

Invisible LAN Operating System

DOS User Manual

© Copyright 1995 Invisible Software, Inc.

Web:

www.invisiblesoft.com

Email:

invisoft@invisiblesoft.com

Invisible Software Program License Agreement

The programs in this package are copyrighted. By using them, you indicate acceptance of the following terms and conditions. If you do not agree with these terms and conditions, return the programs to the place of purchase; and your money will be refunded.

1. License. You may use the programs on a single local area network, and you may make a reasonable number of copies of the programs for backup purposes.

2. Restrictions. You may not use the programs on more than one local area network at the same time. You may not distribute copies of the programs or documentation to others, or place them into any electronic bulletin board or information retrieval system. You may not modify or reverse engineer the programs. You may not remove, alter, or circumvent any serialization or copy protection mechanism that is built in to the programs.

3. Limited Warranty on Diskettes. If a diskette in this package is defective, Invisible Software will replace it at no charge if the defective diskette is returned to Invisible Software, shipping prepaid, within 90 days of the date of purchase.

4. Limited Warranty on Software. Invisible Software warrants that the programs will operate substantially as described in the documentation. If you report a significant software defect in writing within 90 days of the date of purchase, and Invisible Software is not able to correct the defect, then you may return the programs and documentation to the place of purchase; and your money will be refunded.

5. Disclaimer. IN NO EVENT WILL INVISIBLE SOFTWARE BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAMS EVEN IF INVISIBLE SOFTWARE OR AN AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. This agreement will be governed by the laws of the State of California.

6. U.S. Government Restricted Rights. The software and documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights at 48 CFR 52.227-19, as applicable. Contractor/manufacturer is Invisible Software, Inc.

TRADEMARKS

Invisible LAN, Invisible Network, Invisible Software, NET/30, NET/30 For Windows, Ultra Server, Invisible LAN Remote, Invisible Ethernet, Invisible RAM, Invisible RAM 386, Invisible EMS, TransBIOS, CACHE/30, and PopMaster are trademarks of Invisible Software, Inc.

IBM, IBM PC, PC/XT, PC AT, PS/2, Micro Channel, PC Network, and PC LAN Program are trademarks of International Business Machines Corporation.

PostScript is a trademark of Adobe Systems, Inc.

SCAT, PEAK, NEAT, and AT/386 are trademarks of Chips and Technologies.

Windows, MS-DOS, and EMM386 are trademarks of Microsoft Corporation.

LaserJet and PCL are trademarks of Hewlett-Packard Company.

LaserWriter is a trademark of Apple Computer.

Novell and Netware are trademarks of Novell, Inc.

QEMM-386 and DesqView are trademarks of Quarterdeck Office Systems.

386-MAX is a trademark of Qualitas.

Contents

Preface	ix
---------------	----

Part 1 — Command Line Utilities

Introduction to Command Line Utilities	1-1
Command Summary	1-1
Getting Help	1-3
ERRORLEVEL Return Codes	1-5
 Using Network Resources	 2-1
Displaying Current Network Resources	2-1
Managing Connections to Network Disks	2-2
Connecting to a Network Disk	2-2
Disconnecting From a Network Disk	2-5
Managing Connections to Network Printers	2-6
Connecting to a Network Printer	2-6
Disconnecting From a Network Printer	2-7
Error Recovery and Automatic Re-Mapping	2-8
 The Network Clock	 3-1
 Using Network Printers	 4-1
Printing a File	4-1
Printing the Screen	4-3
Truncating the Print Stream	4-3
Manual Truncation	4-3
Automatic Truncation	4-4
Immediate Truncation	4-5
Using PRINTNOW in a Batch File	4-6
PRINTNOW in a Secondary Command Processor	4-6
Sending Printer Set-up Strings	4-7
 Controlling the Print Spooler	 5-1
Displaying the Print Spooler Status	5-1
Setting the Print Spooler State	5-2

Pausing the Print Spooler	5-3
Continuing the Print Spooler	5-3
Modifying the Print Queue	5-4
Restarting the Current Print Job	5-4
Canceling the Current Print Job	5-5
Clearing the Print Queue	5-5
Controlling Form-feeds	5-6
Turning Off Form-Feeds	5-6
Turning On Form-Feeds	5-7
Flow Control for Serial Printers	5-7
Selecting Xon/Xoff	5-8
Selecting DTR	5-8
Direct Printing	5-9
Print Priority	5-10
Creating a Break Page	5-10

Network Software Control 6-1

Dedicated Servers	6-1
Controlling The Disk Cache	6-2
Example 1 — Enabling, Disabling, Flushing	6-3
Example 2 — Changing The Write Policy	6-3
Example 3 — Cache Statistics	6-4
Displaying Network Software Status	6-6
Controlling the Server	6-7
Hiding the Network Software	6-7
Controlling Use of the Speaker	6-8
Tape Backup	6-9
Image Backup	6-9
File-by-File Backup	6-9
Controlling Ultra Server	6-10
Displaying Ultra Server Status	6-10
Unmounting Drives	6-12
Mounting Drives	6-14
Ultra Server in Non-Dedicated Mode	6-15

Logon Commands 7-1

Entering Your Password	7-1
Logging On to the Network	7-2
Logging On	7-3
Logging Off	7-3

Diskless Workstation Commands	8-1
Creating a Boot Diskette	8-1
Creating an Image File	8-2
Configuring the RPL Server	8-3
Starting the Workstations	8-4
Unlinking From the RPL Server	8-5
Custom Startup Procedures	8-6
Memory Management	8-8
Copying the Network ROM	8-8
Relocating the TransBIOS Data Area	8-8
 Memory Management Commands	 9-1
Displaying the Memory Map	9-1
/D — DOS Memory Information	9-2
/X — Expanded Memory Information	9-2
/H — Expanded Memory Handles	9-3
/E — Extended Memory Size	9-4
/C — Chips And Technologies Chipset Information	9-4
/N — Network Software Information	9-7
/S — Shadow RAM Usage Information	9-7
/M — Memory Map	9-8
Using Shadow RAM	9-11
Loading Memory-Resident Programs	9-11
Loading Device Drivers	9-13
Controlling VGA and EGA Graphics Memory	9-15
Enabling VGA or EGA Graphics	9-15
Disabling VGA or EGA Graphics	9-15
Controlling the Default Graphics State	9-16
Clearing the CMOS Memory	9-16

Part 2 — Electronic Mail

Electronic Mail	10-1
Sending Messages	10-1
Receiving Messages	10-3

Part 3 — The Network Manager

- Introduction to the Network Manager 11-1**
 - Starting the Manager 11-1
 - Poll Network, Select Machine 11-3
 - Displaying Computers on the Network 11-3
 - Selecting a Network Computer to Manage 11-3
 - Getting Help 11-5
- Mappings 12-1**
 - Drive Mappings 12-1
 - Displaying the Drive Mappings 12-1
 - Disconnecting a Drive Mapping 12-2
 - Establishing a Drive Mapping (Method #1) 12-3
 - Establishing a Drive Mapping (Method #2) 12-4
 - Printer Mappings 12-5
 - Displaying the Printer Mappings 12-5
 - Disconnecting a Printer Mapping 12-6
 - Establishing a Printer Mapping (Method #1) 12-7
 - Establishing a Printer Mapping (Method #2) 12-8
- Print Stream Truncation 13-1**
- Managing Printers 14-1**
 - Displaying Print Spooler Status 14-1
 - Changing Print Spooler Settings 14-2
 - Setting the Print Spooler State 14-2
 - Controlling Form Feeds 14-3
 - Flow Control 14-4
 - Printer Control 14-4
 - Displaying Print Queue Contents 14-5
 - Changing Print Queue Contents 14-6
- Security 15-1**
 - Security Objects and Bindings 15-2
 - Users 15-4
 - Displaying Users 15-4
 - Creating Users 15-4
 - Changing User Definitions 15-5

Deleting Users	15-6
Groups	15-6
Displaying Groups	15-7
Creating Groups	15-7
Changing Group Definitions	15-8
Deleting Groups	15-8
Group Memberships	15-8
Assigning Members to a Particular Group	15-8
Assigning Group Memberships to a Particular User	15-9
Shortnames	15-10
Access Rights	15-10
Displaying Shortnames	15-12
Creating Shortnames	15-13
Changing Shortname Definitions	15-13
Deleting Shortnames	15-14
Shortname Permissions	15-14
Permissions For a Particular Shortname	15-14
Shortname Permissions For a Particular User or Group	15-15
Using Shortnames	15-15
Using Shortnames in the MAP Command	15-16
Using Shortnames in the MENU program	15-17
Using Shortnames in the Setup Program	15-17
Miscellaneous Functions	15-18
Displaying Miscellaneous Functions	15-18
Controlling Access to Disks	15-19
Controlling Access to Printers	15-19
Controlling Access to Security	15-20
Controlling Access to Server Monitoring	15-20
Controlling Access to the Bulletin Board	15-21
Miscellaneous Permissions	15-21
Permissions For a Particular Miscellaneous Function	15-22
Miscellaneous Permissions For a Particular User or Group	15-23
Saving and Resetting Security	15-24
Security Example	15-24

Server Usage Statistics **16-1**

Server Resources	16-2
Disk Cache Statistics	16-4
Active Users	16-5
Audit Trail	16-6
Viewing the Audit Trail	16-7
Setting the Audit Filter	16-7

Saving the Audit Trail to a File	16-9
Ultra Server Resources	16-10

Part 4 — Appendices and Index

Invisible LAN Command Reference	A-1
Restricted DOS Commands	B-1
Index	C-1

Preface

This manual tells you how to use Invisible LAN at the DOS command line.

- Part 1 describes the command line utilities. You'll learn about a variety of network commands that you can use at the DOS command line. With these commands, you can perform a wide variety of functions, such as defining network disks and printers, controlling the print spooler and disk cache, and logging on to the network.
- Part 2 describes the pop-up electronic mail system, that lets you send and receive messages.
- Part 3 describes the network manager, a menu-driven program for controlling and managing the network. The network manager can perform most of the functions of the command line utilities. In addition it lets you manage security, monitor network performance, and use an extensive on-line help system. The manager also operates by "remote control," so you can manage computers anywhere on the network.
- Part 4 contains appendices and a comprehensive index.

This manual does not describe how to install the Invisible LAN software. Refer to the *Getting Started* manual or the *Installation* manual for installation instructions.

Part 1

Command Line Utilities

Introduction to Command Line Utilities

The *command line utilities* are programs you can use at the DOS command line to control the network. The command line utilities perform a wide variety of functions, such as establishing network connections, controlling network printers, controlling the disk cache, and logging on to the network.

Most of the functions of the command line utilities can also be performed by the menu-driven network manager, which is described in the second half of this manual. The command line utilities are more convenient when you want to do something quickly at the DOS command line, or in a batch file. The menu-driven network manager is more convenient if you like to control the network through a menu interface with extensive on-line help.

In this introductory chapter, we describe:

- Command summary
- Getting help
- Using commands in a batch file

Command Summary

The following table briefly describes each of the command line utilities. You can find a more complete summary in appendix A.

Table 1-1. Command Line Utilities

CACHE	Controls the disk cache, and displays cache status and performance statistics.
CLRCMOS	Erases the computer's CMOS memory to reset the computer's configuration.
DEDICATE	Establishes a dedicated file server.
LOGOFF	Restores the original user name, reversing the effect of LOGON.
LOGON	Enters your user name and password for security permissions.
LSHADOW	Loads a memory-resident program into shadow RAM (memory between 640K and 1M).
MAKEBP	Changes the design of the break page that the print spooler prints at the start of each print job.
MAKEIMG	Creates a boot diskette image file, for use in supporting diskless workstations.
MAP	Creates, destroys, and displays your network connections. Defines your network disks and printers.
NETADDR	Displays or tests the network hardware address or serial number.
NETCLOCK	Gets the date and time from a server and sets your computer's clock.
NETHELP	Displays help information on a specified topic.
NETPRINT	Prints a file.
NW	Controls various aspects of the network software, such as the use of the speaker.
PASSWORD	Enters your password.
PQ	Controls the network print queue. Lets you control form feeds, flow control, printing priority, and direct printing. Displays print queue status information.
PRINTNOW	Immediately truncates the network print streams.
PSETUP	Establishes a set-up string for a network printer.

SHADOW	Displays a memory map and other information about the memory in your computer.
TRUNCATE	Controls automatic truncation of network print streams.
UNLINK	Disconnects a diskless workstation from the remote program load server.
US	Controls Ultra Server, mounts and unmounts drives, and displays Ultra Server status and performance statistics.
VGAOFF	Disables VGA and EGA graphics, increasing DOS memory beyond 640K.
VGAON	Enables VGA and EGA graphics, limiting DOS memory to 640K.

Getting Help

Each command line utility displays help information if you enter the name of the command followed by “?” or “/?”. For example, to get help on the **MAP** command, enter

```
MAP ?
```

or

```
MAP /?
```

To get help on the **NETPRINT** command, enter

```
NETPRINT ?
```

or

```
NETPRINT /?
```

And so on.

In addition to the help that is built in to each command, there is also a program called **NETHELP** that displays information on a wide variety of topics.

The **NETHELP** command is used to display help information. **NETHELP** can display information about Invisible LAN commands, DOS commands, Invisible LAN parameters, and general information.

To get help on a topic, type

NETHELP *topic*

To print the help information, redirect the standard output to the printer, as follows:

NETHELP *topic* >LPT1

NETHELP can display a list of available topics. To list all Invisible LAN commands, type

NETHELP **COMMANDS**

To list frequently-used DOS commands, type

NETHELP **DOS**

To list topics that give general information about Invisible LAN, type

NETHELP **GENERAL**

To list topics that describe Invisible LAN parameters, type

NETHELP **PARAMETERS**

To list all the topics in the help system, type

NETHELP **TOPICS**

To get help using **NETHELP**, type

NETHELP **?**

Example — To get help on the MAP command, type

NETHELP **MAP**

Example — To get help on the ATTRIB DOS command, type

NETHELP ATTRIB

Example — To get information on the parameters that configure the Invisible LAN server, type

NETHELP SERVER PARAMETERS

Example — To get general information about the disk cache, type

NETHELP DISK CACHE

SUMMARY: Each Invisible LAN command displays help information if you enter the name of the command followed by a question mark. In addition, the **NETHELP** command displays help on Invisible LAN commands, Invisible LAN parameters, general information about Invisible LAN, and frequently-used DOS commands.

ERRORLEVEL Return Codes

Each Invisible LAN command returns ERRORLEVEL 1 if it is not successful. If you put one of the commands into a batch file, you can use the IF ERRORLEVEL command to take different actions, depending on whether or not the command was successful. Here is a sample batch file, which demonstrates how to take different actions depending on whether or not a drive mapping is successful:

```
MAP E: \\MIKE\C:
IF ERRORLEVEL 1 GOTO :FAILED
ECHO MAP command was successful!
GOTO :DONE
:FAILED
ECHO MAP command failed!
:DONE
```

SUMMARY: The Invisible LAN command line utilities return an ERRORLEVEL code, so you can write batch files that take different actions depending on whether or not the command is successful.

Using Network Resources

Invisible LAN lets you access network resources (disks and printers) attached to computers other than your own. The *Getting Started* manual introduced a few ways to do this using the **MAP** command. This chapter describes all of **MAP**'s capabilities. It covers three main topics:

- Displaying current network resources
- Managing connections to network disks
- Managing connections to network printers

Before using **MAP**, your computer must be running the Invisible LAN redirector program. You do this by telling the Invisible LAN Setup program (**SETUP30**) that you want to install the redirector. Refer to the *Getting Started* manual or the *Installation* manual for instructions on installing the redirector.

Note — This chapter describes the use of the **MAP** command from the DOS prompt. You can also use the Network Manager (**MENU** program) to do these functions. See chapter 12 for a discussion of the menu system.

Displaying Current Network Resources

Use the **MAP** command to display your current network resources.

To display your network disks and printers, type

MAP

Example — Assume you had previously given the following commands:

```
MAP E: \\ROBERT\C:\ACCOUNTS
MAP LPT1 \\ROBERT\1
MAP D: \\ALICE\C:\
```

To display a list of your network disks and printers, type

```
MAP
```

The screen displays the following list:

```
D: ==> \\ALICE\C:\
E: ==> \\ROBERT\C:\ACCOUNTS
LPT1 ==> \\ROBERT\1
```

SUMMARY: The **MAP** command with no parameters displays a list of your network disks and printers.

Managing Connections to Network Disks

This section explains how to connect to and disconnect from a network disk using the **MAP** command. You can connect to a network disk using either a *drive letter* or a *shortname*. This chapter describes the use of a drive letter; see chapter 15 for a discussion of the use of shortnames. A *drive letter* is a letter A through Z followed by a colon. For example, **E:** is a drive letter.

Connecting to a Network Disk

To use a server's disk drive, use the **MAP** command. **MAP** assigns a drive letter to represent the server's drive. For example, you might use drive letter D: to refer to a server's disk. Once a drive letter is assigned, the drive acts as if it were connected to your own computer. You can use standard DOS commands and programs to access files on the server's disk.

Note — Using the Invisible LAN Setup program (**SETUP30**), you can specify drive mappings to be established automatically whenever you start Invisible LAN. Refer to the *Installation* manual for details.

To assign a drive letter to a server's drive, type

```
MAP d: \\server\ d: [\path] [/W]
```

The parameters have the following meanings:

d:	The drive letter used to refer to the server's disk.
server	The network name of the server.
d: [\path]	A drive and directory path on the server. The \path is optional. If you specify the root directory (\), then you have access to the server's entire disk, including all subdirectories. If you specify any other directory, then you have access only to that particular directory (and its subdirectories). If you omit \path , the default is the root directory.
/W	Indicates that MAP should wait for the server computer to boot up if it is not on the network. /W is optional. If /W is not included, then MAP terminates with an error message if the server computer is not on the network.

Example 1 — A server named ALICE has a fixed disk named C:. To use drive letter F: to refer to ALICE's fixed disk, type

```
MAP F: \\ALICE\C:\
```

Example 2 — A server named ROBERT has a fixed disk named C:. To use drive letter E: to refer to subdirectory \ACCTS on ROBERT's disk, type

```
MAP E: \\ROBERT\C:\ACCTS
```

The table below and Figure 2-1 show some examples of files on Robert's disk and the names you would use to access them:

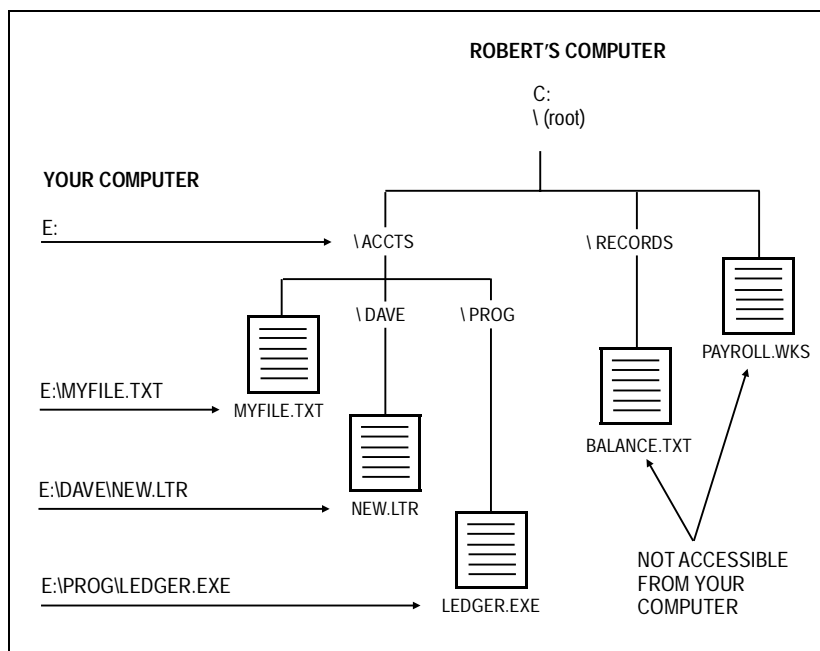


Figure 2-1. Example of File Access Using MAP Command

On Robert

C:\ACCTS\MYFILE.TXT
C:\ACCTS\DAVE\NEW.LTR
C:\ACCTS\PROG\LEDGER.EXE
C:\RECORDS\BALANCE.TXT
C:\PAYROLL.WKS

On Your Computer

E:\MYFILE.TXT
E:\DAVE\NEW.LTR
E:\PROG\LEDGER.EXE
Not Accessible
Not Accessible

Example 3 — This example illustrates the /W option. Suppose that you have two servers, named CASTOR and POLLUX. Each server has a fixed disk named C:, and each wants to use drive letter D: to refer to the other's disk.

On CASTOR, type

MAP D: \\POLLUX\C:\ /W

On POLLUX, type

MAP D: \\CASTOR\C:\ /W

Suppose that you start CASTOR before starting POLLUX. If you didn't use the **/W** option, then CASTOR's **MAP** command would fail, because POLLUX is not started yet. The **/W** option causes CASTOR's **MAP** command to wait until POLLUX is started.

SUMMARY: The **MAP** command establishes a connection between a local drive letter and a server's disk or directory. Once the connection is established, the server's disk behaves as if it were attached to your computer.

Disconnecting From a Network Disk

To break the connection to a network disk, you use the *Discontinue* option of the **MAP** command. Once the connection is broken, you cannot access the network drive unless you reestablish connection with the **MAP** command.

To disconnect from a server's disk, type

```
MAP d: /D
```

The parameter has the following meaning:

d:	The drive letter that currently refers to the server's disk.
-----------	--

Example 1 — Your drive letter F: refers to a fixed disk on a server named ALICE. To disconnect from ALICE's disk, type

```
MAP F: /D
```

Example 2 — You have a fixed disk named C:. To temporarily use drive name C: to refer to the fixed disk on server TERRY, type

```
MAP C: \\TERRY\C:\
```

Now drive letter C: accesses TERRY's fixed disk. You cannot use your own fixed disk. When you are finished using TERRY's disk, type

```
MAP C: /D
```

Now drive letter C: again refers to your own disk.

SUMMARY: The **MAP** command with the **/D** option breaks the connection between a local drive letter and a server's disk.

Managing Connections to Network Printers

This section explains how to connect to and disconnect from a network printer using the **MAP** command.

Connecting to a Network Printer

You connect to a network printer by assigning a *device name* to represent it. For example, you could use device name LPT1 to refer to a server's printer. Once you have assigned a device name, any reference to that name accesses the server's printer.

Note — Using the Invisible LAN Setup program (**SETUP30**), you can specify printer mappings to be established automatically whenever you start Invisible LAN. Refer to the *Installation* manual for details.

To assign a device name to a server's printer, type

MAP LPT x \\server\[n] [/W]

The parameters have the following meanings:

LPTx	The device name used to refer to the server's printer: LPT1, LPT2, or LPT3.
server	The network name of the server.
n	The server's printer number: 1 or 2. This parameter is optional; if omitted, the default is 1.
/W	Indicates that MAP should wait for the server computer to boot up if it is not on the network. /W is optional. If /W is not included and the server computer is not on the network, then MAP terminates with an error message.

Example 1 — A server named ALICE has a printer and has started the print spooler. To use device name LPT1 to refer to ALICE's printer, type

```
MAP LPT1 \\ALICE\
```

or

```
MAP LPT1 \\ALICE\1
```

Example 2 — Server ROBERT has a printer. You want to refer to ROBERT's printer as LPT2 and to wait for server ROBERT to boot up. Type

```
MAP LPT2 \\ROBERT\ /W
```

Example 3 — Server ROBERT has two shared printers. You want to use LPT2 to refer to ROBERT's first network printer and LPT3 to refer to ROBERT's second network printer. Type

```
MAP LPT2 \\ROBERT\1
```

```
MAP LPT3 \\ROBERT\2
```

Note — If your computer is a server, and you share a printer, it is important that you establish a mapping to your own printer. This makes your printer output go through the print spooler. If you don't establish a mapping to your own printer, then your printer output will get mixed together with other users' printer output. When you install the network software with the **Easy Configuration** section of the Setup program, the Setup program automatically creates this printer mapping.

SUMMARY: The **MAP** command establishes a connection between a local device name and a server's printer. Once the connection is established, you use the device name to refer to the server's printer.

Disconnecting From a Network Printer

To break the connection to a network printer, you use the *Discontinue* option of the **MAP** command. Once the connection is broken, you cannot access the network printer unless you reestablish connection with the **MAP** command.

To discontinue the use of a server's printer, type

```
MAP LPTx /D
```

The parameter has the following meaning:

LPTx	The device name currently used to refer to the server's printer: LPT1, LPT2, or LPT3.
-------------	---

Example 1 — You are using device name LPT2 to refer to a printer on a server name ROBERT. To stop using ROBERT's printer, type

```
MAP LPT2 /D
```

Example 2 — You have a printer named LPT1. To temporarily use device name LPT1 to refer to the printer on server TERRY, type

```
MAP LPT1 \\TERRY\
```

Now LPT1 accesses TERRY's printer. You cannot use your own printer. When you are finished using TERRY's printer, type

```
MAP LPT1 /D
```

Now device name LPT1 again refers to your own printer.

SUMMARY: The **MAP** command with the **/D** option breaks the connection between a local device name and a server's printer.

Error Recovery and Automatic Re-Mapping

You may wonder what happens if someone turns off the server while you have drive or printer mappings in effect.

If the server is turned off, your network drives and printers become invalid. If you try to use them, you will get an error message such as "Abort, Retry, Fail" or "Network device no longer exists". If you execute the **MAP** command to

display your drive and printer mappings, the letter **E** appears at the left edge of the screen to indicate that an error occurred.

When the server is turned back on, Invisible LAN automatically re-establishes your drive and printer mappings. It is not necessary to type a new **MAP** command in order to restore the mappings.

Although Invisible LAN automatically re-maps your drives and printers when the server is restarted, it does not re-connect open files. If you are in the middle of an application program when the server is restarted, you may have to exit back to DOS and then restart the application.

SUMMARY: When the server is restarted, Invisible LAN automatically re-establishes any drive and printer mappings that are in effect at the workstation.

The Network Clock

The **NETCLOCK** command is used to set your computer's clock. **NETCLOCK** contacts the specified server and obtains the current date and time. Then **NETCLOCK** sets your computer's clock and displays the date and time on the screen.

To set your computer's clock, type

```
NETCLOCK \\server\ [/W]
```

The parameters have the following meanings:

<i>server</i>	The network name of the server.
<i>/W</i>	Indicates that NETCLOCK should wait for the server computer to boot up if it is not on the network. <i>/W</i> is optional. If it is not included and the server computer is not on the network, then NETCLOCK terminates with an error message.

If your computer does not have a real-time clock, you may want to put a **NETCLOCK** command into your AUTOEXEC.BAT file. Then your computer clock is automatically set when you turn on your computer. (To make this work, you also have to put the **NET30** command into your AUTOEXEC.BAT file).

You can use **NETCLOCK** to synchronize the clocks in all your computers. The benefit of synchronizing the clocks is to provide consistent date and time information in all your disk directories.

Example—To get the date and time from a server named ALICE, type

```
NETCLOCK \\ALICE\
```

SUMMARY: **NETCLOCK** obtains the date and time from a server, and sets your computer's clock.

Using Network Printers

Invisible LAN has several commands for controlling network printers. Chapter 2 described the use of the **MAP** command to gain access to a server's printer. This chapter describes four commands for controlling a network printer: **NETPRINT**, **TRUNCATE**, **PRINTNOW**, and **PSETUP**. It also presents the *Print Screen Key* and the *Print Stream Truncation Key*.

The topics covered in this chapter are:

- Printing a file
- Printing the screen
- Truncating the print stream
- Sending printer set-up strings

Printing a File

You use the **NETPRINT** command to print a file. When Invisible LAN is running, you cannot use the DOS **PRINT** command. (If you try to use it, Invisible LAN prompts you to use **NETPRINT** instead.)

NETPRINT can be used with both network printers and local printers. When used with a network printer, **NETPRINT** sends the file to the server. Printing does not begin until **NETPRINT** has finished sending the file to the server. You can use your computer for other tasks while the actual printing occurs.

When used with a local printer, **NETPRINT** sends the file directly to the printer. **NETPRINT** does not terminate until the entire file has been printed. You cannot use your computer for other tasks while the file is being printed.

To print a file, type

```
NETPRINT filename [ LPTx ] [ /T ]
```

The parameters have the following meanings:

<i>filename</i>	The name of the file to be printed. The filename can include a drive letter and a directory path.
LPTx	The printer to be used: LPT1, LPT2, or LPT3. LPTx is optional. If omitted, the file is printed on LPT1. The specified printer can be either a network printer or a local printer.
/T	Indicates that the printer does not have built-in tab stops. /T is optional. If the printer has built-in tab stops, you should omit /T . (Most printers have built-in tab stops.) If you include /T , then tabs are converted into an equivalent number of spaces.

Example 1—LPT1 refers to a server's printer. To print the file called MY-FILE.TXT, type

```
NETPRINT MYFILE.TXT
```

Example 2—LPT2 refers to a server's printer. To print a file named BOOKS.DOC, type

```
NETPRINT BOOKS.DOC LPT2
```

Example 3—LPT3 refers to a server's printer which does not have built-in tab stops. To print a file named LEDGER in directory C:\ACCTS, type

```
NETPRINT C:\ACCTS\LEDGER LPT3 /T
```

SUMMARY: Use **NETPRINT** to print a file. With Invisible LAN, you cannot use the DOS **PRINT** command.

Printing the Screen

You can print a copy of the monitor screen when running Invisible LAN just as in standard DOS. The screen information is printed to LPT1. If you have assigned LPT1 to refer to a network printer, the screen information is printed on the network printer.

To print the screen, press the *Print Screen Key*. Follow the instructions below that match your computer keyboard:

- If your keyboard has twelve function keys (**F1** through **F12**), press **Print Screen**.
- If your keyboard has ten function keys (**F1** through **F10**), press **Shift-PrtSc**.

SUMMARY: Use the *Print Screen Key* to print a copy of the screen on printer LPT1. This works whether LPT1 is a local or a network printer.

Truncating the Print Stream

When you send a file to a network printer, it is not sent directly to the printer. Instead, the print spooler temporarily saves the file on the server's disk. Printing does not begin until the entire file has been transferred to the server. The print spooler waits until it receives an *end-of-file message* before starting the printing.

Some applications do not send an end-of-file message. If you try to print a file from such an application, Invisible LAN waits for more information and never prints the file. The file remains in the print spooler. If this happens, you must truncate the print stream. *Truncating the print stream* means telling the print spooler that it has received a complete file and should begin the printing.

There are two methods for truncating the print stream: manual and automatic.

Manual Truncation

To truncate the print stream manually, press

Ctrl-Alt-*

You must use the * key on the numeric keypad. On many computers, the * key on the numeric keypad is also labeled **PrtSc**.

When you press **Ctrl-Alt-***, Invisible LAN informs the server's print spooler that it has received a complete file. Any data that is in the print spooler is immediately printed.

Example—You tell your word processor to print your document on network printer 1. The word processor tells you “Printing In Progress”, and then a few seconds later tells you “Printing Complete”. However, nothing comes out on the server's printer, because the print spooler doesn't know that the word processor has finished printing. In this case, press

Ctrl-Alt-*

Printing begins immediately.

Automatic Truncation

When automatic print stream truncation is enabled, Invisible LAN automatically truncates the print stream whenever there is no printer activity for the period of time specified.

To set Invisible LAN to truncate the print stream automatically, you use the **TRUNCATE** command. The command can be used to enable or disable automatic print stream truncation, or to display the current print stream truncation setting.

Option 1: To enable automatic print stream truncation, type

TRUNCATE *time*

where *time* is a number of seconds from 1 to 255.

Option 2: To disable automatic print stream truncation, type

TRUNCATE /D

Option 3: To display the current truncation setting, type

TRUNCATE

Note—Using the Invisible LAN Setup program (**SETUP30**), you can specify an automatic print stream truncation setting to be established every time you start Invisible LAN. Refer to the *Installation* manual for details.

Note—You can also use the Network Manager (**MENU**) program to control automatic print stream truncation. Refer to chapter 13 for details.

Example—To automatically truncate the print stream whenever there is no printer activity for 10 seconds, type

TRUNCATE 10

Now you start your word processor, and use it to print a document. The word processor tells you “Printing In Progress”, and then tells you “Printing Complete”. Ten seconds later, printing begins.

Note—When printing a multi-page document, some word processors pause for several seconds at the end of each page. Make sure that the time specified for automatic truncation is larger than the time the word processor pauses. Otherwise, Invisible LAN might truncate the print stream between two pages of the same document.

Immediate Truncation

With the **TRUNCATE** command, you can establish a printer timeout that truncates the network print streams whenever there is no printer activity for a specified amount of time.

Invisible LAN includes a program called **PRINTNOW** that immediately truncates the network print streams.

To immediately truncate the network print streams, give the command

PRINTNOW

You should never need to type **PRINTNOW** at the DOS command line, since the network print streams are automatically truncated whenever the system is at the DOS prompt. The two main uses for **PRINTNOW** are in batch files and in secondary command processors.

Using PRINTNOW in a Batch File

You can put **PRINTNOW** in a batch file, to truncate the print stream in between two other programs.

For example, suppose that PROG1 and PROG2 are two programs that produce printer output. Suppose you make the following batch file:

```
PROG1  
PROG2
```

Depending on how PROG1 and PROG2 are written, Invisible LAN may combine their output into a single print job. However, suppose you change the batch file to read:

```
PROG1  
PRINTNOW  
PROG2
```

The **PRINTNOW** program truncates the network print streams after PROG1 is executed, thereby making the output from PROG1 and PROG2 go into separate print jobs.

PRINTNOW in a Secondary Command Processor

Some programming languages (databases in particular) have the ability to invoke a secondary command processor. This process is often called “shelling out.” In such a programming language, you can truncate the print streams by invoking a secondary command processor, and making it execute the **PRINTNOW** program.

Technical Note — In a general-purpose programming language like C, BASIC, or Pascal, you shouldn’t “shell out” to truncate the print streams. Instead, you should open and close the network printer device (LPT1, LPT2, or LPT3). When you close a network printer device, the corresponding print stream is immediately truncated.

SUMMARY: With some applications, you must *truncate the print stream* to start the printing. You can manually truncate the print stream by pressing **Ctrl-Alt-***. You can tell Invisible LAN to automatically truncate the print stream by using the **TRUNCATE** command. You can also use the **PRINTNOW** command to immediately truncate the print stream.

Sending Printer Set-up Strings

The features described in this section are for advanced users. If you are a beginning user, you may want to skip this section.

A *printer set-up string* is a sequence of printer control codes used to select printer options such as line spacing or number of characters per line. Whenever you print a file, Invisible LAN automatically sends the control codes to the printer.

Since each user on the network can specify a set-up string, each user can select different printer options. For example, one user could select 8 lines per inch, while another user could choose 6 lines per inch.

Printer set-up strings are specified with the **PSETUP** command. The command can be used to specify a string, to stop using a string, or to display the current string.

Option 1: To specify a set-up string for a network printer, type

PSETUP LPTx=hex_string

The parameters have the following meaning:

LPTx The name of a network printer: LPT1, LPT2, or LPT3.

hex_string A sequence of printer control codes, expressed in hexadecimal. It can have up to 64 characters of printer control codes. Whenever you print a file on the specified network printer, the specified printer control codes are sent to the printer.

Option 2: To stop using a set-up string, type

PSETUP LPTx=

where **LPTx** is the name of a network printer: LPT1, LPT2, or LPT3.

Option 3: To display the current set-up string, type

PSETUP LPTx

where **LPTx** is the name of a network printer: LPT1, LPT2, or LPT3.

If you are using more than one network printer, each network printer can have a different set-up string.

Examples—Printer control codes vary from printer to printer. Consult your printer's instruction manual for a list of the control codes that you can use. However, the following examples work on many printers.

To select 132 characters per line, type

PSETUP LPT1=0F

To select 80 characters per line, type

PSETUP LPT1=12

To select 8 lines per inch, type

PSETUP LPT1=1B30

To select 6 lines per inch, type

PSETUP LPT1=1B32

To select skip-over-perforation (printer prints 54 lines then skips 12), type

PSETUP LPT1=1B4E0C

In most cases, you can select more than one option simply by concatenating the set-up strings. For example, to select 132 characters per line and 8 lines per inch, type

PSETUP LPT1=0F1B30

Note—Printer set-up strings should not be used with PostScript printers.

SUMMARY: A *printer set-up string* is a sequence of printer control codes sent to the printer whenever you print a file. The **PSETUP** command is used to specify printer set-up strings.

Controlling the Print Spooler

When another computer sends a file to your printer, the *print spooler* temporarily stores the file on your disk until it can be printed. The temporary files waiting to be printed are in the *print queue*. Once the files are printed, the print spooler automatically deletes the files from your disk.

This chapter describes how to control the print spooler using the **PQ** and **MAKEBP** commands. You can also control the print spooler with the Network Manager (**MENU** program); refer to chapter 14 for instructions on using the network manager.

The topics covered in this chapter include:

- Displaying the print spooler status
- Setting the print spooler state
- Modifying the print queue
- Controlling form feeds
- Flow control for serial printers
- Direct printing
- Print priority
- Creating a break page

Displaying the Print Spooler Status

To display the current status of the print spooler, type

PQ STATUS

The following items of information are displayed:

- **Print spooler state** — Active or Paused. When active, the print spooler can send data to the printer. When paused, the print spooler cannot send data to the printer.
- **Print priority** — Low, Medium, or High. The print priority determines the amount of time that the server spends sending data to the printer.
- **Direct print setting** — Enabled or Disabled. When direct printing is disabled, the print spooler does not send a job to the printer until the entire job has been received from the workstation. When direct printing is enabled, the print spooler can send a job to the printer while it is being received from the workstation.
- **Number of files in the print queue** — This is the number of temporary files on your disk that are waiting to be printed.
- **Printer(s) used by the print spooler** — LPT1, LPT2, LPT3, COM1, or COM2. For a serial printer (COM1 or COM2), the **method of flow control** is also displayed.
- **Form-feed setting** — Yes or No. If yes, a form feed command is added at the end of each printing job. A *form-feed command* tells the printer to advance the paper, so that the next print job begins at the top of a page.

■ **SUMMARY: PQ STATUS** displays the current status of the print queue.

Setting the Print Spooler State

The print spooler has two possible states: *active* and *paused*.

When the print spooler is *active*, it can send data to the printer. Temporary files stored on your disk are sent to the printer one-by-one.

When the print spooler is *paused*, it cannot send data to the printer. Temporary files stored on your disk stay there until the print spooler goes back to the active state. Other computers can still send files to the print spooler; these files are stored on your disk, where they wait for the print spooler to become active.

Note—If your computer is turned off or rebooted with files still in the print queue, the server will automatically delete them the next time it starts up.

Pausing the Print Spooler

To set the print spooler to the paused state, type

PQ PAUSE

The print spooler immediately stops sending data to the printer. (The printer may continue printing for several seconds, because some data may be stored inside the printer.)

For example, if the paper jams during a printing job, you usually have to pause the print spooler to clear up the jam.

Continuing the Print Spooler

To change the print spooler to the active state, type

PQ CONTINUE

The print spooler resumes sending data to the printer. The data resumes at exactly the point where it was stopped by **PQ PAUSE** (unless you have modified the print queue).

For example, if you paused the print spooler to clear up a paper jam, you would continue the printing job by changing the print spooler status to active.

SUMMARY: **PQ PAUSE** causes the print spooler to stop sending data to the printer. **PQ CONTINUE** causes the print spooler to resume sending data to the printer.

Modifying the Print Queue

When there are several files waiting to be printed, they are stored in the *print queue*. Newly arriving print jobs go to the end of the line. The print job at the head of the line is the one currently being printed.

This section describes the **RESTART**, **CANCEL**, and **CLEAR** options of the **PQ** command. These are used to restart a job, to cancel a job currently printing, and to clear the print queue. All three can be used when the print spooler is active or paused.

Note—The Network Manager (**MENU**) has much more extensive abilities to modify the print queue. For example, you can display a list of the files in the queue, rearrange the files, and delete specific files. Refer to chapter 14 for details.

Restarting the Current Print Job

To restart the current print job from the beginning, type

PQ RESTART

The file currently being printed starts again from the beginning.

If you use **PQ RESTART** when the print spooler is paused, printing will not begin until you give the **PQ CONTINUE** command. When you give **PQ CONTINUE**, printing will begin at the start of the current file.

For example, you can restart the current print job from the beginning if the printout is ruined by a printer malfunction.

Canceling the Current Print Job

To cancel the job currently being printed, type

PQ CANCEL

The file is immediately deleted from the print queue. Printing continues with the next file in the print queue.

If you use **PQ CANCEL** when the print spooler is paused, printing will not begin until you give the **PQ CONTINUE** command. When you give **PQ CONTINUE**, printing will begin at the start of the next file.

Clearing the Print Queue

To cancel all the jobs in the print queue, type

PQ CLEAR

All the files waiting to be printed (including the file currently being printed) are immediately deleted from the print queue. Printing does not continue until the print spooler receives a new print job.

PQ CLEAR does not affect files that are still in the process of being received. It only affects files that have been completely received and are ready to be printed.

SUMMARY: **PQ RESTART** restarts the current print job from the beginning. **PQ CANCEL** cancels the current print job. **PQ CLEAR** cancels all the print jobs.

Controlling Form-feeds

The print spooler prints a series of jobs, one after the other. The print spooler usually sends a *form-feed command* to the printer at the end of each job. The form-feed command tells the printer to advance the paper, so that the next print job will begin at the top of a page.

Two situations in which you may not want the print spooler to send form-feed commands to the printer are when:

- Using a PostScript-compatible printer (e.g., Apple LaserWriter).
- Printing from within a word processor or other application program that already adds a form-feed command at the end of each document.

The **FEED** and **NOFEED** options to the **PQ** command specify whether the print spooler adds a form-feed command at the end of each print job. These options are described in the following sections. **FEED** and **NOFEED** can be used whether the print spooler is paused or active.

Note — With the Invisible LAN Setup program (**SETUP30**), you can specify the initial form-feed setting that is in effect when you start Invisible LAN. Refer to the *Installation* manual for details.

Turning Off Form-Feeds

To set the print spooler not to add a form-feed at the end of each print job, type

PQ NOFEED n

where n is the number of the printer: 1 or 2. If n is omitted, the command refers to printer 1.

Turning On Form-Feeds

To set the print spooler to add a form-feed at the end of each print job, type

PQ FEED n

where n is the number of the printer: 1 or 2. If n is omitted, the command refers to printer 1.

Example—To set the print spooler to add a form-feed command at the end of print jobs for printer 1 but not for printer 2, type

PQ FEED1

PQ NOFEED2

SUMMARY: **PQ NOFEED** turns off the print spooler's form-feed commands. **PQ FEED** turns on the print spooler's form-feed commands.

Flow Control for Serial Printers

There are two different ways to control the flow of data from the computer to a serial printer: *DTR flow control* and *Xon/Xoff flow control*. (DTR stands for *Data Terminal Ready*. Xon/Xoff stands for *Transmit On/Transmit Off*.)

It is outside the scope of this manual to explain the technical differences between DTR and Xon/Xoff flow control. You do need to know which method is used in your printer. Most printers use DTR.

The **XON** and **DTR** options to the **PQ** command specify the method of flow control to be used for each printer. These options are described in the following sections. **XON** and **DTR** can be used when the print spooler is paused or active.

Note — With the Invisible LAN Setup program (**SETUP30**), you can specify the initial flow control setting that is in effect when you start Invisible LAN. Refer to the *Installation* manual for details.

Selecting Xon/Xoff

To set the print spooler to use Xon/Xoff flow control when sending data to the printer, type

PQ XON n

where n is the number of the printer: 1 or 2. If n is omitted, the command refers to printer 1.

When using Xon/Xoff flow control, there are some situations in which the computer may stop sending data to the printer and not start up again. For example, this may happen if you turn off the printer to clear a paper jam. If the computer stops sending data to the printer, repeat the **PQ XON** command to restart the flow of data.

Selecting DTR

To set the print spooler to use DTR flow control when sending data to the printer, type

PQ DTR n

where n is the number of the printer: 1 or 2. If n is omitted, the command refers to printer 1.

Example—To set the print spooler to use Xon/Xoff for printer 1 and DTR for printer 2, type

PQ XON1
PQ DTR2

SUMMARY: There are two ways to control the flow of data from the computer to a serial printer. **PQ XON** tells the print spooler to use *Xon/Xoff flow control*. **PQ DTR** tells the print spooler to use *DTR flow control*.

Direct Printing

To enable direct printing, type

PQ DIRECT

To disable direct printing, type

PQ NODIRECT

In normal operation, the print spooler stores each print job in a file on the server's disk. When a complete print job has been received, the job is then sent to the printer.

Direct printing is a process that allows the print spooler to send a job to the printer at the same time that it is being received from the workstation. Thus, the print spooler does not wait for the complete print job to be received before beginning the actual printing.

You can use **PQ** to turn direct printing on and off while the server is running. You can also use **SETUP30** to specify the initial state of direct printing; refer to the *Installation* manual for details.

SUMMARY: You use the **DIRECT** and **NODIRECT** options of the **PQ** command to enable or disable *direct printing*, which allows the spooler to send a job to the printer at the same time it is being received from the workstation.

Print Priority

To set printing priority to **LOW**, type

PQ LOW

To set printing priority to **MEDIUM**, type

PQ MEDIUM

To set printing priority to **HIGH**, type

PQ HIGH

The *print priority* determines the amount of time that the server devotes to processing network print jobs. A high print priority gives more time to printing, and less time to the user working locally at the server. A low print priority gives less time to printing, and more time to the user working locally at the server.

You can use **PQ** to change the print priority while the server is running. You can also use **SETUP30** to specify the initial print priority; refer to the *Installation* manual for details.

SUMMARY: You use the **LOW**, **MEDIUM**, and **HIGH** options of the **PQ** command to control the printing priority.

Creating a Break Page

Invisible LAN can print a break page at the beginning of each print job. The *break page* is a page that contains the user's name, job title, date and time, and a graphic design. The function of the break page is to separate the print jobs.

The design of the break page is stored on disk. BP_ASCII.DAT is the break page design for ASCII printers, BP_PSCPT.DAT is the design for PostScript printers, and BP_PCL.DAT is the design for PCL printers.

If you wish, you can design your own break page by replacing the BP_ASCII.DAT, BP_PSCPT.DAT, and BP_PCL.DAT files. The **MAKEBP** program lets you make your own break page.

The first step in designing a break page is to create a text file that describes the break page. The text file contains the actual data that is sent to the printer when printing the break page, including any special control codes required by the printer. In addition, the text file contains *escape codes* that specify where to insert the user name, job title, date, and time. When the break page is printed, the print spooler automatically replaces the escape codes with the appropriate values for the print job.

Each escape code begins with a tilde character (~). The following escape codes can be used in the text file:

~d	the day of the month (always 2 digits).
~h	the hour (always 2 digits).
~j	the print job title (always 31 characters). If the actual job title is less than 31 characters, it is extended to 31 characters by appending blanks.
~m	the minute (always 2 digits).
~n	the line feed character (hexadecimal 0A, same as ~x0a).
~o	the month (always 2 digits).
~r	the carriage return character (hexadecimal 0D, same as ~x0d).
~s	the second (always 2 digits).
~t	the tab character (hexadecimal 09, same as ~x09).
~u	the user name (always 15 characters). If the actual user name is less than 15 characters, it is extended to 15 characters by appending blanks.
~xnn	the hexadecimal character 'nn'.
~y	the year (always 2 digits).
~~	a single tilde character.

After creating the text file, you use **MAKEBP** to convert it into the data file required by the print spooler. The command is:

To create a break page data file, type

MAKEBP *infile outfile*

where the parameters have the following meaning:

infile	The name of a text file that you created, which contains the break page description.
outfile	The name of the data file that MAKEBP creates. This should be BP_ASCII.DAT if you are creating a break page for an ASCII printer, or BP_PSCPT.DAT if you are creating a break page for a PostScript printer, or BP_PCL.DAT if you are creating a break page for a PCL printer.

When **MAKEBP** processes your text file, it automatically discards all character codes less than 32 (decimal), including carriage return, line feed, and tab. The only way to send character codes less than 32 to the printer is to use the escape codes.

As examples, we have included the text files that were used to create the default break page. The files are called BP_ASCII.TXT and BP_PSCPT.TXT and BP_PCL.TXT. You may use these files as examples, and as starting points for defining your own break page.

Technical note — When designing a PostScript break page, you must use the **readstring** operator to read the user name and job title into the PostScript program. This is because the user name and job title may contain characters that the PostScript interpreter would normally treat as control codes rather than text. The **readstring** operator lets you bypass the interpreter and read in the text directly. Refer to BP_PSCPT.TXT for an example of how this can be done.

SUMMARY: The **MAKEBP** command lets you change the design of the *break page* which is printed by the print spooler at the beginning of each print job. To use **MAKEBP**, you first create a text file that contains a description of the break page, and then run the **MAKEBP** program to convert the description into the data file format required by the print spooler.

Network Software Control

You can display and control certain parameters of the network software using the **DEDICATE**, **CACHE**, **NW**, and **US** commands. This chapter covers the following topics related to the use of these commands:

- Dedicated servers
- Controlling the disk cache
- Displaying network software status
- Controlling the server
- Hiding the network software
- Controlling the use of the speaker
- Setting up for tape backup
- Controlling Ultra Server
- Ultra Server in Non-Dedicated Mode

Dedicated Servers

To place the file server into dedicated mode, type

DEDICATE

A *dedicated server* is a computer that is devoted exclusively to the task of being a file server. In other words, a dedicated server is a file server that has no local user.

You use the **DEDICATE** command to establish a dedicated server. Simply start Invisible LAN normally, and then run **DEDICATE**.

DEDICATE does two things. First, it allows the server to run faster. And second, if you are using the Invisible LAN disk cache with the cache data in extended memory, then **DEDICATE** also allows the disk cache to run faster. After starting **DEDICATE**, you can press any key to exit from dedicated server mode and return to the normal non-dedicated server mode.

SUMMARY: Use the **DEDICATE** command to set up a dedicated server.

Controlling The Disk Cache

If you have installed the Invisible LAN disk cache, you can use the **CACHE** command to control the cache and display cache status. For instructions on how to install the disk cache, refer to the *Getting Started* manual or the *Installation* manual.

To control the cache, you type the command **CACHE**, using the parameters described below.

To control the cache, type

CACHE [*parameters*]

where the *parameters* determine what action to take. The *parameters* may include one or more of the following:

- | | |
|-----------|--|
| /F | Flush Cache. This command waits until all background write operations are finished, and then completely erases the contents of the cache. |
| /N | Disable Cache and Flush Cache. This command first flushes the cache (in exactly the same way as /F), and then disables the cache. After this command, all disk operations go directly to the hard disk, with no cache. |
| /V | Display Cache Status. This displays the following: (1) Cache enable/disable state; (2) Cache size; (3) Write policy; (4) Hard disk parameters; (5) Cache performance statistics. |

<i>/W=policy</i>	Change Write Policy. <i>/W=0</i> changes the write policy to write-through. <i>/W=1</i> changes the write policy to write-back. <i>/W=2</i> changes the write policy to delayed-write.
<i>/Y</i>	Enable Cache. This command reverses the effect of <i>/N</i> , and allows the cache to operate.
<i>/Z</i>	Reset Statistics To Zero. The cache statistics displayed by <i>/V</i> are reset to zero. This does not affect the operation of the cache in any way. This command is useful mainly for running tests of cache performance.

Example 1 — Enabling, Disabling, Flushing

To turn off the cache, type

```
CACHE /N
```

To turn the cache back on, type

```
CACHE /Y
```

The ***/F*** parameter provides a convenient way to ensure that all data in the cache has been physically written to the disk. If you use the delayed-write option, you should get into the habit of always flushing the cache before turning off or rebooting your computer. To flush the cache, use

```
CACHE /F
```

Example 2 — Changing The Write Policy

The disk cache supports three different *write policies*: write-through, write-back, and delayed-write. The write policy affects what the disk cache does

when DOS writes data to the disk. If you select *write-through*, DOS has to wait until the data is physically written onto the disk. If you select *write-back*, the data is stored in the cache; the actual write is started as soon as possible, but completes at a later time, in background. If you select *delayed-write*, the data is stored in the cache; the actual write does not begin until several seconds later, and is performed entirely in background.

Using the Invisible LAN Setup program (**SETUP30**), you can specify which write policy is selected when you start Invisible LAN. Refer to the *Installation* manual for details. The *Installation* manual also has further information about write policies.

To change the write policy to write-through, use

```
CACHE /W=0
```

To change the write policy to write-back, use

```
CACHE /W=1
```

To change the write policy to delayed-write, use

```
CACHE /W=2
```

Note that you can use more than one parameter in a single command. For example, to enable the cache and also change the write policy to write-back, you could type

```
CACHE /Y /W=1
```

Example 3 — Cache Statistics

To display statistics on the performance of the cache, type

```
CACHE /V
```

The information displayed is similar to the following:

CACHE STATUS

Cache is enabled.

Cache size is 3060K.

Write policy is Write-Back.

DISK PARAMETERS

Drive 0 has 939 cylinders, 8 heads, and 17 sectors.

CACHE PERFORMANCE

Cache hits: Read=2983, Write=2408.

Cache misses: Read=101, Write=614.

Cache hit ratio: Read=96%, Write=79%.

The display is divided into three sections. The first section shows the status of the cache program. It displays:

- Whether the cache is enabled or disabled.
- The actual size of the cache, in kilobytes. (If you used the Setup program to specify the size of the cache, this number may be slightly different than the size you specified.)
- The current write policy: Write-Through, Write-Back, or Delayed-Write.

The second section shows the characteristics of the hard disks. There is one line for each hard disk; the first hard disk is Drive 0, the second hard disk is Drive 1, and so on. For each hard disk, the program shows:

- The total number of cylinders.
- The number of heads in each cylinder.
- The number of sectors in each track.

The third section shows the cache performance. The following data is displayed:

- Read Hits — The number of disk read operations that were satisfied by reading from the cache, instead of reading the hard disk.
- Read Misses — The number of disk read operations that required a read of the hard disk, because the requested data was not in the cache.
- Read Hit Ratio — The percentage of disk reads that were satisfied by reading from the cache, instead of reading the hard disk. The higher the number, the better the performance of the cache.
- Write Hits — The number of disk write operations that overwrote data which was already in the cache.

- **Write Misses** — The number of disk write operations that did not overwrite data already in the cache.
- **Write Hit Ratio** — The percentage of disk writes that overwrote data which was already in the cache. The higher the number, the better the performance of the cache.

At any time, the performance counters can be reset to zero using the `/Z` parameter, as shown:

```
CACHE /Z
```

SUMMARY: The **CACHE** program lets you enable or disable the disk cache, flush the cache, change the write policy, and display cache statistics.

Displaying Network Software Status

To display the status of the network software, type

```
NW STATUS
```

The following information is displayed:

- **Software modules installed**—Server, Redirector, or both.
- **Server state**—active or paused. When the server is *active*, other computers can use your disks and printers. When the server is *paused*, other computers cannot use your disks and printers.
- **Network software visibility**—hidden or visible. The network software is usually *visible*, so that applications designed for network use can tell that they are running on a network. When the software is *hidden*, applications cannot tell that they are running on a network.
- **Access to speaker**—Whether Invisible LAN is allowed to use the computer's speaker.
- **Invisible LAN software version number.**

SUMMARY: Use the **NW STATUS** command to display the status of the network software.

Controlling the Server

You can use the **NW** command to *pause* or *activate* the server. When the server is *paused*, it does not respond to workstations that want to use its disks or printers. A workstation that tries to access the server hangs up until you *activate* the server again.

Most programs use DOS to access the disk. However, a few programs bypass DOS and access the disk directly. To run such a program, you must pause the server. An example is a tape backup program that does an image backup. Another example is the DOS **CHKDSK** command.

Caution—If you have any drive letters or print devices mapped to yourself, make sure you don't use them while the server is paused. If you do, your computer will hang up, and you will have to re-boot.

To pause the server, type

NW PAUSE

To activate the server, type

NW CONTINUE

SUMMARY: Use the **NW PAUSE** and **NW CONTINUE** commands to pause and continue the server.

Hiding the Network Software

When the network software is *hidden*, application programs cannot tell that they are operating on a network. An application cannot tell the difference between a network drive and a local drive.

When the network software is *visible*, a “network-aware” application program can detect that it is operating on a network. It can tell which drive letters are network drives and which are local drives.

Some application programs are intentionally designed so that they won't run on a network. For example, tape backup programs which perform file-by-file backup are sometimes designed this way. If you want to use such a program, you must hide the network software.

To hide the network software, type

NW HIDE

To make the network software visible, type

NW UNHIDE

SUMMARY: Use the **NW HIDE** and **NW UNHIDE** commands to control the visibility of the network software to other applications.

Controlling Use of the Speaker

The redirector beeps the speaker when the server is slow in responding to a network request. The mail system beeps the speaker when it receives a message. With these commands, you can control whether this happens.

To prevent the redirector and mail system from using the computer's speaker, type

NW NOAUDIO

To allow the redirector and mail system to use the computer's speaker, type

NW AUDIO

SUMMARY: Use the **NW NOAUDIO** and **NW AUDIO** commands to control the use of the computer's speaker.

Tape Backup

The most common use of the **NW** command is to allow the use of tape backup programs on the network.

There are two kinds of tape backup: *image backup* and *file-by-file* backup.

Image Backup

Image backup makes an exact copy of the disk sector by sector. Image backup does not use DOS to read files; it simply reads disk sectors.

If you have a tape drive installed in your computer, you can make an image backup of your own disk. You cannot make image backups of other disks across the network. If your system is a server, you must make sure that no one uses your disk while you are making an image backup.

To do this, pause the server before starting the image backup by typing

NW PAUSE

File-by-File Backup

File-by-file backup systems copy individual files onto the tape. The software uses DOS to read the individual files.

If you have a tape drive in your computer, you can make file-by-file backups of your own disk, as well as other disks across the network. Since network disks appear as additional drive letters, you can simply direct the tape software to back up files from a network disk. However, some backup software refuses to back up files from a network disk. If this happens, you can get around it by hiding the network software. When the network software is hidden, the backup software cannot tell that it is working on a network disk. To hide the network software, type

NW HIDE

SUMMARY: Some tape backup software does not function properly on a network system. You can sometimes get the tape backup software to work by hiding the network software using the **NW HIDE** command.

Controlling Ultra Server

Ultra Server is the high-performance version of the Invisible LAN file server. It is intended mainly for dedicated servers. Ultra Server requires a 386 or 486 computer. It uses 32-bit code, multitasking, and extensive caching to operate at very high speed.

If you have installed Ultra Server, you can use the **US** command to control Ultra Server and display status information. For instructions on how to install the Ultra Server, refer to the *Getting Started* manual or the *Installation* manual.

Displaying Ultra Server Status

To display the status of Ultra Server, type

US STATUS

The information displayed is similar to the following:

CACHED DRIVES

Drive C: Type=Fixed Disk, Status=Mounted.

Drive E: Type=CD-ROM, Status=Mounted.

CACHE USAGE

Open Files: Current=7, Maximum=52, Limit=500.

Record Locks: Current=15, Maximum=24, Limit=1000.

Kilobytes I/O: Read=21012K, Write=13163K.

Cache Memory: Data=4884K, Directory=163K,
File/Lock=39K.

CACHE PERFORMANCE

Read: Hit=10896, Miss=312, Hit Ratio=97%.

Write: Hit=5904, Miss=1398, Hit Ratio=88%.

Directory: Hit=1157, Miss=125, Hit Ratio=90%.

Channel: Hit=2448, Miss=738, Hit Ratio=76%.

The display is divided into three sections. The first section lists all the cached drives. (By default, Ultra Server caches each installed drive from C: to Z:.) For each drive, the program displays:

- The type of drive: fixed disk or CD-ROM. A fixed disk is a read/write drive, whereas a CD-ROM is a read-only drive.
- The drive status: mounted or unmounted. A mounted drive can be accessed normally. An unmounted drive cannot be accessed.

The second section shows usage of Ultra Server resources. The following information is shown:

- The number of files currently open, the maximum number of files that have been open at one time since Ultra Server was started, and the limit on open files as defined in the NET30.INI file.
- The number of record locks currently established, the maximum number of record locks that have been established at one time since Ultra Server was started, and the limit on record locks as defined in the NET30.INI file.
- The total amount of data read and written by users since Ultra Server was started, in kilobytes.
- The amount of extended and hyper-extended memory available for caching, in kilobytes. The cache memory is broken down into three categories: (1) file data; (2) directory entries; and (3) file handles and record locks.

The third section shows the cache performance. The following is displayed:

- Read Hits — The number of file read operations that were satisfied by reading from the cache, instead of reading the hard disk.
- Read Misses — The number of file read operations that required a read of the hard disk, because the requested data was not in the cache.
- Read Hit Ratio — The percentage of file reads that were satisfied by reading from the cache, instead of reading the hard disk. The higher the number, the better the performance of the cache.
- Write Hits — The number of file write operations that overwrote data which was already in the cache.
- Write Misses — The number of file write operations that did not overwrite data already in the cache.
- Write Hit Ratio — The percentage of file writes that overwrote data which was already in the cache. The higher the number, the better the performance of the cache.
- Directory Hits — The number of file open operations where the required directory entry was already in the cache.
- Directory Misses — The number of file open operations where the required directory entry was not in the cache.
- Directory Hit Ratio — The percentage of file opens where the required directory entry was already in the cache. The higher the number, the better the performance of the cache.
- Channel Hits — The number DOS read/write operations where Ultra Server already had a DOS handle open for the file.
- Channel Misses — The number of DOS read/write operations where Ultra Server had to open a DOS file handle, because it did not already have an open handle for the file.
- Channel Hit Ratio — The percentage of DOS read/write operations where Ultra Server already had a DOS handle open for the file. The higher the number, the better the performance of the cache.

Unmounting Drives

Each cached drive can be either mounted or unmounted. When the drive is *mounted*, users can access it normally. When the drive is *unmounted*, it cannot be accessed. When you start Ultra Server, it automatically mounts all cached drives.

For drives with removeable media (like CD-ROMs), you must unmount the drive before removing the disk, and then mount the drive again after inserting a new disk. This allows the contents of the cache to be updated properly.

To unmount one or more drives, type

```
US UNMOUNT [ d: ] ...
```

or

```
US DOWN [ d: ] ...
```

The symbol “[d:]...” indicates an optional list of drive letters. If you don’t include a list of drive letters, then the command affects all cached drives.

The difference between **UNMOUNT** and **DOWN** lies in what happens if there are open files on the drive(s). If there are open files, the **US UNMOUNT** command terminates with an error message and does not unmount the drive(s). The **US DOWN** command closes any open files and then unmounts the drive(s).

Note — After unmounting a drive, it is still possible to list the drive’s directory. However, it is not possible to open any files or modify the disk in any way. The software is intentionally designed this way to prevent unexpected DOS error messages.

Note — Ultra Server establishes a cache *blackout zone* in the network directory (usually C:\NET30). Files located in the network directory are never cached, even if the network directory is on a cached drive. Also, files located in subdirectories of the network directory are never cached. Files in the cache blackout zone are always accessible, even if you unmount the drive that contains the network directory.

Caution — Unmounting the drive that contains **COMMAND.COM** may cause DOS to lock up if **COMMAND.COM** becomes inaccessible. To prevent this from happening, put **COMMAND.COM** in an uncached area, either on an uncached drive or within the blackout zone. Be sure to update your **COMSPEC** environment variable to reflect the new location.

Example — To unmount both drive D: and drive E:, type

```
US UNMOUNT D: E:
```

Example — To close all files on both drive D: and drive E:, and then unmount the two drives, type

```
US DOWN D: E:
```

Example — To unmount all cached drives, type

```
US UNMOUNT
```

Example — To close all files on drive F:, and then unmount the drive, type

```
US DOWN F:
```

Mounting Drives

After unmounting a drive, you need to mount it if you want to use it again.

To mount one or more drives, type

```
US MOUNT [ d: ] . . .
```

The symbol “[*d:*]...” indicates an optional list of drive letters. If you don’t include a list of drive letters, then the command affects all cached drives.

Example — To mount both drive D: and drive E:, type

```
US MOUNT D: E:
```

Example — To mount all cached drives, type

```
US MOUNT
```

Example — To mount drive F:, type

US MOUNT F:

SUMMARY: The **US** program lets you display Ultra Server status information, unmount drives, and mount drives.

Ultra Server in Non-Dedicated Mode

Ultra Server is intended mainly for dedicated file server applications. However, you can run Ultra Server in non-dedicated mode if you wish.

To run Ultra Server in non-dedicated mode, you need to obey the following special rules:

- Direct access to cached drives is prohibited. Cached drives may be accessed only via drive mappings. Therefore, the server must establish drive mappings to itself if it requires access to the cached drives. The Invisible LAN redirector automatically establishes the necessary mappings.
- You cannot use the following DOS commands on the computer running Ultra Server: SUBST, JOIN, and ASSIGN.
- It is not possible to run Windows 386 enhanced mode on the computer running Ultra Server. It is possible to run Windows standard mode, provided that you enable Windows support in the Setup program, and you configure Ultra Server to leave some extended memory free for Windows to use.

SUMMARY: You can run Ultra Server in non-dedicated mode, provided you access cached drives only via drive mappings, don't use the SUBST, JOIN, or ASSIGN commands, and don't run Windows 386 enhanced mode.

Logon Commands

Security is an optional part of Invisible LAN. If you choose to have security, you use the Network Manager (**MENU** program) to set up the security system, as described in chapter 15. When security is active, Invisible LAN verifies security permissions every time someone establishes a drive or printer mapping, accesses the bulletin board, or manages the server.

Security permissions are based on user names and passwords. You use the logon commands to enter your user name and password. This chapter describes:

- Entering your password
- Logging on to the network

Entering Your Password

Entering a password is the only contact most users have with security.

Option 1: To enter your password, type

PASSWORD *password*

Replace *password* with your password. The person in charge of the server can tell you your password.

Option 2: If you want to be prompted to enter your password, type

PASSWORD **/P**

When you give this command, **PASSWORD** prompts you to type in your password. The password you type is not displayed on the screen, so anyone looking over your shoulder will not see your password. This form of the command is recommended if you put **PASSWORD** into a batch file, because you don't have to put your actual password in the batch file.

Example 1—Your password is SECRET. Type

```
PASSWORD SECRET
```

Example 2—You need to access two different servers. On server ROBERT, your password is ANGELFOOD. On server JANET, your password is MONITOR. You want to use drive letter F: to refer to shortname NETDISK on server ROBERT, and you want to use drive letter G: to refer to shortname ACCTS on server JANET. Type

```
PASSWORD ANGELFOOD  
MAP F: \\ROBERT\\NETDISK  
PASSWORD MONITOR  
MAP G: \\JANET\\ACCTS
```

If you put these commands into a batch file, you probably wouldn't want to put your actual passwords into the batch file, because anyone could discover your passwords just by reading the batch file. So you would use the **/P** option of the **PASSWORD** command, like this:

```
PASSWORD /P  
MAP F: \\ROBERT\\NETDISK  
PASSWORD /P  
MAP G: \\JANET\\ACCTS
```

When you run this batch file, it prompts you to enter your first password. You type ANGELFOOD, and press **Enter**. The batch file does the mapping for drive F:, and prompts you to enter your second password. You type MONITOR, and press **Enter**. The batch file then performs the mapping for drive G:.

Note— Using the Invisible LAN Setup program (**SETUP30**), you can specify a password to be in effect automatically when you start Invisible LAN. Refer to the *Installation* manual for details.

SUMMARY: Use the **PASSWORD** command to enter your password. The password is checked when you attempt to access a network resource.

Logging On to the Network

The Invisible LAN security system is based on user names. The user name is established when you start Invisible LAN. With the **MENU** program (de-

scribed in chapter 15), you specify which users are able to access which network resources.

This can be inconvenient if you move around the network, using several different machines. Security permissions are tied to your machine, and do not follow you as you move from machine to machine.

To overcome this problem, Invisible LAN includes two programs called **LOGON** and **LOGOFF**. With these programs, you can obtain access to your security permissions from any machine in the network.

Logging On

To establish access to your security permissions from any machine in the network, type

LOGON

The **LOGON** command prompts you to enter your user name and password. After running **LOGON**, you have the security permissions of the name and password that you entered. For example, every time you establish a drive or printer mapping, the security permissions are verified using the name and password entered with **LOGON**.

Note — **LOGON** only changes the name used for verifying security permissions. It does not change the name used for electronic mail, or for the polling function of the **MENU** program.

Logging Off

To reverse the effect of the **LOGON** command, type

LOGOFF

The **LOGOFF** command restores the machine's original user name. After running **LOGOFF**, you have the machine's original security permissions.

Note — **LOGOFF** does not restore the original password. You can use the **PASSWORD** command (after running **LOGOFF**) to restore the password.

Note — Drive and printer mappings established before running **LOGOFF** will remain in effect after running **LOGOFF**. Use the **MAP** command to discontinue any mappings you do not want to use with the original user name.

SUMMARY: The **LOGON** and **LOGOFF** commands are used to log on and off the network. **LOGON** lets you enter a new user name and password, while **LOGOFF** restores the original user name.

Diskless Workstation Commands

A *diskless workstation* is a computer without disk drives. Except for the lack of disk drives, a diskless workstation is just like any other computer — it has the same system unit, keyboard, and screen.

Because it lacks disk drives, a diskless workstation cannot be started (booted up) in the usual way. Usually, when you start a computer it loads the disk operating system (DOS) from the disk drive. A diskless workstation must load DOS from somewhere else. With Invisible LAN, it loads DOS from a server on the network called the *Remote Program Load Server*.

To use diskless workstations, one computer on the network must be set up as a Remote Program Load Server. Any Invisible LAN file server can serve this function. This chapter tells you how to set up and use a Remote Program Load Server. It also describes the use of the **NETADDR** command to establish different startup procedures for each diskless workstation on the network.

Creating a Boot Diskette

To set up a Remote Program Load Server, you must first create a *boot diskette*.

A *boot diskette* contains all the files needed to start a computer and access the network. At a minimum, it must contain the DOS system files and enough of the Invisible LAN program files so that you can start the network and map in to the server.

The procedure for creating a boot diskette is:

Step 1. Insert the blank diskette in drive A:.

Step 2. Format the diskette, and copy the DOS system files onto the diskette, by typing

FORMAT A:/S

Step 3. Copy all the Invisible LAN program files needed to start the network onto the diskette. The names of the required program files are listed in the text file called FLOPPY.TXT.

Step 4. Make an initialization file for each diskless workstation, and put it on drive A:. To do this, load the Invisible LAN Setup program (**SETUP30**). Use it to create an initialization file on drive A: for each diskless workstation. Make sure to give each initialization file a different filename, and specify a different user name for each diskless workstation.

Remember that since the workstations are diskless, you do not need to install a disk cache. Also, the only possible reason for installing the server is to share a printer; in this case, you need a RAM Disk on the diskless workstation to hold the print spool files.

Step 5. Create a CONFIG.SYS file for the diskless workstations, and put it on drive A:. You can use **SETUP30** to create the CONFIG.SYS file, or you can create the file yourself with a text editor. If you create the file yourself, remember to install the CACHE30.SYS and N30DEV.SYS device drivers. All the diskless workstations must share the same CONFIG.SYS file.

Step 6. If your diskless workstations need any additional files to start up (such as device drivers), copy the files onto drive A: now.

Step 7. If you wish, you may create an AUTOEXEC.BAT file for the diskless workstations. Create the file with a text editor, and put it on drive A:. If you have more than one diskless workstation, it is possible for each workstation to have a different AUTOEXEC procedure; refer to the description of the **NETADDR** command later in this chapter.

SUMMARY: A *boot diskette* contains all the files needed to start a workstation, including the DOS system files and the Invisible LAN program files.

Creating an Image File

Once you have created a boot diskette, the second step in setting up a Remote Program Load Server is to create an *image file* on the server's fixed disk. The image file contains an exact copy of the entire boot diskette. Diskless workstations use this image file when they start up.

To create a boot diskette image file, type

MAKEIMG *d:* *image_file*

The parameters have the following meanings:

d:	The drive where the boot diskette is located (A: or B:). Usually this is A:.
image_file	The name of the image file that MAKEIMG will create. You can optionally include a drive and path as part of the name.

Example—You want to create an image file named **BOOTDISK.IMG** and place the file in directory **C:\NET30**. Insert your boot diskette in drive A: and type

MAKEIMG A: C:\NET30\BOOTDISK.IMG

SUMMARY: **MAKEIMG** creates an *image file*. The image file contains an exact copy of the boot diskette.

Configuring the RPL Server

After creating the image file, you need to configure the Remote Program Load Server. This is done using the Invisible LAN Setup program (**SETUP30**). Here are the steps:

Step 1. Run the **SETUP30** program.

Step 2. Use the **Load/Create Initialization File** selection to load the server's initialization file into memory.

Step 3. Select **Advanced Configuration** from the Main Menu to bring up the Advanced Configuration Menu. Then select **Server Parameters** to bring up the Server Parameters screen.

Step 4. Enter the name of the image file into the **RPL Image** field. You must enter the full drive and path. For example, if the image file is named **BOOTDISK.IMG** and is located in directory **C:\NET30**, you should enter **C:\NET30\BOOTDISK.IMG**.

Step 5. Press **Enter** or **F9** to complete the entry and return to the Advanced Configuration Menu. Then press **Esc** to return to the Main Menu.

Step 6. Use the **Save Initialization File** selection to save the server's initialization file back to the disk.

After changing the server's initialization file, you need to reboot the system (press **Ctrl-Alt-Del**) and re-start the server in order for the new parameters to take effect.

SUMMARY: Configuring the Remote Program Load Server requires that the name of the image file be placed in the server's initialization file. This can be done with the **SETUP30** program.

Starting the Workstations

To start a diskless workstation, you need to enable the TransBIOS/NetBIOS ROM on the network card. When you start the diskless workstation, the network ROM takes control of the system, contacts the Remote Program Load Server, and loads DOS from the boot diskette image file.

The diskless workstation starts up exactly as if the boot diskette were in drive A:. Any CONFIG.SYS and AUTOEXEC.BAT files on the boot diskette are executed by the diskless workstation.

Once the diskless workstation is started, you can refer to the boot diskette as drive A:. For example, the command **DIR A:** displays a directory of the boot diskette.

After starting the diskless workstation, you need to use the **NET30** command to start Invisible LAN. Since all the diskless workstations in the network have to share the same boot diskette image, there will be several Invisible LAN initialization files on the boot diskette; one for each diskless workstation. Therefore, when you type the **NET30** command, you must indicate which initialization file you want to use. For example, if your initialization file is named ROBERT.INI, you would type the following command to start Invisible LAN:

NET30 ROBERT

Note that by using the **NETADDR** command, you can have each diskless workstation automatically start up with the correct initialization file. **NETADDR** is described later in this chapter.

SUMMARY: When a diskless workstation is turned on, it starts up exactly as if the boot diskette were in drive A:. It does so by accessing the image of the boot diskette contained in the image file on the Remote Program Load Server.

Unlinking From the RPL Server

If you have a computer with a floppy disk drive installed (but no fixed disk), you can use it as if it were a diskless workstation. To do so, just leave the floppy disk drive empty when you turn on the computer. It contacts the Remote Program Load Server just as if it were a diskless workstation.

When you start up this way, you cannot use your floppy drive, because drive letter A: refers to the image of the boot diskette on the Server and not to your own disk drive.

To use your own floppy disk drive, you must break the connection with the Remote Program Load Server using the **UNLINK** command. Follow this procedure:

Step 1. Use the **MAP** command to gain access to the server's disk. For example, to gain access to SERVER disk C:, type

```
MAP C: \\SERVER\C:\
```

Step 2. Switch to the server's disk. Using the previous example, type

```
C:
```

Step 3. Use the **PATH** command to specify the directories containing the DOS and Invisible LAN program files, for example

```
PATH=C:\DOS;C:\NET30
```

Step 4. Use the **SET COMSPEC** command to identify the location of the DOS file COMMAND.COM. An example is:

```
SET COMSPEC=C:\DOS\COMMAND.COM
```

Step 5. Unlink by typing

```
UNLINK
```

SUMMARY: The **UNLINK** command breaks the connection with the Remote Program Load Server and gives you access to your own floppy disk drive.

Custom Startup Procedures

Option 1. To display the network address or serial number, type

NETADDR /V

Option 2. To test for a specified network address or serial number, type

NETADDR *nnnn*

where *nnnn* is a network address or serial number. **NETADDR** returns ERRORLEVEL 0 if the network address or serial number matches *nnnn*, or ERRORLEVEL 1 if they don't match. If **NETADDR** is unable to determine the network address or serial number, it returns ERRORLEVEL 255.

Option 3. To return the network address as an ERRORLEVEL, type

NETADDR

If the network board has an address between 0 and 255, then **NETADDR** returns an ERRORLEVEL equal to the network address. Otherwise, it returns ERRORLEVEL 255. **Note** — This option is included for compatibility with old versions of Invisible LAN. We recommend using option 2 instead of option 3.

The **NETADDR** command is intended to be used in a batch file. It lets you obtain the address or serial number of the network hardware, and execute a different procedure depending on the result. **NETADDR** is most useful when setting up an AUTOEXEC.BAT file for diskless workstations, because it lets you specify a different startup procedure for each workstation.

If you don't know the address or serial number of your network hardware, you can use **NETADDR /V** to display it.

Example — Suppose you have three diskless workstations. Station MIKE has serial number 9284, station VINCE has serial number 9656, and station REGINA has serial number 9472. You have set up three initialization files called MIKE.INI, VINCE.INI and REGINA.INI, and you want to start each workstation with the appropriate initialization file. You can do this as follows:

```
REM Check for MIKE
NETADDR 9284
IF ERRORLEVEL 255 GOTO :FAILED
IF ERRORLEVEL 1 GOTO :NOTMIKE
NET30 MIKE
GOTO :DONE

:NOTMIKE
REM Check for VINCE
NETADDR 9656
IF ERRORLEVEL 255 GOTO :FAILED
IF ERRORLEVEL 1 GOTO :NOTVINCE
NET30 VINCE
GOTO :DONE

:NOTVINCE
REM Check for REGINA
NETADDR 9472
IF ERRORLEVEL 255 GOTO :FAILED
IF ERRORLEVEL 1 GOTO :NOTREGINA
NET30 REGINA
GOTO :DONE

:NOTREGINA
ECHO Unrecognized station address!
GOTO :DONE

:FAILED
ECHO Unable to read station address!

:DONE
```

SUMMARY: The **NETADDR** command is used in a batch file. It lets you execute different procedures, depending on the address or serial number of the network hardware.

Memory Management

The Invisible RAM memory managers can be used on diskless workstations. Since the memory managers are selected and configured by the Invisible LAN initialization file, it is possible for each diskless workstation to use the memory manager that is most appropriate for its hardware.

All the usual features are available when using the memory managers on diskless workstations. However, there are two features that are of special importance to diskless workstations. These are discussed below.

Copying the Network ROM

On a diskless workstation, you must enable the TransBIOS/NetBIOS ROM on the network card. On AT-class computers, ROMs are much slower RAM (this is why the RAM version of TransBIOS/NetBIOS gives better performance than the ROM version). So, on AT-class computers, it would be desirable to start up using the ROM and then switch over to RAM.

Five of the Invisible RAM memory managers have the ability to do this: the NEAT, AT/386, SCAT, PEAK, and 386 VIRTUAL memory managers. When you load one of these memory managers, it automatically detects that you are using the network ROM. Then it disables the ROM, and inserts RAM at the address which the ROM occupied. Finally, it copies the contents of the ROM into the RAM.

The result is that the ROM code now executes at RAM speed. This allows diskless workstations to enjoy the high performance of the RAM version of TransBIOS/NetBIOS.

Relocating the TransBIOS Data Area

When the TransBIOS/NetBIOS ROM starts up, it “steals” some RAM from the top of DOS memory. This has two undesirable consequences: first, it reduces the memory available to DOS; and second, it makes it impossible to frontfill DOS memory (*frontfill* means increasing DOS memory beyond 640K, usually to 736K on a color system or 704K on a monochrome system).

All the memory managers can overcome this problem. The memory managers can move the TransBIOS data area to a different location. The data area can be moved into low DOS memory, or into shadow RAM. Either way, once the data area is moved, it is possible to frontfill DOS memory. And if the data area

is moved to shadow RAM, the “stolen” RAM once again becomes available to DOS.

The workstation’s initialization file determines if the data area is moved to low DOS memory, or to shadow RAM. Using **SETUP30**, you control this with the Data Location parameter on the TransBIOS parameter screen. (To get to the TransBIOS parameter screen, select **Advanced Configuration** from the Main Menu, and then select **TransBIOS Parameters** from the Advanced Configuration Menu.) If you select **DOS** for Data Location, the data area is moved to low DOS memory. If you select **SHADOW** for Data Location, the data area is moved to shadow RAM.

SUMMARY: The Invisible RAM memory managers have two special features for diskless workstations: copying the network ROM to RAM in order to increase performance, and relocating the TransBIOS data area in order to free up DOS memory.

Memory Management Commands

This chapter describes several commands you can use with the Invisible RAM memory managers. These commands let you:

- Display the memory map
- Use shadow RAM
- Control VGA and EGA graphics memory
- Clear the computer's CMOS memory

Displaying the Memory Map

To display information about the memory in your computer, type

SHADOW [*options*]

where the *options* determine which information is to be displayed. The *options* may include one or more of the following:

- | | |
|-----------|---|
| /A | All. Display all of the following information. |
| /C | Chips and Technologies chipset. Display information about special memory-management chips manufactured by Chips and Technologies. (These chips are built in to many AT-type computers.) |
| /D | DOS. Display information about DOS memory. |
| /E | Extended. Display the size of extended memory. |

/H	Handles. Display a table of all expanded memory handles.
/M	Memory map. Display a complete memory map of the system.
/N	Network software. Display information about the memory usage of Invisible LAN.
/S	Shadow RAM. Display the usage of shadow RAM.
/X	Expanded. Display information about expanded memory.

/D — DOS Memory Information

If you include the **/D** or **/A** parameter, **SHADOW** produces a display similar to the following:

```
DOS version number: 3.30.
Total DOS memory: 736K.
Free DOS memory: 638K.
```

The first line indicates which version of DOS you are using.

The second line indicates the total amount of memory available for DOS.

The third line indicates the amount of DOS memory that is available for application programs.

/X — Expanded Memory Information

You can display information about expanded memory by including the **/X** or **/A** parameter.

If there is no expanded memory manager software installed, **SHADOW** displays the following:

Expanded Memory Manager: Not installed.

If there is an expanded memory manager installed, **SHADOW** produces a display similar to the following:

Expanded Memory Manager: Installed.

Version number: 4.0.

Total expanded memory: 2048K.

Free expanded memory: 1824K.

EEMS (enhanced EMS) functions: Available.

The first line indicates that the expanded memory manager is installed.

The second line gives the version number of the expanded memory software.

The third line gives the total amount of expanded memory in the system.

The fourth line gives the amount of expanded memory that is available for use by application programs.

The fifth line tells whether the expanded memory manager software supports the *enhanced EMS* (EEMS) functions. These extra functions are not part of the official EMS specification, but are used by some application programs.

/H — Expanded Memory Handles

When an application uses expanded memory, it obtains a *handle* from the expanded memory manager. The handle lets the expanded memory manager keep track of which portion of the expanded memory belongs to each application program.

If you include the **/H** or **/A** parameter, **SHADOW** displays a table of all the expanded memory handles currently in use, in a form similar to the following:

EMS handles, names, and sizes:

0 SYSTEM 512K.

1 NET30-C1 1088K.

Each line in the table shows three items of information:

- The handle number. This can range from 0 to 255. Handle number 0 is created by the expanded memory manager itself; other handles are created by application programs.

- The handle name, if any. An application program can optionally assign a name to a handle. Some expanded memory managers assign a name to handle 0 (Invisible RAM always assigns the name SYSTEM to handle 0).
- The amount of expanded memory allocated to the handle, in kilobytes.

/E — Extended Memory Size

If you include the **/E** or **/A** parameter, **SHADOW** displays the amount of extended memory in the system, in a form similar to the following:

Extended memory size: 1024K.

Note—On an XT-type computer, the size displayed is always zero.

Note—If you have installed Invisible RAM 386, the size displayed is the amount of memory reserved for extended memory applications, not the total extended memory in the computer.

Note—If you have installed the Invisible LAN disk cache in extended memory, the size displayed does not include the amount of memory used by the disk cache.

/C — Chips And Technologies Chipset Information

Chips and Technologies is a company that makes special chips which are used in many PCs. These special chips provide advanced memory management features. For this reason, **SHADOW** displays information about these special chips, if you specify the **/C** or **/A** parameter.

Chips and Technologies makes four different special chips that provide advanced memory management features:

- The NEAT chipset (used with the 286 or 386SX).
- The AT/386 chipset (used with the 386).
- The SCAT chipset (used with the 286).
- The PEAK chipset (used with the 386 or 486).

Each chipset has the ability to provide RAM in the area between 640K and 1024K, in the area normally used for BIOS ROMs and the video system. You

can speed up the execution of BIOS code by copying the BIOS ROMs into RAM. If you install Invisible RAM, you can also use this “shadow RAM” to hold memory-resident programs and device drivers. The NEAT and SCAT chipsets also have a built-in expanded memory controller.

If there is no Chips and Technologies chipset in your computer, **SHADOW** displays the following:

Chips and Technologies chipset: Not present.

If the NEAT chipset is present in your computer, **SHADOW** produces a display similar to the following:

Chips and Technologies chipset: NEAT version B.
Total RAM on motherboard: 1024K.
640K to 1M memory relocation: Disabled.
Shadow RAM: Available.
Expanded memory controller: Enabled.
EMS I/O port address: 02E8.
EMS memory base address: E000.

If the AT/386 chipset is present in your computer, **SHADOW** produces a display similar to the following:

Chips and Technologies chipset: AT/386 version B.
Total RAM on motherboard: 1024K.
Shadow RAM: Available.

If the SCAT chipset is present in your computer, **SHADOW** produces a display similar to the following:

Chips and Technologies chipset: SCAT version A.
Total RAM on motherboard: 4096K.
640K to 1M memory relocation: Disabled.
Shadow RAM: Available.
Expanded memory controller: Enabled.
EMS memory size: 1024K.
Expanded memory I/O ports: Enabled.
EMS I/O port address: 208.

If the PEAK chipset is present in your computer, **SHADOW** produces a display similar to the following:

Chips and Technologies chipset: PEAK version D.

Total RAM on motherboard: 4096K.

Shadow RAM: Available.

Cache: Enabled.

Cache size: 256K.

In each case, the first line of the display identifies the type of chipset that is installed in your computer, and tells you which version of the chipset you have. The second line tells you the total amount of RAM installed on the motherboard (this number does not include any RAM installed on expansion boards).

In the case of the NEAT or SCAT chipset, the third line indicates if memory relocation is enabled or disabled. If there is exactly 1024K RAM on the motherboard, the first 640K is used for DOS. NEAT and SCAT offer two options for the use of the remaining 384K. If *memory relocation* is disabled, the remaining 384K is mapped into segments A000-FFFF, where it can be used to hold copies of BIOS ROMs. If *memory relocation* is enabled, the remaining 384K is mapped into segments 10000-15FFF, where it can be used as extended or expanded memory. (If there is more than 1024K RAM on the motherboard, then memory relocation must be disabled.)

The next line on the display indicates if RAM is available to hold copies of BIOS ROMs, and for use as shadow RAM. In order for RAM to be available, there must be at least 1024K RAM on the motherboard, and, in the case of the NEAT and SCAT chipsets, memory relocation must be disabled. **Note** — To use the chipset RAM as shadow RAM, you need to install the appropriate version of Invisible RAM.

For the NEAT and SCAT chipsets, the display also includes information about the built-in expanded memory controller. **Note** — To use the chipset's expanded memory controller, you need to install the appropriate version of Invisible RAM.

For the PEAK chipset, the display includes information about the built-in cache. This cache speeds up access to the computer's main memory.

Note — To change the configuration of the chipset, you need to use your computer's set-up program.

/N — Network Software Information

You can display information about the network software by including the **/N** or **/A** parameter. If Invisible LAN is not installed, **SHADOW** displays the following:

NET/30 TransBIOS network software: Not installed.

If Invisible LAN is installed, **SHADOW** produces a display similar to the following:

NET/30 TransBIOS network software: Installed.
TransBIOS data segment address: C800.
TransBIOS data segment size: 24K.

The first line indicates that Invisible LAN is installed.

The second line tells you the address of the TransBIOS data segment.

The third line tells you the size of the TransBIOS data segment, in kilobytes.

/S — Shadow RAM Usage Information

If you include the **/S** or **/A** parameter, **SHADOW** displays information about shadow RAM.

If you have not created shadow RAM (by loading Invisible RAM and specifying the appropriate parameters), the **SHADOW** program displays the following:

Shadow RAM Manager: Not installed.

If you have created shadow RAM, **SHADOW** displays information similar to the following:

Shadow RAM Manager: Installed.
Total shadow RAM: 192K.
Free shadow RAM: 128K.
Largest loadable program size: 84K.

The first line indicates that the shadow RAM manager is installed. This means you can use the **LSHADOW** programs to load TSR's (terminate-stay-resident programs) and device drivers into shadow RAM. Also, you can use the shadow RAM to hold the Invisible LAN software.

The second line indicates the total amount of shadow RAM that is available for loading memory-resident programs. This figure includes not only shadow RAM, but also all RAM that is used to increase (*frontfill*) the size of DOS memory; thus, it indicates the total increase in the amount of RAM available under DOS.

The third line indicates the amount of unused shadow RAM available for loading memory-resident programs.

The fourth line indicates the size of the largest contiguous block of shadow RAM. This is the size of the largest single program you can load into shadow RAM, since a program must always be loaded into a single contiguous block of shadow RAM. **Note**—Most TSRs use more memory when first loaded than they do after they become resident. To load a TSR into shadow RAM, the “largest loadable program size” must be big enough for all the memory required when the program first loads, as well as after it becomes resident.

/M — Memory Map

If you include the **/M** or **/A** parameter, **SHADOW** displays a map of all the memory in the computer system. It is similar to the following:

0000-9FFF	DOS	RAM
A000-AFFF	DOS	SHADOW RAM
B000-B7FF	DOS	ENHANCED-EMS RAM
B800-BFFF	VIDEO	RAM
C000-C5FF	ROM	
C600-C7FF		
C800-DFFF	SHADOW	RAM
E000-EFFF	STANDARD-EMS	RAM
F000-FFFF	BIOS	

Each line shows a range of addresses, followed by a description of what memory is located there. The following words may appear in the description:

DOS — The memory is usable by DOS applications.

RAM — The address range contains read/write memory.

ROM — The address range contains a BIOS ROM for a plug-in adapter board.

BIOS — The address range contains the motherboard's built-in ROM BIOS.

VIDEO — The address range is reserved for use by the video system.

STANDARD-EMS — The address range contains page frames used for expanded memory. These page frames make up the standard EMS area that is used expanded memory (EMS) applications.

ENHANCED-EMS — The address range contains page frames used for expanded memory. These page frames are not part of the standard EMS area. Only a few applications use this type of page frame.

SHADOW — The address range contains shadow RAM supplied by Invisible RAM. This memory can be used to hold memory resident programs and device drivers, and the Invisible LAN operating system.

HIGH — The address range contains high RAM supplied by Invisible RAM. This memory can only be used by specially designed application programs.

ROM-COPY — The address range contains RAM which holds a copy of a ROM (either a BIOS ROM for a plug-in adapter board, or the computer's built-in ROM BIOS). This allows the ROM code to execute at the faster speed of RAM.

CHIPSET — The address range contains memory supplied by the Chips and Technologies chipset. This memory can be used to hold copies of BIOS ROMs, thereby speeding up execution of BIOS code.

WRITE-PROTECTED — The address range contains memory supplied by the Chips and Technologies chipset which has been write-protected, so that it cannot be modified. This allows the chipset memory to act as if it was a ROM (ROMs cannot be modified)

Where appropriate, more than one word can appear in the description. Here are explanations for the more commonly encountered combinations:

DOS RAM — Read/write memory available to DOS applications. The word DOS should never appear without RAM.

DOS SHADOW RAM — Shadow RAM that has been used to increase (frontfill) DOS memory.

DOS HIGH RAM — High RAM that has been used to increase (frontfill) DOS memory.

DOS ENHANCED-EMS RAM — Expanded memory that is located within the DOS memory space.

VIDEO RAM — Read/write memory used by the video system. If VIDEO appears without RAM, it means that the address range is reserved for the video system, but there is currently no memory in the range; this occurs for address

range A000-AFFF with an EGA or VGA video card operating in text mode.

SHADOW VIDEO — An address range that can contain shadow RAM, but the shadow RAM was temporarily disabled with the **VGAON** program.

HIGH VIDEO — An address range that can contain high RAM, but the high RAM was temporarily disabled with the **VGAON** program.

STANDARD-EMS RAM — Indicates a portion of the standard EMS area that currently has memory enabled. If STANDARD-EMS appears without RAM, it means the address range is part of the standard EMS area, but there is no memory currently mapped there.

ENHANCED-EMS RAM — Indicates an enhanced EMS page frame that currently has memory enabled. If ENHANCED-EMS appears without RAM, it means the address range is mappable by the expanded memory manager, but there is no memory currently mapped there.

SHADOW RAM — Read/write memory supplied by Invisible RAM that is useable as shadow RAM. The memory can be used by the **LSHADOW** programs for loading TSR's and device drivers, or for frontfill, or for the Invisible LAN software.

HIGH RAM — Read/write memory supplied by Invisible RAM that is useable as high RAM. The memory can be used by specially designed programs, or for frontfill.

CHIPSET RAM — Read/write memory supplied by the Chips and Technologies chipset.

ROM CHIPSET — Memory supplied by the Chips and Technologies chipset, which contains a copy of a BIOS ROM for a plug-in adapter board.

ROM CHIPSET WRITE-PROTECTED — Memory supplied by the Chips and Technologies chipset, which contains a copy of a BIOS ROM for a plug-in adapter board, and is write-protected so it cannot be modified.

BIOS CHIPSET WRITE-PROTECTED — Memory supplied by the Chips and Technologies chipset, which contains a copy of the motherboard's built-in ROM BIOS, and is write-protected so it cannot be modified.

Note—A blank line indicates an address range that has no memory of any type.

SUMMARY: The **SHADOW** command displays a great deal of information about your computer's memory, including a complete memory map.

Using Shadow RAM

Many computer users like to use memory-resident programs (also called terminate-stay-resident programs or TSRs). The memory-resident programs include pop-up notepads, calculators, calendars, telephone dialers, spelling checkers, and keyboard enhancers, as well as network software.

A problem that many users encounter is that the memory-resident programs may use a lot of memory, especially if several are installed. After loading all your memory-resident programs, you may not have enough DOS memory left to run your application software.

Invisible RAM lets you load memory-resident programs into shadow RAM, so that they do not use any DOS memory. Depending on your system configuration, you may have as much as 256K of shadow RAM available for loading memory-resident programs.

Loading Memory-Resident Programs

Invisible RAM includes a program called **LSHADOW.COM** which is used to load memory-resident programs into shadow RAM.

To load a program into shadow RAM, type

LSHADOW [*/A*] *filename* [*parameters*]

The parameters have the following meanings:

<i>/A</i>	An optional parameter that alters the behavior of LSHADOW , and is required for some programs. Most programs do not require <i>/A</i> .
<i>filename</i>	The name of the memory-resident program. You must specify the complete file name of the program, including the .COM or .EXE extension. If the program file is not in the current directory, you should include the complete drive and path specification.
<i>parameters</i>	Optional command-line parameters that you want to specify for the memory-resident program. The meaning of these parameters varies depending on the pro-

gram. Type the same parameters that you would use if you were loading the program from the DOS command line.

Note—LSHADOW does not use the DOS PATH to find program files. If the memory-resident program is not in the current directory, you must include a path specification with the filename.

Note—In order to use **LSHADOW**, you must tell the memory manager to create some shadow RAM, using the appropriate parameters.

Note—Do not attempt to use **LSHADOW** to load the Invisible LAN operating system software into shadow RAM. Invisible LAN is designed to load itself into shadow RAM without the use of **LSHADOW**. Use the network configuration parameters (in the **SETUP30** program) to make Invisible LAN use shadow RAM.

Example 1—You have a memory-resident program called SK.COM. To load the program into shadow RAM, type

LSHADOW SK.COM

Example 2—You have memory-resident software called KEYMACS.EXE, which is installed on your hard disk in directory C:\KEY. To load the program into shadow RAM, type

LSHADOW C:\KEY\KEYMACS.EXE

Example 3—You want to install the DOS print spooler program, PRINT.COM, which is located in directory C:\DOS. You want to include parameters to tell the print spooler to use printer LPT2 and a print buffer size of 1000 bytes. Type

LSHADOW C:\DOS\PRINT.COM /D:LPT2 /B:1000

In this example, **/D:LPT2** and **/B:1000** are parameters that are passed to the PRINT.COM program. Refer to the DOS Reference Manual for detailed information on the PRINT.COM program.

Example 4—For this example, suppose that the memory-resident program UTILITY.COM does not load successfully without the **/A** parameter. To load it with the **/A** parameter, type

Technical Note—The /A parameter makes **LSHADOW** increase the value of the BIOS memory size variable before loading the program. Some programs examine the BIOS memory size, and get confused if the value is too small.

Loading Device Drivers

Invisible RAM includes a program called **LSHADOW.SYS** which is used to load device drivers into shadow RAM.

To load a device driver into shadow RAM, place the following line into the CONFIG.SYS file:

DEVICE=LSHADOW.SYS [/A] *filename* [*parameters*]

The parameters have the following meanings:

/A	An optional parameter that alters the behavior of LSHADOW.SYS , and is required for some device drivers. Most device drivers do not require /A.
<i>filename</i>	The name of the device driver. You must specify the complete file name of the device driver, including the .SYS extension. If the file is not in the root directory of your boot disk, you should include a drive and path.
<i>parameters</i>	Optional command-line parameters that you want to specify for the device driver. The meaning of these parameters varies depending on the device driver. Use the same parameters that you would use if you were loading the device driver into DOS memory.

Important Note—In order to use **LSHADOW.SYS**, you must install Invisible RAM from the CONFIG.SYS file; refer to the text file INVRAM.TXT for instructions. The CONFIG.SYS lines that install Invisible RAM must come before the **DEVICE=LSHADOW.SYS** line.

Note—In order to use **LSHADOW**, you must tell the memory manager to create some shadow RAM, using the appropriate parameters.

Note—**LSHADOW.SYS** uses approximately 120 bytes of DOS memory. If

the device driver you are loading is smaller than 120 bytes, you are better off to simply load it into DOS memory. The two Invisible LAN device drivers (**CACHE30.SYS** and **N30DEV.SYS**) are small enough that you are better off loading them into DOS memory.

Example 1—To load the device driver **ANSI.SYS** into shadow RAM, use the statement

```
DEVICE=LSHADOW.SYS ANSI.SYS
```

Example 2—You have a mouse driver called **MOUSE.SYS** which is on your hard disk in directory C:\MOUSE. To load it in shadow RAM, use the statement

```
DEVICE=LSHADOW.SYS C:\MOUSEMOUSE.SYS
```

Example 3—You want to install the IBM DOS RAMDISK program, **VDISK.SYS**, which is located in directory C:\DOS. **VDISK** requires the **/A** parameter. Use the statement shown below. In this example, 128 is a parameter passed to **VDISK**.

```
DEVICE=LSHADOW.SYS /A C:\DOS\VDISK.SYS 128
```

Technical Note—The **/A** parameter makes **LSHADOW.SYS** increase the value of the BIOS memory size variable before loading the device driver. Some device drivers examine the BIOS memory size, and get confused if the value is too small.

SUMMARY: The **LSHADOW** commands are used with Invisible RAM. They let you load memory-resident programs and device drivers into shadow RAM (memory located between 640K and 1M), so they do not take up any DOS memory.

Controlling VGA and EGA Graphics Memory

Invisible RAM increases the size of DOS memory beyond 640K. This presents a problem if you have a VGA or EGA video system, because the high-resolution graphics modes use the same memory that is required to increase DOS memory.

Invisible RAM deals with this problem by allowing you to disable the high-resolution graphics modes of the VGA or EGA video system. When you disable high-resolution graphics, DOS memory is increased to 736K, but you can only use the text mode and the low-resolution graphics modes (also called the CGA graphics modes).

When you enable high-resolution graphics, DOS memory is limited to a maximum of 640K.

Enabling VGA or EGA Graphics

To enable the high-resolution graphics modes of a VGA or EGA video system, type

VGAON

After running **VGAON**, you can use the high-resolution graphics modes. **VGAON** reduces the size of DOS memory down to 640K.

Disabling VGA or EGA Graphics

To disable the high-resolution graphics modes of a VGA or EGA video system, type

VGAOFF

After running **VGAOFF**, you cannot use the high-resolution graphics modes. **VGAOFF** increases the size of DOS memory as much as possible, usually to 736K.

Controlling the Default Graphics State

Normally, the VGA or EGA high-resolution graphics are enabled when Invisible RAM is first loaded. In order to disable high-resolution graphics and increase DOS memory size above 640K, you must run the **VGAOFF** program.

If you wish, you may instruct Invisible RAM to disable the high-resolution graphics as soon as it loads. Then, DOS memory size is immediately increased above 640K. You can run the **VGAON** program to enable the high-resolution graphics whenever you want to. For instructions on doing this, refer to the *Installation* manual, or the text file INVRAM.TXT.

SUMMARY: The **VGAON** and **VGAOFF** commands are used with Invisible RAM. They control the use of high-resolution graphics memory. You can switch between using the memory for graphics, or making the memory available to DOS programs.

Clearing the CMOS Memory

On rare occasions, there may be problems when you attempt to change the configuration of a Chips and Technologies chipset. This happens mostly with older versions of computers that have the NEAT chipset. The computer may “remember” the old configuration and refuse to adapt itself to the new configuration, even if you run the computer’s set-up program.

CLRCMOS completely erases the computer’s old configuration. If you have problems changing the configuration of a chipset, run **CLRCMOS**. Then you can run the computer’s set-up program, and establish the new configuration.

Caution—After running **CLRCMOS**, you will have to set up the computer from scratch (entering memory size, diskette drive types, fixed disk drive type numbers, and so on). Don’t run **CLRCMOS** unless you know how to do this.

SUMMARY: The **CLRCMOS** command erases the computer’s CMOS memory, thereby erasing all configuration information.

Part 2

Electronic Mail

Electronic Mail

Invisible LAN includes an *electronic mail* system which lets you communicate with other network users by sending and receiving messages. The mail system is a small program which remains resident in your computer's memory. When you want to send a message, you press a special "hot key" on the keyboard, and the program "pops up" onto the screen. When you receive a message, the program automatically pops up and displays the message.

This chapter describes how to:

- Send messages
- Receive messages

You install the mail program with the Invisible LAN Setup program (**SETUP30**). Refer to the *Getting Started* manual or the *Installation* manual for instructions on installing mail.

Sending Messages

To send a message, follow this procedure:

Step 1. Activate the mail program by pressing **Ctrl-Alt-Backspace** (hold down the **Ctrl** and **Alt** keys, and then press the **Backspace** key). A four-line window appears at the top of the screen as shown in figure 10-1.

Step 2. In the first line of the window, type the network name of the computer to which you are sending the message.

Step 3. In the second line of the window, type the message. Your message is limited to one line.

Step 4. Press **F2** to send the message.

Step 5. Press **Esc** to exit the mail program.

Table 10-1 shows the keys you can use when entering your message.

Table 10-1. Mail Message Keys

Key	Function
Ctrl-Alt-Backspace	Enter Mail
Esc	Exit mail
Up Arrow	Cursor up
Down Arrow	Cursor down
Enter Tab	Cursor to next field
Left Arrow	Cursor left
Right Arrow	Cursor right
Backspace	Delete character to the left of cursor
Del	Delete character at cursor
Ins	Toggle between insert mode and overwrite mode
Home	Cursor to start of line
End	Cursor to end of line
Ctrl-End	Delete from cursor to end of line
F2	Send message
F6	Compose reply
F10	Clear window

Example — You want to send the message “Please turn on the printer, I need to print my report” to the user named REGINA.

1. Press **Ctrl-Alt-Backspace**. The mail window pops up onto the screen.
2. On the first line, type “REGINA”.
3. On the next line, type “Please turn on the printer, I need to print my report.”
4. Press **F2** to send the message.
5. Press **Esc** to exit the Mail program.

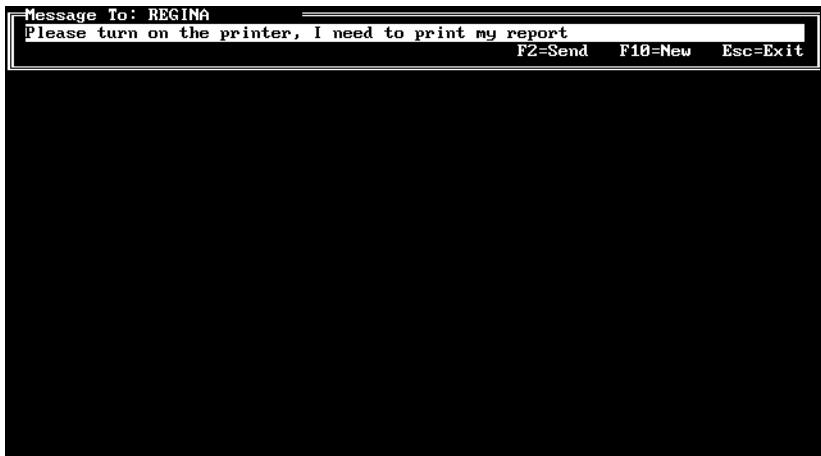


Figure 10-1. Sending a message

Note — The mail program window can pop up only if your screen is in 80-column text mode. It cannot pop up if the screen is in graphics mode or 40-column text mode.

Receiving Messages

When your computer receives a message, the speaker beeps three times, and the mail window appears at the top of the screen as shown in figure 10-2.

The mail window shows you the name of the person who sent the message and the text of the message.

After reading the message, you have three options:

- Send a reply to the sender
- Compose a message to another person
- Exit from mail

Each option is described below.

To send a reply to the sender, press F6—The second line of the window is cleared, so that you can type the reply. The first line of the window is automatically filled in with the correct name. After typing your reply, press **F2** to send it.



Figure 10-2. Receiving a message

To compose a message to another person, press F10—Both lines of the window are cleared, so you can type both a message and the name of the person to whom you want it sent. Press **F2** to send the message.

To exit from mail, press Esc—The mail window disappears, and you can return to your application program.

Note—If you don't want mail to beep the speaker, you can give the command **NW NOAUDIO**. To turn the speaker back on, give the command **NW AUDIO**. See chapter 6 for a description of this use of the **NW** command.

Part 3

The Network Manager

Introduction to the Network Manager

Invisible LAN includes a menu-driven Network Manager program. The manager can perform all network management functions, including:

- Network polling
- Drive and printer mappings
- Print stream truncation
- Print spooler status
- Shortname definitions
- Security
- Server usage monitoring

An important feature of the manager is *remote management*. Most of the manager's functions can be used not only on your own computer, but also on other computers across the network. With remote management, you can control the network software in other computers, as if by remote control.

Starting the Manager

To start the manager, type

MENU

If you have a monochrome VGA screen (like many laptop computers), the display may be easier to read if you start the manager with the command

MENU /B

The program loads into memory and displays the Main Menu as shown in figure 11-1. You operate the program using the keys shown in table 11-1.

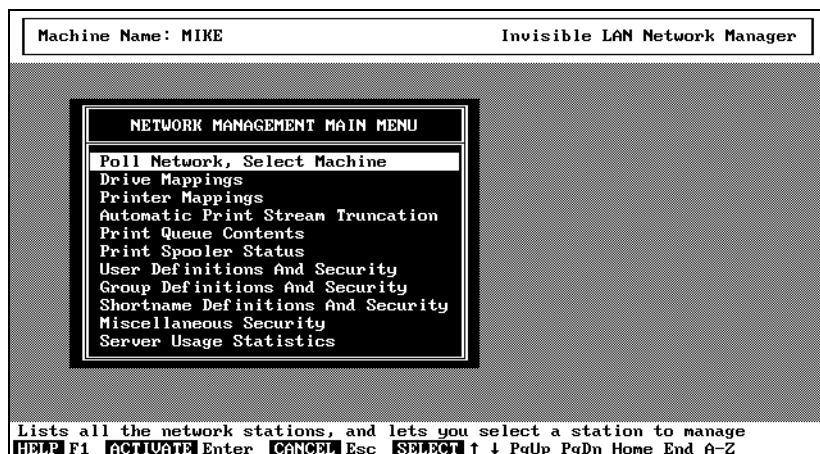


Figure 11-1. The Network Manager Main Menu

Table 11-1. Keys Used with Network Manager

Key	Function
F1	Help —Display help.
Esc	Cancel —Abort the current operation and return to previous menu.
Enter F9	Activate —If you are at a menu, ENTER activates your menu selection. If you have just typed some information, ENTER or F9 makes the program act on your information.
Up Arrow Down Arrow PgUp PgDn Home (or Ctrl-PgUp) End (or Ctrl-PgDn)	Select —If you are at a menu, use these keys to indicate your selection. If you are typing information, use these keys to select a field. If you are reading text, use these keys to scroll the text.
Right Arrow Left Arrow Ins Del Backspace Home End	Edit —When typing information, use these keys to correct typing mistakes.

Poll Network, Select Machine

Use this menu choice to list the computers on the network and to select a machine to manage.

Displaying Computers on the Network

The manager polls the network to find all computers that are running Invisible LAN. For each computer, the manager displays its name, its address or serial number, and its installed modules (server, redirector, or both).

To poll the network and display the network computers, select and activate **Poll Network, Select Machine**. (Use the up/down arrow keys to move the selection bar over **Poll Network, Select Machine**, and then press **Enter**.) The screen displays the network computers as shown in figure 11-2.

Selecting a Network Computer to Manage

Once the network computers are displayed, you can select one to manage. You can manage any machine in the network: either your own machine, or another machine. All of the manager's functions operate on the computer you select. If you select a remote computer, the manager lets you manage the computer by remote control.



Figure 11-2. Sample Network Polling Display

To choose a computer to manage, simply select the computer from the list of computers on the network. The *Action Menu* appears as shown in figure 11-3.

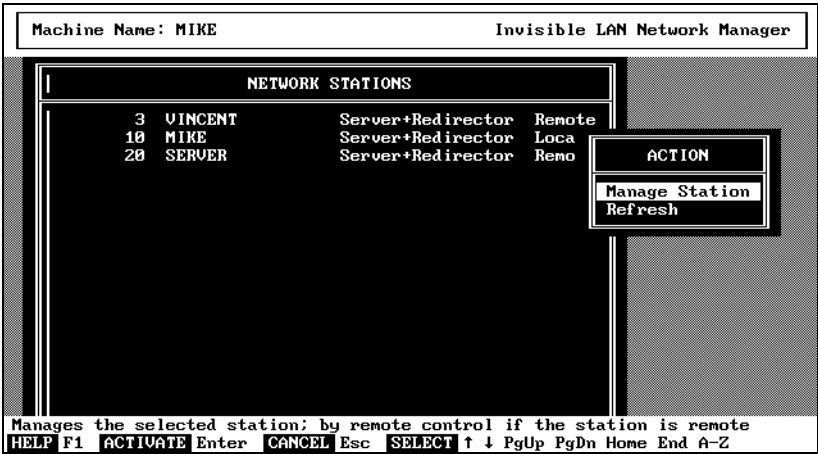


Figure 11-3. Action Menu

If you choose **Manage Station**, the manager returns to the Main Menu as shown in figure 11-1 with the name of the computer you selected on the top line. Any of the actions you take now affect that computer.

If you choose **Refresh**, the manager polls the network again and updates the list of stations.

As an example of the use of this command, suppose you have just sent a print job to a server. You could use the manager to examine the server's print queue and see how many print jobs are ahead of yours. You could even move your job to the front of the queue — all by remote control from your workstation.

SUMMARY: The **Poll Network, Select Machine** item on the manager's Main Menu displays a list of all computers in the network and lets you select one to manage.

Getting Help

To get help while using the network manager, press **F1**.

When you press **F1**, the manager displays help information on the panel you are currently using. This help information is called *context-sensitive*, because the information displayed varies depending on what you are doing at the time you request help.

If you press **F1** twice, the display shows general help information for operating the manager program.

When you are finished viewing help information, press **Esc**.

In addition to the help information displayed by **F1**, the manager also helps you by displaying the active keys at the bottom of the screen. And in many cases the manager also displays a line of text at the bottom of the screen which briefly describes the functions of the program.

■ **SUMMARY:** Press **F1** to get help while using the network manager.

Mappings

Invisible LAN lets you access disks and printers that are attached to computers other than your own. *Mapping* is the method by which you obtain access to a server's disk or printer. The mapping section of the network manager (**MENU** program) gives you control over your mappings.

This chapter covers:

- Drive mappings
- Printer mappings

Drive Mappings

A *drive mapping* is a logical connection between one of your drive letters (A: through Z:) and a server's disk. Every time you refer to the drive letter, you actually refer to the server's disk.

For example, suppose you make drive letter **E:** refer to a server's disk **C:**. Then, any operation you perform on drive **E:** is automatically sent across the network and performed on the server's disk **C:**. This allows you to access the server's disk exactly as if it were attached directly to your own computer.

Displaying the Drive Mappings

To work with your drive mappings, select **Drive Mappings** on the network manager Main Menu. The display shows a list of your drive mappings similar to figure 12-1.

For each drive letter, the display shows whether it is a local or network drive. If it is a network drive, the display shows the name of the server, the server's drive letter or shortname, and the server's directory path.

Example — If your drive letter F: refers to disk C: on server ALICE, the drive mapping is shown as:

```
F: ==> \\ALICE\C:
```

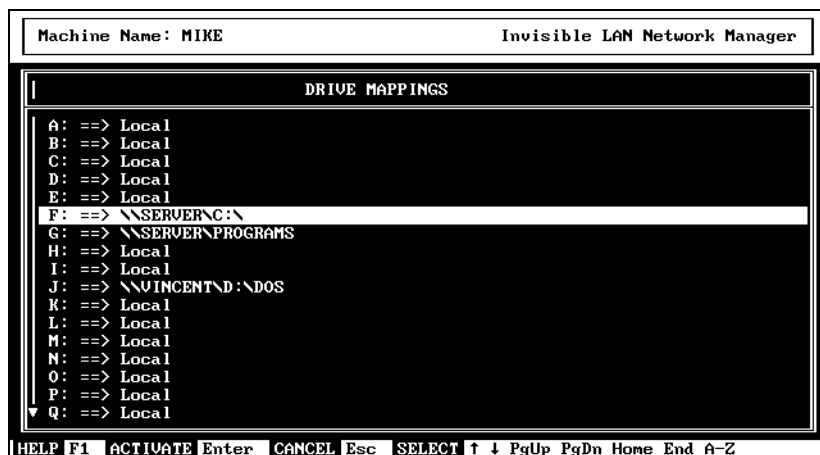


Figure 12-1. Drive Mapping Display

Example — Suppose your drive letter G: is mapped to directory C:\ACCTS on ROBERT's disk. This is shown as:

G: ==> \\ROBERT\C:\ACCTS

Example — Suppose your drive letter K: refers to the shortname LETTERS on server MAIN. (A *shortname* is the network name of a directory on the server's disk. You define shortnames in the Invisible LAN security system, as described in chapter 15.) This is shown as:

K: ==> \\MAIN\LETTERS

Disconnecting a Drive Mapping

To remove a drive mapping, proceed as follows:

- **Step 1.** Select a drive mapping from the displayed list. The Change Drive Mapping panel appears, as shown in figure 12-2.
- **Step 2.** Type an asterisk (*) in the **Server's Name** field, and then press **Enter** or **F9**.

The drive mapping is immediately terminated.

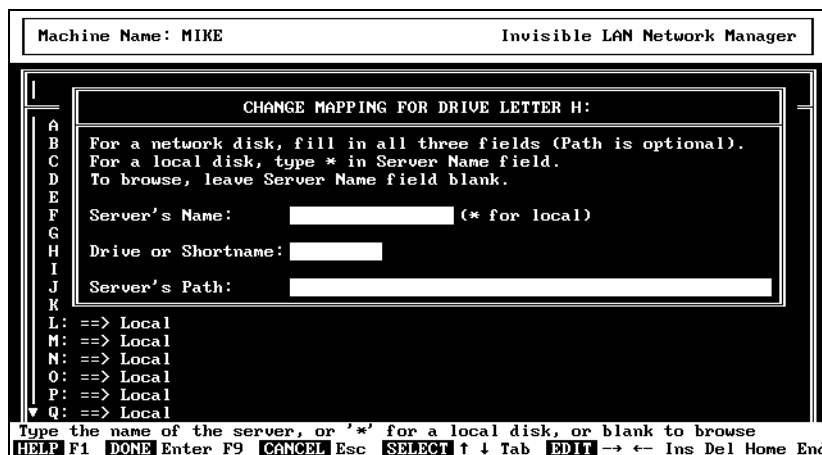


Figure 12-2. Change Drive Mapping Panel

Establishing a Drive Mapping (Method #1)

If you want to create a drive mapping, and you want to type in the network path, proceed as follows:

- Step 1. Select a drive letter from the Drive Mappings panel. The Change Drive Mapping panel appears, as shown in figure 12-2.
- Step 2. Type the name of the file server into the **Server's Name** field.
- Step 3. Type the server's drive letter or shortname into the **Drive or Shortname** field.
- Step 4. Optionally, type a directory path into the **Server's Path** field. If you type a path, the drive mapping refers to the directory you specify. If you leave this field empty, the drive mapping refers to the root directory.
- Step 5. Press **Enter** or **F9** to establish the mapping.

Example — Suppose you want to make drive letter J: refer to directory C:\DOS on server REGINA. You would first select J: from the Drive Mapping panel list. Then type REGINA into the **Server's Name** field, type C: into the **Drive or Shortname** field, and type DOS into the **Server's Path** field.

Establishing a Drive Mapping (Method #2)

If you want to create a drive mapping, and you don't want to type in the network path, follow the steps below:

- **Step 1.** Select a drive letter from the Drive Mappings panel. The Change Drive Mapping panel appears, as shown in figure 12-2.
- **Step 2.** Leave the **Server's Name** field blank, and press **Enter** or **F9**. The manager displays a list of file servers, as shown in figure 12-3.

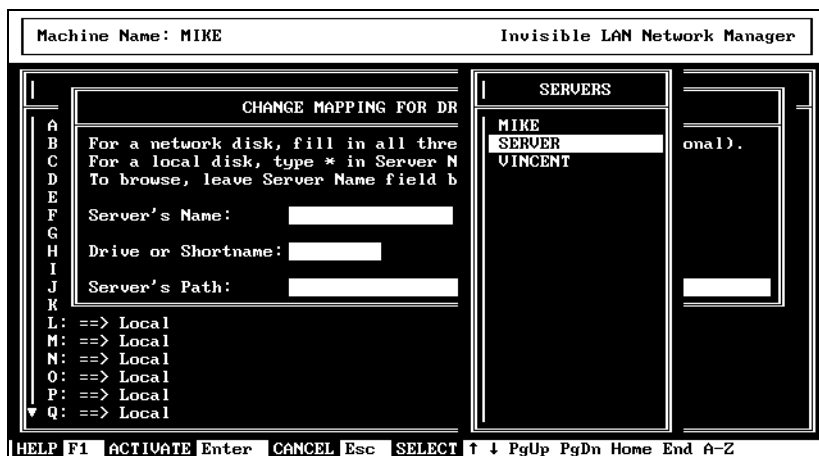


Figure 12-3. Drive Mapping Server List

- **Step 3.** Select a server from the list and press **Enter**. The manager shows you a list of available drives and shortnames on the selected server, as in figure 12-4. This list only shows the drives and shortnames that you have permission to use.
- **Step 4.** Select a drive or shortname and press **Enter**. Your selections for server and drive or shortname are automatically transferred to the Change Drive Mapping panel.
- **Step 5.** Optionally, type a directory path into the **Server's Path** field. If you type a path, the drive mapping refers to the directory you specify. If you leave this field empty, the drive mapping refers to the root directory.
- **Step 6.** Press **Enter** or **F9** to establish the mapping.

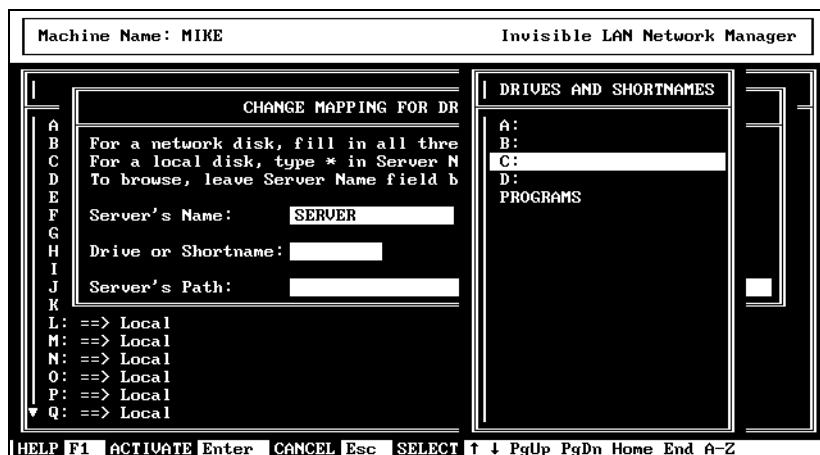


Figure 12-4. List of Network Drives and Shortnames

SUMMARY: The **Drive Mappings** selection on the Main Menu displays your current drive mappings. It also lets you disconnect your existing drive mappings and establish new drive mappings. When you establish a new drive mapping, you can browse the network and create the network path by selecting from menus.

Printer Mappings

A *printer mapping* is a logical connection between one of your print devices (LPT1, LPT2, or LPT3) and a server's printer. Every time you refer to the print device, you actually refer to the server's printer.

For example, suppose you make print device **LPT2** refer to a server's printer. Then, anything you print on **LPT2** is automatically sent across the network and printed on the server's printer. This allows you to access the server's printer exactly as if it were attached directly to your own computer.

Displaying the Printer Mappings

To work with your printer mappings, select **Printer Mappings** on the network manager Main Menu. The display shows a list of your printer mappings similar to figure 12-5.

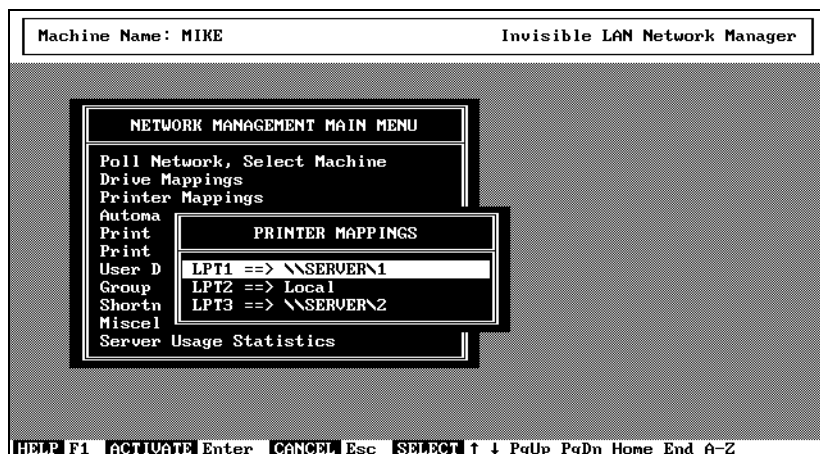


Figure 12-5. Printer Mapping Display

For each printer, the display shows whether it is a local printer or a network printer. If it is a network printer, the display shows the name of the server and the server's printer number.

Example — If your print device LPT1 refers network printer #1 on server ALICE, the printer mapping is shown as:

LPT1 ==> \\ALICE\1

Example — Suppose your print device LPT3 is mapped to network printer #2 on ROBERT. This is shown as:

LPT3 ==> \\ROBERT\2

Disconnecting a Printer Mapping

To remove a printer mapping, proceed as follows:

- **Step 1.** Select a printer mapping from the displayed list. The Change Printer Mapping panel appears, as shown in figure 12-6.
- **Step 2.** Type an asterisk (*) in the **Server's Name** field, and then press **Enter** or **F9**.

The printer mapping is immediately terminated.

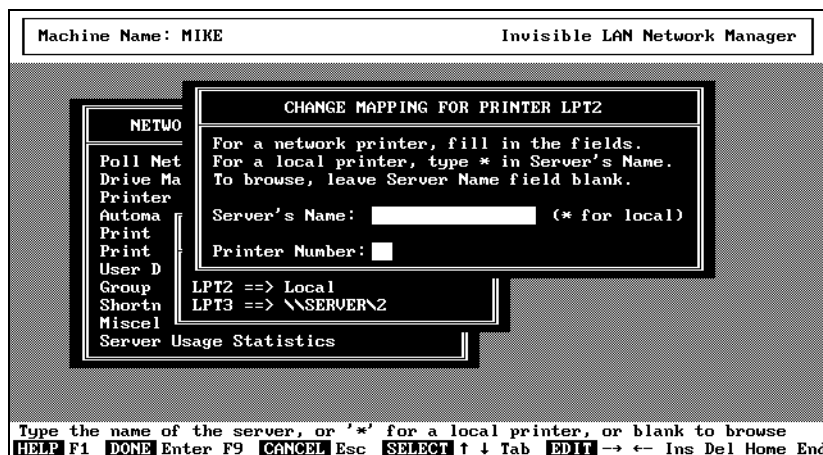


Figure 12-6. Change Printer Mapping Panel

Establishing a Printer Mapping (Method #1)

If you want to create a printer mapping, and you want to type in the network path, proceed as follows:

- Step 1. Select a printer mapping from the displayed list. The Change Printer Mapping panel appears, as shown in figure 12-6.
- Step 2. Type the name of the file server into the **Server's Name** field.
- Step 3. Optionally, type a printer number into the **Printer Number** field. If you leave this field empty, the printer mapping refers to printer #1.
- Step 4. Press **Enter** or **F9** to establish the mapping.

Example — Suppose you want to make print device LPT1 refer to printer #2 on server REGINA. You would first select LPT1 from the Printer Mapping panel. Then type REGINA into the **Server's Name** field, and type 2 into the **Printer Number** field.

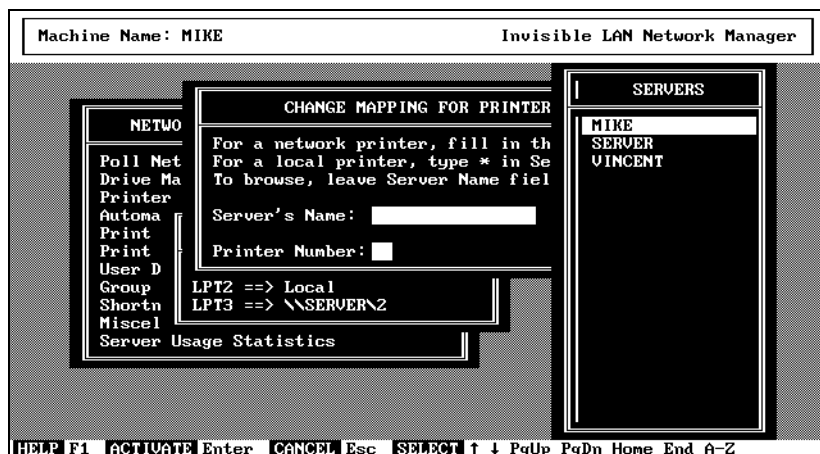


Figure 12-7. Printer Mapping Server List

Establishing a Printer Mapping (Method #2)

If you want to create a printer mapping, and you don't want to type in the network path, follow the steps below:

- **Step 1.** Select a printer mapping from the displayed list. The Change Printer Mapping panel appears, as shown in figure 12-6.
- **Step 2.** Leave the **Server's Name** field blank, and press **Enter** or **F9**. The manager displays a list of file servers, as shown in figure 12-7.

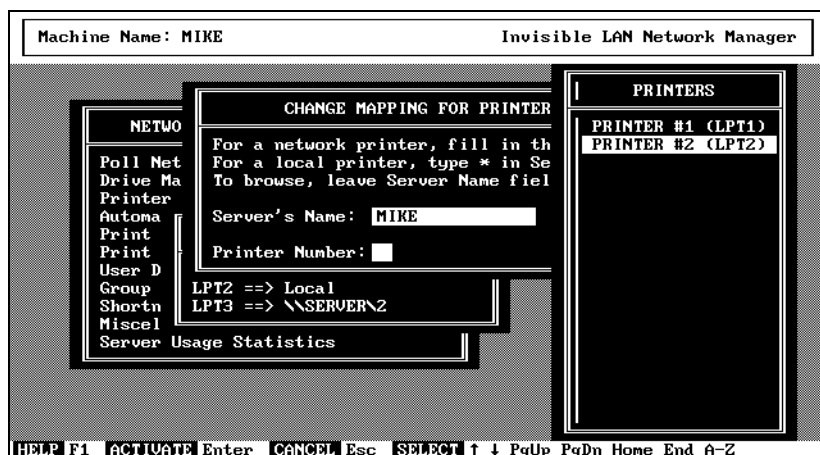


Figure 12-8. List of Network Printers

- Step 3. Select a server from the list and press **Enter**. The manager shows you a list of available printers on the selected server, as in figure 12-8. This list only shows the printers that you have permission to use.
- Step 4. Select a printer and press **Enter**. Your selections for server and printer number are automatically transferred to the Change Printer Mapping panel.
- Step 5. Press **Enter** or **F9** to establish the mapping.

SUMMARY: The **Printer Mappings** selection on the Main Menu displays your current printer mappings. It also lets you disconnect your existing printer mappings and establish new printer mappings. When you establish a new printer mapping, you can browse the network and create the network path by selecting from menus.

Print Stream Truncation

When you send a file to a network printer, it is not sent directly to the printer. Instead, the print spooler temporarily saves the file on the server's disk. Printing does not begin until the entire file has been transferred to the server. The print spooler waits for an *end-of-file message* before starting the printing.

Some DOS applications do not send an end-of-file message. If you try to print a file from such an application, Invisible LAN waits for more information and never prints the file. The file remains in the print spooler. If this happens, you must truncate the print stream. *Truncating the print stream* means telling the print spooler that it has received a complete file and should begin the printing.

When automatic print stream truncation is enabled, Invisible LAN automatically truncates the print stream whenever there is no printer activity for the period of time specified. The use of the **TRUNCATE** command to control print stream truncation was described in chapter 4. Now we explain how to perform the same functions using the network manager.

To display or change the truncation time, select **Automatic Print Stream Truncation** from the Main Menu. The display shows a data panel similar to figure 13-1.

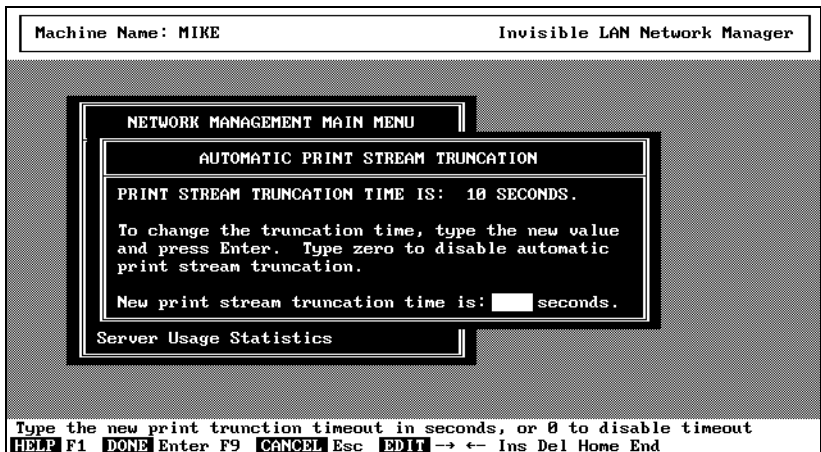


Figure 13-1. Automatic Print Stream Truncation Panel

The current status is displayed in the first line of the panel. If enabled, it gives the current time setting in seconds.

- To enable the automatic print stream truncation, type in a non-zero number and press **Enter**.
- To disable the automatic print stream truncation, type in zero and press **Enter**.
- To leave the setting unchanged, press **Esc** to exit from the panel.

These functions can be performed both locally and remotely.

SUMMARY: The **Automatic Print Stream Truncation** item on the manager's Main Menu lets you display and change the automatic print stream truncation setting.

Managing Printers

This chapter describes how to use the network manager program (**MENU**) to manage a server's printers. Some of these functions can also be performed from the DOS command line, using the **PQ** command (see chapter 4). However, **MENU** provides more extensive management capabilities than **PQ**, and **MENU** has the ability to manage printers by "remote control."

The topics covered are:

- Displaying Print Spooler status
- Changing Print Spooler settings
- Displaying Print Queue Contents
- Changing Print Queue Contents

Displaying Print Spooler Status

The *print spooler* is the program that receives print jobs from network users and sends them to the server's printer. If you select **Print Spooler Status** from the manager's Main Menu, you see a status display similar to figure 14-1.

The panel shows the following information:

- **Print spooler state**—active or paused. When active, the print spooler can send data to the printer. When paused, the print spooler cannot send data to the printer.
- **Number of files in the print queue**—This is the number of temporary files on your disk that are waiting to be printed.
- **Form-feed setting**—Yes or No. If yes, a form feed command is added at the end of each print job. A *form-feed command* tells the printer to advance the paper, so that the next print job begins at the top of a page.
- **Printer used by the print spooler**—LPT1, LPT2, LPT3, COM1, or COM2.
- **Flow control method**—PARALLEL, DTR, or XON/XOFF. For a parallel printer (LPT1, LPT2, or LPT3), the flow control method is always PARALLEL. For a serial printer (COM1 or COM2), the flow control

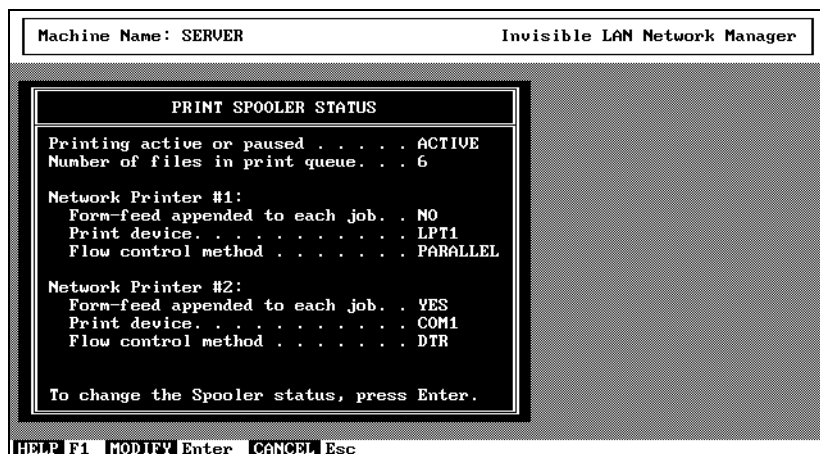


Figure 14-1. Typical Print Spooler Status Panel

method can be either DTR (for *Data Terminal Ready*) or XON/XOFF (for *Transmit-On/Transmit-Off* or *Xon/Xoff*).

SUMMARY: The Print Spooler Status Panel displays the current settings of the print spooler program.

Changing Print Spooler Settings

To change the settings of the print spooler, select **Print Spooler Status** from the manager's Main Menu, and then press **Enter**. An *Action Menu* appears as shown in figure 14-2.

All the print spooler settings can be changed from the Action Menu. The following sections describe how.

Setting the Print Spooler State

The print spooler has two possible states: *active* and *paused*.

When the print spooler is *active*, it can send data to the printer. Temporary files stored on your disk are sent to the printer one-by-one.

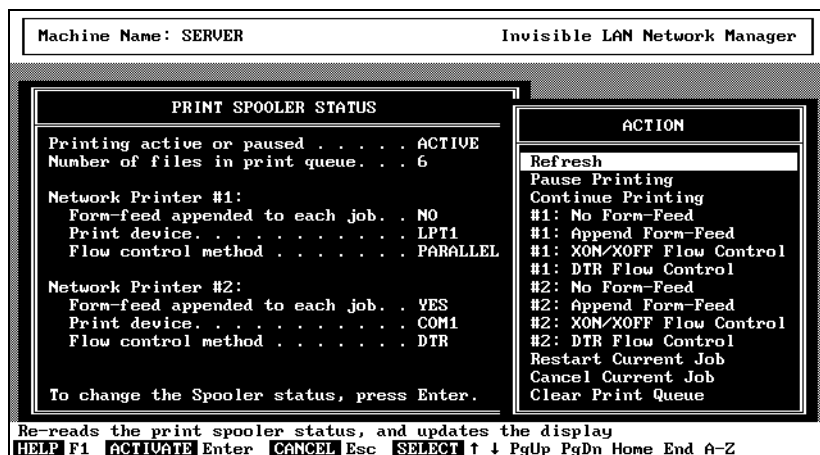


Figure 14-2. Print Spooler Action Menu

When the print spooler is *paused*, it cannot send data to the printer. Temporary files stored on your disk stay there until the print spooler goes back to the active state. Other computers can still send files to the print spooler; these files are stored on your disk, where they wait for the print spooler to become active.

To set the print spooler to the paused state, select **Pause Printing** from the Action menu. To return to the active state, select **Continue Printing** from the Action Menu.

Controlling Form Feeds

The print spooler prints a series of jobs, one after the other. The print spooler usually sends a *form-feed command* to the printer at the end of each job. The form-feed command tells the printer to advance the paper, so that the next print job will begin at the top of a page.

Two situations in which you may not want the print spooler to send form-feed commands to the printer are when:

- Using a PostScript printer.
- Printing from within a word processor or other application program that already adds a form-feed command at the end of each document.

Using the Action Menu, you can turn the form-feed option on and off. To disable the form-feed option, select **No Form-Feed**. To enable the form-feed option, select **Append Form-Feed**. If you have two network printers, the

option can be set separately for each printer.

Note — With the Invisible LAN Setup program (**SETUP30**), you can specify the initial form-feed setting that is in effect when you start Invisible LAN. Refer to the *Installation* manual for details.

Flow Control

There are two different ways to control the flow of data from the computer to a serial printer: *DTR flow control* and *Xon/Xoff flow control*. (DTR stands for *Data Terminal Ready*. Xon/Xoff stands for *Transmit On/Transmit Off*.)

It is outside the scope of this manual to explain the technical differences between DTR and Xon/Xoff flow control. You do need to know which method is used in your printer. Most printers use DTR.

Using the Action Menu, you can change the flow control method. To use Xon/Xoff flow control, select **Xon/Xoff Flow Control**. To use DTR flow control, select **DTR Flow Control**. If you have two network printers, the flow control method can be set separately for each printer.

Note — With the Invisible LAN Setup program (**SETUP30**), you can specify the initial flow control setting that is in effect when you start Invisible LAN. Refer to the *Installation* manual for details.

Printer Control

There are three options on the Action Menu that let you control the printer:

- **Restart Current Job** restarts the current print job from the beginning.
- **Cancel Current Job** cancels the print job that is currently printing. Printing continues with the next job in the print queue.
- **Clear Print Queue** cancels all the jobs in the print queue. Printing does not continue until the print spooler receives a new print job.

Note — If you want to selectively delete individual jobs from the print queue, you can do so with the Print Queue Action Menu, described later in this chapter.

SUMMARY: The Print Spooler Action Menu lets you set the print spooler state, select form-feed and flow control options, and control the printer.

Displaying Print Queue Contents

To display the print queue contents, choose **Print Queue Contents** from the Main Menu. The display shows a list of all the files in the print queue, as in figure 14-3.

Machine Name: SERVER				Invisible LAN Network Manager			
PRINT QUEUE CONTENTS							
P	MIKE	67165	8-24-92	00:01	#1	[Write - SYSINI.WRI]	
Q	VINCENT	10252	8-24-92	00:03	#2	[HARDWARE.TXT]	
Q	VINCENT	65039	8-24-92	00:04	#2	[NETINI.TXT]	
Q	MIKE	12841	8-24-92	00:08	#1	[Paintbrush - ZIGZAG.>	
Q	MIKE	5888	8-24-92	00:10	#2		
H	MIKE	64155	8-24-92	00:11	#1	[README.TXT]	
HELP F1 ACTIVATE Enter CANCEL Esc SELECT ↑ ↓ PgUp PgDn Home End A-Z							

Figure 14-3. Typical Print Queue Contents Display

For each file, the following information is displayed:

- The print job status. The status is shown as a single letter: **P** if the job is currently printing, **Q** if the job is queued (i.e., ready to print and waiting for the printer to become available), or **H** if the job is on hold.
- The name of the user who submitted the print job.
- The size of the file, in bytes.
- The date and time that the print job was submitted.
- The destination printer number (#1 or #2).
- The print job title. If the print job was submitted by the **NETPRINT** program, the print job title is the name of the file. If the print job was submitted from Microsoft Windows, then the job title is assigned by the Windows application.

SUMMARY: You can use the **Print Queue Contents** function on the manager's Main Menu to display the contents of the print queue for a local or remote printer.

Changing Print Queue Contents

You can change the print queue once it is displayed. You can rearrange files in the queue, so that more important files are printed first. You can also delete individual files from the queue, and place individual files on hold.

To change the print queue, simply select a file from the displayed list, and press Enter. An *Action Menu* appears, as shown in figure 14-4.

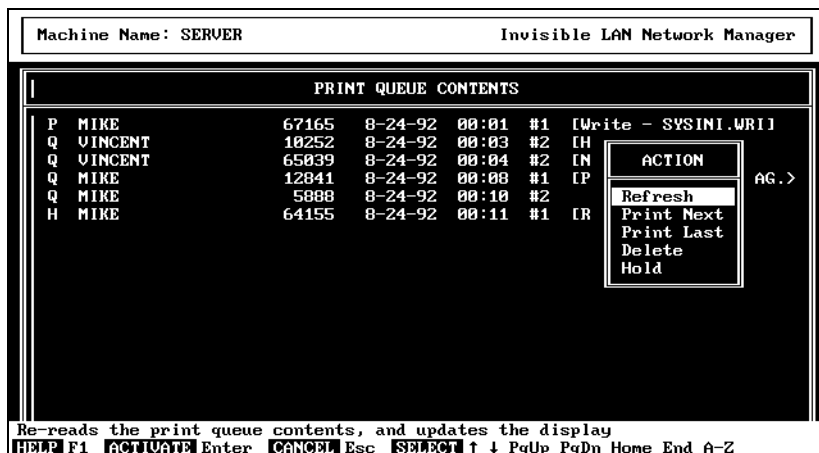


Figure 14-4. Print Queue Action Menu

From the Action Menu, you can perform the following five operations:

- Choose **Refresh** to update the print queue contents display.
- Choose **Print Next** to move the selected file to the front of the queue, so the selected file will be the next file to print. If the selected file is on hold, it is released from hold. If the file is currently printing, it is interrupted and started over again from the beginning.
- Choose **Print Last** to move the selected file to the end of the queue, so the selected file will be the last file to print. If the selected file is on hold,

it is released from hold. If the file is currently printing, it is interrupted; the next time the file prints, printing starts over from the beginning.

- Choose **Delete** to delete the selected file from the queue. If the selected file is currently printing, it is interrupted.
- Choose **Hold** to place the selected file on hold. When the file is on hold, it remains in the queue but does not print until you manually release the file from hold (with **Print Next** or **Print Last**). If the selected file is currently printing, it is interrupted; when you release the file from hold, printing starts over from the beginning.

SUMMARY: You can use the Print Queue Action Menu to rearrange the files in the print queue, delete individual files from the print queue, and place print jobs on hold.

Security

Invisible LAN supports a full security system. Security is optional. If you're not interested in security, you can ignore the security system.

With the security system, you can define both users and groups. A *user* is an individual, who can optionally have a *password* to verify his or her identity. A *group* is an arbitrary set of users. Groups provide a convenient way to grant permissions to many users at once. (Also, in the bulletin board system, groups are a convenient way to send a message to many users at once.)

You also use the security system to define shortnames. A *shortname* is a name that represents a directory on the server's disk. The shortname has *access rights* that specify what types of operations are allowed; for example, read-only or execute-only.

The security system lets you specify which users and groups are allowed to use each shortname. It also lets you specify which users and groups are permitted access to other resources, such as network printers and the bulletin board system.

This chapter describes the security system. It includes the following topics:

- Security objects and bindings
- Users
- Groups
- Shortnames
- Miscellaneous functions
- Saving and resetting security
- Security example

Security Objects and Bindings

The Invisible LAN security system is based on two concepts: *objects* and *bindings*. An *object* is an entity that is under the control of the server. There are four types of objects:

- **User** — An individual at an Invisible LAN workstation. A user can optionally have a *password* that serves to verify the user's identity. In addition, a user may optionally have a *comment*.
- **Group** — A collection of users. You specify which users belong to the group. A group may optionally have a *comment*.
- **Shortname** — A name that refers to a directory on the server's disk. A shortname has *access rights* that define what types of operations users can perform in the directory (for example, read-only).
- **Miscellaneous function** — A network printer or other network resource that is located on the server.

A *binding* is a relationship between two objects. There are five types of bindings:

- A user can be a member of a group.
- A user can have permission to use a shortname. This allows the user to access the directory to which the shortname refers, subject to the shortname's access rights.
- A group can have permission to use a shortname. This allows every member of the group to access the directory to which the shortname refers, subject to the shortname's access rights.
- A user can have permission to perform a miscellaneous function. This allows the user to use the resource or perform the function.
- A group can have permission to perform a miscellaneous function. This allows every member of the group to use the resource or perform the function.

Object and bindings are summarized in tables 15-1 and 15-2.

SUMMARY: There are four types of *objects* in the Invisible LAN security system: *users*, *groups*, *shortnames*, and *miscellaneous functions*. These objects are related by *bindings*. The five types of binding are: user's membership in a group; user's permission to use shortname; group's permission to use shortname; user's permission to use miscellaneous function; group's permission to use miscellaneous function.

Table 15-1. Security Objects

Object	Description	Attributes
User	Individual	Name, Password (optional), Comment (optional)
Group	Collection of users	Name, Comment (optional)
Shortname	Name that refers to a drive and directory on server's disk	Name, Definition, Access rights
Miscellaneous function	Network printer or other resource	None

Table 15-2. Security Bindings

Binding	Meaning
User — Group	User is a member of the group
User — Shortname	User has permission to use the directory to which the shortname refers
Group — Shortname	Every member of group has permission to use the directory to which the shortname refers
User — Miscellaneous function	User has permission to use the network resource
Group — Miscellaneous function	Every member of group has permission to use the network resource

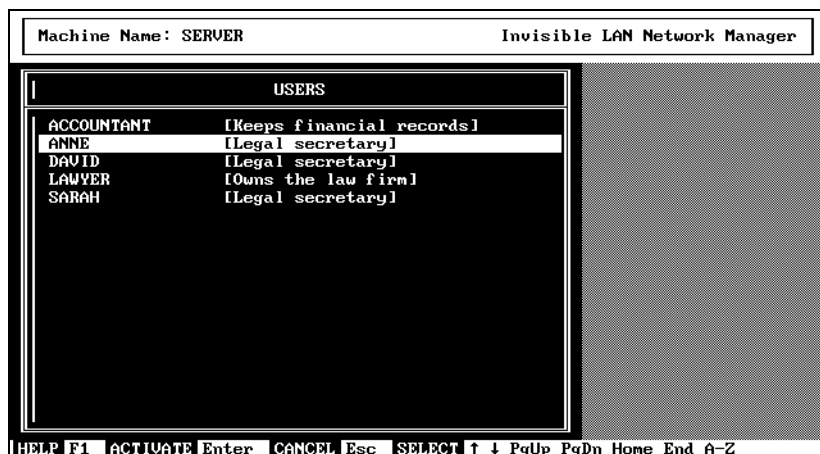


Figure 15-1. User Definitions Panel

Users

A *user* is an individual working at an Invisible LAN workstation. The server keeps a list of all known users. For each user, the server records the user's name, password, and a comment. The password and comment are optional, but every user is required to have a name.

Displaying Users

To display users, choose **User Definitions and Security** on the Main Menu. A list of users appears, as shown in figure 15-1.

For each user, Invisible LAN displays:

- The user name.
- The user comment, if any.

Creating Users

Before you can give a user permission to use network disks, printers, and other resources, you must add the user to the list of known users. This is called

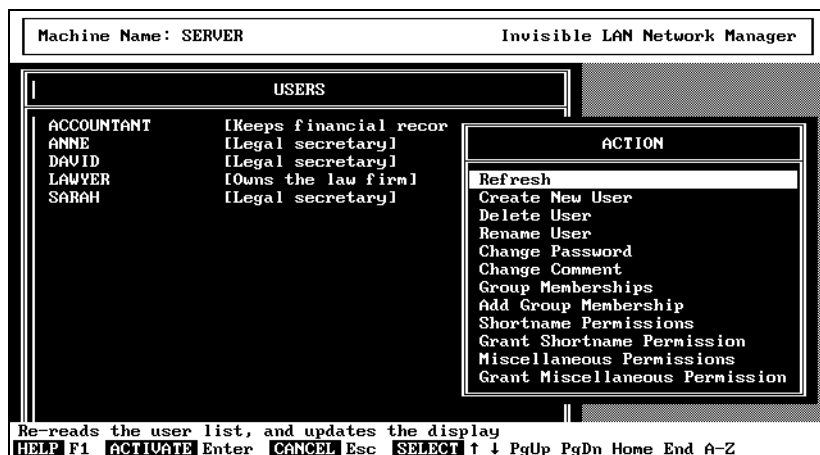


Figure 15-2. User Action Menu

“creating a user.”

To create a user, first display the list of users as described above. Press **Enter** to bring up the Action Menu as shown in figure 15-2. Choose **Create New User**, and then enter the user name, password, and comment.

A newly created user is automatically a member of the group named EVERY-ONE. The new user has no other group memberships or security permissions.

Changing User Definitions

You can change a user’s name, password, and/or comment.

To change a user definition, select a user from the list of users, and press **Enter** to bring up the Action Menu shown in figure 15-2.

- To change the selected user’s name, choose **Rename User** on the Action Menu.
- To change the selected user’s password, choose **Change Password** on the Action Menu.
- To change the selected user’s comment, choose **Change Comment** on the Action Menu.

When you change a user definition, the user retains all its group memberships and security permissions.

Deleting Users

To delete a user, select a user from the list of users, and then choose **Delete User** from the Action Menu.

SUMMARY: A *user* is an individual at an Invisible LAN workstation. A user has a name, an optional password, and an optional comment. The **User Definitions and Security** item on the Main Menu lets you display, create, change, and delete users.

Groups

A *group* is a collection of users. Invisible LAN automatically creates a group called EVERYONE, and automatically makes all users members of EVERYONE. When you create your own groups, you can specify which users are members of the group.

The server keeps a list of all known groups. For each group, the server records the group's name and a comment. The comment is optional, but every group is required to have a name.



Figure 15-3. Group Definitions Panel

Displaying Groups

To display groups, choose **Group Definitions and Security** on the Main Menu. A list of groups appears, as shown in figure 15-3.

For each group, Invisible LAN displays:

- The group name.
- The group comment, if any.

Creating Groups

Before you can give a group permission to use network disks, printers, and other resources, you must add the group to the list of known groups. This is called “creating a group.”

To create a group, first display the list of groups as described above. Press **Enter** to bring up the Action Menu as shown in figure 15-4. Choose **Create New Group**, and then enter the group name and comment.

A newly created group has no members and no security permissions.



Figure 15-4. Group Action Menu

Changing Group Definitions

You can change a group's name and/or comment.

To change a group definition, select a group from the list of groups, and press **Enter** to bring up the Action Menu shown in figure 15-4.

- To change the selected group's name, choose **Rename Group** on the Action Menu.
- To change the selected group's comment, choose **Change Comment** on the Action Menu.

When you change a group definition, the group retains all its members and security permissions.

Deleting Groups

To delete a group, select a group from the list of groups, and then choose **Delete Group** from the Action Menu.

Group Memberships

When you create a group, you specify which users are members of the group. There are two approaches to assigning group memberships. You can pick a particular group, and then specify which users are members of the group. Or, you can pick a particular user, and then specify which groups the user belongs to. Both methods are described below.

Assigning Members to a Particular Group

To display or change the members of a particular group, proceed as follows:

- Step 1. Display the list of groups by choosing **Group Definitions and Security** on the Main Menu.
- Step 2. Select a group from the list, and press **Enter** to bring up the Action Menu shown in figure 15-4.

You can now perform the following operations:

- To display a list of the users in the selected group, choose **Users in Group** from the Action Menu.

- To remove a user from the selected group, first display the list of users in the group, then choose the user you want to remove and press **Enter**.
- To display a list of the users *not* in the selected group, choose **Add User To Group** from the Action Menu.
- To add a user to the selected group, first display the list of users *not* in the group, then choose the user you want to add and press **Enter**.

Assigning Group Memberships to a Particular User

To display or change the group memberships of a particular user:

- Step 1. Display the list of users by choosing **User Definitions and Security** on the Main Menu.
- Step 2. Select a user from the list, and press **Enter** to bring up the Action Menu shown in figure 15-2.

You can now perform the following operations:

- To display a list of the groups that include the selected user, choose **Group Memberships** from the Action Menu.
- To remove the selected user from a group, first display the list of groups that include the selected user, then choose the group and press **Enter**.
- To display a list of the groups that do *not* include the selected user, choose **Add Group Membership** from the Action Menu.
- To add the selected user to a group, first display the list of groups that do *not* include the selected user, then choose the group and press **Enter**.

SUMMARY: A *group* is a collection of users. A group has a name and an optional comment. Groups are a convenient way to grant security permissions to many users at once. There is a predefined group called EVERYONE that contains all users. The **Group Definitions and Security** item on the Main Menu lets you display, create, change, and delete groups. When you create a group, you can specify which users are members of the group.

Shortnames

A *shortname* is an abbreviation that stands for a particular directory on the server's disk. For example, LETTERS could refer to the directory C:\WORDPROC\LTTRS on the server's disk.

You use the network manager to create a shortname. Once the shortname is created, you can use the shortname when you establish a drive mapping. You can think of the shortname as being the *network name* of the directory, because network users can access the directory by using the shortname.

The advantages to using shortnames include:

- Users don't have to know the server's drive letter and path; they simply use the shortname.
- The server's directory structure can be changed without affecting users, provided the shortname is redefined to refer to the new directory name.
- A shortname has *access rights* that specify what types of operations users can perform when using the shortname.
- You can control access to a shortname (and the directory to which it refers) with the security system.

Access Rights

Every shortname has a set of *access rights*. The access rights specify what types of operations users can perform when using the shortname. There are six different access rights as shown in table 15-3.

Table 15-3. Shortname Access Rights

<i>Access Right</i>	<i>Meaning</i>
READ ACCESS	Users can read files.
WRITE ACCESS	Users can modify existing files.
CREATE ACCESS	Users can create new files, delete files, rename files, change file attributes, make subdirectories, and remove subdirectories.
LIST ACCESS	Users can list the contents of the directory.
EXECUTE ACCESS	Users can execute DOS program files.
SHARING ACCESS	Users can share files normally.

A shortname can have any combination of the six access rights. For example, if a shortname has READ+LIST+EXECUTE+SHARING ACCESS, then users can read files, list the directory, and execute program files, but they cannot modify existing files or create new files.

Example 1 — A shortname with READ+WRITE+CREATE+LIST+EXECUTE+SHARING ACCESS allows users unlimited access to the directory. Users can perform any desired operation when using the shortname. This is the default set of access rights.

Example 2 — A shortname with READ+LIST+EXECUTE+SHARING ACCESS allows read-only access to the directory. Users can perform any operation that involves reading from the directory, but they cannot modify the contents of the directory in any way.

Example 3 — A shortname with LIST+EXECUTE+SHARING ACCESS allows execute-only access to the directory. Users can execute any programs in the directory, but they cannot copy the program files.

Example 4 — A shortname with READ+WRITE+SHARING ACCESS lets a user read or modify any file in the directory, provided the user knows the name of the file. Since the user cannot list the directory, the user cannot discover the names of other files in the directory.

Note — When you create a shortname, you should always give it SHARING access, so that Invisible LAN will enforce the normal rules for sharing files. The only exception is if you are running software designed for Novell Netware

that requires “Novell shareable” files. In this case, you can turn off SHARING access to simulate “Novell shareable.”

Note — When a shortname has SHARING access, Invisible LAN enforces the normal DOS rules for sharing files. This means that if two users attempt to use the same file at the same time, one of them will get a Sharing Violation message, unless they are running multi-user software that is designed to allow simultaneous access to the same file. When you turn off SHARING access, Invisible LAN allows multiple users to access the same file at the same time, even if they are running single-user software that would normally cause a Sharing Violation.

Note — EXECUTE access applies only to the execution of DOS programs. In order to execute Windows programs, you need to have READ access.

Displaying Shortnames

To display shortnames, choose **Shortname Definitions and Security** on the Main Menu. A list of shortnames appears, as shown in figure 15-5.

For each shortname, Invisible LAN displays:

- The shortname name.
- The shortname access rights: R, W, C, L, E, and/or S (for READ, WRITE, CREATE, LIST, EXECUTE, and SHARING).
- The disk directory to which the shortname refers.

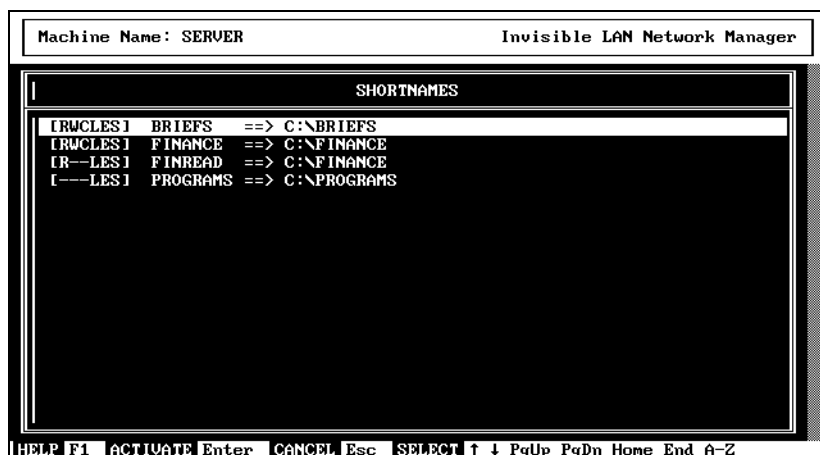


Figure 15-5. Shortname Definitions Panel

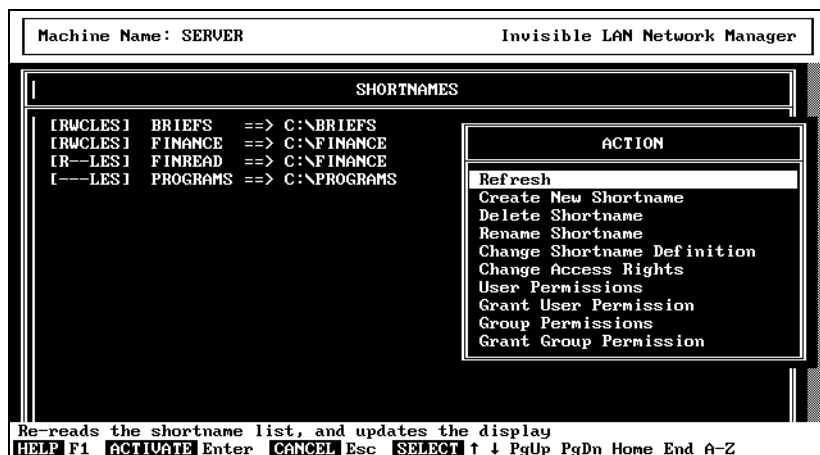


Figure 15-6. Shortname Action Menu

Creating Shortnames

To create a new shortname, first display the list of shortnames as described above. Press **Enter** to bring up the Action Menu shown in figure 15-6. Choose **Create New Shortname** from the Action Menu, and then enter the shortname's name, the disk directory to which the shortname refers, and the shortname's access rights.

When you create a new shortname, the group named **EVERYONE** is automatically given permission to use it. A newly created shortname has no other security permissions aside from **EVERYONE**.

Changing Shortname Definitions

You can change a shortname's name, disk directory, and/or access rights.

To change a shortname definition, select a shortname from the list of shortnames, and press **Enter** to bring up the Action Menu as in figure 15-6.

- To change the selected shortname's name, choose **Rename Shortname** on the Action Menu.
- To change the selected shortname's disk directory, choose **Change Shortname Definition** on the Action Menu.
- To change the selected shortname's access rights, choose **Change Access Rights** on the Action Menu.

When you change a shortname definition, the shortname retains all its security permissions.

Deleting Shortnames

To delete a shortname, select a shortname from the list of shortnames, and then choose **Delete Shortname** from the Action Menu.

Shortname Permissions

When you create a shortname, the group **EVERYONE** is automatically given permission to use it. This means that anyone on the network can use the shortname.

If you want to restrict access to the shortname, you must specify which users and groups have permission to use the shortname.

There are two approaches to assigning shortname permissions. You can pick a particular shortname, and then specify which users and groups are permitted to use it. Or, you can pick a particular user or group, and then specify which shortnames the user or group has permission to use. Both methods are described below.

Permissions For a Particular Shortname

To display or change the list of users or groups with permission to use a particular shortname, proceed as follows:

- Step 1. Display the list of shortnames by choosing **Shortname Definitions and Security** on the Main Menu.
- Step 2. Select a shortname from the list, and press **Enter** to bring up the Action Menu shown in figure 15-6.

You can now perform the following operations:

- To display a list of the users or groups who have permission to use the selected shortname, choose **User Permissions** or **Group Permissions** from the Action Menu.
- To deny permission for a user or group to use the selected shortname, first display the list of users or groups who have permission to use the shortname. Then choose the user or group and press **Enter**.
- To display a list of the users or groups who do *not* have permission to use

the selected shortname, choose **Grant User Permission** or **Grant Group Permission** from the Action Menu.

- To give permission for a user or group to use the selected shortname, first display the list of users or groups who do *not* have permission to use the shortname. Then choose the user or group and press **Enter**.

Shortname Permissions For a Particular User or Group

To display or change the shortname permissions of a particular user or group, proceed as follows:

- Step 1. Display the list of users by choosing **User Definitions and Security** on the Main Menu. Or, display the list of groups by choosing **Group Definitions and Security** on the Main Menu.
- Step 2. Select a user or group from the list, and press **Enter** to bring up the Action Menu shown in figure 15-2 or 15-4.

You can now perform the following operations:

- To display a list of the shortnames that the selected user or group has permission to use, choose **Shortname Permissions** from the Action Menu.
- To deny permission for the selected user or group to use a shortname, first display the list of shortnames that the selected user or group has permission to use. Then choose the shortname and press **Enter**.
- To display a list of the shortnames that the selected user or group does *not* have permission to use, choose **Grant Shortname Permission** from the Action Menu.
- To grant permission for the selected user or group to use a shortname, first display the list of shortnames that the selected user or group does *not* have permission to use. Then choose the shortname and press **Enter**.

Using Shortnames

Shortnames can be used any time that you establish a drive mapping. From the DOS prompt, you use shortnames in the **MAP** and **MENU** programs. In the Invisible LAN Setup program, you use shortnames when specifying the initial drive mappings. All of these options are discussed in the following paragraphs.

Using Shortnames in the MAP Command

At the DOS prompt, you use the **MAP** command to establish drive and printer mappings. When establishing drive mappings, you may use a shortname as described below:

To use a shortname in a MAP command, type

```
MAP d: \\server\shortname[\path] [/W]
```

The parameters have the following meanings:

d:	The drive letter used to refer to the server's disk.
server	The network name of the server.
shortname	Specifies a drive and directory on the server. It must have been previously defined on the server, and you must be authorized to use it based on the security permissions granted by the server.
[\path]	A subdirectory path from the shortname directory. The \path is optional. If you omit \path, then you have access to the directory that the shortname refers to, including all subdirectories. If you include \path, then you have access only to that particular subdirectory (and its subdirectories).
/W	Indicates that MAP should wait for the server computer to boot up if it is not on the network. /W is optional. If /W is not included, then MAP terminates with an error message if the server computer is not on the network. /W is most often used when you have two servers, and each server wants to use the other's disk.

Example — Suppose that LETTERS is a shortname that refers to directory C:\WORDPROC\LTTRS on server MIKE's disk. To make your drive letter F: refer to this directory, type

```
MAP F: \\MIKE\LETTERS
```

Using Shortnames in the MENU program

The **MENU** program provides DOS users with a menu-driven interface for managing the network. To use a shortname in the **MENU** program, select **Drive Mappings** on the manager Main Menu. The screen displays the current drive mappings.

Select the drive letter to be mapped to the server's disk. The program prompts you for the necessary information. At the **Drive Or Shortname** prompt, enter the shortname.

Example — Suppose that **LETTERS** is a shortname that refers to directory C:\WORDPROC\LTTRS on server **MIKE**'s disk. To make your drive letter F: refer to this directory:

1. Choose **Drive Mappings** from the manager Main Menu.
2. Select drive letter F: from the list.
3. In response to the **Server's Name** prompt, enter **MIKE**.
4. In response to the **Drive Or Shortname** prompt, enter **LETTERS**.
5. In response to **Server's Path**, press **Enter**.

Your drive letter F: now refers to **MIKE**'s directory C:\WORDPROC\LTTRS.

Using Shortnames in the Setup Program

You can use the Invisible LAN Setup program to define initial drive mappings that are established automatically when you start Invisible LAN. The initial drive mappings are defined in the **Drive Mappings** section of **Advanced Configuration**.

When you specify the initial drive mappings, the Setup program prompts you to enter **Server's Name**, **Drive Or Shortname**, and **Server's Path**. At the **Drive Or Shortname** prompt, you may enter a shortname.

SUMMARY: A *shortname* is the network name of a disk directory on the server. Each shortname has a name, a definition (the name of the disk directory), and a set of access rights. The access rights define what types of operations users can perform in the disk directory: read, write, create, list, execute, and share. The **Shortname Definitions and Security** item on the Main Menu lets you display, create, change, and delete shortnames. You can define shortname permissions for users and groups. A shortname can be used any time you specify a network path for a drive mapping.

Miscellaneous Functions

A *miscellaneous function* is network printer or other resource that is under the server's control. Miscellaneous functions let you use the security system to control access to printers and other network resources.

All the miscellaneous functions are automatically pre-defined by Invisible LAN. You cannot create your own miscellaneous functions, and you cannot modify or delete the pre-defined miscellaneous functions.

Displaying Miscellaneous Functions

To display miscellaneous functions, choose **Miscellaneous Security** on the Main Menu. A list of miscellaneous functions appears, as shown in figure 15-7.

Invisible LAN displays the name or description of each miscellaneous function. The functions control access to disks, printers, security, server monitoring, and the bulletin board. All five types of functions are described in the following paragraphs.

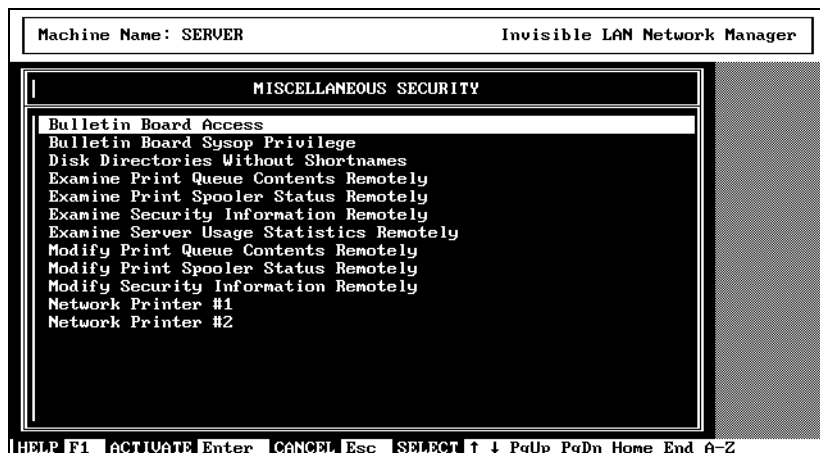


Figure 15-7. Miscellaneous Security Panel

Controlling Access to Disks

When you establish a drive mapping, you have the option of using either a shortname or a disk directory. For example, you can use a network path like `\\SERVER\LETTERS` (using the shortname `LETTERS`), or like `\\SERVER\C:\WORDPROC\LTTTS` (where no shortname is used).

We have already seen how to assign security permissions to shortnames, so you can control who has access to each shortname. The following miscellaneous function lets you control who can establish drive mappings without using a shortname.

- **Disk Directories Without Shortnames** — Controls who can establish a drive mapping without using a shortname.

By default, the group `EVERYONE` has permission to perform this function. This allows everyone to have unlimited access to all the server's disk directories.

If you want to limit access to the server's disks, you must deny `EVERYONE` permission to use this function, and then use shortnames to specify who has access to which directories.

Controlling Access to Printers

There are six miscellaneous functions that control access to the network printers:

- **Network Printer #1** — Controls who can use network printer #1.
- **Network Printer #2** — Controls who can use network printer #2.
- **Examine Print Spooler Status Remotely** — Controls who can display the status of the print spooler from a remote workstation. (A user working locally at the server can always examine print spooler status.)
- **Modify Print Spooler Status Remotely** — Controls who can modify the status of the print spooler from a remote workstation. (A user working locally at the server can always modify print spooler status.)
- **Examine Print Queue Contents Remotely** — Controls who can display the list of files in the print queue from a remote workstation. (A user working locally at the server can always examine the print queue contents.)
- **Modify Print Queue Contents Remotely** — Controls who can rearrange and delete the files in the print queue from a remote workstation. (A user working locally at the server can always modify the print queue contents.)

By default, the group `EVERYONE` has permission to perform all these functions. This allows everyone to have unlimited access to network printers.

If you want to restrict access to the network printers, you must deny permission for **EVERYONE** to perform these functions, and then grant permissions to selected users and groups.

Controlling Access to Security

For the security system to remain secure, you must restrict who is allowed to update the security information. Otherwise, users could access any function simply by giving themselves permission!

Two miscellaneous functions let you control who can display and change security information:

- **Examine Security Information Remotely** — Controls who can display security information from a remote workstation. (A user working locally at the server can always examine security information.)
- **Modify Security Information Remotely** — Controls who can change the security information from a remote workstation. (A user working locally at the server can always modify security information.)

Security information includes user names, group names, shortname definitions, group memberships, shortname permissions for users and groups, and miscellaneous permissions for users and groups.

By default, the group **EVERYONE** has permission to perform both of these functions. This means that everyone has unrestricted ability to display and change the security information.

To have a secure system, you must restrict the ability to modify security information. You may also want to restrict the ability to examine security information. To do this, you must deny permission for **EVERYONE** to perform these functions, and then grant permission to selected users and groups.

If you don't grant anyone access to these functions, only a user working at the server can change the security system.

Controlling Access to Server Monitoring

One miscellaneous function lets you control who can monitor the usage of server resources:

- **Examine Server Usage Statistics Remotely** — Controls who can display server usage information from a remote workstation. (A user working locally at the server can always examine usage information.)

Server usage information includes the number of open files, number of record locks, amount of data read or written, amount of time the server has been running, disk cache statistics, audit trail, and list of logged-in users.

By default, the group **EVERYONE** has permission to perform this function. This means that everyone can display server usage statistics. If you want to restrict access to this function, you must deny permission to **EVERYONE**, and then grant permission to selected users and groups.

If you don't grant anyone access to this function, only a user working at the server can examine server usage statistics.

Controlling Access to the Bulletin Board

Every Invisible LAN server has a built-in bulletin board system. The bulletin board is both a store-and-forward mail system and also an electronic forum where users can exchange information and experiences.

Two miscellaneous functions let you control access to the bulletin board system:

- **Bulletin Board Access** — Controls who can send and receive messages on the bulletin board from a remote workstation. (A user working locally at the server can always send and receive messages on the bulletin board.)
- **Bulletin Board Sysop Privilege** — Controls who has sysop (SYStem OPerator) privilege when working at a remote workstation. (A user working locally at the server always has sysop privilege.) A user with sysop privilege can read all the messages on the bulletin board (including private messages), and perform administrative functions on the bulletin board.

By default, the group **EVERYONE** has permission for **Bulletin Board Access**. This means that anyone can send and receive messages on the bulletin board. If you want to restrict access to the bulletin board, you must deny permission to **EVERYONE**, and then grant permission to selected users and groups.

By default, no one has permission for **Bulletin Board Sysop Privilege**. This means that only a user working locally at the server has sysop privilege. If you want other users to have sysop privilege, you must grant the privilege to selected users and groups.

Miscellaneous Permissions

By default, the group **EVERYONE** has permission for all miscellaneous functions (except **Bulletin Board Sysop Privilege**). This means that anyone on the network can perform these functions.

If you want to restrict access to a miscellaneous function, you must specify which users and groups have permission to use the miscellaneous function.

There are two approaches to assigning miscellaneous permissions. You can pick a particular miscellaneous function, and then specify which users and groups are permitted to use it. Or, you can pick a particular user or group, and then specify which miscellaneous functions the user or group has permission to use. Both methods are described below.

Permissions For a Particular Miscellaneous Function

To display or change the list of users or groups with permission to use a particular miscellaneous function, proceed as follows:

- **Step 1.** Display the list of miscellaneous functions by choosing **Miscellaneous Security** on the Main Menu.
- **Step 2.** Select a miscellaneous function from the list, and press **Enter** to bring up the Action Menu shown in figure 15-8.

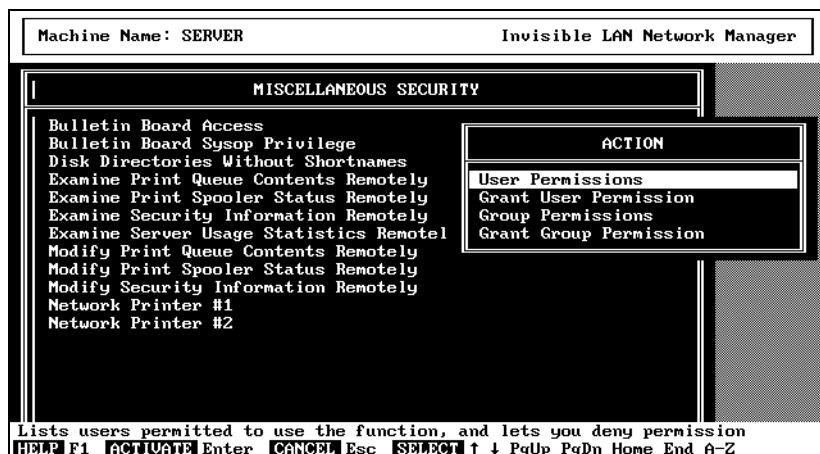


Figure 15-8. Miscellaneous Security Action Menu

You can now perform the following operations:

- To display a list of the users or groups who have permission to use the selected miscellaneous function, choose **User Permissions** or **Group Permissions** from the Action Menu.
- To deny permission for a user or group to use the selected miscellaneous function, first display the list of users or groups who have permission to use the miscellaneous function. Then choose the user or group and press **Enter**.

- To display a list of the users or groups who do *not* have permission to use the selected miscellaneous function, choose **Grant User Permission** or **Grant Group Permission** from the Action Menu.
- To give permission for a user or group to use the selected miscellaneous function, first display the list of users or groups who do *not* have permission to use the miscellaneous function. Then choose the user or group and press **Enter**.

Miscellaneous Permissions For a Particular User or Group

To display or change the miscellaneous permissions of a particular user or group, proceed as follows:

- Step 1. Display the list of users by choosing **User Definitions and Security** on the Main Menu. Or, display the list of groups by choosing **Group Definitions and Security** on the Main Menu.
- Step 2. Select a user or group from the list, and press **Enter** to bring up the Action Menu shown in figure 15-2 or 15-4.

You can now perform the following operations:

- To display a list of the miscellaneous functions that the selected user or group has permission to use, choose **Miscellaneous Permissions** from the Action Menu.
- To deny permission for the selected user or group to use a miscellaneous function, first display the list of miscellaneous functions that the selected user or group has permission to use. Then choose the miscellaneous function and press **Enter**.
- To display a list of the miscellaneous functions that the selected user or group does *not* have permission to use, choose **Grant Miscellaneous Permission** from the Action Menu.
- To grant permission for the selected user or group to use a miscellaneous function, first display the list of miscellaneous functions that the selected user or group does *not* have permission to use. Then choose the miscellaneous function and press **Enter**.

SUMMARY: A *miscellaneous function* is a network printer or other network resource. The **Miscellaneous Security** item on the Main Menu lets you display miscellaneous functions. You can define miscellaneous permissions for users and groups.

Saving and Resetting Security

The security system settings are stored on the server's disk in a file called BINDERY.DAT. BINDERY.DAT is located in the same directory where the Invisible LAN program files are located (usually C:\NET30).

To save the state of the security system, make a copy of BINDERY.DAT. You can restore the security system by re-booting the computer (press **Ctrl-Alt-Del**), restoring BINDERY.DAT from the copy, and then re-starting Invisible LAN.

To reset the security system back to the default state, you should re-boot the system and delete BINDERY.DAT. The next time you start the server, it will automatically create a new BINDERY.DAT with a default security system.

Note — BINDERY.DAT is a read-only file. To replace or delete it, you must use the DOS **ATTRIB** command to make the file read/write.

SUMMARY: The file BINDERY.DAT contains the information needed to save and restore the state of the security system.

Security Example

In this section, we give an extended example of a security system. We go through the entire process of creating a security system, step by step.

For our example, we use a hypothetical law firm. In our law firm, there are five computer users:

- **LAWYER**, the lawyer who owns the law firm.
- **ACCOUNTANT**, an accountant who handles all the firm's finances.
- **SARAH**, a legal secretary.
- **DAVID**, a legal secretary.
- **ANNE**, a legal secretary.

Every user has a computer that is connected to the network. In addition, there is a server on the network. All the files on the server's disk are organized into three directories:

- **C:\BRIEFS** contains legal briefs. We want **LAWYER** and all the legal secretaries to have access to this directory, but not **ACCOUNTANT**.

- C:\FINANCE contains the firm's financial records. We want ACCOUNTANT to have access to this directory. LAWYER also has access to this directory, but on a read-only basis. The legal secretaries do not have access to this directory.
- C:\PROGRAMS contains program files, such as word processors and spreadsheets. We want everyone to have access to this directory, but on an execute-only basis.

The server also has two printers:

- Printer #1 is a daisy-wheel printer used for printing letters and reports. We want everyone to have access to this printer.
- Printer #2 is a laser printer that is used for printing legal forms. We want only the legal secretaries to have access to this printer.

Finally, only LAWYER has permission to change the security settings.

We now go through the steps involved in setting up this security system, beginning from scratch with a default security system.

Step 1: Create the users.

First we create the five users in this network. This, and every other operation in this example, is done at the server.

- Select **User Definitions and Security** on the manager Main Menu.
- Press **Enter** to bring up the User Action Menu.
- Select **Create New User**.
- Enter the user name LAWYER. Optionally, you can also enter a password or comment. Press **Enter** or **F9** to complete the entry.
- Repeat the above steps to create users ACCOUNTANT, SARAH, DAVID, and ANNE.
- Press **Esc** to return to the Main Menu.

Step 2: Create a group.

All the legal secretaries have exactly the same security permissions. Therefore, we create a group named SECRETARIES. This way, we can give security permissions to all the secretaries as a group.

- Select **Group Definitions and Security** on the manager Main Menu.
- Press **Enter** to bring up the Group Action Menu.
- Select **Create New Group**.
- Enter the group name SECRETARIES. Optionally, you can also enter a

comment. Press **Enter** or **F9** to complete the entry.

- Select SECRETARIES from the Group Panel. The Group Action Menu appears again.
- Select **Add User To Group**. A list of users appears.
- Select SARAH from the list of users. When asked “Add User to Group?,” respond **Yes**.
- Select DAVID from the list of users. When asked “Add User to Group?,” respond **Yes**.
- Select ANNE from the list of users. When asked “Add User to Group?,” respond **Yes**.
- Press **Esc** several times to return to the Main Menu.

Step 3: Create the secured shortnames.

We need to create a shortname for each of the directories C:\BRIEFS, C:\FINANCE, and C:\PROGRAMS. In fact, we need two shortnames for the directory C:\FINANCE, because one user needs read/write access to this directory while another user needs read-only access to this directory.

- Select **Shortname Definitions and Security** on the manager Main Menu.
- Press **Enter** to bring up the Shortname Action Menu.
- Select **Create New Shortname**.
- For “shortname” enter BRIEFS. For “server’s drive” enter C. For “server’s path” enter \BRIEFS. Enter **Y** for all the access rights. Then press **Enter** or **F9** to complete the entry. This establishes BRIEFS as the shortname for directory C:\BRIEFS, with read/write access rights.
- Press **Enter** to bring up the Shortname Action Menu.
- Select **Create New Shortname**.
- For “shortname” enter FINANCE. For “server’s drive” enter C. For “server’s path” enter \FINANCE. Enter **Y** for all the access rights. Then press **Enter** or **F9** to complete the entry. This establishes FINANCE as the shortname for directory C:\FINANCE, with read/write access rights.
- Press **Enter** to bring up the Shortname Action Menu.
- Select **Create New Shortname**.
- For “shortname” enter FINREAD. For “server’s drive” enter C. For “server’s path” enter \FINANCE. Enter **Y** for “permit reading,” “permit directory listing,” and “permit execute.” Enter **N** for “permit writing” and “permit create/delete.” Then press **Enter** or **F9** to complete the entry. This establishes FINREAD as the shortname for directory C:\FINANCE, with

read-only access rights.

- Press **Enter** to bring up the Shortname Action Menu.
- Select **Create New Shortname**.
- For “shortname” enter PROGRAMS. For “server’s drive” enter C. For “server’s path” enter \PROGRAMS. Enter **Y** for “permit directory listing” and “permit execute.” Enter **N** for “permit reading,” “permit writing,” and “permit create/delete.” Then press **Enter** or **F9** to complete the entry. This establishes PROGRAMS as the shortname for directory C:\PROGRAMS, with execute-only access rights.

Step 4: Establish shortname permissions.

We now have four shortnames: BRIEFS, FINANCE, FINREAD, and PROGRAMS. When you created the shortnames, Invisible LAN automatically gave the group EVERYONE permission to use the shortnames. This is fine for PROGRAMS, because we want everyone to be able to use PROGRAMS. However, we definitely don’t want everyone to be able to use BRIEFS, FINANCE, and FINREAD. So we need to change the permissions for these shortnames.

- Still at the Shortnames Panel, select BRIEFS. The Shortname Action Menu reappears.
- Select **Group Permissions**. A list of groups appears.
- Select EVERYONE. When asked “Deny Permission to Group?,” answer **Yes**. Now the group EVERYONE does not have permission to use the shortname BRIEF.
- Press **Esc** to return to the Action Menu.
- Select **Grant Group Permission**. A list of groups appears.
- Select SECRETARIES. When asked “Grant Permission to Group?,” answer **Yes**. Now all the legal secretaries have permission to use the shortname BRIEF.
- Press **Esc** to return to the Action Menu.
- Select **Grant User Permission**. A list of users appears.
- Select LAWYER. When asked “Grant Permission to User?,” answer **Yes**. Now LAWYER has permission to use the shortname BRIEF.
- Press **Esc** twice to return to the Shortnames Panel.
- At the Shortnames Panel, select FINANCE. The Shortname Action Menu reappears.
- Select **Group Permissions**. A list of groups appears.
- Select EVERYONE. When asked “Deny Permission to Group?,” answer

Yes. Now the group **EVERYONE** does not have permission to use the shortname **FINANCE**.

- Press **Esc** to return to the Action Menu.
- Select **Grant User Permission**. A list of users appears.
- Select **ACCOUNTANT**. When asked “Grant Permission to User?,” answer **Yes**. Now **ACCOUNTANT** has permission to use the shortname **FINANCE**.
- Press **Esc** twice to return to the Shortnames Panel.
- At the Shortnames Panel, select **FINREAD**. The Shortname Action Menu reappears.
- Select **Group Permissions**. A list of groups appears.
- Select **EVERYONE**. When asked “Deny Permission to Group?,” answer **Yes**. Now the group **EVERYONE** does not have permission to use the shortname **FINREAD**.
- Press **Esc** to return to the Action Menu.
- Select **Grant User Permission**. A list of users appears.
- Select **LAWYER**. When asked “Grant Permission to User?,” answer **Yes**. Now **LAWYER** has permission to use the shortname **FINREAD**.
- Press **Esc** several times to return to the Main Menu.

Step 5: Restrict mappings to shortnames only.

We have now established the desired security permissions for all our shortnames. However, it is still possible for anyone to map directly into the server’s C: drive, and access any file. To prevent this, we must force everyone to use shortnames.

- Select **Miscellaneous Security** on the manager Main Menu.
- Select **Disk Directories Without Shortnames**. An Action Menu appears.
- Select **Group Permissions**. A list of groups appears.
- Select **EVERYONE**. When asked “Deny Permission to Group?,” answer **Yes**. Now nobody can establish drive mappings without using one of the shortnames.
- Press **Esc** twice to return to the Miscellaneous Security Panel.

Step 6: Establish printer permissions.

By default, the group **EVERYONE** has permission to use both network printers. This is fine for printer #1, since we want everyone to have access to

this printer. However, we want only the legal secretaries to have access to printer #2.

- Still at the Miscellaneous Security Panel, select **Network Printer #2**. An Action Menu appears.
- Select **Group Permissions**. A list of groups appears.
- Select **EVERYONE**. When asked “Deny Permission to Group?,” answer **Yes**. Now nobody can use printer #2.
- Press **Esc** to return to the Action Menu.
- Select **Grant Group Permission**. A list of groups appears.
- Select **SECRETARIES**. When asked “Grant Permission to Group?,” answer **Yes**. Now all the legal secretaries have permission to use printer #2.
- Press **Esc** twice to return to the Miscellaneous Security Panel.

Step 7: Restrict access to security functions.

By default, the group **EVERYONE** has permission to modify the security settings. We want to restrict access so that only **LAWYER** can modify the security settings.

- Still at the Miscellaneous Security Panel, select **Modify Security Information Remotely**. An Action Menu appears.
- Select **Group Permissions**. A list of groups appears.
- Select **EVERYONE**. When asked “Deny Permission to Group?,” answer **Yes**. Now nobody can modify the security settings, except a user working locally at the server.
- Press **Esc** to return to the Action Menu.
- Select **Grant User Permission**. A list of users appears.
- Select **LAWYER**. When asked “Grant Permission to User?,” answer **Yes**. Now only **LAWYER** (and anyone working locally at the server) has permission to modify the security settings.
- Press **Esc** several times to return to the Main Menu.

Now our security system is complete. At this point, the users can establish their drive and printer mappings.

LAWYER could use the following mappings:

```
MAP D: \\SERVER\PROGRAMS
MAP E: \\SERVER\BRIEFS
MAP F: \\SERVER\FINREAD
MAP LPT1 \\SERVER\1
```

ACCOUNTANT could use the following mappings:

```
MAP D: \\SERVER\PROGRAMS
MAP F: \\SERVER\FINANCE
MAP LPT1 \\SERVER\1
```

All of the legal secretaries could use these mappings:

```
MAP D: \\SERVER\PROGRAMS
MAP E: \\SERVER\BRIEFS
MAP LPT1 \\SERVER\1
MAP LPT2 \\SERVER\2
```

SUMMARY: This example demonstrates how to create users, groups, and shortnames. It shows how to establish permissions for users and groups to access shortnames. And finally, it shows how to establish permissions for users and groups to access network printers and security functions.

Server Usage Statistics

As the server operates, it constantly keeps track of a variety of network resources: file handles, record locks, logged-in users, and so forth. You can use the network manager (**MENU** program) to display statistics on the usage of server resources.

Server usage statistics are valuable for evaluating the server configuration. For example, if you find that the server is running out of file handles, you could reconfigure the server to allow a larger number of files.

To view the server usage statistics, select **Server Usage Statistics** on the main menu. The server usage menu appears, as shown in figure 16-1. From this menu, you can get information on:

- Server resources
- Disk cache statistics
- Active users
- Audit trail
- Ultra Server resources

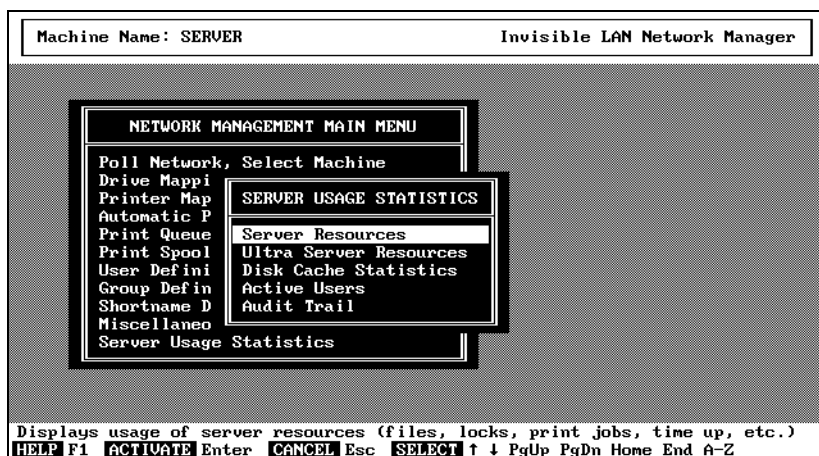


Figure 16-1. Server Usage Menu

Server Resources

Choose **Server Resources** to display the server usage panel, as shown in figure 16-2.

Machine Name: SERVER		Invisible LAN Network Manager	
SERVER USAGE			
Number of Users		Open Files	
Current:	2	Current:	2
Maximum:	3	Maximum:	50
Limit:	16	Limit:	800
		Record Locks	
		Current:	0
		Maximum:	0
		Limit:	800
Spool Files		Kilobytes I/O	
Current:	6	Read:	22489
Maximum:	6	Write:	9565
Limit:	200	Print:	274
		Time Up	
		Days:	0
		Hours:	6
		Minutes:	14
To refresh the server usage statistics, press Enter.			
HELP F1 MODIFY Enter CANCEL Esc			

Figure 16-2. Server Usage Display

The server usage panel shows information on the overall usage and configuration of server resources. The following items are displayed:

- **Current Users** — The number of users currently logged in to the server.
- **Maximum Users** — The maximum number of users that have been logged in to the server at any one time since the server was started.
- **Limit on Users** — The upper limit on the number of users that can be logged in to the server, as defined in the server's NET30.INI file.
- **Current Files** — The total number of network files that are currently open on the server.
- **Maximum Files** — The maximum number of network files that have been open at any one time since the server was started.
- **Limit on Files** — The upper limit on the number of network files that can be open at one time, as defined in the server's NET30.INI file.
- **Current Locks** — The total number of record locks that are currently in use on the server.

- **Maximum Locks** — The maximum number of record locks that have been in use at any one time since the server was started.
- **Limit on Locks** — The upper limit on the number of record locks that can be in use at one time, as defined in the server's NET30.INI file.
- **Current Spool Files** — The total number of print spool files that currently exist on the server. (This item is omitted if the server does not have a print spooler.)
- **Maximum Spool Files** — The maximum number of print spool files that have existed at any one time since the server was started. (This item is omitted if the server does not have a print spooler.)
- **Limit on Spool Files** — The upper limit on the number of print spool files that can exist at one time, as defined in the server's NET30.INI file. (This item is omitted if the server does not have a print spooler.)
- **Kilobytes Read** — The total amount of data that has been read from the server, in kilobytes.
- **Kilobytes Written** — The total amount of data that has been written to the server, in kilobytes.
- **Kilobytes Printed** — The total amount of data that has been spooled to the server's print spooler, in kilobytes. (This item is omitted if the server does not have a print spooler.)
- **Time Up** — The time that the server has been running, in days, hours, and minutes.

You may press **Enter** at any time to update the display.

The server usage statistics let you evaluate the server's configuration. The "maximums" are particularly valuable, because they let you anticipate and prevent problems before they occur. For example, suppose that **maximum files** shows 48, while **limit on files** shows 50. Then you know that you are very close to running out of files. You would probably want to reconfigure the server to allow more files, to ensure that you won't run out.

SUMMARY: The server usage panel displays information on the overall usage of server resources, such as users, files, and record locks. You can use it to evaluate the server configuration.

Disk Cache Statistics

If the Invisible LAN disk cache is running on the server, you can display the cache statistics. Choose **Disk Cache Statistics** on the server usage menu to display cache statistics, as shown in figure 16-3.

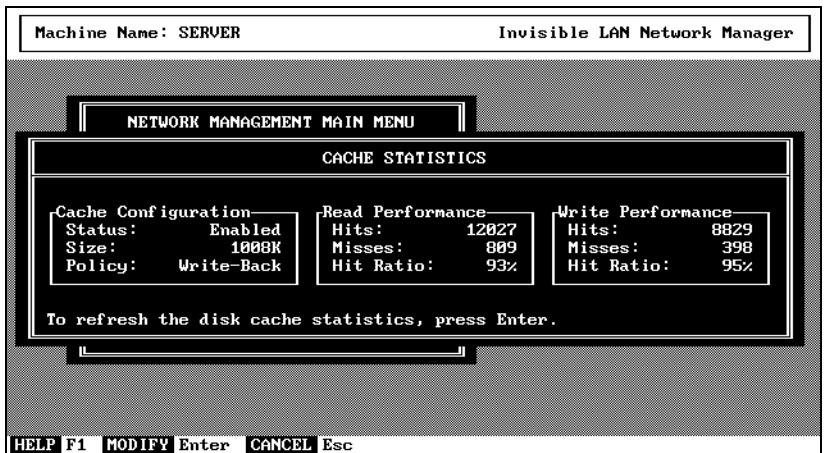


Figure 16-3. Disk Cache Statistics Display

The following items are displayed:

- **Cache Status** — Enabled or disabled.
- **Cache Size** — The actual size of the cache, in kilobytes. (The actual size of the cache may be slightly different than the size you specified in the NET30.INI file.)
- **Write Policy** — Write-through, write-back, or delayed-write. *Write-through* means that whenever DOS performs a disk write, it must wait until the data is physically written to the disk. *Write-back* and *delayed-write* both mean that disk writes are stored in the cache and then written to the disk at a later time, in background. The difference is that write-back begins the disk write as soon as possible, while delayed-write does not begin the disk write until several seconds later.
- **Read Hits** — The number of disk read operations that were satisfied by reading from the cache, instead of reading the hard disk.
- **Read Misses** — The number of disk read operations that required a read of the hard disk, because the requested data was not in the cache.

- **Read Hit Ratio** — The percentage of disk reads that were satisfied by reading from the cache, instead of reading the hard disk. The higher the number, the better the performance of the cache.
- **Write Hits** — The number of disk write operations that overwrote data which was already in the cache.
- **Write Misses** — The number of disk write operations that did not overwrite data already in the cache.
- **Write Hit Ratio** — The percentage of disk writes that overwrote data which was already in the cache. The higher the number, the better the performance of the cache.

You may press **Enter** at any time to update the display.

SUMMARY: The cache statistics panel displays information on the status and performance of the Invisible LAN disk cache.

Active Users

Choose **Active Users** on the server usage panel to display a list of users who are currently logged in to the server. The list shown is similar to figure 16-4.

Machine Name: SERVER

Invisible LAN Network Manager

ACTIVE USERS

User Name	Files	Max-F	Locks	Max-L
MIKE	0	1	0	0
VINCENT	2	50	0	0

To update the user list, press Enter.

HELP F1 MODIFY Enter CANCEL Esc

Figure 16-4. Active User Display

For each user in the list, Invisible LAN displays information about the user's usage of server resources. The following items are displayed:

- **Current Files** — The number of files that the selected user currently has open on the server.
- **Maximum Files** — The maximum number of files that the selected user has had open on the server at one time, since logging in to the server.
- **Current Locks** — The number of record locks that the selected user is currently using on the server.
- **Maximum Locks** — The maximum number of record locks that the selected user has had in use on the server at one time, since logging in to the server.

You may press **Enter** at any time to update the display.

SUMMARY: The active user panel lists the users that are currently logged in to the server, and displays each user's usage of network files and record locks.

Audit Trail

The *audit trail* is a disk file which contains a record of server activity. Each entry in the audit trail represents one of the following actions:

- The server was started.
- A drive mapping was established.
- A printer mapping was established.
- A file was opened.
- A print job was submitted.
- The bulletin board was accessed.

The use of an audit trail is optional. If you want the server to maintain an audit trail, you must configure the server so as to enable the audit trail. Refer to the *Installation* manual for instructions on configuring the server.

Machine Name: SERVER

Invisible LAN Network Manager

AUDIT TRAIL

▲	OPEN	MIKE	05-28-92	19:36:17	BBSNDX.DAT
	BBS	MIKE	05-28-92	19:36:17	
	OPEN	MIKE	05-28-92	18:59:50	FLOPPY.TXT
	D-MAP	MIKE	05-28-92	18:59:27	C:
	OPEN	VINCENT	05-28-92	18:57:06	README.TXT
	OPEN	VINCENT	05-28-92	18:57:06	BACKUP.COM
	PRINT	MIKE	05-28-92	18:55:30	
	PRINT	MIKE	05-28-92	18:55:06	
	P-MAP	MIKE	05-28-92	18:53:21	#1
	D-MAP	MIKE	05-28-92	18:52:58	PROGRAMS
	PRINT	VINCENT	05-28-92	18:51:53	
	PRINT	VINCENT	05-28-92	18:51:34	
	OPEN	VINCENT	05-28-92	18:50:58	README.TXT
	D-MAP	VINCENT	05-28-92	18:50:09	C:
	P-MAP	VINCENT	05-28-92	18:49:59	#2
	PRINT	MIKE	05-28-92	18:49:40	
▼	OPEN	VINCENT	05-28-92	18:47:39	XCOPY.EXE

HELP F1 MODIFY Enter CANCEL Esc SCROLL ↑ ↓ PgUp PgDn Home End

Figure 16-5. Audit Trail Display

Viewing the Audit Trail

To view the audit trail, choose **Audit Trail** on the server usage menu. Invisible LAN displays a panel listing the 150 most recent entries in the audit trail, as shown in figure 16-5. For each entry, the following information is displayed:

- The type of action (file open, print job, etc.)
- The name of the user who performed the action.
- The date and time at which the action occurred.
- The name of the file, printer, drive, or shortname that was accessed.

At any time, you can press **Enter** to bring up an action menu, as shown in figure 16-6. Choose **Refresh** from the action menu to re-read the server's audit trail and update the display.

Setting the Audit Filter

By default, the display shows all entries in the audit trail. In some cases, you will not be interested in all the entries. You can set an *audit filter* to specify which audit trail entries interest you. Once you set the filter, Invisible LAN only displays those audit trail entries that satisfy the conditions in the filter.

To set an audit trail filter, choose **Set Filter** on the action menu. This brings up the audit filter panel, as shown in figure 16-7. On this panel, you can

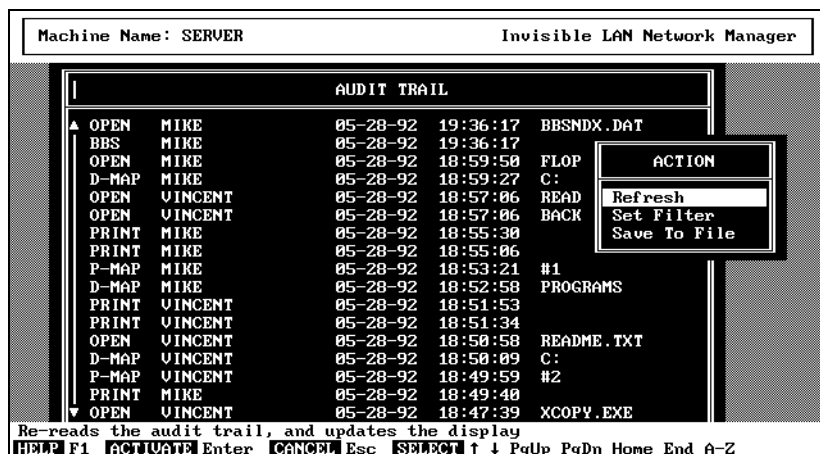


Figure 16-6. Audit Trail Action Menu

specify three different filters:

- *The types of operations to display.* With the six **Types of Operations** fields, you can select any combination of the six possible operations (server started, drive mapping, printer mapping, file open, print job submission, and bulletin board access). Put a **Y** in the field if you want Invisible LAN to display the corresponding operation.

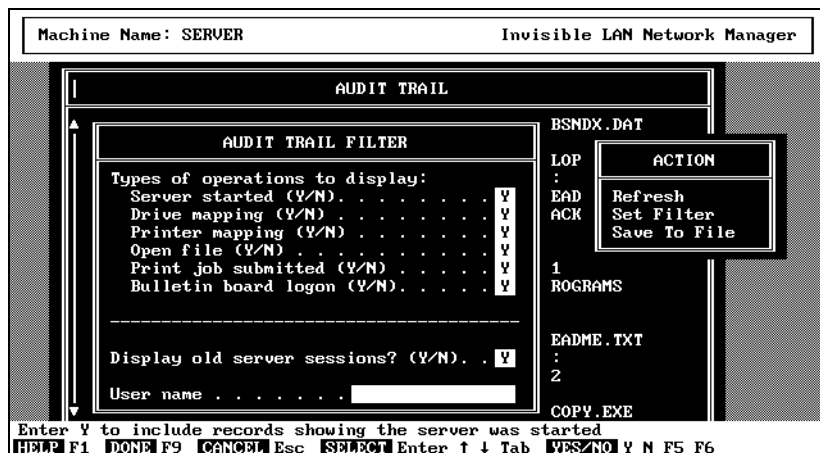


Figure 16-7. Audit Trail Filter Panel

- *Whether or not to display old server sessions.* Since the audit trail is stored in a file, it is possible to view audit trail entries from previous runs of the file server. Put an **Y** in the **Display Old Server Sessions** field if you want to view entries from previous server sessions.
- *A user name.* You can restrict the audit trail display to the actions of a particular user. Type a user name into the **User Name** field if you want to restrict the audit trail display to the specified user's actions. Leave the field empty to display the actions of all users.

After setting an audit filter, press **F9** to activate the new filter and return to the audit trail display. Only entries that satisfy your filter settings are displayed.

Press **Esc** if you want to exit the audit filter panel without changing the audit filter.

Saving the Audit Trail to a File

If you wish, you can save the audit trail to a file. This allows you to make a permanent record of the audit trail. It also lets you view all the entries in the audit trail. (The display only shows the 150 most recent entries, but when you save the audit trail to a file all the entries are saved, regardless of how many there are.)

Choose **Save to File** on the action menu if you want to save the audit trail to a file. Invisible LAN prompts you to enter the filename.

The audit trail is saved as an ASCII file. You can examine the file using any program that can display ASCII text files, such as a text editor. If you have set an audit filter, only entries that satisfy the filter are saved.

SUMMARY: The *audit trail* is a record of the activity on the server. You can display the contents of the audit trail, or save it to a file. You can also set an *audit filter* that tells Invisible LAN which audit trail entries you are interested in displaying or saving.

Ultra Server Resources

Ultra Server is the high-performance version of the Invisible LAN file server. It is intended mainly for dedicated servers. Ultra Server requires a 386 or 486 computer. It uses 32-bit code, multitasking, and extensive caching to operate at very high speed.

If you have installed Ultra Server, you can use the **Ultra Server Resources** menu item to display status information. For instructions on how to install the Ultra Server, refer to the *Getting Started* manual or the *Installation* manual.

When you install Ultra Server, it runs in parallel with the standard server. The Ultra Server usage panel only displays information on files handled by Ultra Server. Information on files handled by the standard server is displayed on the standard server usage panel.

Choose **Ultra Server Resources** to display the Ultra Server usage panel, as shown in figure 16-8.

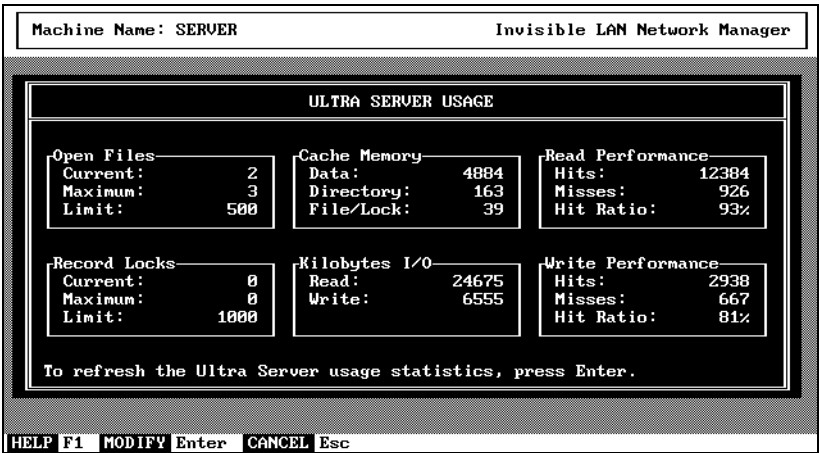


Figure 16-8. Ultra Server Usage Display

The Ultra Server usage panel shows information on the overall usage and configuration of Ultra Server resources. The following items are displayed:

- **Current Files** — The total number of network files that are currently open on Ultra Server.
- **Maximum Files** — The maximum number of network files that have been open at any one time since Ultra Server was started.

- **Limit on Files** — The upper limit on the number of network files that can be open at one time, as defined in the server's NET30.INI file.
- **Current Locks** — The total number of record locks that are currently in use on Ultra Server.
- **Maximum Locks** — The maximum number of record locks that have been in use at any one time since Ultra Server was started.
- **Limit on Locks** — The upper limit on the number of record locks that can be in use at one time, as defined in the server's NET30.INI file.
- **Data Memory** — The amount of extended and hyper-extended memory that Ultra Server uses to cache file data, in kilobytes.
- **Directory Memory** — The amount of extended and hyper-extended memory that Ultra Server uses to cache directory entries, in kilobytes.
- **File/Lock Memory** — The amount of extended and hyper-extended memory that Ultra Server uses for file handles and record locks, in kilobytes.
- **Kilobytes Read** — The total amount of data that has been read from Ultra Server, in kilobytes.
- **Kilobytes Written** — The total amount of data that has been written to Ultra Server, in kilobytes.
- **Read Hits** — The number of file read operations that were satisfied by reading from the cache, instead of reading the hard disk.
- **Read Misses** — The number of file read operations that required a read of the hard disk, because the requested data was not in the cache.
- **Read Hit Ratio** — The percentage of file reads that were satisfied by reading from the cache, instead of reading the hard disk. The higher the number, the better the performance of the cache.
- **Write Hits** — The number of file write operations that overwrote data which was already in the cache.
- **Write Misses** — The number of file write operations that did not overwrite data already in the cache.
- **Write Hit Ratio** — The percentage of file writes that overwrote data which was already in the cache. The higher the number, the better the performance of the cache.

You may press **Enter** at any time to update the display.

SUMMARY: The Ultra Server usage panel displays information on the overall usage of Ultra Server resources, such as files, record locks, and cache memory. It also displays information on the performance and usage of the cache. You can use it to evaluate the Ultra Server configuration.

Part 4

Appendices and Index

Invisible LAN

Command Reference

Establish one or more remote bridge connections on a remote host (this command is part of Invisible LAN Remote):

BRIDGE [*site_name*] [*site_name*] . . .

site_name Name of remote site

Disconnect one or more remote sites or clients on a remote host (this command is part of Invisible LAN Remote):

BRIDGE /D [*name*] [*name*] . . .

name Name of remote site or client

Display remote host connection status (this command is part of Invisible LAN Remote):

BRIDGE

Control the disk cache:

CACHE *parameters*

/F Flush cache

/N Disable and flush cache

/V Display cache status

/W=*policy* Write policy: write-through (0), write-back (1), or delayed-write (2)

/Y Enable cache

/Z Reset cache statistics to zero

Erase CMOS RAM on an AT-type computer, to reset the computer's configuration (this command is part of Invisible RAM):

CLRCMOS

Set up a dedicated file server:

DEDICATE

Hang up the telephone on a remote login client (this command is part of Invisible LAN Remote):

HANG_UP

Return to your original user name:

LOGOFF

Enter your user name and password:

LOGON

Load memory-resident program into shadow RAM (this command is part of Invisible RAM):

LSHADOW [*/A*] *filename* [*parameters*]

<i>/A</i>	Alter BIOS memory variable
<i>filename</i>	Name of program to load
<i>parameters</i>	Parameters for program being loaded

Create break page data file:

MAKEBP *infile: outfile*

<i>infile:</i>	Text file with break page description
<i>outfile</i>	Name of data file to create

Create boot diskette image file:

MAKEIMG *d:* *filename*

d: Source diskette drive (A: or B:)
filename Name of image file to create

Establish a drive mapping, using a drive and directory:

MAP *d:* *\\server\d:[\path]* [*/W*]

d: Local drive letter to use
server Name of the server computer
d: Server's drive letter
\path Optional directory path on server
/W Wait for server to be started

Establish a drive mapping, using a shortname:

MAP *d:* *\\server\shortname* [*\path*] [*/W*]

d: Local drive letter to use
server Name of the server computer
shortname Server's shortname
\path Optional subdirectory path on server
/W Wait for server to be started

Discontinue a drive mapping:

MAP *d:* /D

d: Local drive letter

Establish a printer mapping:

MAP LPT x \\server\[#] [/W]

LPTx	Local device name to use
server	Name of the server computer
#	Optional server's printer number (1 or 2)
/W	Wait for server to be started

Discontinue a printer mapping:

MAP LPT x /D

LPTx	Local device name
--------------------------	--------------------------

Display all current drive and printer mappings:

MAP

Start the Invisible LAN menu-driven network manager:

MENU [/B]

/B	Use black-and-white mode
-----------	---------------------------------

Start the Invisible LAN Operating System:

NET30 [init_file]

init_file	Name of initialization file
------------------	------------------------------------

Display the network address or serial number:

NETADDR /V

Check for a specified network address or serial number, return ERRORLEVEL 0 if match, ERRORLEVEL 1 if not, ERRORLEVEL 255 if error:

NETADDR *nnnn*

nnnn Network address or serial number

Get the date and time, and set the computer's clock:

NETCLOCK *\\server* [/W]

server Name of the server computer

/W Wait for server to be started

Start the network diagnostic program, which is used to test the network hardware:NETDIAG command

NETDIAG

Get help on a specified topic:

NETHELP *topic*

topic Subject on which help is desired

Print a file (works with network printers and local printers):

NETPRINT *filename* [LPTx] [/T]

filename Name of the file to print

LPTx Printer device name

/T Expand tabs to spaces

Network software control:

NW *option*

AUDIO	Enable use of the speaker
CONTINUE	Continue operation of the server
HIDE	Hide the network software
NOAUDIO	Disable use of the speaker
PAUSE	Temporarily stop the server
STATUS	Display network software status
UNHIDE	Make the network software visible

Enter your password:

PASSWORD *password*

password Your password

Prompt for password:

PASSWORD */P*

Control the server's print queue:

PQ *option*

CANCEL	Cancel the job currently being printed
CLEAR	Delete all jobs in the print queue
CONTINUE	Continue sending data to the printer
DIRECT	Enable direct printing
DTR [#]	Select DTR flow control (# = printer number)
FEED [#]	Enable form feeds (# = printer number)
HIGH	Set print priority to HIGH
LOW	Set print priority to LOW
MEDIUM	Set print priority to MEDIUM
NODIRECT	Disable direct printing
NOFEED [#]	Disable form feeds (# = printer number)
PAUSE	Temporarily stop sending data to the printer
RESTART	Restart the job currently being printed
STATUS	Display print queue status
XON [#]	Select Xon/Xoff flow control (# = printer number)

Immediately truncate the print stream:

PRINTNOW

Establish a set-up string for a network printer:

PSETUP LPTx=*hex_string*

LPTx **Network printer device name**

hex_string **String of printer control codes, in hexadecimal**

Stop using a set-up string for a network printer:

PSETUP LPTx=

LPTx **Network printer device name**

Display the set-up string for a network printer:

PSETUP LPTx

LPTx **Network printer device name**

Start the Invisible LAN Quick Setup program:

QSETUP [/B]

/B **Use black-and-white mode**

Start the remote bridge configuration program (this command is part of Invisible LAN Remote):

RBRIDGE [/B]

/B **Use black-and-white mode**

Start the modem configuration program (this command is part of Invisible LAN Remote):

RCONFIG [/B]

/B Use black-and-white mode

Display diagnostic information about the operation of the serial protocol (this command is part of Invisible LAN Remote):

RDIAG [/B]

Start the remote host security program (this command is part of Invisible LAN Remote):

RSECURE [/B]

/B Use black-and-white mode

Write a specified value to a specified I/O port:

SETPORT [*address*] [*value*]

address Address of I/O port in hexadecimal

value Value to write to I/O port in hexadecimal

Start the Invisible LAN Setup program:

SETUP30 [/B]

/B Use black-and-white mode

Display memory map information (this command is part of Invisible RAM):

SHADOW [*options*]

/A	All information
/C	Chips and Technologies chipset information
/D	DOS memory usage
/E	Extended memory information
/H	Table of expanded memory handles
/M	Memory map
/N	Network information for Invisible LAN
/S	Shadow RAM usage
/X	Expanded memory information

Enable automatic print stream truncation:

TRUNCATE *time*

time **Print stream truncate time, in seconds**

Disable automatic print stream truncation:

TRUNCATE /D

Display automatic print stream truncation setting:

TRUNCATE

Disconnect from Remote Program Load Server:

UNLINK

Unmount one or more drives controlled by Ultra Server, after closing all open files on the drives:

US DOWN [*d:*] . . .

[*d:*]... **Optional list of drive letters**

Mount one or more drives controlled by Ultra Server:

US MOUNT [*d:*] . . .

[*d:*]... Optional list of drive letters

Display Ultra Server status information:

US STATUS

Unmount one or more drives controlled by Ultra Server:

US UNMOUNT [*d:*] . . .

[*d:*]... Optional list of drive letters

Disable high-resolution VGA or EGA graphics and enable frontfill (this command is part of Invisible RAM):

VGAOFF

Enable high-resolution VGA or EGA graphics and disable frontfill (this command is part of Invisible RAM):

VGAON

Enable special processing for WINSTART.BAT under Windows:

WINSTR

Get help:

BRIDGE ?
CACHE ?
DEDICATE ?
LOGOFF ?
LOGON ?
LSHADOW ?
MAKEBP ?
MAKEIMG ?
MAP ?
NET30 ?
NETADDR ?
NETCLOCK ?
NETDIAG ?
NETHELP ?
NETPRINT ?
NW ?
PASSWORD ?
PQ ?
PRINTNOW ?
PSETUP ?
RDIAG ?
SETPORT ?
SHADOW ?
TRUNCATE ?
UNLINK ?
US ?
VGAOFF ?
VGAON ?
WINSTRT ?

Restricted DOS Commands

When the network software is installed, there are restrictions on the use of certain DOS commands. Usually, this is because the commands access the disk at the disk BIOS level. Table B-1 lists the restrictions.

Table B-1. Restricted DOS Commands

<i>DOS Command</i>	<i>Restrictions</i>
APPEND	Use APPEND <i>after</i> starting Invisible LAN. APPEND cannot be used before Invisible LAN is started. APPEND works on both local and network disks.
CHKDSK	You can only use CHKDSK on local disks. If you are a File Server, you cannot use CHKDSK on a local hard disk unless you use NW PAUSE.
DISKCOMP	You can only use DISKCOMP on local disks. On network disks, use COMP or FC instead of DISKCOMP.
DISKCOPY	You can only use DISKCOPY on local disks. On network disks, COPY or XCOPY instead.
FASTOPEN	Use FASTOPEN <i>before</i> starting Invisible LAN. FASTOPEN cannot be used after Invisible LAN is started. FASTOPEN only affects local disks.
FDISK	You can only use FDISK on local disks.
FORMAT	You can only FORMAT local disks.
JOIN	You can only JOIN local disks. If you are a File Server, you can only use JOIN <i>before</i> starting Invisible LAN; any joins created before starting Invisible LAN remain in effect.

LABEL	You cannot change the volume label on a network disk. Use VOL instead of LABEL to display the volume label of a network disk.
MSCDEX	Use MSCDEX (the CD-ROM extensions) <i>before</i> starting Invisible LAN.
PRINT	PRINT is not compatible with the network. You can use NETPRINT instead of PRINT.
RECOVER	You can use RECOVER with local disks.
SCANDISK	You can only use SCANDISK on local disks. If you are a File Server, you cannot use SCANDISK on a local hard disk unless you use NW PAUSE.
SUBST	You can only SUBST local disks. If you are a File Server, you can only use SUBST <i>before</i> starting Invisible LAN; any substitutions created before starting Invisible LAN remain in effect. If Ultra Server is running on your computer, you cannot use SUBST at all.
SYS	You can only use SYS with local disks.
VERIFY	VERIFY only affects local disks.

Index

A

- access rights, 15-10, 15-12 to 15-13
 - see also* shortname
- action menu
 - group, 15-7 to 15-8, 15-15, 15-23
 - miscellaneous security, 15-22
 - poll network, 11-4
 - shortname, 15-13 to 15-14
 - user, 15-5 to 15-6, 15-9, 15-15, 15-23
- active users
 - see* server usage statistics
- APPEND DOS command, B-1
- AT/386 chipset, 9-4 to 9-5
 - configuring, 9-6
- ATTRIB DOS command, 15-24
- AUDIO
 - see* NW
 - see* speaker
- audit filter
 - see* audit trail
- audit trail, 16-6
 - displaying (menu), 16-7
 - filter (menu), 16-7
 - saving (menu), 16-9
- AUTOEXEC.BAT, 3-1
- automatic print stream truncation
 - see* print stream truncation
- automatic print stream truncation (menu item)
 - see* manager
- automatic remapping, 2-8

B

- beeper
 - see* speaker
- bell
 - see* speaker
- BINDERY.DAT, 15-24
- binding, 15-2
 - group membership, 15-2 to 15-3
 - group permission for miscellaneous function, 15-2 to 15-3
 - group permission for shortname, 15-2 to 15-3
 - user permission for miscellaneous function, 15-2 to 15-3
 - user permission for shortname, 15-2 to 15-3
- BIOS, 9-9
- blackout zone
 - see* Ultra Server
- boot diskette, 8-1
- boot diskette image file
 - see* image file
- break page, 5-10, 5-12
 - see also* MAKEBP
- BRIDGE command, A-1
- browsing (menu)
 - drive mappings, 12-4
 - printer mappings, 12-8
- bulletin board
 - security, 15-21
 - sysop, 15-21

C

- cache, 6-2
 - disabling, 6-2 to 6-3
 - enabling, 6-3
 - flushing, 6-2 to 6-3
 - resetting statistics, 6-3, 6-6
 - status, 6-2, 6-4, 16-4
 - write policy, 6-3, 16-4
- CACHE command, 6-1 to 6-2, A-1
- CACHE/30
 - see* cache

CANCEL
 see PQ
chipset information
 see SHADOW command
chipset RAM, 9-9
CHKDSK DOS command, 6-7, B-1
CLEAR
 see PQ
clock
 see network clock
CLRCMOS command, 9-16, A-2
comment
 group, 15-3, 15-6 to 15-8
 user, 15-3 to 15-5
COMP DOS command, B-1
COMSPEC
 see SET COMSPEC
CONFIG.SYS, 9-13
CONTINUE (print spooler)
 see PQ
CONTINUE (server)
 see NW
control codes (printer)
 see printer set-up string
conventional memory, 9-2, 9-8
conventional memory information
 see SHADOW command
COPY DOS command, B-1
create access
 see access rights

D

data terminal ready
 see flow control
date
 see network clock
DEDICATE command, 6-1, A-2
DEVICE DOS command, 9-13
device name, 2-6, 12-5
DIRECT
 see PQ
direct printing, 5-2, 5-9

- directory path, 2-3, 12-3 to 12-4, 15-16
- discontinue option, 2-5, 2-8
- disk cache
 - see* cache
- disk directories without shortnames
 - see* miscellaneous security
- DISKCOMP DOS command, B-1
- DISKCOPY DOS command, B-1
- diskless workstation, 8-1, 8-5
- DOS memory
 - see* conventional memory
- DOS memory information
 - see* SHADOW command
- DOWN (Ultra Server)
 - see* US
- drive letter, 2-2 to 2-3, 12-1, 12-3, 15-16
- drive mappings
 - changing (command), 2-3, 2-5, 15-16
 - changing (menu), 12-2 to 12-4, 15-17
 - displaying (command), 2-1, 2-8
 - displaying (menu), 12-1
- drive mappings (menu item)
 - see* manager
- DTR
 - see* flow control
 - see* PQ

E

- EGA
 - see* enhanced graphics adapter
- electronic mail
 - see* mail
- EMS
 - see* expanded memory
- EMS handle table
 - see* SHADOW command
- enhanced EMS, 9-9
- enhanced graphics adapter, 9-15
 - see also* high-resolution graphics
- ERRORLEVEL, 1-5
- EVERYONE, 15-5 to 15-6, 15-13 to 15-14, 15-19 to 15-21
 - see also* group

- examine print queue contents remotely
 - see* miscellaneous security
- examine print spooler status remotely
 - see* miscellaneous security
- examine security information remotely
 - see* miscellaneous security
- execute access
 - see* access rights
- expanded memory, 9-2 to 9-3
- expanded memory information
 - see* SHADOW command
- expanded memory manager, 9-2
- expanding tabs
 - see* printing a file
- extended memory, 9-4
- extended memory information
 - see* SHADOW command

F

- FASTOPEN DOS command, B-1
- FC DOS command, B-1
- FDISK DOS command, B-1
- FEED
 - see* PQ
- file server
 - see* server
- file-by-file backup (tape), 6-9
- flow control (for serial printer), 5-7
 - DTR selection (command), 5-8
 - DTR selection (menu), 14-4
 - Xon/Xoff selection (command), 5-8
 - Xon/Xoff selection (menu), 14-4
- form feed (for printer), 5-2, 5-6, 14-1, 14-3
 - disabling (command), 5-6
 - disabling (menu), 14-3
 - enabling (command), 5-7
 - enabling (menu), 14-3
- FORMAT DOS command, 8-1, B-1
- frontfill (memory), 8-8, 9-8

G

graphics

see high-resolution graphics

group, 15-2, 15-6

action menu, 15-7 to 15-8, 15-15, 15-23

changing definition, 15-8

comment, 15-3, 15-6 to 15-8

creating, 15-7

deleting, 15-8

displaying list of, 15-7

EVERYONE, 15-5 to 15-6, 15-13 to 15-14, 15-19 to 15-21

miscellaneous permissions, 15-22 to 15-23

name, 15-3, 15-6 to 15-8

permissions, 15-2

shortname permissions, 15-14 to 15-15

user memberships, 15-8 to 15-9

group definitions and security (menu item)

see manager

H

HANG_UP command, A-2

help, 11-2, 11-5, A-11

HIDE

see NW

hiding

see network software

HIGH

see PQ

high RAM, 9-9

high-resolution graphics

conflict with frontfill, 9-15

disabling, 9-15

enabling, 9-15

hot key, 10-1

I

image backup (tape), 6-9

image file, 8-2 to 8-3

initialization file

 creating, 8-2

 specifying, 8-4

Invisible RAM

 installing in CONFIG.SYS, 9-13

 on diskless workstations, 8-8

J

JOIN DOS command, B-1

K

keys

see mail

see manager

see print screen key

see print stream truncation key

L

LABEL DOS command, B-2

list access

see access rights

logging off, 7-3

logging on, 7-3

LOGOFF command, 7-2 to 7-3, A-2

LOGON command, 7-2 to 7-3, A-2

LOW

see PQ

LSHADOW command, 9-8, 9-11, A-2

M

- mail, 10-1
 - keys, 10-2 to 10-4
 - receiving messages, 10-3
 - sending messages, 10-1
 - speaker, use of, 6-8, 10-3 to 10-4
- main menu
 - see* manager
- MAKEBP command, 5-10, 5-12, A-2
- MAKEIMG command, 8-3, A-3
- manager
 - drive mappings, 12-1, 15-17
 - group definitions and security, 15-7 to 15-8, 15-15, 15-23
 - keys, 11-2
 - main menu, 11-1
 - miscellaneous security, 15-18, 15-22
 - poll network, select machine, 11-3
 - printer mappings, 12-5
 - remote management, 11-1, 11-3
 - server usage statistics, 16-1
 - shortname definitions and security, 15-12, 15-14
 - user definitions and security, 15-4, 15-9, 15-15, 15-23
- manual print stream truncation
 - see* print stream truncation
- map (memory)
 - see* SHADOW command
- MAP command, 2-1, A-3 to A-4
 - connecting to network disk with shortname, 15-16
 - connecting to network disk without shortname, 2-3
 - connecting to network printer, 2-6
 - disconnecting from network disk, 2-5
 - disconnecting from network printer, 2-8
 - discontinue option, 2-5, 2-8
 - displaying network resources, 2-1 to 2-2, 2-8
 - wait option, 2-3, 2-6, 15-16
- mappings
 - see* drive mappings
 - see* printer mappings
- MEDIUM
 - see* PQ

- memory map
 - see* SHADOW command
- memory relocation
 - see* NEAT chipset
- MENU command, 11-1, A-4
- menu system
 - see* manager
- miscellaneous security, 15-2, 15-18
 - action menu, 15-22
 - bulletin board access, 15-21
 - bulletin board sysop privilege, 15-21
 - disk directories without shortnames, 15-19
 - displaying list of, 15-18
 - examine print queue contents remotely, 15-19
 - examine print spooler status remotely, 15-19
 - examine security information remotely, 15-20
 - examine server usage statistics remotely, 15-20
 - group permissions, 15-22 to 15-23
 - modify print queue contents remotely, 15-19
 - modify print spooler status remotely, 15-19
 - modify security information remotely, 15-20
 - network printer #1, 15-19
 - network printer #2, 15-19
 - permissions, 15-2
 - user permissions, 15-22 to 15-23
- miscellaneous security (menu item)
 - see* manager
- modify print queue contents remotely
 - see* miscellaneous security
- modify print spooler status remotely
 - see* miscellaneous security
- modify security information remotely
 - see* miscellaneous security
- MOUNT (Ultra Server)
 - see* US
- MSCDEX DOS command, B-2

N

- name
 - group, 15-3, 15-6 to 15-8
 - shortname, 15-3, 15-12 to 15-13
 - user, 15-3 to 15-5

- name (changing), 7-3
- NEAT chipset, 9-4 to 9-5
 - configuring, 9-6
 - expanded memory controller, 9-6
 - memory relocation, 9-6
 - resetting configuration, 9-16
- NET30 command, 8-4, A-4
- NETADDR command, 8-6, A-4 to A-5
- NetBIOS
 - ROM, 8-4, 8-8
- NETCLOCK command, 3-1, A-5
 - wait option, 3-1
- NETHELP command, A-5
- NETPRINT command, 4-1 to 4-2, 14-5, A-5, B-2
- network clock, 3-1
- network disk
 - connecting, 2-3, 12-3 to 12-4, 15-16 to 15-17
 - disconnecting, 2-5, 12-2
- network printer
 - connecting, 2-6, 12-7 to 12-8
 - disconnecting, 2-8, 12-6
 - see also* printer number
- network printer #1
 - see also* miscellaneous security
- network printer #2
 - see also* miscellaneous security
- network resources
 - displaying (command), 2-1, 2-8
 - displaying (menu), 12-1, 12-5
 - see also* using network resources
- network software
 - displaying status, 6-6
 - hiding, 6-7 to 6-8
 - unhiding, 6-7 to 6-8
- network software memory information
 - see* SHADOW command
- NOAUDIO
 - see* NW
- NODIRECT
 - see* PQ
- NOFEED
 - see* PQ
- NW command, 6-1, A-6
 - AUDIO, 6-8
 - CONTINUE, 6-7
 - HIDE, 6-8

NOAUDIO, 6-8
PAUSE, 6-7, B-1 to B-2
STATUS, 6-6
UNHIDE, 6-8

O

object, 15-2
 group, 15-2 to 15-3
 miscellaneous function, 15-2 to 15-3
 shortname, 15-2 to 15-3
 user, 15-2 to 15-3

P

password
 entering, 7-1, 7-3
 user, 15-3 to 15-5
PASSWORD command, 7-1, A-6
path
 see directory path
PATH DOS command, 8-5
PAUSE (print spooler)
 see PQ
PAUSE (server)
 see NW
PEAK chipset, 9-4, 9-6
 configuring, 9-6
permissions
 group, 15-2, 15-15, 15-23
 miscellaneous security, 15-2, 15-22
 shortname, 15-2, 15-14
 user, 15-2, 15-15, 15-23
poll network and select machine (menu item)
 see manager
PQ command, A-6
 CANCEL, 5-5
 CLEAR, 5-5
 CONTINUE, 5-3
 DIRECT, 5-9

- DTR, 5-8
- FEED, 5-7
- HIGH, 5-10
- LOW, 5-10
- MEDIUM, 5-10
- NODIRECT, 5-9
- NOFEED, 5-6
- PAUSE, 5-3
- RESTART, 5-4
- STATUS, 5-1
- XON, 5-8
- print device
 - see* device name
- PRINT DOS command, 4-1, B-2
- print priority, 5-2, 5-10
- print queue, 5-1, 5-4
 - changing contents, 14-6
 - clearing (command), 5-5
 - displaying contents, 14-5
 - see also* print spooler
- print queue contents (menu item)
 - see* manager
- print screen key, 4-3
- print spooler, 5-1
 - active state, 5-2, 14-1 to 14-2
 - cancel print job (command), 5-5
 - cancel print job (menu), 14-4
 - continuing (command), 5-3
 - continuing (menu), 14-3
 - direct print (command), 5-9
 - displaying status (command), 5-1
 - displaying status (menu), 14-1
 - paused state, 5-2, 14-1, 14-3
 - pausing (command), 5-3
 - pausing (menu), 14-3
 - priority (command), 5-10
 - restart print job (command), 5-4
 - restart print job (menu), 14-4
 - see also* flow control (for serial printer)
 - see also* form feed (for printer)
 - see also* print queue
- print spooler parameters
 - spool files, 16-3
- print spooler status (menu item)
 - see* manager

- print stream truncation, 4-3
 - automatic (command), 4-4
 - automatic (menu), 13-1
 - immediate, 4-5
 - manual, 4-3
- print stream truncation key, 4-3
- printer control code
 - see* printer set-up string
- printer mappings
 - changing (command), 2-6, 2-8
 - changing (menu), 12-6 to 12-8
 - displaying (command), 2-1, 2-8
 - displaying (menu), 12-5
- printer mappings (menu item)
 - see* manager
- printer number, 2-6, 5-6 to 5-8, 12-6 to 12-7
- printer set-up string, 4-7
- printing a file, 4-1 to 4-2
- printing the screen, 4-3
- PRINTNOW command, 4-5, A-7
 - in batch file, 4-6
 - in secondary command processor, 4-6
- PSETUP command, 4-7, A-7

Q

- QSETUP command, A-7

R

- RBRIDGE command, A-7
- RCONFIG command, A-8
- RDIAG command, A-8
- read access
 - see* access rights
- receiving messages
 - see* mail
- RECOVER DOS command, B-2
- redirector
 - speaker, use of, 6-8

- remote management
 - see* manager
- remote program load server, 8-1, 8-5
 - configuration, 8-3
 - see also* image file
- resident program
 - see* memory-resident program
- RESTART
 - see* PQ
- ROM copy, 8-8, 9-9
- RPL
 - see* remote program load server
- RSECURE command, A-8

S

- SCANDISK DOS command, B-2
- SCAT chipset, 9-4 to 9-5
 - configuring, 9-6
 - expanded memory controller, 9-6
 - memory relocation, 9-6
- security, 15-1
 - example, 15-24
 - saving and resetting, 15-24
- security binding
 - see* binding
- security object
 - see* object
- security permissions
 - see* permissions
- sending messages
 - see* mail
- server
 - active state, 6-6 to 6-7
 - continuing, 6-7
 - dedicated, 6-1
 - paused state, 6-6 to 6-7
 - pausing, 6-7
- server parameters
 - files, 16-2
 - record locks, 16-3
 - sessions, 16-2

- server usage statistics, 16-1
 - active users, 16-5
 - audit trail, 16-6
 - disk cache statistics, 16-4
 - security, 15-20
 - server resources, 16-2
 - Ultra Server resources, 16-10
- server usage statistics (menu item)
 - see* manager
- SET COMSPEC DOS command, 8-5
- set-up string
 - see* printer set-up string
- SETPORT command, A-8
- setup program
 - easy configuration, 2-7
 - loading initialization file, 8-3
 - saving initialization file, 8-4
 - server parameters, 8-3
 - starting, A-7 to A-8
- SETUP30 command, A-8
- SHADOW command, 9-1, A-9
 - chipset information, 9-1, 9-4
 - DOS memory information, 9-1 to 9-2
 - EMS handle table, 9-2 to 9-3
 - expanded memory information, 9-2
 - extended memory information, 9-1, 9-4
 - memory map, 9-2, 9-8
 - network software memory information, 9-2, 9-7
 - shadow RAM information, 9-2, 9-7
- shadow RAM, 9-7, 9-9, 9-11
 - loading device drivers, 9-13
 - loading memory-resident programs, 9-11
 - using for network software, 9-12
 - with AT/386 chipset, 9-6
 - with NEAT chipset, 9-6
 - with PEAK chipset, 9-6
 - with SCAT chipset, 9-6
- shadow RAM information
 - see* SHADOW command
- sharing access
 - see* access rights
- shortname, 12-3, 15-2, 15-10
 - access rights, 15-3, 15-10, 15-12 to 15-13
 - action menu, 15-13 to 15-14
 - changing definition, 15-13
 - creating, 15-13

- definition, 15-3, 15-12 to 15-13
- deleting, 15-14
- displaying list of, 15-12
- group permissions, 15-14 to 15-15
- name, 15-3, 15-12 to 15-13
- permissions, 15-2
- use in Drive Mappings menu item, 15-17
- use in initial drive mappings, 15-17
- use in MAP command, 15-16
- user permissions, 15-14 to 15-15
- shortname definitions and security (menu item)
 - see* manager
- software status
 - see* network software
- speaker
 - disabling, 6-8, 10-4
 - enabling, 6-8, 10-4
 - mail system's use of, 6-8, 10-3 to 10-4
 - redirector's use of, 6-8
- spooler
 - see* print spooler
- standard EMS, 9-9
- STATUS (network software)
 - see* NW
- STATUS (print spooler)
 - see* PQ
- STATUS (Ultra Server)
 - see* US
- SUBST DOS command, B-2
- SYS DOS command, B-2

T

- tabs
 - see* printing a file
- tape backup, 6-8 to 6-9
- time
 - see* network clock
- track buffer
 - see* cache
- TransBIOS
 - data location, 9-7
 - data size, 9-7

U

- Ultra Server, 6-10, 16-10
 - blackout zone, 6-13
 - displaying status (command), 6-10
 - displaying status (menu), 16-10
 - mounting drives, 6-14
 - non-dedicated mode, 6-15
 - unmounting drives, 6-12 to 6-13
- Ultra Server parameters
 - files, 16-11
 - record locks, 16-11
- UNHIDE
 - see* NW
- unhiding
 - see* network software
- UNLINK command, 8-5, A-9
- UNMOUNT (Ultra Server)
 - see* US
- upper memory
 - see* shadow RAM
- US command, 6-1
 - DOWN, 6-13, A-9
 - MOUNT, 6-14, A-10
 - STATUS, 6-10, A-10
 - UNMOUNT, 6-13, A-10
- usage statistics
 - see* server usage statistics
- user, 15-2, 15-4
 - action menu, 15-5 to 15-6, 15-9, 15-15, 15-23
 - changing definition, 15-5
 - comment, 15-3 to 15-5
 - creating, 15-4
 - deleting, 15-6
 - displaying list of, 15-4
 - group memberships, 15-8 to 15-9
 - miscellaneous permissions, 15-22 to 15-23
 - name, 15-3 to 15-5
 - password, 15-3 to 15-5
 - permissions, 15-2

- shortname permissions, 15-14 to 15-15
- user definitions and security (menu item)
 - see* manager
- user name (changing), 7-3
- users (active)
 - see* server usage statistics
- using network resources, 2-1 to 2-2, 2-6, 3-1, 12-2 to 12-4, 12-6 to 12-8, 15-16 to 15-17

V

- VERIFY DOS command, B-2
- VGA
 - see* video graphics array
- VGAOFF command, 9-15, A-10
- VGAON command, 9-15, A-10
- video
 - see* enhanced graphics adapter
 - see* high-resolution graphics
 - see* video graphics array
- video buffer, 9-9
- video graphics array, 9-15
 - see also* high-resolution graphics
- video RAM
 - see* video buffer
- VOL DOS command, B-2

W

- wait option, 2-3, 2-6, 3-1, 15-16
- window (screen)
 - see* mail
- WINSTR command, A-10
- write access
 - see* access rights
- write policy
 - see* cache
- write-back
 - see* cache

write-through
 see cache

X

XCOPY DOS command, B-1

XON

see PQ

XON/XOFF

see flow control

