) if no response or if failed, try broadcast.

AS/U in a Subnetted Domain

WINS Client Support

The secondary WINS server can only be configured if a primary WINS server is also configured.

The NetBIOS name cache can still be used to access the IP address of a computer. To add or delete names in the local NetBIOS name cache, use the **nbutil** utility. When WINS client support is enabled, name resolution is done in the following order:

1. the local NetBIOS name cache is searched,
2. a name query is sent directly to a WINS server, and
3. a name query is sent by broadcast to the computers' local subnet.

The WINS server provides a distributed database for registering and querying dynamic computer name-to-IP address mapping in a routed network environment. With WINS client support, AS/U servers will operate more seamlessly in routed networks.

Windows NT 4.0 Client Interoperability

Two NetBIOS features provide interoperability with Windows NT 4.0 clients. AS/U NetBIOS allows Windows NT 4.0 clients to connect to AS/U servers as follows:

- by using non-fully qualified DNS names or,
- by IP address (for example: `\\192.170.128.21\share`).

Enabling WINS Client Support

Use the following steps to enable WINS client support:

1. After installing AS/U, stop the AS/U server and RFC-NetBIOS.
 - a. **net stop server** (to stop AS/U Server)
 - b. **/opt/lmu/netbios/bin/nbutil -N stop** (to stop NetBIOS)
2. Configure the IP address of the WINS server in the NetBIOS configuration file (`/etc/opt/lmu/netbios/nbconfig`) using `/opt/lmu/netbios/bin/autoconfig`. The syntax is as follows (refer to the next section for a list of autoconfig options):
`/opt/lmu/netbios/bin/autoconfig -w WINS Server IP Address`

NOTE

Note: the IP address of the WINS server is not the IP address of the AS/U server.

Example:

/opt/lmu/netbios/bin/autoconfig -w 15.13.1.1

3. Restart NetBIOS and the AS/U Server
 - a. **/opt/lmu/netbios/bin/nbutil -N start** (to start NetBIOS).
 - b. **net start server** (to start AS/U Server)
4. Ensure all clients are configured for WINS. Clients supporting WINS are Windows NT clients, Windows 95, and Windows for Workgroups 3.11 with 32-bit TCP/IP. LAN Manager 2.2c clients cannot use WINS.

Disabling WINS Client Support

Use the following steps to disable WINS client support:

1. Stop the AS/U server and RFC-NetBIOS.
 - net stop server** (to stop the AS/U Server)
 - /opt/lmu/netbios/bin/nbutil stop** (to stop NetBIOS).
2. Remove the WINS server IP address in the NetBIOS configuration file (**/etc/opt/lmu/netbios/nbconfig**) using **/opt/lmu/netbios/bin/autoconfig**.
 - Example: **/opt/lmu/netbios/bin/autoconfig -w 0 [-s 0]**
3. Restart NetBIOS and the AS/U Server.
 - a. **/opt/lmu/netbios/bin/nbutil -N start** (to start NetBIOS).
 - b. **net start server** (to start the AS/U Server)

Using the Autoconfig Utility

The **/opt/lmu/netbios/bin/autoconfig** utility saves existing configuration data in the NetBIOS **nbconfig** file. It only updates the data related to the option you specify. For example, if you specify **autoconfig -w IP address**, the utility adds information about the WINS server address to the previously saved data.

Following are the options for the **autoconfig** utility:

**autoconfig [-l lan#][-u 1 | 0][-w WINS server IP address]
[-s Secondary WINS server IP address][-i IP address]
[-b Broadcast address][-m Subnet mask]**

- **-l lan#** specify a LAN card to configure NetBIOS to. example:
autoconfig -l lan0
- **-u 1 | 0** configure UDP ports to single LAN card
- **-w WINS server IP address** specify a WINS Server IP Address
example: **autoconfig -w 15.13.2.3**
- **-s secondary WINS server IP address** specify a secondary
(backup) WINS Server IP Address example: **autoconfig -s 15.13.2.4**
- **-i IP address** specify an IP address that NetBIOS should bind to.
example: **autoconfig -i 15.13.2.5**
- **-b Broadcast address** specify a broadcast Address example:
autoconfig -v 15.13.255.255
- **-m Subnet mask** specify a subnet mask for NetBIOS to use.
example: **autoconfig -m 255.255.248.0**

Usage Notes

The **autoconfig -l** option is normally used to configure NetBIOS. This option will configure NetBIOS with the IP address, broadcast address, and subnet mask configured for the *lan* interface specified. The **autoconfig -i -b, -m** and **-u** options are only needed in special circumstances when you need to override the default configuration information obtained from the *lan* interface with the **-l** option.

Name Resolution in Subnetted Domains without WINS

If your Advanced Server domain does not have WINS, you can manually configure NetBIOS names in a cache, hostfile or database. For Microsoft clients and servers you must manually populate the WINS name server database, the DNS database, or the LMHOSTS file with the name and IP address of the Advanced Server/9000. For Advanced Server/9000 servers, you must manually populate the NetBIOS name caches with the names and IP addresses of the NT Server and Advanced Server/9000s. (There is no need to populate client names in the Advanced Server/9000 NetBIOS name cache because it supports from-name caching).

From-name caching is when NetBIOS caches the source name and IP address of datagrams sent from the local subnet or a different subnet. It is for datagrams sent to a *unique* name register by the server or datagrams sent from different subnets. It adds the sender NetBIOS name and IP address to the name cache with a life of 10 minutes. From-name caching is only applicable for unique client and server NetBIOS names not domain (group) names.

NetBIOS will multicast datagrams sent to a group name with multiple entries in the name cache.

These approaches enable the following features to work in a subnetted domain:

1. UAS Replication
2. File Replication
3. Trusted Domains
4. Remote Administration
5. Mapuname
6. Client Logon

Manually Configuring NetBIOS Names

If an Advanced Server domain spans routers and does not use WINS, Advanced Server/9000 can operate in the domain that spans routers by manually populating the NetBIOS name caches on the Advanced Server/9000s. Every AS/U server in each subnet must have a name cache that contains the server names and IP addresses of every AS/U and NT Server within the domain that is on a different subnet. Also, the name cache must contain an entry for the domain name and IP address of each AS/U and NT server on different subnets. This is done using the **nbutil** utility. See Advanced Server/9000 subnetted domain example.

Advanced Server/9000 Access

To allow an Advanced Server/9000 to access another Advanced Server/9000 and/or NT Server in the same domain but on different subnets, manually add the Server name and Domain name with their corresponding IP address of the remote Advanced Server/9000 and NT Servers to the Advanced Server/9000 NetBIOS name cache.

Example in a Subnetted Domain:

This example illustrates how to properly configure a NetBIOS name cache on a Advanced Server/9000 to enable functionality in a subnetted domain.

The domain 'SUB_DOM' contains NT and Advanced Server/9000s on multiple subnets. The following servers are in 'SUB_DOM'

AS/U Server 'ASU_Serv1' is on subnet A. Its IP address is 200.1.1.1.
AS/U Server 'ASU_Serv2' is on subnet B. Its IP address is 200.1.2.1. The
NT Server 'NT_Serv3' is on subnet B. Its IP address is 200.1.2.2.

To manually populate the cache on ASU_Serv1, issue the following commands.

```
nbutil -a ASU_Serv2 -A 200.1.2.1 -V
```

```
nbutil -a NT_Serv3 -A 200.1.2.2 -V
```

```
nbutil -a SUB_DOM -A 200.1.2.1 -D
```

```
nbutil -a SUB_DOM -A 200.1.2.2 -D
```

To manually populate the cache on ASU_Serv2, issue the following commands.

```
nbutil -a ASU_Serv1 -A 200.1.1.1 -V
```

```
nbutil -a SUB_DOM -A 200.1.1.1 -D
```

You can also add entries to the Advanced Server/9000 NetBIOS name cache by editing the `/etc/opt/lmu/netbios/nbhost` file and executing `nbutil -L` to load the entries from the file to the cache.

NOTE

The location of the NetBIOS name cache was moved from `/etc/opt/lmu/wanext/nbhost` to `/etc/opt/lmu/netbios/nbhost`. When the name cache is loaded with the `nbutil -L` or when the name cache is saved with `nbutil -s`, the file `/etc/opt/lmu/netbios/nbhost` is used. Move any existing `nbhost` file to `/etc/opt/lmu/netbios/nbhost`.

Below are the `/etc/opt/lmu/netbios/nbhost` file entries of ASU_Serv1 and ASU_Serv2 in the above example:

`/etc/opt/lmu/netbios/nbhost` file on ASU_Serv1

```
ASU_Serv2 200.1.2.1 #SERVER  
NT_Serv3 200.1.2.2 #SERVER  
SUB_DOM 200.1.2.1 #DOM  
SUB_DOM 200.1.2.2 #DOM
```

`/etc/opt/lmu/netbios/nbhost` file on ASU_Serv2

```
ASU_Serv1 200.1.1.1 #SERVER  
SUB_DOM 200.1.1.1 #DOM
```

NOTE

Note: It is important to use the `-V` and `-D` options with `nbutil` or the `#SERVER`, and `#DOM` keywords in the `nbhost` file in order to correctly populate the name cache.

Non Advanced Server/9000 Access

To allow a Windows NT 3.51 Server, Windows NT 3.51 Workstation, LAN Manager 2.2c client, or a Windows 95 client to access Advanced Server/9000s in the same domain but on a different subnet you must use at least one of the access methods listed below:

1. Enable WINS lookup on the client or NT Server and manually add each Advanced Server/9000 name and Domain name with their corresponding IP address into the database of the WINS server.

AS/U in a Subnetted Domain

Manually Configuring NetBIOS Names

2. Edit the client's or NT Server's **lmhosts** file to include each Advanced Server/9000's NetBIOS name and IP address with the #DOM:domain name option, that is, add the following line to the **lmhosts** file:

```
1.2.3.4 Server_name #PRE #DOM:Server_Dom
```

Administering the NetBIOS Name Cache

You can display and manipulate the entries in a name cache with the `nbtutil` command. You must be root to run `nbtutil`.

There is a maximum of 4096 entries in the NetBIOS name cache.

If you enter: `nbtutil ?` A menu of the options is displayed:

You can use the command line to specify `nbtutil` options.

The following table describes the options that you can specify with the `nbtutil` command.

Option	Description
<code>-a name -A address</code> <code>[-l char], [-v], [-D],</code> <code>[-P],</code>	Adds an entry to the cache with the specified NetBIOS name and IP address. <code>-l</code> sets the last byte for the name; a space (0x20) is the default. <code>-v</code> designates a NetBIOS server name and adds two entries into the name cache. <code>-D</code> designates a domain controller name and adds two entries into the name cache. <code>-P</code> designates a primary domain controller name.
<code>-c</code>	Clears the entire cache.
<code>-d name [-l hexbyte]</code>	Deletes an entry in the cache with the specified NetBIOS name. <code>-l</code> sets the last byte for the name; a space (0x20) is the default.
<code>-g name</code> <code>[-l hexbyte] [-v]</code>	Displays the IP address associated with the specified NetBIOS name. <code>-l</code> sets the last byte for the name; a space (0x20) is the default.
<code>-i</code>	Displays the status of the cache.
<code>-n name</code> <code>[-l hexbyte] -v</code>	Print NetBIOS name table (of the machine that has the NetBIOS name registered).

AS/U in a Subnetted Domain
Administering the NetBIOS Name Cache

Option	Description
-p [-v]	Prints the contents of the cache. -v displays the output in verbose mode.
-C	Print current NetBIOS configuration data.
-L	Loads entries from the /etc/opt/lmu/netbios/nbhost file into the proxy name cache.
-N start stop	Starts or stops NetBIOS.
-S	Save entries in the proxy name cache to the file /etc/opt/lmu/netbios/nbhost .

A NetBIOS name is 16 bytes long. If you specify a name that is less than 16 bytes, the name is padded with spaces.

Note that a NetBIOS name with a last byte of 0 is considered a *different* name than a name with a space for the last byte. For example, the following `nbutil` commands add *two* different entries to the proxy name cache:

```
nbutil -a duncan -A 18.13.112.155
nbutil -a duncan -A 18.13.112.155 -l 0
```

The first command adds the name `duncan` with a space as the last byte. The second command adds the name `duncan` with a 0 as the last byte. The `-v` option displays the entire NetBIOS name, including the pad characters and the last byte, in hexadecimal values. For example, if you enter:

```
nbutil -p -v
```

the two entries for the name `duncan` are displayed:

```
44 55 4E 43 41 4E 20 20 20 20 20 20 20 20 20 20 (DUNCAN)
Addr: 18.13.112.155
44 55 4E 43 41 4E 20 20 20 20 20 20 20 20 0 (DUNCAN)
Addr: 18.13.112.155
```

To delete the second entry for `duncan`, you must specify the `-l 0` option. For example, enter:

```
nbutil -d duncan -l 0
```

This removes the second entry for `duncan`. The name `duncan`, with a space as the last byte, remains in the proxy cache.

Using the `nbutil -L` option, the node's proxy name cache information can be loaded from the file `/etc/opt/lmu/netbios/nbhost`. You can edit the **nbhost** file to include NetBIOS names to IP address mappings following these guidelines:

- The file name you edit and use for the name cache must be **`/etc/opt/lmu/netbios/nbhost`**.
- Each entry must be on a separate line.
- Place the NetBIOS name in the first column, followed by the IP address.
- Separate the NetBIOS name and IP address by at least one space or tab.
- If the last character in the NetBIOS name (16th character) is a non-printing character, enclose the NetBIOS name in quotes and use `\nn` to specify the non-printing character as hexadecimal. For example: `"node78 \03"`
`15.2.125.234.`
- The `"#"` character is used to denote comments in the file.

The heading contents of the **nbhost** file contain the guidelines and example entries as shown below:

AS/U in a Subnetted Domain
Administering the NetBIOS Name Cache

```
#
# This is the NBHOST file used by the HP 9000 RFC NetBIOS Name Cache
#
# This file contains the mappings of NetBIOS names to IP addresses.
# Each entry should be kept on an individual line.
# The NetBIOS name should be placed in the first column followed by
# the IP address.
# The address and the computer name must be separated by at least one
# space or tab.
# The "#" character is used to denote comments.
#
# Non-printing characters to be used as the 16th and last character in
# the NetBIOS name must be embedded by first enclosing the NetBIOS name
# in quotations then using "\nn" notation to specify a hex value for the
# non-printing character.
#
# The RFC NetBIOS name cache supports both unique and group name entries.
# All NBHOST file entries are considered unique unless marked as group
# name.
# The group name marker "#GROUP" must be placed following the netbios
# name and IP address.
# The IP address and the group name marker must be separated by at least
# one space or tab.
#
# The following are sample entries
#
# rob_pc 15.1.12.34
# "mac_pc \00" 15.3.32.5
# "node78 \03" 15.2.125.234
# TEST.DOM 15.1.12.34 #GROUP
# TEST.DOM 15.3.121.48 #GROUP
```

8 Troubleshooting

This chapter describes how to troubleshoot a computer running Advanced Server for UNIX Systems. 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 Advanced Server involves gathering data about the problem and analyzing that data to determine the specific cause of the problem. Advanced Server 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 Advanced Server 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 Advanced 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.

Advanced Server Troubleshooting Tools

Advanced 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

Advanced Server includes multiple tools that can be used to assess the operational status of the server at any given time. As a server administrator, frequent assessment of server status will improve your ability 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 Viewer

A number of events related to the daily operation of the server can be tracked using Event Viewer. 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.

For information about Event Viewer, see Advanced Server Concepts and Planning.

NOTE

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

Server Statistics

Advanced 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 Server Manager. This provides details about current client-server sessions and the resources being used by those sessions.

Cumulative Statistics

To view cumulative server usage data, use the `net statistics` command at the Advanced 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 Advanced Server:

Statistic	Description
Statistics since	Tells when this set of statistics began (either at the last server startup or the last time the statistics were cleared).
Sessions accepted	Tells how many times users connected to the server.
Sessions timed-out	Tells how many user sessions were closed because of inactivity.
Sessions errored-out	Tells how many user sessions ended because of error.

Kilobytes sent	Tells how many KBytes of data the server transmitted.
Kilobytes received	Tells how many KBytes of data the server received.
Mean response time (msec)	Tells the average response time for processing remote server requests. This always will be 0 for UNIX system servers.
System errors	This does not apply to UNIX 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.
Comm devices accessed	Not supported on Advanced 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 UNIX system servers.

Session Information

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 Advanced Server 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 Advanced 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.

Closing Sessions

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 Advanced Server 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 Advanced Server command prompt.

Open Resources

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 Advanced 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 Advanced Server command prompt.

Print Subsystem Event Logging

Advanced Server maintains a separate print log for each printer share and each UNIX 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: `/var/opt/asu/lanman/shares/printlog`.

Tools Providing Automatic Status on the Server

Quick response time is critical when dealing with server problems. Being aware of a problem at the time it occurs can decrease greatly the effect that the problem may have on the server user community.

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

Alerter Service

Advanced Server 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 Advanced Server Registry.
- The number of bad access attempts exceeds a threshold set in the Advanced Server Registry.
- The number of bad password attempts exceeds a threshold set in the Advanced Server Registry.
- Errors were encountered during start of the Net Logon service.
- A printer is malfunctioning.

- A print request has been deleted or completed.

UNIX System and Advanced Server Features

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

For example, using the UNIX system job scheduling feature (CRON), various data gathering tools provided by Advanced Server, and some of the standard UNIX 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 UNIX system administrators at regular intervals.

Tools for Debugging Server Problems

Advanced Server includes UNIX system commands that can be used to troubleshoot server problems. These commands are executed at the Advanced 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 Advanced 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 Advanced 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.

Advanced Server 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  0:00lmx.alerter
root  17713 17461  0  12:03:32  0:00lmx.srv -s 1
root  17722 17874  0  12:03:35  0:00lmx.srv -s 2
root  17726  1      0  12:03:36  0:01lmx.dmn
root  17728  1      0  12:03:36  0:01lmx.browser
root  17744  1      0  12:03:28  0:00lmx.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, vnum=0) on 17713
ORANGE (nwnum=0, vnum=0) on 17713
PEAR (nwnum=0, vnum=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 vnum value specifies whether this is the client computer's first VC or an additional one.

regconfig

The `regconfig` command is used to query or change Advanced 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 and the AS/ U Administrator to change key values.)

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

For more information about the registry, see Appendix A, "Advanced Server Registry."

regcheck

The `regcheck` command is used to check and repair the Advanced Server Registry file. This command checks only the internal structure of the Advanced 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 wish 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.

For more information about the `lanman.ini` file, see the Appendix B, “Lanman.ini File.”

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 `man acladm` at the Advanced Server command prompt.

Troubleshooting Procedures

Troubleshooting Advanced Server 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

Advanced Server runs on a UNIX 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 Advanced 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 Advanced 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 Advanced 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 it is not a bad cable connection. For a single client it is easy to check to determine whether the problem occurs regardless of which server the client tries to use.

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 PING a server machine from a particular client, 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 Advanced 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 Advanced Server will not work. All Advanced 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 UNIX System Functionality

If all of the network connectivity modules check out properly, the next item to verify is the UNIX operating system on the computer hosting Advanced Server. 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 UNIX system administrator documentation.

Advanced Server 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.

Troubleshooting
Troubleshooting Procedures

- 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 Advanced Server

If you determine that all of the underlying software is functioning properly, then you should check Advanced Server 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 Advanced 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      34521   0       Feb28   5:03    lmx.ctrl
root      35681   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 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.

Troubleshooting
Troubleshooting Procedures

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

```
SYSTEM\CurrentControlSet\Services\Advanced  
Server\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$  
NETLOGON  
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, 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
Advanced Server for UNIX Systems
Sharename      Type      Used as      Comment
-----
DOSUTIL        Disk      DOS Utilities
NETLOGON       Disk      Logon Scripts Directory
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 Advanced 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 Advanced 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 UNIX system access permissions.
 - If necessary, use the MS-DOS `attrib` to change the file attributes. You also can use the Properties menu in Windows Explorer.
 - Use the `udir` command to display UNIX system permissions (user, owner, group).

Differences Between System Access Permissions

This section describes the differences between the access permissions of the UNIX system and a network running Advanced Server software. It explains the UNIX system access permissions — how to display them and how to change them with the `uchmod` command. The `uchmod` command is an MS-DOS executable command residing in the `DOSUTIL` shared directory.

An Advanced Server is a computer that also is running the UNIX operating system. All of its files also are UNIX system files with their own set of UNIX system access permissions.

UNIX system access permissions on an Advanced Server file will be compatible with the Advanced Server only if the UNIX system access permissions are changed explicitly. If these UNIX system access permissions are modified, they can prevent access to a file or directory even if Advanced Server access permissions grant access.

For example, if a user has Advanced Server change permission for a file, then this file needs to have the UNIX system equivalent of change permission (RWX) in order for the user to perform all of the operations allowed by the Advanced Server change permission (read, write, create, and execute).

However, if you changed the file's UNIX system permissions, eliminating the write (W) permission for everyone other than the file's owner, then no one but the owner can alter or remove the file, regardless of the generous Advanced Server permissions.

Advanced Server automatically adds the appropriate UNIX system access permissions when files and directories are created on the network. These permissions are determined by two keywords in the Advanced Server Registry: `UnixFilePerms` and `UnixDirectoryPerms`.

Check whether the values assigned to these keywords provide the desired UNIX system protection for your files and directories. These keywords are in the following key:

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

For more information, see Appendix A, "Advanced Server Registry."

For more information about security and access permissions, see *Advanced Server Concepts and Planning*.

UNIX System Access Permissions

The UNIX system assigns access permissions to all directories and files. These UNIX system access permissions, together with Advanced Server file and permissions, determine whether you can read, write, or create directories and files on the server.

NOTE

Note It is not necessary to know the UNIX system access permissions assigned to directories and files unless these access permissions prevent access when Advanced Server permissions appear to allow access.

Access is determined through access permissions assigned by Advanced Server and the UNIX system. Advanced Server access permissions assigned to files or directories are based on the access permissions assigned to the individual user. These access permissions can be found in the access control list that resides on Advanced Server.

UNIX System Group Permissions and Advanced Server

The effect of setting UNIX system group permissions on Advanced Server files is limited. In the UNIX system, the group field is used for storing information about file attributes. When a file is accessed from a client computer, its group may change to reflect its attributes (for example, to DOS---). Therefore, it is inadvisable to rely on UNIX system group permissions to restrict access to Advanced Server files *unless keepunixgroups is set to yes*.

UNIX System Permissions on Directories

UNIX system permissions on all directories in the path leading to a file must be at least read and execute (RX) for users to access files on Advanced Server successfully.

Turning Off UNIX System Permission Checking

If the protection of Advanced Server files provided by UNIX system permissions can be ignored, and if it is appropriate to rely solely on Advanced Server permissions to manage file access, you can set the `IgnoreUnixPermissions` keyword to 1 (ignore UNIX system permissions) in the Advanced Server Registry. This keyword is in the following key:

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

This will cause Advanced Server to ignore all UNIX system permissions on files except for read-only permissions, which are translated into read-only file attributes when client computers attempt to access files.

For more information about the Advanced Server Registry, see Appendix A.

UNIX System File and Directory Permissions

UNIX system file and directory permissions are assigned by a default set of access permissions on the system upon creation of files and directories. The UNIX system distinguishes the following three types of users with respect to access permissions:

1. **User** — If you own a UNIX 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.
2. **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 UNIX system group `other`, as are all others with home directories. This assignment enables you to share data easily with other network users, but prevents UNIX system users in different groups from reading or changing your files.
3. **Other** — You can assign access permissions to files and directories that you own for all UNIX 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.

When a user attempts to access a file or directory, access to the server is allowed or denied depending on the permissions assigned to that user.

Understanding UNIX System Access Permissions

You can use the `udir` command to check the current UNIX system access permissions of any file or directory. The Modes column of the `udir` command shows the UNIX system access permissions for each file and directory. These access permissions are displayed as three sets of three access permissions each. The first set shows the user/owner access permissions. The second set shows the group access permissions. The third set shows the access permissions provided to other UNIX system users. Following are the access permissions abbreviations and their meanings:

Permission	Description
r	Permission to display or read the file or directory.
w	Permission to modify or write to the file or to create or remove files in the directory.
x	Permission to execute the file or move to the directory. Client application files do not need execute permission because they execute under the client computer's operating system, not the UNIX system.
-	The relevant permission is denied.
l	Mandatory locking is enabled.

The following access permissions rarely appear in a display but are described here for completeness:

Permission	Description
s	Whenever a file with this permission is executed, regardless of who executes it, the invoked process takes on the identity of the file's owner (or group) for the duration of the execution.
t	If space is available, a text file with this permission stays in swap space after execution. This permission speeds UNIX system program loading.

Changing UNIX System Access Permissions

You can use the `uchmod` command from a client computer to change the UNIX system access permissions for files and directories.

With the `uchmod` command, you enter only the access permissions you want to change. You do not have to enter all of the permission characters. For example, to change the write permission on a file named `budget` so that it cannot be modified, you would enter the following command:

```
uchmod -w budget
```

Maintaining Permissions for Specific Files

Some programs, such as Microsoft Word, maintain temporary files by renaming the source file to a temporary name. Then, when the user saves the file, these programs create a new file with the name of the source file. The temporary file is then deleted.

The permissions that have been assigned to a specific file are not assigned to the new file which has the same file name. These permissions apply only to the original file which was renamed to the temporary file name and then deleted. The updated file is treated as a completely new file by Advanced Server which means it inherits the permissions of the directory in which it resides.

Files that are likely to go through this kind of updating process should be maintained in directories that have the permissions you want these files to inherit.

Tighten File Security when `CreateUnixUser=0`

When the value `CreateUnixUser` is set to `0` in the registry, HP-UX accounts are not created for AS/U users. When such a user creates a new file from a down level client (Windows 3.1 or Word for Windows), the file will be owned by the HP-UX user `lmworld`.

AS/U treats files owned by `lmworld` as owned by the server user `SYSTEM`. This prevents users, other than those who have explicit permissions to do so, from taking ownership or modifying permissions for such files.

Solving Browsing Problems

Some of the common problems that you may encounter while using the Computer Browser service are listed below, followed by recommended resolutions.

Problem

The browse list on the backup domain controller does not contain all of the domain servers. For example, the list of servers that is displayed as a result of executing the net view command from a backup domain controller is incomplete.

Resolution

It can take as long as 12 minutes for the system to update the browse list. The administrator can edit the Advanced Server Registry on the backup domain controller to change the value of the BackupUpdate keyword to the value (in seconds) for which updates are desired. Note that increasing the browse update frequency will generate increased network traffic.

The BackupUpdate keyword is located in the following key:

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

The Computer Browser service must be stopped and restarted for the change to take effect.

For more information on changing registry values, see Appendix A, "Advanced Server Registry."

Solving Printing Problems

Some of the common problems that may arise when using shared printer queues are listed below, followed by recommended resolutions.

Problem

Windows NT client computers cannot connect to the printer.

Resolution

You must associate the printer with an appropriate driver. Follow these steps to change the printer-driver association on the AS/U server. Note, you must be administrator or have printer operator capability.

1. From a Windows NT client computer, select the printer whose driver you wish to change in the **Printers** folder on the AS/U server.
2. Click on **File Properties**. If you receive a Printer Properties error, select **No**. This may occur if a valid printer driver already has been installed. Ignore error messages here.
3. Select the correct printer driver.
4. Share the printer if it is not already shared.

You may need to insert the Windows NT CD to obtain the appropriate driver. The system will confirm that the printer driver is being uploaded to the Advanced Server.

Problem

Changes made to Windows NT client printers and jobs are not displaying automatically.

Resolution

Manually refresh the screen by pressing F5 key. This is required to update the screen whenever you pause, resume, delete, or add printers.

Problem

There is no separator page.

Resolution

Advanced Server/9000 does not support separator pages.

Problem

Characters sent to printer are printing differently.

Resolution

Refer to your printer manual to set the printer for “no parity.”

Problem

Print jobs in the queue are not printing.

Resolution

1. Verify that the printer cable is connected according to the printer manufacturer’s instructions.
2. Verify that the printer is turned on, selected (on-line), has paper, is not jammed, and has no other obvious problems.
3. Verify that the printer or printer queue has not been paused, held, or is in error. If it has been paused or held, continue or restart the printer or print queue.
4. Verify that you can print from the UNIX system console. If not, consult your UNIX system documentation.
5. If an AS/U device is continually in error even after `net device /restart`, this may be due to incorrect HP-UX lp options on an AS/U queue routed to that device. To correct this problem, the print queue with the invalid HP-UX lp options in its `TYPES=` parameter must be purged of all print jobs and then the `TYPES=` parameter corrected to the right value.

NetBIOS Troubleshooting Tools and Hints

If you suspect a NetBIOS problem, there are several things you can do to resolve or isolate the problem before contacting HP support personnel.

- To ensure that NetBIOS is running:

1. Look for the NetBIOS demon process by typing at the HP-UX prompt:

```
ps -ef | grep netdemon
root 6239 1 0 Oct 29 ? 0:01
/opt/lmu/netbios/bin/netdemon
```

or

2. Try to restart NetBIOS with the **nbutil** tool found in directory **/opt/lmu/netbios/bin**. For example,

```
./nbutil -N start
nbutil
NetBIOS is already running
```

3. Use **lanscan** to view the *network interface* over which NetBIOS is running. That network interface must be in the `up` state. For example:

```
lanscan
```

Hardware Path	Station Address	Dev lu	Hardware State	Net-Interface Name	Unit	State	NM ID	Encapsul Methods	Mjr Num
2.0.2	0x080009935930	0	UP	lan0		UP	4	ETHER	52
6.0.2	0x080009935931	1	UP	lan1		UP	5	ETHER	52

4. Use **ifconfig** to bring a network interface up or down or set the IP address and subnet mask. For more information, see the **ifconfig** man page. For example:

```
ifconfig lan0
```

```
lan0: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
inet 15.1.11.107 netmask fffff800 broadcast 15.1.101.255
```

5. To check which interface is being used by NetBIOS, check the current NetBIOS configuration data as follows:

```
/opt/lmu/netbios/bin/nbutil -C
Node Type : Broadcast
IP Address : 15.1.11.107
Broadcast Address : 15.1.101.255
Subnet Mask : 255.255.248.0
```

- If configured properly, the IP address found in the output should match the chosen interface. In the example above, the IP address 15.1.11.107 found in the output matches interface `lan0` displayed with the `ifconfig` command.

If the IP address did not match the interface, or if you desire to run NetBIOS over a different interface (`lan1` for example), you can use `autoconfig` to configure NetBIOS. `autoconfig` is a NetBIOS script found in the directory `/opt/lmu/netbios/bin`. For example,

```
$ nbutil -N stop
nbutil
Stopping NetBIOS
$ autoconfig -l lan1
$ nbutil -N start
nbutil
Starting NetBIOS
```

- If AS/U is unable to connect to other computers, you may want to verify that the problem is not caused by other networking software or hardware. Try to ping into and out of the server. If you are unfamiliar with `ping`, you can obtain information by typing `man ping`.

Example #1:

```
$ ping 15.1.11.107 512 3
PING 15.1.11.107: 512 byte packets
512 bytes from 15.1.11.107: icmp_seq=0. time=1. ms
512 bytes from 15.1.11.107: icmp_seq=1. time=0. ms
512 bytes from 15.1.11.107: icmp_seq=2. time=0. ms
----15.1.11.107 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/1Note: To stop ping, use
CTRL-C.
```

Example #2:

```
$ ping 15.1.11.107 512 5
PING 15.1.11.107: 512 byte packets
----15.1.11.107 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

Notice the percentage packet loss. Example #2 shows a failure. If ping fails, the problem is in the computer's ability to access the network and is not a NetBIOS problem.

- If ping is successful, you may want to try the NetBIOS test program **nbtest** found in directory **/opt/lmu/netbios/bin**. For example,

```
$ nbtest -server nbt_name_test &
[1]      8041
$ nbtest -client nbt_name_test 512 5
nbtest
*****WARNING: nbtest is an unsupported tool*****
Calling 'nbt_name_test' . . .
Sending 512 bytes, 5 times
Took 1 seconds, 5 packets/second, 2560 bytes/second
$ kill -9 8041 {process id from above}
```

The **nbtest -h** command will provide more information about the test program. If you have a second server system, try the test with the **-server** on one system and the **-client** on the other.

- If you are using NetBIOS in a subnetted environment, the **netstat -rn** command will display IP routing information which may help to diagnose network problems. The **route** command is used to manipulate the network routing tables. Online **man** pages are available for **netstat** and **route**.
- Many NetBIOS error conditions and resource warnings are logged to a system log. You can view recently printed diagnostic messages with **dmesg**. For example,

```
$ dmesg | grep -i netbios
WARNING: netbios - Resource map - rnd low.
```

This error suggests that NetBIOS's resource map is low (short on memory). If you find a similar error, you may want to increase memory for NetBIOS by increasing the size of the kernel parameter **nrfc_nb** via SAM. For more information on the **nrfc_nb** kernel parameter, see the "Tuning" section of the Logging and Tuning chapter in this guide.

- System error and warning messages (including NetBIOS) can be found in the file **/var/adm/syslog/syslog.log**.
- NetBIOS warning messages when running **autoconfig** script: **autoconfig** is a script used to create the file **/etc/opt/lmu/netbios/nb/nbconfig**. You can run the script during

installation of NetBIOS or during regular system administration activities. The following warning messages could appear when running the autoconfig script:

```
NB autoconfig: lan0 is not configured for this system
NB autoconfig: nbconfig file not created - check
manual
```

The warning message is due to the state of the LAN interface passed into the autoconfig script or the default LAN interface (**lan0**) state being DOWN. Executing the *lanscan* command can verify the state, and whether the interface is a valid interface. AS/U chooses **lan0** as the default LAN interface. This is based on the most common configuration. If **lan0** is not present or down, then a warning message will occur during installation. The installation process will continue even though the default LAN interface is not available. You can execute the autoconfig script after the installation and specify the LAN interface.

```
WARNING: No Lan Adapter was specified [-l <lan#>]
WARNING: lan0 will be used as the default lan adapter
WARNING: nbconfig file will be updated with data from
lan0
```

The above warning message will appear when you execute the autoconfig script without specifying a LAN interface and the **nbconfig** file does not exist.

Troubleshooting
NetBIOS Troubleshooting Tools and Hints

9 Software Availability in Native Languages

European Character Support

AS/U provides European character support for Windows 95 and Windows NT clients. AS/U also supports MS-DOS and Windows 3.x clients using PC437, PC850, or PC861 code pages. To enable European character support for Windows 95 and Windows NT, which includes applications running in DOS-PROMPT windows under these environments, the AS/U server must be started with the environment variable LANG set to the appropriate HP-UX locale. For example, for German characters support:

```
export LANG=de_DE.iso88591
```

```
net start server
```

or

Set the **lanman.ini** parameter `[lmxserver]lang=de_DE.iso88591`, then type:

```
net start server.
```

The **lanman.ini** parameter `[lmxserver]lang` may be used to override the LC_CTYPE setting of the LANG variable. The default for this entry is "", which will take the locale from the HP-UX LANG variable. HP recommends that you explicitly set the **lanman.ini** parameter `[lmxserver]lang` to the desired locale to prevent accidentally starting AS/U in an incorrect locale.

To enable European character support for MS-DOS and Windows 3.x clients, and certain 16-bit Windows applications running under Windows 95, the following **lanman.ini** parameter has been added to AS/U:

```
[hpparms] msdoscodepage=437
```

Following are the currently supported values for this parameter:

```
msdoscodepage=437 MS-DOS Latin US (default)
```

```
msdoscodepage=850 MS-DOS Latin 1
```

```
msdoscodepage=861 MS-DOS Icelandic
```

The AS/U server must be running in an ISO8859-1 locale for meaningful mapping of the selected European `[hpparms]msdoscodepage` parameter.

The AS/U server must be restarted for the `[hpparms]msdoscodepage` parameter change to take effect. See appendix in this guide for information on how to change keywords in the **lanman.ini** file.

You cannot administer resource permissions on shares that contain German umlauts in their names from the Windows 95 Explorer. Permissions can be administered if the resource is accessed through the Network Neighborhood. Microsoft has acknowledged this behavior but has indicated that it is by design, and no fixes will be forthcoming.

Japanese Character Support

AS/U supports Japanese character sets as follows:

- AS/U supports only Japanese in Shift-JIS encoding. The EUC codeset is not supported.
- Japanese capability of AS/U is only supported on HP-UX 10.20. It requires no additional disk space and memory than that of the AS/U running in English mode.
- The following clients have been tested with AS/U with Japanese:
 - MS-DOS 5.0/V or higher
 - MS LAN Manager 2.1J
 - Windows 95 Japanese
 - Windows NT 3.51 Japanese

- To enable AS/U Japanese capabilities,
please start AS/U processes with LANG=ja_JP.SJIS globally:

```
LANG=ja_JP.SJIS
export LANG
net start server
```

or with every invocation of AS/U commands:

```
LANG=ja_JP.SJIS net start server
LANG=ja_JP.SJIS net user USER1
```

or

Set the **lanman.ini** parameter [lmxserver]lang=ja_JP.SJIS,
then type:

```
net start server.
```

HP recommends this last method which will prevent accidentally starting AS/U in an incorrect locale.

- Japanese is supported for the following:
 - File/directory names.
 - File contents.
 - Printing.
 - All fields of comment/remark/message of **net** command.

Japanese is not supported for share names, domain names, user login names or user passwords.

- DOS utilities `uchmod.exe`, `ud.exe`, `uren.exe`, and `udir.exe` are not supported for Japanese file/directory name.
- The bundled server management tools for Windows NT workstation and Windows 95 are not supported on Japanese Windows NT workstation(J) and Windows 95(J).
- AS/U cannot handle the following Shift-JIS characters because the unicode conversion table differs between HP and Microsoft. The HP conversion table conforms to the Unicode standard, whereas the Microsoft conversions are a variant to support backward compatibility with earlier Microsoft platforms (Windows 95, Windows 3.1).

SJIS code	8160	8161	817C	8191	8192	81CA
HP Unicode	301C	2016	2212	00A2	00A3	00AC
MS Unicode	FF5E	2225	FF0D	FFE0	FFE1	FFE2

As a workaround, you can modify the `iconv` conversion table bundled with HP-UX using the following procedure from the HP-UX prompt.

CAUTION

This procedure facilitates Microsoft NT and Windows 95 interoperability. However, it modifies original operating system files and may break other applications which depend on the original contents of these conversion tables such as those relying on UNIX-based interoperability of SJIS and Unicode.

1. Stop the server

```
net stop server
```

2. Modify the `sjtouc` entries:

```
dmpxlt /usr/lib/nls/iconv/tables/sjis=ucs2 > sjtouc  
vi sjtouc  
0X8160 0X301c -----> 0X8160 0Xff5e  
0X8161 0X2016 -----> 0X8161 0X2225  
.....  
0X81ca 0Xac -----> 0X81ca 0Xffe2
```

3. Make a backup of the conversion table:

```
cp /usr/lib/nls/iconv/tables/sjis=ucs2 sjis=ucs2.org  
genxlt sjtouc > /usr/lib/nls/iconv/tables/sjis=ucs2
```

4. Modify the **uctosj** entries:

```
dmpxlt /usr/lib/nls/iconv/tables/ucs2=sjis > uctosj  
vi uctosj  
0X301c 0X8160 -----> 0Xff5e 0X8160  
0X2016 0X8161 -----> 0X2225 0X8161  
.....  
0Xac 0X81ca -----> 0Xffe2 0X81ca
```

5. Make a backup of the conversion table:

```
cp /usr/lib/nls/iconv/tables/ucs2=sjis ucs2=sjis.org  
genxlt uctosj > /usr/lib/nls/iconv/tables/ucs2=sjis  
LANG=ja_JP.SJIS net start server
```

6. Again, please keep the original files so that you can recover if problems occur.

- AS/U cannot handle the following characters as file or directory names from Windows 95(J) clients. 8470 - 8491 (SJIS code)

Windows 95(J) converts the characters to their uppercase (8440 - 8460) and tries to access them, when the a character in the above range is given as a file or directory name. As AS/U does not support uppercase-to-lowercase conversion for 2-byte characters. They cannot be handled by AS/U. No workaround.

- AS/U can only run batch files from Windows 95(J) clients if the file or directory names are specified in the 8.3 format. This is not a Japanese specific problem but an MS-DOS limitation.

Example: The following batch files cannot run.

```
g:\a1234567890\test.bat  
g:\a123456\test567890.bat
```

No workaround.

Advanced Server Registry

This appendix provides the following information:

- Overview of the Advanced Server Registry structure.
- Description of Registry Editor.
- Description of AS/U Administrator.
- Descriptions of the Advanced Server Registry keys and values.

For information about the Advanced Server parameters that are stored in the lanman.ini file and how lanman.ini file parameters are mapped to Advanced Server Registry keys, see Appendix B, "Lanman.ini File."

Advanced Server Registry Structure

The Advanced 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 Advanced 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 Advanced Server Registry is stored in the `/var/opt/lanman/datafiles` directory on the Advanced Server computer.

Value Entries in the Registry Keys

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

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.

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.

Advanced Server Registry
Advanced Server Registry Structure

The following table lists and defines the data types currently used by the system.

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
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 Advanced 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 Advanced 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 Advanced Server Registry using the Windows NT Registry Editor, you must connect to Advanced 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 Advanced 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 "Accessing the Registry of a Remote Computer" in Registry Editor Help.

WARNING

Using the Windows 95 Registry Editor to edit the Advanced 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

As shown in the following figure, Registry Editor displays data in two panes. The value entries in the right pane are associated with the selected key in the left pane. 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.

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 asterisk (*) key on the numeric keypad.
Collapse a branch of a selected registry key.	Press ENTER or (-) on the numeric keypad.

Using AS/U Administrator

You can modify many of the values in the Advanced Server Registry using the AS/U Administrator. Using this tool allows you to modify specific keys in the registry which govern the performance of Advanced Server. Using AS/U Administrator (unlike the Registry Editor) allows you to choose from among lists of allowable values for each key. In this way, you are less likely to accidentally corrupt the data in your registry file.

AS/U Administrator is included in the ASTOOLS share. This program must be installed on a Windows NT Workstation (Versions 3.51 or 4.0.) computer serving as administrative network client as described in the *Advanced Server/9000 Installation Guide*.

To start AS/U Administrator, click on its icon or execute the **Run** command in the Windows NT Start menu. In the **Select Computer** field, enter the name of the Advanced Server whose registry file you wish to configure. Configuration data for the selected computer will be displayed on the AS/U Administrator **Version** tab. To view or change Advanced Server Registry values, click on the **Policy** tab.

The following table lists the policies and their associated Advanced Server Registry keys that can be modified using AS/U Administrator.

The following table lists the policies and their associated Advanced Server Registry keys that can be modified using AS/U Administrator.

Policy	Advanced Server Registry Key
Alerter Service	(SYSTEM\Current\ControlSet\Services\Alerter\Parameters) IncludeMessageHeader CountNotOnNetworkCache NotOnNetworkCacheTimeout
Computer Browser Service	(SYSTEM\CurrentControlSet\Services\Browser\Parameters) MasterUpdate

Advanced Server Registry
Using AS/U Administrator

Policy	Advanced Server Registry Key
Connected Clients	BackupUpdate
	BackupRecovery
	MoreLog
	(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters)
	LogonQuery
	QueryDelay
	RelogonDelay
File Name Space Mapping	(SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters)
	AutoDisconnect
	(SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters)
	NamespaceMapping
	UniqueSuffixLength
	MixedCaseSupport
	TruncatedExtensions
Netlogon Service	MappingSeparator
	(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters)
	Scripts
	Pulse (PDC only)
	Update (BDC only)
	Randomize (BDC only)
SSIPasswdAge (BDC only)	

Policy	Advanced Server Registry Key
Server Announcement	(SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters) Hidden SrvAnnounce LmAnnounce
UNIX Account Mapping	(SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters) CreateUnixUser
UNIX File System Integration	(SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters) IgnoreUnixPermissions UnixDirectoryCheck UnixFilePerms UnixDirectoryPerms UseUnixLocks RootOwnsFilesCreatedOnNFS
Users Alerts	(SYSTEM\CurrentControlSet\Services\AdvancedServer\AlertParameters) AertAdminOnLicenseOverFlow AlertUserOnLicenseOverFlow (SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters) AccessAlert ErrorAlert LogonAlert

Registry Keys and Values

This section describes the Advanced Server Registry keys that are changed during administration. You may want to modify these values directly using the AS/U Administrator or a registry editor. You do not need to be concerned with every key in the Advanced Server Registry; only those keys that you may have reason to change are described.

The Advanced 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
  \Replicator
```

NOTE

The server must be stopped and then restarted in order for most changes to the Advanced Server Registry to take effect.

Advanced Server Key Descriptions

The Advanced Server subkey of the Advanced Server Registry contains the following subkeys:

```
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 Advanced Server Alert 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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

File Service Parameters Entries

The Registry path that contains entries for the Advanced 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 Advanced Server resources.

Default: 6

EnableSoftCompat REG_DWORD 0, 1, or 2

Specifies how Advanced 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

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 Advanced 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 Advanced 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 UNIX 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 UNIX 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 UNIX system permissions when working with files and directories. For example, enabling this option would allow Advanced Server users to write to or delete files for which they have sufficient Advanced Server permissions even though only UNIX system read permissions had been granted to those files.

Default: 0 (enforce UNIX system permissions)

You can change the value of this key using the AS/U Administrator.

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 UNIX system to Windows NT file name mapping. The default is a tilde (~), the same as in UNIX 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 "~asu~", the name will be mapped to "my_~asu~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 AS/U Administrator.

MaxFileSizeInKB REG_DWORD 100 - infinity

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

Default: 20000

MemoryMapFiles REG_DWORD 0 or 1

Specifies whether the server uses the UNIX 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 UNIX 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 AS/U Administrator.

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 UNIX 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 UNIX system to Windows NT mapping is enabled. This allows Windows NT-style clients, such as Windows 95 and Windows NT to access files with file names containing characters that are illegal in Windows NT (? " \ < > * | :).

A value of 3 specifies that both UNIX system to 8.3 and UNIX system to Windows NT mappings are enabled.

Default: 0

You can change the value of this key using the AS/U Administrator.

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 UNIX system volumes as NTFS or actual UNIX 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: 1

You can change the value of this key using the AS/U Administrator.

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 distinguish 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 UNIX system to 8.3 file mapping.)

Default: 1 (Do not replace last character with a tilde.)

Advanced Server Registry
Advanced Server Key Descriptions

You can change the value of this key using the AS/U Administrator.

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 AS/U Administrator.

UnixCloseCount REG_DWORD 1 - 20

The number of least-recently accessed open files that the server closes transparently to avoid reaching the UNIX 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 Advanced Server will allow clients to write to UNIX 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 UNIX 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 Advanced Server (as determined by checking group memberships of directory); and a value of 2 ignores UNIX system directory permissions.

Default: 1

You can change the value of this key using the AS/U Administrator.

UnixDirectoryPerms REG_DWORD 0 - 511

The UNIX system permissions for newly-created directories.

Default: 509 (0775 octal)

You can change the value of this key using the AS/U Administrator.

UnixFilePerms REG_DWORD 0 - 4095

The UNIX system permissions for newly-created files.

Default: 1460 (02664 octal)

You can change the value of this key using the AS/U Administrator.

UnixQuotas REG_DWORD 0 or 1

Specifies whether Advanced Server provides UNIX system disk quota support. This ensures that creating or writing to the file is performed under the UNIX system UID of the UNIX system user to which the Advanced 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 HFS file systems. This is true to the extent of the ability of these file systems to support UNIX system quotas.

Default: 0 (no support for disk quotas)

UseNfsLocks REG_DWORD 0 or 1

Specifies whether the server tries to set UNIX 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 Advanced 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 UNIX file system.

Default: 0 (locks are not reflected in UNIX file system)

You can change the value of this key using the AS/U Administrator.

WriteBehind REG_DWORD 0 or 1

Specifies whether physical UNIX system writes are performed before or after the server responds to the client. If UNIX 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 UNIX 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 Advanced Server Net Administration is as follows:

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

NetAdminGroupName REG_SZ Character string

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

Default: DOS----

NetAdminPath REG_SZ Character string up to 256 characters

The UNIX 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 UNIX 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 Advanced 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.

If you chose to disable Windows NT-style printing during an upgrade procedure, resulting in the setting of this value to 1, then you can enable this feature by changing this value to 0. See the *Advanced Server/9000 Concepts and Planning Guide* for more information about Windows NT-style printing.

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 UNIX system directory. Because Advanced 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: 16384 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

Advanced Server Registry
Advanced Server Key Descriptions

MaxMessageSize REG_DWORD 1024 - infinity

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

Default: 4356 (bytes)

MaxPrintQueueNameLength REG_DWORD 1 - 255 characters

Provides dynamic control of the allowable length of the name of a printer queue. LP subsystem commands currently allow class names to be as large as 255 characters, but jobs sent to these classes cannot be controlled and many of the UNIX 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 Advanced Server 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: Advanced Server for HP 9000 Systems

NativeOS REG_SZ Character string

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

Default: UNIX B.10.20

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 Advanced Server 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: 300 (KBytes)

Process Parameters Entries

The Registry path that contains entries for the Advanced 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: 1 (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.

Advanced Server Registry
Advanced Server Key Descriptions

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 Advanced 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 an Advanced 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 Advanced 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 Advanced 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 UNIX 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.

Advanced Server Registry
Advanced Server Key Descriptions

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:

Client Range	Minimum sessions per lmx.srv	Maximum 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

Client Range	Minimum sessions per lmx.srv	Maximum sessions per lmx.srv
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 Advanced 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

LsarpMaxCalls 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

Advanced Server Registry
Advanced Server Key Descriptions

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 Advanced 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 the Advanced 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 Advanced 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 UNIX system user account to every new Advanced 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 UNIX system accounts are to be created. Note that new Advanced Server users are assigned to the UNIX system lmworld account.

Default: 0 (do not create UNIX system user account)

You can change the value of this key using the AS/U Administrator.

Exclude REG_SZ Character string

Specifies existing UNIX system user IDs excluded from being assigned to Advanced Server user accounts. If an Advanced Server user account is created whose name matches an existing UNIX system user account whose ID is contained in the exclude list, a new UNIX system user account will be generated automatically and assigned to the Advanced Server user account. This can be used to ensure that certain existing UNIX system user accounts never are assigned automatically to newly-created Advanced 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 UNIX system user account to a newly-created Advanced Server user account. If you select 1, then the system does not assign existing UNIX system user accounts. Instead, new UNIX system user accounts are generated automatically and assigned to Advanced Server user accounts when they are created.

Default: 0 (A new Advanced Server user account can be assigned automatically to an existing UNIX system user account with an equal or similar name, provided that the UNIX 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 UNIX 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 UNIX 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 an Advanced Server user account changes, this key changes the home directory of the associated UNIX system user account to match the Advanced Server home directory.

Default: 0 (do not synchronize home directories)

UserComment REG_SZ Character string

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

Default: Advanced Server for UNIX 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 Advanced 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

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

Advanced Server Registry
Advanced Server Key Descriptions

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)

You can change the value of this key using the AS/U Administrator.

Browser Service Parameters

The Registry path that contains entries for the Advanced 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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

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.
- Security — LSA, SC Manager, Security, Security Account Manager, Spooler.
- System — Alerter, Browser, EventLog, NetLogon, Print, Rdr, SAM, server, Service Control Manager, Srv, 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)

Advanced Server Registry
Advanced Server Key Descriptions

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.

Lanman Server Parameters

The Registry path that contains entries for the Advanced Server LAN Manager service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\  
LanmanServer\Parameters
```

AccessAlert REG_DWORD 0 - infinity

Specifies the number of resource access violations that can occur before the server sends an alert to the `alernames` list.

Default: 5

You can change the value of this key using the AS/U Administrator.

AutoDisconnect REG_DWORD 0 - 3600 (60 hours)

Specifies the interval in minutes that the server waits before dropping the virtual circuit to an inactive client.

Default: 0 (no automatic disconnect)

You can change the value of this key using the AS/U Administrator.

ErrorAlert REG_DWORD 0 - infinity

Specifies the number of errors that can occur before the server sends an alert to the alertnames list.

Default: 5

You can change the value of this key using the AS/U Administrator.

Hidden REG_DWORD 0 or 1

Specifies whether the server is hidden on the network. If the server is not hidden, it announces its presence set in the SrvAnnounce and LmAnnounce keys.

Default: 0 (server is visible)

You can change the value of this key using the AS/U Administrator.

LmAnnounce REG_DWORD 0 or 1

Specifies whether a server should announce itself with the old LAN Manager-type announcement in addition to the new Windows NT-type announcement. This key has an effect only if the value of the Hidden key is 0.

Default: 0 (Use only Windows NT-type announcement.)

You can change the value of this key using the AS/U Administrator.

LogonAlert REG_DWORD 0 - infinity

Specifies the number of logon violations that can occur before the server sends an alert to the alertnames list.

Default: 5

You can change the value of this key using the AS/U Administrator.

SrvAnnounce REG_DWORD 1 - infinity

Specifies the interval in seconds at which the server announces its presence to the network. This key has an effect only if the value of the Hidden key is 0.

Default: 180 (3 minutes)

You can change the value of this key using the AS/U Administrator.

Advanced Server Registry
Advanced Server Key Descriptions

SrvComment REG_SZ String up to 48 characters

Specifies the descriptive comment that the server sends when it announces its presence to the network.

Default: Advanced Server for UNIX

UserPath REG_SZ Path

Specifies the UNIX system directory on the server to be used as a default parent directory for home directories for new user accounts.

Default: c:\home\lanman

Net Logon Service Parameters

The Registry path that contains entries for the Advanced 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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

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

You can change the value of this key using the AS/U Administrator.

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

You can change the value of this key using the AS/U Administrator.

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

You can change the value of this key using the AS/U Administrator.

Scripts REG_EXPAND_SZ

Specifies the location of the logon scripts directory.

Default on primary domain controller:

%SystemRoot%\var\opt\asu\lanman\shares\asu\repl\export\scripts

Default on backup domain controller:

%SystemRoot%\var\opt\asu\lanman\shares\asu\repl\import\scripts

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

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)

You can change the value of this key using the AS/U Administrator.

Replicator Service Entries

The Registry path that contains entries for the Advanced 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\asu\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\asu\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.

Advanced Server Registry

Advanced Server Key Descriptions

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 UNIX system group account name for replicated directories.

Default: DOS----

UnixDirectoryOwner **REG_SZ** Character string

Specifies the UNIX system user account name for replicated directories.

Default: lmxadmin

UnixFileGroup **REG_SZ** Character string

Specifies the UNIX system group account name for replicated files.

Default: DOS----

UnixFileOwner **REG_SZ** Character string

Specifies the UNIX system user account name for replicated files.

Default: lmxadmin

Lanman.ini File

This appendix lists and describes the lanman.ini file parameters that can be modified to improve Advanced Server performance. It also contains tables which indicate the disposition of parameters that were in earlier versions of the lanman.ini file and now are in the Advanced Server Registry.

When Advanced Server is installed, the lanman.ini file contains some default parameter values. Other parameters and the titles of the sections in which they reside are added when you change the Advanced 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/asu/lanman/bin` 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.

When you want to set the value of a parameter to something other than the default, you must edit 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.

To change a parameter in the **lanman.ini** file:

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

```
/opt/asu/lanman/bin/srvconfig -p | more
```

2. Edit the **lanman.ini** file using `vi` or a similar text editor. You may have to add a section heading to the file, for example `[lmsserver]`. You then need to add a “parameter=value” pair to the appropriate section of the **lanman.ini** file.
3. After you edit the file, you must stop and restart the server in order for the new values to take effect.

You can also use the `srvconfig -s` command to set parameter values in the **lanman.ini** file, as follows:

Lanman.ini File

File Syntax

`/opt/asu/lanman/bin/srvconfig -s section,parameter=value`

For more information about the `srvconfig` command, type `man srvconfig` at the HP-UX 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.

NOTE

The **lanman.ini** file contains additional parameters that are not included in the following tables. These parameters are for debugging purposes and should never be modified.

[Server] Section Parameters

Parameter	Description, Values, and Default Setting
listenname	If set, this is the server's name on the network. To change the value of the listenname parameter, use the setservername command. For more information about this command, type man setservername at the HP-UX command prompt. Values: any name of 1-15 characters; default: null
maxclients	Identifies the maximum number of simultaneous client sessions that the server can support.
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, spooler

[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: domain

[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.
country	The country code for server-generated messages. Values:

Country	Code	Country	Code
Asia	099	Latin America	003
Australia	061	Netherlands	031
Belgium	032	Norway	047
Canada	002	Portugal	351
Denmark	045	Spain	034
Finland	358	Sweden	046
France	033	Switzerland	041
Germany	049	United Kingdom	044
Italy	039	United States	001
Japan	081		

	Default: 001
dll_dir	The path to the directory containing message text files used by Advanced server UNIX system commands. Default: /var/opt/asu/lanman/shares/asu/system32
lang	Defines the character set that Advanced server uses for processing client requests. Default:
listenextension	The extension that the UNIX 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: no extension

Lanman.ini File
File Parameters

Parameter	Description, Values, and Default Settings
listennamechk	If set to yes, it forces any name specified with the listenname parameter to be different than the UNIX machine name or the UNIX machine name with a .serve extension in order to avoid name conflicts with the UNIX Listener. Default: no
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/asu/lanman/addon/lmaddon
lmgetmsg_path	Search order for message text files used by Advanced Server. Default: netmsg.dll, kernel32.dll, localspl.dll, asumsg.dll

Parameter	Description, Values, and Default Settings
mapaclblob	<p>Configures whether to use memory-mapped file operations when accessing the Advanced Server Access Control List database.</p> <p>Values: yes, no; default: yes</p>
mapchangelogblob	<p>Configures whether to use memory-mapped file operations when accessing the Advanced Server Change Log database.</p> <p>Values: yes, no; default: yes</p>
maplsablob	<p>Configures whether to use memory-mapped file operations when accessing the Advanced Server Local Security Authority database.</p> <p>Values: yes, no; default: yes</p>
mapregistryblob	<p>Configures whether to use memory-mapped file operations when accessing the Advanced Server Registry database.</p> <p>Values: yes, no; default: no</p>
mapsamblob	<p>Configures whether to use memory-mapped file operations when accessing the Advanced Server Security Accounts Manager database.</p> <p>Values: yes, no; default: yes</p>
maxfilesize	<p>The maximum file size, in KBytes, that the UNIX system redirector will allow a “local UNIX user” to create on a local system.</p> <p>Values: 100 - unlimited; default: 20000</p>

Lanman.ini File
 File Parameters

Parameter	Description, Values, and Default Settings
msgforward	<p>Specifies if Advanced Server implements message forwarding between clients. Implementation of message forwarding is not recommended.</p> <p>Values: yes (implement forwarding) or no (do not implement forwarding); default: no</p>
nativelm	<p>An additional field in the session setup request/ response.</p> <p>Default: Advanced Server for HP 9000 sys.</p>
nativeos	<p>An additional field in the session setup request/ response.</p> <p>Default: HP-UX B.10.20 A</p>
netaddonpath	<p>The directory in which the Advanced Server looks for dynamic libraries on startup. Dynamic libraries found in the directory are bound into the Advanced Server 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.</p> <p>Values: A path up to a maximum of 256 characters; default: /opt/asu/lanman/addon/networks</p>
nethelpfile	<p>The location of the help file used by the net help command (relative to /var/opt/asu/lanman/datafiles/msgfiles).</p> <p>Default: /var/opt/asu/lanman/datafiles/msgfiles/net.hlp</p>

Parameter	Description, Values, and Default Settings
netmsgwait	<p>The interval, in seconds, that the server waits for a response when it sends a message that requires one.</p> <p>Values: 0 - unlimited; default: 300</p>
network	<p>The network device names and NetBIOS name- passing type for the network(s) the server should use.</p> <p>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:</p> <ol style="list-style-type: none"><li data-bbox="873 940 1341 1003">1. The device name for virtual circuit access.<li data-bbox="873 1024 1393 1087">2. The device name for datagram network access.<li data-bbox="873 1108 1365 1192">3. A digit identifying the NetBIOS interface convention used by the two devices above.<li data-bbox="873 1213 1386 1402">4. The name of the transport provider, as returned by the nlsprovider system call. (For networks not configured to accept incoming connections through the UNIX system Listener program, this can be any arbitrary string.) <p>Default: /dev/netbios/dev/netbiosdg,0,netbios</p>

Lanman.ini File
 File Parameters

Parameter	Description, Values, and Default Settings
prebinduxredir	<p>Controls the name that the UNIX system Net command binds when it uses the UNIX system redirector (uxredir). If this parameter is set to yes, the server pre-binds a NetBIOS name that will be used by all UNIX system Net commands. Because this name is pre-bound, the Net command does not need to bind its own name, and this quickens the UNIX 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.</p> <p>Values: yes, no; default: yes</p>
secsources	<p>The names of the modules that can write to the security log.</p> <p>Default: The server initializes the value of this parameter at startup.</p>
stacksize	<p>The size of the stack, in bytes, for each task internal to the server.</p> <p>Values:12000 - unlimited; default: 40000</p>
sysources	<p>The names of the modules that can write to the system log.</p> <p>Default: The server initializes the value of this parameter at startup.</p>

[Fsi] Section Parameters

Parameter	Description, Values, and Default Settings
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/asu/lanman/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: /opt/asu/lanman/lib
fsmmap	File system type identifiers that map unknown file systems to known file system types. Values: a comma-separated list of mappings; default: unknown:hfs,nfs:nfs,vxfs:hfs,sfs:hfs,cdfs:hfs
fsnosupport	Maps unknown file system to specified file system. Default: hfs
remotemounts	The names of file system types that indicate remotely mounted file systems. Default: nfs

Lanman.ini File
File Parameters

[Hpparms] Section Parameters

Parameter	Description, Values, and Default Settings
keepunixgroups	Specifies whether the Advanced Server/9000 will retain the UNIX gids for files and directories created by AS/U 9000. Values: yes, no; default: no
maxdiskspacereported	Total and free disk space reported by Advanced Server/9000 for a shared disk. The default value of 0 means ignore this keyword and report the disk space as it is. Values: 0 KByte - 4194303 Default: 0 KByte

[Psi] Section Parameters

Parameter	Description, Values, and Default Settings
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/asu/lanman/addon/psaddon

[Spooler] Section Parameters

The Advanced Server/9000 Spooler service was designed to work with most HP-UX spoolers. The configurable entries that follow provide the Advanced Spooler service with an interface to the system's native spooler. Systems using the HP-UX lp spooler will not require any changes to the following entries. Modifications are not recommended other than those listed earlier in this guide for OpenSpool or HPDPS support.

Parameter	Description, Values, and Default Settings
admin	<p>When the Advanced Server/9000 submits a print job, the user name is in upper case. In the case where ADMIN prints, the HP lp spooler must map this name to the user lmxadmin, since this is the HP-UX user for admin.</p> <p>Default: ADMIN</p>
cancelcmd	<p>Fully qualified path to HP-UX command to cancel <i>job-id</i> %s.</p> <p>Default: LANG=C /usr/bin/cancel %s</p>
cancelkey	<p>Upon canceling a print job, the output (stdout) of the cancel command is checked for this entry. The cancel operation succeeds if this string is found.</p> <p>Default: cancelled</p>
lmxadmin	<p>When a job is submitted by admin, it is sent to HP-UX lp spooler as lmxadmin.</p> <p>Default: lmxadmin</p>
lmxguest	<p>When a job is submitted for Advanced Server/9000 users without HP-UX accounts, the job is sent to HP-UX with lmxguest as owner.</p> <p>Default: lmxguest</p>
lpcmd	<p>Fully qualified path to HP-UX command to submit destination %s.</p> <p>Default: LANG=C /usr/bin/lp -d%s</p>
lpcopiesopt	<p>HP-UX switch to be used with lpcmd to specify number of copies to print, where %d is number of copies.</p> <p>Default: -n%d</p>

Lanman.ini File
File Parameters

Parameter	Description, Values, and Default Settings
lpkey	<p>Upon submittal of a job to print, the output (stdout) of the command is scanned for this string, where %s will be the position of the space delimited <i>job-id</i> returned by the HP-UX spooler.</p> <p>Default: request id is %s</p>
lptitleopt	<p>HP-UX switch to be used with <code>lpcmd</code> to specify the title of a print job, where %s is the title.</p> <p>Default: -t"%s"</p>
maxjobs	<p>Maximum number of jobs to allocate space for in shared memory.</p> <p>Values: 0-700</p> <p>Default: 200</p>
maxprinters	<p>Maximum number of printers to allocate space for in shared memory.</p> <p>Values: 0-256</p> <p>Default: 20</p>
maxqueues	<p>Maximum number of queues to allocate space for in shared memory.</p> <p>Values: 0-256</p> <p>Default: 80</p>
maxworkint	<p>Time interval in seconds that <code>lpx.sched</code> checks changes in spooler status if there are no activities pending.</p> <p>Default: 600</p>

Parameter	Description, Values, and Default Settings
minworkint	<p>Time interval in seconds that <code>lpx.sched</code> checks for completion of jobs sent to the HP-UX spooler. A large number will yield inaccurate job status to the Advanced Server, while a small number will increase CPU utilization by <code>lpx.sched</code> while there are Advanced Server/9000 jobs in the HP-UX spooler.</p> <p>Default: 5</p>
statjcmd	<p>Fully qualified path to HP-UX command to check for the status of a job, given its <i>job-id</i> %s. Note that this <i>job-id</i> must be the same as that which was returned and scanned in by the entry <code>lpkey</code>.</p> <p>Default: <code>LANG=C /usr/bin/lpstat %s</code></p>
statjkey	<p>Upon execution of <code>statjcmd</code>, the output (stdout) of the command is scanned for this entry. The default <code>fscanf(3S)</code> regular expression for this entry searches for the HP-UX spooler job id in the form of xxx-yyy, where yyy are digits. Note that there is currently a limit of 20 characters for storage of the HP-UX spooler job id in the Advanced Server/9000 spooler. The Advanced Server/9000 spooler cannot function if the HP-UX spooler returns job ids of length greater than 20 characters.</p> <p>Default: <code>%[^\n-%[0-9]</code></p>
statjkey	<p>Upon execution of <code>statjcmd</code>, the output (stdout) of the command is scanned for this entry. Note that the <code>\</code> characters serve to include spaces on both side of "on".</p> <p>Default: <code>\ on \</code></p>

Lanman.ini File
File Parameters

Parameter	Description, Values, and Default Settings
statjskey	This entry specifies the delimiter that separates the printer name and job number in the job-id returned by the HP-UX spooler. This entry must reflect the delimiter in the entry statjkey. For example, the default works for the HP-UX lp spooler's designation lj3_2-726 for a print job. Default: -
statpcmd	Fully qualified path to HP-UX command to check for existence of the printer %s. Default: LANG=C /usr/bin/lpstat -p%s
statpkey	Upon execution of the statpcmd, the output (stdout) of the command is scanned for this entry. If entry exists, the printer exists. Default: printer

Technically, the **cmd* entries are used as the format for `fprintf(3S)` calls in the HPLP PSI Library. The **cmd* entries are used to fork HP-UX shells to execute the HP-UX spooler commands. The **key* entries are used as the format for `fscanf(3S)` to select from the stdout of the preceding commands.

It is important to note that incorrect information for the **key* and **cmd* entries will almost certainly break the HPLP PSI Library! For example, the number of % selectors must never be greater than that which is given in the default.

Lanman.ini File Parameter Mapping to Registry Keys

The following tables list the parameters in the **lanman.ini** file that existed in earlier versions of Advanced Server and whether they have been moved to the Advanced Server Registry, to the new lanman.ini file, or are obsolete. The parameters that were moved to the Advanced Server Registry are listed with their new value names.

The **lanman.ini** file parameters are listed according to the sections in which they reside in the file.

[Server] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
accessalert	LanmanServer\Parameters	AccessAlert
alertnames	Alerter\Parameters	
autodisconnect	LanmanServer\Parameters	AutoDisconnect
enablesftcompat	AdvancedServer\FileServiceParameters	EnableSoftCompat
enable_soft_file_ext	AdvancedServer\FileServiceParameters	EnableSoftFileExtensions
erroralert	LanmanServer\Parameters	ErrorAlert
listenname ¹	Control\ComputerName\ComputerName	ComputerName
logonalert	LanmanServer\Parameters	LogonAlert
maxauditlog	EventLog\Security	MaxSize
maxclients	None (lanman.ini file)	
maxerrlog	EventLog\System	MaxSize

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
srvannounce	LanmanServer\Parameters	SrvAnnounce
srvcomment	LanmanServer\Parameters	SrvComment
srvhidden	LanmanServer\Parameters	Hidden
svservices	None (lanman.ini file)	
userpath	LanmanServer\Parameters	UserPath

¹The listenname parameter is in the lanman.ini file as well as the Advanced Server Registry under \SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName.

[Workstation] Section Parameter Mappings to Registry Keys

Lanman.ini Parameter	Advanced Server Registry Key Name	Value Name
domain	None (lanman.ini file)	

[Uidrules] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
exclude	AdvancedServer\UserServiceParameters	Exclude
forceunique	AdvancedServer\UserServiceParameters	ForceUniqueUnixUserAccount
maxuid	AdvancedServer\UserServiceParameters	MaxUnixUid ¹
minuid	AdvancedServer\UserServiceParameters	MinUnixUid ¹
usrcomment	AdvancedServer\UserServiceParameters	UserComment

¹These values are not displayed by default but can be configured in the Advanced Server Registry.

[Netlogon] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
logonquery	Netlogon\Parameters	LogonQuery
maxclisess	AdvancedServer\ProcessParameters	NumCLIENT_SESSION
maxquery	None (obsolete)	
maxsrvsess	AdvancedServer\ProcessParameters	NumSERVER_SESSION
pulse	Netlogon\Parameters	Pulse
querydelay	Netlogon\Parameters	QueryDelay
randomize	Netlogon\Parameters	Randomize

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
relogondelay	Netlogon\Parameters	RelogonDelay
scripts	Netlogon\Parameters	Scripts
ssipasswdage	Netlogon\Parameters	SSIPasswdAge
update	Netlogon\Parameters	Update

[Lmxserver] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
aclfile	None (obsolete)	
aclgroup	None (obsolete)	
aclowner	None (obsolete)	
aclperms	None (obsolete)	
admingroupid	AdvancedServer\NetAdminParameters	NetAdminGroupName
adminpath	AdvancedServer\NetAdminParameters	NetAdminPath
adminuserid	AdvancedServer\NetAdminParameters	NetAdminUserName
alertadmin	None (obsolete)	
alerterrorlog	None (obsolete)	
alertmessage	None (obsolete)	
alerton	None (obsolete)	
alertprinting	None (obsolete)	
alertuser	None (obsolete)	

Lanman.ini File
Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
anncmailslot	None (lanman.ini file)	
appretention	Eventlog\Application	Retention
appsources	Eventlog\Application	Sources
auditretention	Eventlog\Security	Retention
blobmapping	None (obsolete)	
byemessage	AdvancedServer\Parameters	SendByeMessage
clispooltime	None (lanman.ini file)	
cntsharecache	AdvancedServer\ShareParameters	ShareCacheCount
cntsharereads	AdvancedServer\ShareParameters	ShareReadCount
controllock	None (obsolete)	
coreok	AdvancedServer\ProcessParameters	CoreOK
country	None (lanman.ini file)	
cpipgroup	None (obsolete)	
cpipname	None (obsolete)	
cpipowner	None (obsolete)	
cpipperms	None (obsolete)	
creatunixuser	AdvancedServer\UserServiceParameters	CreateUnixUser
dirperms	AdvancedServer\FileServiceParameters	UnixDirectoryPerms
eafileprefix	AdvancedServer\FileServiceParameters	EASizePrefix
errorretention	Eventlog\System	Retention
errsources	None (obsolete)	
feabufsize	AdvancedServer\FileServiceParameters	MaxEASize
fileflush	AdvancedServer\FileServiceParameters	ForceFileFlush

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
fileperms	AdvancedServer\FileServiceParameters	UnixFilePerms
forcediracl	AdvancedServer\FileServiceParameters	ForceDirectoryAcl
forcefileacl	AdvancedServer\FileServiceParameters	ForceFileAcl
gcbuffer	AdvancedServer\Parameters	SizeGcBufferPoolInKB
getapipe	None (lanman.ini file)	
groupadd	None (obsolete)	
groupdel	None (obsolete)	
grpupdate	AdvancedServer\UserServiceParameters	GroupUpdateTime
hashsize	AdvancedServer\ProcessParameters	NumHashTables
ignoresigpwr	UPS\Parameters	IgnoreSIGPWR
ipctries	AdvancedServer\Parameters	MaxIpcTryCount
keepadmshares	AdvancedServer\ShareParameters	KeepAdministrativeShares
listenextension	None (lanman.ini file)	
listennamechk	None (lanman.ini file)	
listenqlen	None (lanman.ini file)	
lmaddonpath	None (lanman.ini file)	
lmxmsgfile	None (lanman.ini file)	
lmsrv	None (obsolete)	
lmxtimesource	None (obsolete)	
locale	None (obsolete)	
locknap	AdvancedServer\ProcessParameters	LockNapInMSec
lptmpdir	None (lanman.ini file)	
lsafile	None (obsolete)	

Lanman.ini File
Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
lsagroup	None (obsolete)	
lsaowner	None (obsolete)	
lsaperms	None (obsolete)	
mailslotgroup	None (obsolete)	
mailslothold	AdvancedServer\Parameters	MaxMailslotReadTime
mailslotowner	None (obsolete)	
mailslotperms	None (obsolete)	
maxadminoutput	None (obsolete)	
maxapplog	EventLog\Application	MaxSize
maxdirbufsize	AdvancedServer\Parameters	MaxDirectoryBufferSize
maxfilesize	None (lanman.ini file)	
maxlocknap	AdvancedServer\ProcessParameters	MaxLockTimeInSeconds
maxmsdepth	None (obsolete)	
maxmsgsize	AdvancedServer\Parameters	MaxMessageSize
maxmux	None (obsolete)	
maxopenfiles	None (obsolete)	
maxrawsize	AdvancedServer\Parameters	MaxRawSize
maxvcperproc	AdvancedServer\ProcessParameters	MaxVCPerProc
maxsvcwait	AdvancedServer\Parameters	MaxServiceWaitTime
maxvcs	AdvancedServer\ProcessParameters	MaxVCs
memorymap	AdvancedServer\FileServiceParameters	MemoryMapFiles
minsmbworkers	AdvancedServer\ProcessParameters	MinSmbWorkerTasks
minvcperproc	AdvancedServer\ProcessParameters	MinVCPerProc

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
msdirgroup	None (obsolete)	
msdirname	None (obsolete)	
msdirowner	None (obsolete)	
msdirperms	None (obsolete)	
msgforward	None (lanman.ini file)	
msgheader	Alerter\Parameters	IncludeMessageHeader
nativelm	None (lanman.ini file)	
nativeos	None (lanman.ini file)	
netaddonpath	None (lanman.ini file)	
nethelpfile	None (lanman.ini file)	
nethmsgfile	None (obsolete)	
netmsgwait	None (lanman.ini file)	
network	None (lanman.ini file)	
newusershell	AdvancedServer\UserServiceParameters	NewUserShell
nfslocks	AdvancedServer\FileServiceParameters	UseNfsLocks
nonexistusers	Alerter\Parameters	CountNotOnNetworkCache
nosendtime	Alerter\Parameters	NotOnNetworkCacheTimeout
numnetsndbufs	None (obsolete)	
oplocktimeout	AdvancedServer\FileServiceParameters	OplockTimeout
packageid	None (obsolete)	
passmgmt	None (obsolete)	
polltime	None (obsolete)	
prebinduxredir	None (lanman.ini file)	

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
qnamelen	AdvancedServer\Parameters	MaxPrintQueueNameLength
qsched	AdvancedServer\Parameters	CheckPrintQueueInMinutes
queuealloc	None (obsolete)	
rdatrend	AdvancedServer\FileServiceParameters	ReadAheadCount
relmajor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MajorVersion
relminor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MinorVersion
samdir	None (obsolete)	
samgroup	None (obsolete)	
samowner	None (obsolete)	
samperms	None (obsolete)	
sbstelladmin	AdvancedServer\AlertParameters	AlertAdminOnLicenseOverflow
sbstelluser	AdvancedServer\AlertParameters	AlertUserOnLicenseOverflow
schedlogfile	None (obsolete)	
secsources	Eventlog\Security	Sources
sharefile	None (obsolete)	
sharegroup	None (obsolete)	
sharemkdir	AdvancedServer\ShareParameters	MakeUnixDirectoriesOn Share
shareowner	None (obsolete)	
shareperms	None (obsolete)	
shmgroup	None (obsolete)	
shmowner	None (obsolete)	

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
shmperms	None (obsolete)	
spareserver	AdvancedServer\ProcessParameters	KeepSpareServer
sparesrvtime	AdvancedServer\ProcessParameters	SpareServerTime
spipe	None (obsolete)	
srvstathelpfile	None (lanman.ini file)	
stacksize	None (lanman.ini file)	
startscript	None (obsolete)	
stoponcore	AdvancedServer\ProcessParameters	StopOnCore
svcinit	None (obsolete)	
svcscrip	None (obsolete)	
syncaclfile	AdvancedServer\FileServiceParameters	SyncAclFileOnWrite
synchomedir	AdvancedServer\UserServiceParameters	SyncUnixHomeDirectory
sysources	Eventlog\System	Sources
terminator	None (obsolete)	
tokensidlimit	None (obsolete)	
unixdirchk	AdvancedServer\FileServiceParameters	UnixDirectoryCheck
unixlocks	AdvancedServer\FileServiceParameters	UseUnixLocks
useoplock	AdvancedServer\FileServiceParameters	UseOplocks
userremark	AdvancedServer\UserServiceParameters	UserComment
ustructs	AdvancedServer\ProcessParameters	NumUStructs
uxclosecount	AdvancedServer\FileServiceParameters	UnixCloseCount
vcdistribution	AdvancedServer\ProcessParameters	VCDistribution
write_behind	AdvancedServer\FileServiceParameters	WriteBehind

[Replicator] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
exportlist	Replicator\Parameters	ExportList
exportpath	Replicator\Parameters	ExportPath
guardtime	Replicator\Parameters	GuardTime
importlist	Replicator\Parameters	ImportList
importpath	Replicator\Parameters	ImportPath
interval	Replicator\Parameters	Interval
logon	Replicator	ObjectName
password	None (obsolete)	
pulse	Replicator\Parameters	Pulse
random	Replicator\Parameters	Random
repl_dirgroup	Replicator\Parameters	UnixDirectoryGroup
repl_dirowner	Replicator\Parameters	UnixDirectoryOwner
repl_dirperms	None (obsolete)	
repl_filegroup	Replicator\Parameters	UnixFileGroup
repl_fileowner	Replicator\Parameters	UnixFileOwner
repl_fileperms	None (obsolete)	
replicate	Replicator\Parameters	Replicate
tryuser	Replicator\Parameters	TryUser

[Fsi] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
closeinodecnt	None (obsolete)	
fsaddonpath	None (lanman.ini file)	
fslibname	None (lanman.ini file)	
fslibpath	None (lanman.ini file)	
fsmap	None (lanman.ini file)	
fsnosupport	None (lanman.ini file)	
maxfstypes	None (obsolete)	
nfsroot	AdvancedServer\FileServiceParameters	RootOwnsFilesCreatedOnNFS
ntfs	AdvancedServer\FileServiceParameters	ReportNTFS
remotemounts	None (lanman.ini file)	

[Psi] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
maxspoolers	None (obsolete)	
psaddonpath	None (lanman.ini file)	

[Version] Section Parameter Mapping to Registry Key

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
lan_manager	None (obsolete)	

[Browser] Section Parameter Mappings to Registry Keys

Lanman.ini File Parameter	Advanced Server Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
backuprecovery	Browser\Parameters	BackupRecovery
backupupdate	Browser\Parameters	BackupUpdate
lmannounce	LanmanServer\Parameters	LmAnnounce
masterupdate	Browser\Parameters	MasterUpdate
morelog	Browser\Parameters	MoreLog

Lanman.ini File

Lanman.ini File Parameter Mapping to Registry Keys

Index

- A**
- access control list, 43
 - accessalert, 187
 - aclfile, 190
 - aclgroup, 190
 - acowner, 190
 - aclperms, 190
 - admingroupid, 190
 - Administrator privilege, 16
 - adminpath, 190
 - adminuserid, 190
 - Advanced Server
 - administering at the command prompt, 11
 - software availability in native languages, 125
 - troubleshooting, 93
 - Advanced Server commands
 - acladm, 13, 102
 - blobadm, 13
 - delshmem, 13
 - elfread, 72, 96, 107
 - joindomain, 14
 - lmat, 13
 - lmshare, 14
 - lmshell, 14, 100
 - lmstat, 14, 100
 - mapuname, 14
 - netevent, 14
 - regcheck, 14, 101, 110
 - regconfig, 14, 101
 - regload, 14, 110
 - samcheck, 15, 102
 - setdomainname, 15
 - setservername, 15
 - srvconfig, 15, 102, 110, 170
 - ud, 15
 - Advanced Server Registry
 - AS/U Administrator
 - keys that can be modified, 137
 - using, 137
 - data types, 134
 - description, 133
 - keys
 - compared to directories, 133
 - root keys, described, 133
 - structure, 133
 - Registry Editor
 - commands, 136
 - connecting to server, 135
 - keyboard actions for viewing data, 135, 136
 - starting, 135
 - using, 135
 - viewing registry, 135
 - value entries
 - compared to files, 133
 - integer data type, 133
 - size limitations, 133
 - viewing registry, 135
 - Advanced Server Registry keys
 - AccessAlert, 162
 - AclCacheSize, 142
 - AlertAdminOnLicenseOverflow, 141
 - AlertNames, 159
 - AlertUserOnLicenseOverflow, 141
 - AutoDisconnect, 162
 - BackupRecovery, 160
 - BackupUpdate, 160
 - BrowserMaxCalls, 155
 - CategoryCount, 162
 - CategoryMessageFile, 162
 - CheckPrintQueueInMinutes, 149
 - CoreOk, 151
 - CountNotOnNetworkCache, 159
 - CreateUnixUser
 - REG_DWORD, 157
 - DisableUpLevelPrinting, 149
 - EnableSoftCompat, 142
 - EnableSoftFileExtensions, 142
 - ErrorAlert, 163
 - EventlogMaxCalls, 155
 - EventMessageFile, 162
 - Exclude, 158
 - ExportList, 166
 - ExportPath, 166
 - File, 161
 - ForceDirectoryAcl, 142
 - ForceFileAcl, 143
 - ForceFileFlush, 143
 - ForceUniqueUnixUserAccount, 158
 - GroupUpdateTime, 158
 - GuardTime, 166
 - Hidden, 163
 - IgnoreUnixPermissions, 143
 - ImportList, 166
 - ImportPath, 167
 - IncludeMessageHeader, 159
 - Interval, 167
 - KeepAdministrativeShares, 157
 - KeepSpareServer, 151
 - LmAnnounce, 163
 - LockNapInMSec, 151
 - LogonAlert, 163
 - LogonQuery, 164
 - LsarpMaxCalls, 155
 - MakeUnixDirectoriesOnShare, 157
 - MappingSeparator, 143
 - MasterUpdate, 160
 - MaxDirectoryBufferSize, 149
 - MaxFilesInDirectory, 167
 - MaxFileSizeInKB, 144
 - MaxIpcTryCount, 149
 - MaxLockTimeInSeconds, 151
 - MaxMailslotReadTime, 149
 - MaxMessageSize, 150
 - MaxPrintQueueNameLength, 150
 - MaxRawSize, 150
 - MaxServiceWaitTime, 150
 - MaxSize, 161

Index

- MaxVCPerProc, 152
 - MaxVCs, 152
 - MemoryMapFiles, 144
 - MinSmbWorkerTasks, 152
 - MixedCaseSupport, 144
 - MoreLog, 160
 - NameSpaceMapping, 144
 - NativeLM, 150
 - NativeOS, 150
 - NetAdminGroupName, 148
 - NetAdminPath, 148
 - NetAdminUserName, 148
 - NetlogonMaxCalls, 155
 - NewUserShell, 158
 - NotOnNetworkCacheTimeout, 160
 - NumCIStructs, 152
 - NumCLIENT_SESSION, 152
 - NumHashTables, 153
 - NumSERVER_SESSION, 153
 - NumUStructs, 153
 - OplockTimeout, 145
 - Pulse, 164
 - QueryDelay, 164
 - Random, 167
 - Randomize, 165
 - ReadAheadCount, 145
 - RelogonDelay, 165
 - Replicate, 167
 - ReportNTFS, 145
 - Retention, 161
 - RootOwnsFilesCreatedOnNFS, 145
 - SamrMaxCalls, 156
 - Scripts, 165
 - SendByeMessage, 151
 - ShareCacheCount, 157
 - ShareReadCount, 157
 - SizeGcBufferPoolInKB, 151
 - Sources, 162
 - SpareServerTime, 153
 - SpoolssMaxCalls, 156
 - SrvAnnounce, 163
 - SrvComment, 164
 - SrvsvcMaxCalls, 156
 - SSIPasswdAge, 165
 - StopOnCore, 153
 - SvctlMaxCalls, 156
 - SyncAclFileOnWrite, 145
 - SyncUnixHomeDirectory, 158
 - TruncatedExtensions, 145
 - TryUser, 168
 - TypesSupported, 162
 - UniqueSuffixLength, 146
 - UnixCloseCount, 146
 - UnixDirectoryCheck, 42, 146
 - UnixDirectoryGroup, 168
 - UnixDirectoryOwner, 168
 - UnixDirectoryPerms, 146
 - UnixFileGroup, 168
 - UnixFileOwner, 168
 - UnixFilePerms, 147
 - UnixQuotas, 147
 - Update, 165
 - UseNfsLocks, 147
 - UseNfsLocks and
 RootOwnsFilesCreatedOnNFS, 67
 - UseOplocks, 147
 - UserComment, 159
 - UserPath, 164
 - UserRemark, 159
 - UseUnixLocks, 147
 - VCDistribution, 153
 - WinregMaxCalls, 156
 - WkssvcMaxCalls, 156
 - WriteBehind, 76, 148
 - alertadmin, 190
 - alerterrorlog, 190
 - alertmessage, 190
 - alertnames, 187
 - alerton, 190
 - alertprinting, 190
 - alertuser, 190
 - anncmailslot, 191
 - appretention, 191
 - appsources, 191
 - AS/U Administrator
 - keys that can be modified, 137
 - using, 137
 - auditretention, 191
 - autoconfig, 121
 - autoconfig command syntax, 82
 - autodisconnect, 187
- ### B
- backup
 - directories needing, 35
 - backup,directories needing, 35
 - backuprecovery, 199
 - backupupdate, 199
 - Batch oplocks, 75
 - blobmapping, 191
 - byemessage, 191
- ### C
- cacheadm command, 89
 - CD ROM file systems, 64
 - chgrp command, 45
 - client write errors, 76
 - clispooltime, 191
 - closeinodecnt, 198
 - cntsharecache, 191
 - cntsharereads, 191
 - confirmation of net command, 19
 - controllock, 191
 - Copying
 - Windows 95 Registry Editor files, 135
 - coreok, 191
 - country, 191
 - cpigroup, 191
 - cpipname, 191
 - cpipowner, 191
 - cpipperms, 191
 - CreateUnixUser, 28
 - creatunixuser, 191

Index

D

dirperms, 191
disk space reported, configuring, 56
DNS database, 85
domain, 188
DOS attributes, retaining, 41

E

eafileprefix, 191
elfread command, 72
enable_soft_file_ext, 187
enablessoftcompat, 187
erroralert, 187
errorretention, 191
errsources, 191
European character support, 126
event logging, 72
exclude, 189
executables, 12
exportlist, 197
exportpath, 197

F

feabufsize, 191
file access permissions, HP-UX, 43
file interlocking, 46
file locks, maximum, 77
fileflush, 191
fileperms, 192
files per process, 77
forcediracl, 192
forcefileacl, 192
forceunique, 189
ForceUniqueUserAccount, 28
fsaddonpath, 198
fslibname, 198
fslibpath, 198
fsmap, 198
fsnosupport, 198

G

gcbuffer, 192
getapipe, 192
GIDs, retaining, 41
group permissions, 43
groupadd, 192
groupdel, 192
grpupdate, 192
guardtime, 197

H

hashsize, 192
HPDPS spooler, 60

I

ignoresigpwr, 192
importlist, 197
importpath, 197
inodes, open, 77
ipctries, 192

J

Japanese character support, 128
joindomain command, 14

K

keepadmshares, 192
keepunixgroups, 29, 41, 182
Keys
 in the Registry, 133

L

lan interface, overriding default configuration, 84
lan_manager, 199
Lanman.ini file
 changing parameter, 171
 parameter description, 173
 parameter mapping to registry keys, 187
 syntax, 171

Lanman.ini file parameters

admin, 183
anncmailslot, 174
appsources, 174
cancelcmd, 183
cancelkey, 183
country, 174
dll_dir, 175
domain, 174
fsaddonpath, 181
fslibname, 181
fslibpath, 181
fsmap, 181
fsnosupport, 181
keepunixgroups, 41
lang, 175
listenextension, 175
listenname, 173
listennamechk, 176
listenqlen, 176
lmaddonpath, 176
lmgetmsg_path, 176
lmxadmin, 183
lmxguest, 183
lpcmd, 183
lpcopiesopt, 183
lpkey, 184
lptitleopt, 184
mapaclblob, 177
mapchangelogblob, 177
maplsablob, 177
mapregistryblob, 177
mapsamblob, 177
maxclients, 173
maxdiskspacereported, 56
maxfilesize, 177
maxjobs, 184
maxprinters, 184
maxqueues, 184
maxworkint, 184
minworkint, 185
msgforward, 178
nativelm, 178

Index

-
- nativeos, 178
 - netaddonpath, 178
 - nethelpfile, 178
 - netmsgwait, 179
 - network, 179
 - prebinduxredir, 180
 - psaddonpath, 182
 - remotemounts, 181
 - secsources, 180
 - srvconfig command, 170
 - srvservices, 173
 - stacksize, 180
 - statjcmd, 185
 - statjkey, 185
 - statjpcmd, 186
 - statjpkey, 185
 - statjskey, 186
 - sysources, 180
 - limit on files per process, 77
 - listenextension, 192
 - listenname, 187
 - listennamechk, 192
 - listenqlen, 192
 - lmaddonpath, 192
 - lmannounce, 199
 - lmworld, 43
 - lmx.srv processes, 77
 - lmxmsgfile, 192
 - lmxsrsv, 192
 - lmxtimesource, 192
 - local server defined, 16
 - locale, 192
 - locknap, 192
 - log files, viewing, 73
 - log in as root, 16
 - logged in as root, 16
 - logon, 197
 - logonalert, 187
 - lp spooler, 58
 - lptmpdir, 192
 - lsafile, 192
 - lsagroup, 193
 - lsaowner, 193
 - lsaperms, 193
- M**
- mailslotgroup, 193
 - mailslothold, 193
 - mailslotowner, 193
 - mailslotperms, 193
 - mapuname
 - procedure for use, 27
 - masterupdate, 199
 - maxadminoutput, 193
 - maxapplog, 193
 - maxauditlog, 187
 - maxclients, 187
 - maxclients tuning, 74
 - maxclisess, 189
 - maxdirbufsize, 193
 - maxdiskspacereported, 56, 182
 - maxerrlog, 187
 - maxfiles, 77
 - maxfilesize, 193
 - maxfstypes, 198
 - maximum open files, 77
 - maxlocknap, 193
 - maxmsdepth, 193
 - maxmsgsize, 193
 - maxmux, 193
 - maxopenfiles, 193
 - maxquery, 189
 - maxrawsize, 193
 - maxspoolers, 198
 - maxsrvsess, 189
 - maxsvcwait, 193
 - maxuid, 189
 - maxvcperproc, 193
 - maxvcs, 193
 - memorymap, 193
 - minsmbworkers, 193
 - minuid, 189
 - minvcperproc, 193
 - morelog, 199
 - msdirgroup, 194
 - msdirname, 194
 - msdirowner, 194
 - msdirperms, 194
 - msdoscodepage, 126
 - msgforward, 194
 - msgheader, 194
- N**
- name resolution with WINS, 81
 - name resolution without WINS, 85
 - name resolution, client, 81
 - nativelm, 194
 - nativeos, 194
 - nbconfig file, 83
 - nbhost file, 91
 - nbutil utility, 82
 - Net command
 - administering local server, 16
 - online help, 22
 - paging through screens, 18
 - typing path names at client computers, 21
 - typing path names at the server, 20
 - understanding command syntax, 21
 - using abbreviations, 19
 - using command confirmation, 19
 - using passwords, 18
 - Net commands
 - net access, 23
 - net accounts, 23
 - net admin, 23
 - net auditing, 23
 - net browser, 24
 - net computer, 24
 - net config, 24
 - net config server, 24
 - net continue, 24
 - net device, 24

Index

- net file, 24, 98
- net group, 24
- net help, 24
- net helpmsg, 25
- net localgroup, 25
- net logoff, 25
- net logon, 25
- net password, 25
- net pause, 25
- net perms, 25
- net print, 25
- net send, 25
- net session, 25, 27, 98
- net share, 26
- net sid, 26
- net start, 26, 107
- net statistics, 26, 96
- net status, 26
- net stop, 26
- net time, 26
- net trust, 26
- net user, 26
- net version, 26
- net view, 26, 109, 110
- net commands
 - running net logon before, 23
 - net logon before net trust, 23
- netaddonpath, 194
- NetBIOS
 - configuring memory usage, 74
 - troubleshooting, 120
- NetBIOS name cache, adding
 - names to, 82
- nethelpfile, 194
- nethmsgfile, 194
- netmsgwait, 194
- network, 194
- network routing tables,
 - manipulating, 122
- newusershell, 194
- nfile, 77
- nflocks, 77
- NFS use with AS/U, 66
- nfslocks, 194
- nfsroot, 198
- ninode, 77
- NIS interoperability, 69
- nonexistusers, 194
- nosendtime, 194
- nproc, 77
- nrfc_nb kernel parameter, 74
- ntfs, 198
- number of file locks, maximum,
 - 77
- number of open inodes,
 - maximum, 77
- number of processes, maximum,
 - 77
- number of semaphore identifiers, 78
- number of semaphores,
 - maximum, 78
- numnetsndbufs, 194
- O**
- open files, maximum, 77
- OpenSpool spooler, 59
- oplocktimeout, 194
- P**
- packageid, 194
- passmgmt, 194
- password, 197
- password in net command, 18
- Permissions (system access)
 - on UNIX system, 113
 - turning off UNIX system
 - permission checking, 114
- pfs_mount, 64
- ping examples, 121
- polltime, 194
- prebinduxredir, 194
- proxy name cache
 - maximum entries, 89
- psaddonpath, 198
- pulse, 189, 197
- Q**
- qnamelen, 195
- qsched, 195
- querydelay, 189
- queuealloc, 195
- R**
- random, 197
- randomize, 189
- rdatrend, 195
- Registry
 - copying Windows 95 Registry Editor files, 135
 - description, 131
 - keys, 133
 - security, 135
 - See also Registry Editor, 134
 - viewing, 135
- Registry Editor
 - keyboard actions for viewing
 - Registry data, 136
 - See also Registry, 135
 - viewing Registry, 135
- relmajor, 195
- relminor, 195
- relogondelay, 190
- remote server defined, 16
- remotemounts, 198
- repl_dirgroup, 197
- repl_dirowner, 197
- repl_dirperms, 197
- repl_filegroup, 197
- repl_fileowner, 197
- repl_fileperms, 197
- replicate, 197
- root directory path
 - modifying, 12
- routed networks, operating in,
 - 82

Index

S

samdir, 195
samgroup, 195
samowner, 195
samperms, 195
sbstelladmin, 195
sbstelluser, 195
schedlogfile, 195
scripts, 190
secsources, 195
Security
 Registry, modifying, 135
semaphore undo entries, 78
semni, 78
semns, 78
semnu, 78
semume, 78
shared memory identifiers, 78
shared memory segments,
 maximum, 78
sharefile, 195
sharegroup, 195
sharemkdir, 195
shareowner, 195
shareperms, 195
shmgroup, 195
shmmx, 78
shmmni, 78
shmowner, 195
shmperms, 196
shmseg, 78
spareserver, 196
sparesrvtime, 196
special characters, 20
spipe, 196
spooler service, 58
srvannounce, 188
srvcomment, 188
srvhidden, 188
srvservices, 188
srvstathelpfile, 196
ssipasswdage, 190
stacksize, 196

stacksize, setting for NIS, 69
startscript, 196
stoponcore, 196
svcinit, 196
svcscrip, 196
syncaclfile, 196
synchomedir, 196
sysevent.evt file, 73
syssources, 196

T

terminator, 196
tokensidlimit, 196
Troubleshooting
 assessing status of server
 Alerter service, 99
 elfread command, 96
 Event Viewer, 95
 open resources, 98
 print subsystem event log-
 ging, 99
 Server Manager, 96, 97, 98,
 111
 server statistics, 96
 session information, 97
 UNIX system scripting fea-
 ture, 100
 viewing events, 95
 browsing problems, 117
 checking the network, 104
 debugging server problems,
 100
 debugging tools
 acladm command, 102
 lmshell command, 100
 lmstat command, 100
 regcheck command, 101
 regconfig command, 101
 samcheck command, 102
 srvconfig command, 102
 isolating problems
 maximum number of users,

 110
 messages in error logs, 107
 registry corrupted, 110
 resources shared properly,
 108
 server contact from client,
 110
 server contacted from con-
 sole, 109
 server running, 106
 services running, 107
 NetBIOS protocol status, 105
 physical network, 104
 printing problems, 118
 problems on the server, 106
 procedures
 checking the network, 104
 isolating the problem, 106
 shared resource, 110
 transport protocol, 104
 UNIX system functionality,
 105
tryuser, 197

U

uchmod command, 48, 52, 112,
 116
ud command, 48, 53
udir command, 48, 111, 115
UNIX system access permissions
 changing, 116
 differences between UNIX and
 Advanced Server, 112
 directory permissions, 113
 file and directory permissions,
 114
 group permissions and
 Advanced Server, 113
 maintaining for specific files,
 116
 turning off checking, 114
 understanding, 115

Index

unixdirchk, 196
UnixDirectoryCheck, 42
UnixDirectoryCheck and
 keepunixgroups, 42
UnixDirectoryPerms, 40
UnixFilePerms, 40
unixlocks, 196
update, 190
uren command, 51
uren command
 , 48
useoplock, 196
userpath, 188
userremark, 196
UseUnixLocks, 46
UseUnixLocks and UseOplocks
 usage with NFS, 68
usrcomment, 189
ustructs, 196
uxclosecount, 196

V

vcdistribution, 196
VCDistribution tuning, 74
viewing registry, 135

W

Windows 95
 Registry Editor files, copying,
 135
WINS client support, 81
WINS database, 81
WINS server, primary and
 secondary, 81
write_behind, 196
WriteBehind, setting, 76