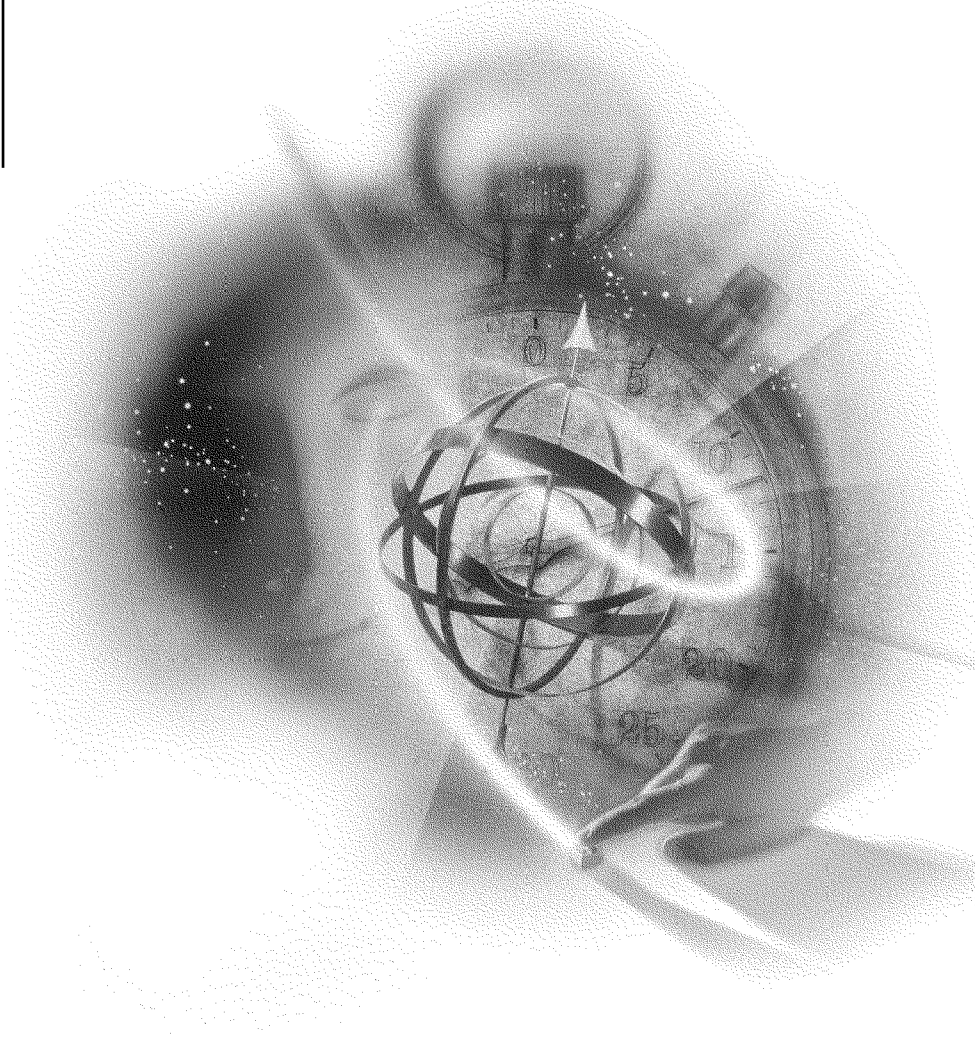


NetWare System Administration



NetWare® 3.12
NETWORKING SOFTWARE

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1990-1993 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

System Administration
July 1993

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell, NetWare, and the N design are registered trademarks of Novell, Inc.

DR DOS is a registered trademark of Novell, Inc.

EXOS is a registered trademark of Novell, Inc.

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

IPX/SPX is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE2-32 is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Directory Services and NDS are trademarks of Novell, Inc.

NetWare DOS Requester is a trademark of Novell, Inc.

Novell RX-Net is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWire is a registered service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Packet Burst is a trademark of Novell, Inc.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

How to Use This Manual	25
Purpose	25
Organization	26
1 File Server Utilities	29
Overview	29
Console Commands	29
Loadable Modules	29
SERVER	29
ABORT REMIRROR	30
Why Use ABORT REMIRROR?	30
Command Format	30
Command Parameter	30
Stop Remirroring a Logical Partition	30
Additional Information	30
ADD NAME SPACE	31
Why Use ADD NAME SPACE?	31
Command Format	31
Command Parameters	31
Additional Information	31
Reversing ADD NAME SPACE	34
Set Up a Volume to Store Non-DOS Files	34
List the Current Name Space	34
BIND	35
Why Use BIND?	35
Command Format	35
Command Parameters	35
Driver Parameters	36
Protocol Parameters	37
Bind a Protocol to a Driver	38

BROADCAST	41
Why Use BROADCAST?	41
Command Format	41
Command Parameters.	41
Additional Information	41
Send a Console Message	42
CDROM	43
Why Use CDROM?	43
Command Format	43
Command Parameters.	43
Using CDROM	43
Display Help Information.	43
List the CD-ROM Devices	44
List All Volumes Identified on the CD-ROM Devices	44
Dismount a CD-ROM Volume	45
Request the Root Directory of a Volume	45
Mount a CD-ROM Volume	46
Change the Media in a CD-ROM drive	46
Decrease the Time Required to Remount a Volume	46
CLEAR STATION	47
Why Use CLEAR STATION?	47
Command Format	47
Command Parameters.	47
Remove All File Server Resources from a Workstation	47
CLIB	49
Why Use CLIB?	49
Command Format	49
Command Parameters.	49
Additional Information	49
Load CLIB	49
CLS	51
Why Use CLS?	51
Command Format	51
Clear the File Server Console Screen	51
CONFIG	52
Why Use CONFIG?	52
Command Format	52
Additional Information	52
Display Configuration Information	53
DISABLE LOGIN	54
Why Use DISABLELOGIN?	54
Command Format	54
Prevent Users from Logging in to the File Server	54

DISABLE TTS	55
Why Use DISABLE TTS?	55
Command Format	55
Disable TTS in the File Server	55
DISKSET	56
Why Use DISKSET?	56
Command Format	56
Command Parameters	56
Using DISKSET.	57
DISMOUNT	58
Why Use DISMOUNT?	58
Command Format	58
Dismount a Volume.	58
DISPLAY NETWORKS.	59
Why Use DISPLAY NETWORKS?	59
Command Format	59
Display a List of Networks	59
DISPLAY SERVERS	61
Why Use DISPLAY SERVERS?	61
Command Format	61
Display a List of File Servers	61
DOWN	62
Why Use DOWN?	62
Command Format	62
Additional Information	62
Down the File Server	62
EDIT	64
Why Use EDIT?	64
Command Format	64
Command Parameters	64
Edit or Create Text Files	64
ENABLE LOGIN	65
Why Use ENABLE LOGIN?	65
Command Format	65
Allow Users to Log In	65
ENABLE TTS.	66
Why Use ENABLE TTS?	66
Command Format	66
Additional Information	66
Enable TTS in the File Server	66

EXIT	68
Why Use EXIT?	68
Command Format	68
Return to DOS after Downing the File Server	68
Warm Boot the File Server.	68
INSTALL.	69
Why Use INSTALL?	69
Command Format	69
Command Parameters.	69
Main screen	69
Load INSTALL	72
Add a Hard Disk to the File Server	72
Replace a Hard Disk	74
Recover Volume Data from an Unmirrored Hard Disk.	76
Format a Hard Disk	76
Create NetWare Partitions	79
Delete Partitions	81
Edit Hot Fix Information	82
Mirror or Duplex Hard Disks	84
Unmirror Hard Disks	86
Test Hard Disks for Bad Blocks	86
Create a Volume	89
Delete a Volume	91
Rename a Volume	92
Increase the Size of a Volume.	93
Copy the SYSTEM and PUBLIC Files.	95
Change the File Server's Name	95
Change the File Server's Internal Network Number	96
Create the AUTOEXEC.NCF File	97
Edit the AUTOEXEC.NCF File.	98
Create the STARTUP.NCF File	102
Edit the STARTUP.NCF File.	102
Install, Uninstall, or Configure a Product on the File Server	104
Exit INSTALL	105
IPXS	106
Why Use IPXS?	106
Command Format	106
Command Parameters.	106
Additional Information	106
Load IPXS	106

KEYB	107
Why Use KEYB?	107
Command Format	107
Command Parameters	107
Load KEYB	107
LIST DEVICES	108
Why Use LIST DEVICES?	108
Command Format	108
Display Device Information	108
Additional Information	108
LOAD	109
Why Use LOAD?	109
Command Format	109
Command Parameters	110
Additional Information	111
Load a Module	112
Troubleshoot LOAD	113
LOAD disk driver	120
Why Use LOAD <i>disk driver</i> ?	120
Command Format	120
Command Parameters	121
Additional Information	122
Load a Disk Driver in an ISA (AT Bus) Computer	125
Load a Disk Driver for the Internal Disk Controller (Microchannel)	127
Load a Disk Driver for a Disk Controller Board (Microchannel)	128
Upgrade a Disk Driver	129
Troubleshooting the Host Bus Adapter Driver	130
LOAD LAN driver	133
Why Use LOAD <i>LAN driver</i> ?	133
Command Format	134
Command Parameters	134
Driver Parameters	134
Additional Information	139
LAN Driver Parameters	140
Load a LAN Driver in an EISA File Server	149
Load a LAN driver in an ISA (AT bus) File Server	150
Load a LAN Driver in a Microchannel File Server	152
Change an Optional Parameter of a Loaded Driver	153
Load a Driver More than Once	155
Upgrade a LAN Driver	158
Troubleshooting LAN Drivers	159

LOAD <i>name space</i>	162
Why Use LOAD <i>name space</i> ?	162
Command Format	162
Command Parameters.	162
Additional Information	163
Load Name Space	165
Upgrade Name Space	166
LOAD <i>NLM utility</i>	167
Why Use Load <i>NLM utility</i> ?	167
Command Format	167
Command Parameters.	167
Load an NLM Utility	168
MAGAZINE	169
Why Use MAGAZINE?.	169
Command Format	169
Command Parameters.	169
MATHLIB	170
Why Use MATHLIB?.	170
Command Format	170
Command Parameters.	170
Additional Information	170
Load MATHLIB	170
MATHLIBC	171
Why Use MATHLIBC?.	171
Command Format	171
Command Parameters.	171
Additional Information	171
Load MATHLIBC.	171
MEDIA	172
Why Use MEDIA?	172
Command Format	172
Command Parameters.	172
MEMORY	173
Why Use MEMORY?	173
Command Format	173
Additional Information	173
Display the Total Amount of Memory	173
MIRROR STATUS.	174
Why Use MIRROR STATUS?	174
Command Format	174
Display Status of Mirrored Logical Partitions	174

MODULES	175
Why Use MODULES?	175
Command Format	175
Additional Information	175
List the Loaded Modules	176
MONITOR	177
Why Use MONITOR?	177
Command Format	177
Command Parameters	177
Load MONITOR	178
Interpret the Main MONITOR Screen.	179
Use “Available Options” Menu	180
List Active Connections.	183
List Physical Record Locks for a User	185
Clear a Connection	186
List Open Files	186
List System Hard Disks	187
List Volume Segments Per Hard Disk	188
Change the “Read After Write Verify” Status of the Hard Disk	190
Flash the Hard Disk Light.	191
Activate/Deactivate a Hard Disk	192
Mount/Dismount a Removable Media Device	193
Lock/Unlock a Removable Media Device.	195
List LAN Drivers and Statistics	196
List System Modules	198
List Resources Used by System Modules	199
Lock the File Server Console	200
Unlock the File Server Console.	201
Check the Status of a File	201
View Mounted Volumes	202
View Memory Statistics	203
View Tracked Resources	205
Checking a Server’s Processor Utilization	207
Exit MONITOR	208
MOUNT	209
Why Use MOUNT?	209
Command Format	209
Mount a New Volume or One that Is Not Used Often	209
Mount Several Volumes	209
NAME	210
Why Use NAME?	210
Command Format	210
Display the Name of the File Server	210

NLICLEAR (Not-Logged-In CLEAR)	211
Why Use NLICLEAR?	211
Command Format	211
Command Parameters.	211
NOTIFY	211
POLL= <i>number</i>	211
CONN= <i>number</i>	212
Additional Information	212
NMAGENT	213
Why Use NMAGENT?	213
Command Format	213
Command Parameters.	213
Additional Information	213
Load NMAGENT	213
NUT	214
Why Use NUT?	214
Command Format	214
Command Parameter	214
NWSNUT	215
Why Use NWSNUT?	215
Command Format	215
Command Parameters.	215
OFF	216
Why Use OFF?	216
Command Format	216
Clear the File Server Console Screen	216
PROTOCOL	217
Why Use PROTOCOL?	217
Command Format	217
Command Parameters.	217
View the Kinds of Protocols and Frame Types on Your Network	218
Add a New Protocol or Frame to Your Network	218
PSERVER.	220
Why Use PSERVER?	220
Command Format	220
REGISTER MEMORY.	221
Why Use REGISTER MEMORY?	221
Command Format	221
Command Parameters.	221
Additional Information	221
Register Memory Above 16 MB	222

REMIRROR PARTITION	223
Why Use REMIRROR PARTITION?	223
Command Format	223
Command Parameter	223
Start Remirroring a Logical Partition	223
Additional Information	223
REMOTE	224
Why Use REMOTE?	224
Command Format	224
Command Parameters	224
Additional Information	224
Load REMOTE	224
Set Up Autoloading of Remote Console	225
REMOVE DOS	226
Why Use REMOVE DOS?	226
Command Format	226
Additional Information	226
Remove DOS from the File Server	226
RESET ROUTER	227
Why Use RESET ROUTER?	227
Command Format	227
Reset the Router Table	227
ROUTE	228
Why Use ROUTE?	228
Command Format	228
Command Parameters	228
Parameters	229
Additional Information	232
Set Up the File Server for Source Routing	232
Change a Source Routing Parameter	232
RPL	234
Why Use RPL?	234
Command Format	234
Command Parameters	234
Load RPL	234
Additional Information	234
RS232	235
Why Use RS232?	235
Command Format	235
Command Parameters	235

RSPX	236
Why Use RSPX?	236
Command Format	236
Command Parameters.	236
Additional Information	236
Load RSPX	236
SBACKUP	237
Why Use SBACKUP?	237
Command Format	237
Command Parameters.	237
Additional Information	237
SCAN FOR NEW DEVICES.	238
Why Use SCAN FOR NEW DEVICES?	238
Command Format	238
Check for New Hardware Devices	238
SEARCH	239
Why Use SEARCH?	239
Command Format	239
Command Parameters.	239
Additional Information	240
Display the Current Search Paths	240
Add a Search Path	240
Delete a Search Path	241
SECURE CONSOLE	242
Why Use SECURE CONSOLE?	242
Command Format	242
Additional Information	242
Unauthorized NLMs	242
Secure the File Server from Unauthorized System Programs	243
SEND	244
Why Use SEND?	244
Command Format	244
Command Parameters.	244
Additional Information	244
Send a Console Message	245
SERVER.	246
Why Use SERVER?	246
Command Format	246
Command Parameters.	246
Boot the File Server	247
Boot with an Alternate STARTUP File	247
Boot without a STARTUP.NCF File	248
Boot without an AUTOEXEC.NCF File	248
Boot with a Different Cache Buffer Size	248

SET	250
Why Use SET?	250
Command Format	250
Additional Information	251
Configuring Other Types of Operating System Functions	252
Entering Parameters	252
Using Parameters that Control the Allocation of Services	254
Parameters	254
View Current Operating System Configurations	260
Change an Operating System Parameter at the Console Prompt	260
Change an Operating System Parameter in the STARTUP.NCF File	261
Understand the Operating System Parameters	262
SET TIME	291
Why Use SET TIME?	291
Command Format	291
Additional Information	291
Set the Date and Time on the File Server	292
SET TIMEZONE	293
Why Use SET TIMEZONE?	293
Command Format	293
Command Parameters	293
Display the Time Zone Information	294
Change the Time Zone Information	295
SPEED	296
Why Use SPEED?	296
Command Format	296
View the Processor Speed	296
SPOOL	297
Why Use SPOOL?	297
Command Format	297
SPXCONFIG	298
Why Use SPXCONFIG?	298
Command Format	298
Command Parameters	298
Set SPX Parameters in a Single Command or in an .NCF File	299
Use SPXCONFIG Interactively to Change SPX Parameters	299
SPXS	300
Why Use SPXS?	300
Command Format	300
Command Parameters	300
Additional Information	300
Load SPXS	300

STREAMS	301
Why Use STREAMS?	301
Command Format	301
Command Parameters.	301
Load STREAMS	301
TIME.	302
Why Use TIME?	302
Command Format	302
Additional Information	302
View the File Server's Date and Time	302
TLI	303
Why Use TLI?	303
Command Format	303
Command Parameters.	303
Additional Information	303
Load TLI	303
TRACK OFF	304
Why Use TRACK OFF?	304
Command Format	304
Turn Off the Router Tracking Screen	304
TRACK ON	305
Why Use TRACK ON?.	305
Command Format	305
Signal the Router to Display Packets	305
Additional Information	305
UNBIND	308
Why Use UNBIND?	308
Command Format	308
Command Options	308
Unbind a Protocol from a Driver	310
Change the Network Number for the Cabling	311
UNLOAD	312
Why Use UNLOAD?	312
Command Format	312
Additional Information	312
Unload a Loadable Module	314
Troubleshooting UNLOAD	314
UPS	316
Why Use UPS?	316
Command Format	316
Command Parameters.	316
Add an Uninterruptible Power Supply (UPS)	317
Troubleshooting UPS	318

UPS STATUS	319
Why Use UPS STATUS?	319
Command Format	319
Check Power Supply Status	319
UPS TIME	321
Why Use UPS TIME?	321
Command Format	321
Command Parameters	321
Change the UPS Discharge and Recharge Times	322
VERSION	323
Why Use VERSION?	323
Command Format	323
View Version Information and Copyright Notice	323
VOLUMES	324
Why Use VOLUMES	324
Command Format	324
View Mounted Volumes	324
VREPAIR	325
Why Use VREPAIR?	325
Command Format	325
Command Parameters	325
Additional Information	325
Repair a Volume or Remove Name Space Entries	327
Set VREPAIR Options	329

2 Remote Management 331

Overview	331
Introduction	332
Who Can Use Remote Management?	332
How Does Remote Management Work?	333
What Types of Communication Links Can I Set Up?	335
Setting Up Remote Management	339
Hardware and Software Requirements for Remote Management	340
Adding Remote Capability to a NetWare v3.1x File Server	341
Adding Remote Capability to a Standalone PC	343
Using a Remote Console	343
Activating RCONSOLE from a Network Workstation	344
Procedure	344
Activating ACONSOLE from a Network Station	345
Procedure	345
Activating ACONSOLE from a Standalone PC	347
Exiting the Remote Console	347
Exit from the “Available Options” Menu	347
Exit from the Remote System Console Prompt	347

Using the Remote Console for Administrative Tasks	348
Use Remote Management Screens and Menus	349
Scan File Server Directories	350
Reboot a File Server from a Remote Console	350
Transfer Files to a Remote File Server	351
Upgrade a LAN or Disk Driver	354
Configuring the Modem	356
Modify the Modem Configuration	356
Create or Modify the Modem Phone List	356

3 Troubleshooting Guide 359

Overview	359
Maintenance Tips	360
Memory Maintenance	360
Disk Maintenance	363
Security Maintenance	365
Bindery Maintenance	366
Volume Maintenance	367
Flow Charts	368
Common Problems	382
File Server, Hard Disk, and Volume Problems	382
General Solutions	383
Console Commands Cannot Be Entered at the File Server Console, or They Do Not Function Correctly	384
The File Server Does Not Keep Track of Time Correctly	385
The File Server “Hangs” After Mounting the Last Volume	385
The Operating System Reports Fat Errors When the File Server is First Booted After the Installation of an RX-Net Network Board	386
A Hard Disk Cannot Be Accessed. (The Format or Surface Test Options in Install Will Not Run, for Example)	386
None of the Volumes, Including SYS:, Were Mounted	387
The Operating System Reports Disk Errors When a Volume is Being Mounted	388
The Operating System Reports Memory Errors When a Volume is Being Mounted	388
A Volume Cannot Be Mounted Because of Corrupted Directory Entry Tables or FATs	391
A Volume Cannot Be Mounted Because a Name Space Module Was Not Loaded First	392
Communication Problems	393
General Solutions	393
The File Server Does Not Boot After a Network Board Is Installed	395
The File Server Could Not Be Found by the Workstations on the Network	395
File Servers Do Not Recognize Each Other on the Network	397
Responses from the File Server Are Noticeably Slow	398
Workstations Can Log In, But Periodically Lose Their Connections to the File Server	399
ARCnet-Specific Problems	400

Ethernet-Specific Problems	401
Token-Ring-Specific Problems	402
Workstation Problems	403
Possible Solutions	403
Application Problems	405
General Installation Problems	405
Application Problems: Compatibility	407
Application Problems: File I/O	408
Application Problems: File and Record Locking	411
Application Problems: DOS Utilities	413
Application Problems: General Failure	414
Application Problems: Miscellaneous	416
TTS Problems	419
If You Need More Help	421

A Custom LAN Driver Statistics Shown in MONITOR 423

3C503 Custom Statistics	424
3C503ResetCount	424
CarrierSenseLostCount	424
EnqueuedSendsCount	424
ExcessCollisionsCount	424
GotNothingCount	424
ReceiveFIFOOverrunErrorCount	425
ReceiverMissedPacketCount	425
RxPagingErrorCount	425
TotalCollisionsCount	425
TransmitTimeoutCount	425
UnderrunErrorCount	425
UnsupportedFramePacketCount	425
UnsupportedMulticastCount	426
3C505 Custom Statistics	426
# of Ethernet 802.2 Packets Received	426
# of Ethernet 802.3 Packets Received	426
# of Ethernet_II Packets Received	426
# of Ethernet_SNAP Packets Received	426
# of Unsupported Frame From Packets Received	426
GetNICCommandTimeOut	426
NICCmdLengthMismatch	427
NICCmdRequestDMSIsActive	427
NICCmdRequestInvalid	427
NICCommandTooBig	427
NICCommandTooLarge	427
NICCommandTooSmall	427

NotDoingDMACount	427
ResetNICCount	427
3C523 Custom Statistics	428
EnqueuedSendsCount.	428
RBD_act_cnt Not Set	428
Recv Buffer Two Bytes Off.	428
Reset82586	428
RxDMAOverrun	428
RxFailedTestsSoltWasTrashed	428
RxMediaMismatch	428
RxPacketsMisalignedAndCRCError	429
RxPacketsWithCRCError	429
RxTrashedNoNICRxBuffers	429
TxCollisions	429
TxDefer	429
TxDMAUnderrun	429
TxLostClearToSend	429
TxNoCarrierSense	429
TxQueuedNoTB	430
TxTrashedMaxRetriesReached	430
TxTrashedNoCommandBlocks	430
TxTrashedTooManyCollisions	430
UnsupportedFramePacketCount	430
NE2 Custom Statistics.	430
BackToBackSends.	430
CarrierSenseLostCount	430
ExcessCollisions	431
OverflowReSends	431
Overrun	431
PagingError	431
PageZeroErrors	431
ReceiveError.	431
RxMulticastPacket	432
RxPagingErrorCount.	432
TotalCollisionsCount.	432
TransmitFailed	432
TransmitTimeoutCount	432
UnderrunErrorCount	432
UnsupportedMulticastCount	432
NE1000 Custom Statistics.	433
CarrierSenseLostCount	433
EnqueuedSendsCount.	433
ExcessCollisionsCount	433
GotNothingCount	433

In32BitModeCount	433
NE1000ResetCount	433
ReceiveFIFOOverrunErrorCount	434
ReceiverMissedPacketCount	434
RxPagingErrorCount	434
TotalCollisionsCount	434
TransmitTimeoutCount	434
UnderrunErrorCount	434
UnsupportedFramePacketCount	434
UnsupportedMulticastCount	435
NE2-32 and NE2000 Custom Statistics	435
BackToBackSendCount	435
CarrierSenseLostCount.	435
EnqueuedSendsCount	435
ExcessCollisionsCount	435
GotNothingCount	435
NE2000ResetCount	436
ReceiveFIFOOverrunErrorCount	436
ReceiverMissedPacketCount	436
RxPagingErrorCount	436
TotalCollisionsCount	436
TransmitTimeoutCount	436
UnderrunErrorCount	436
UnsupportedFramePacketCount	437
UnsupportedMulticastCount	437
NE3200 Custom Statistics	437
Transmit Retry Failure	437
No Nic Board Receive Buffers	437
Number Of Resets To Nic	437
PCN2 Custom Statistics	437
802.2PacketsReceived	437
BadTransmitCompleteInterruptCount	438
CurrentEnqueuedCount	438
EnqueuedSendsCount	438
GotNothingCount	438
HotCarrierInterruptCount	438
No82588InterruptCount.	438
PCN2ResetCount.	438
ReceivedShortPacketCount	438
ReceiveUnderrunErrorCount	439
SNAPPacketsReceivedCount	439
TotalTransmitErrorCount	439
UnsupportedFramePacketCount	439
WeirdInterruptCount	439

TOKEN Custom Statistics	439
Abort Delimiters	439
A/C Errors	440
Bad Correlator Count	440
Burst Errors	440
Frame Copied Errors	440
Frequency Errors	440
Internal Errors	440
Last Ring Status	440
Line Errors	441
Lost Frames	441
Receive Congestion Errors	441
Token Error	441
Unknown ARB Request	441
TRXNET Custom Statistics	442
Fatal Retransmissions	442
First Halves Cancelled	442
Number of Orphaned Packets	443
Raw Transmissions	443
Sends Cancelled	443
Sends Ignored—Driver Shut Down	443
Spurious Interrupts	443
Timed Out Receive ECBs	443
Timed Out Sends	444

B Tracked Resources Displayed in MONITOR 445

AES Process Call-Backs	446
Alloc Short Term Memory (Bytes)	446
C Library BSD Sockets	446
Cache Movable Memory (Bytes)	447
Cache Non-Movable Memory (Bytes)	447
Console Command Handlers	447
Disk Adapter Locks	447
Disk Drive Locks	447
Disk File System Partition Locks	447
Disk Raw Partition Locks	448
Event Notification Call-Backs	448
Hardware Interrupt Handlers	448
Interrupt Time Call-Backs	448
IPX Sockets	448
LSL AES Event Call-Backs	448
LSL Default Protocol Stacks	448
LSL Packet Receive Buffers	449
LSL Pre-Scan Protocol Stacks	449

LSL Protocol Stacks	449
NCP Extensions	449
Network Management Managers	449
Network Management Objects	449
Network Management Triggers	449
Permanent Memory (Bytes)	450
Poll Procedure Call-Backs	450
Processes	450
Processor Exception Handlers	450
Registered Disk Adapters	450
Registered Hardware Options	450
Registered MLID Boards	451
Remote Server Sessions (Instances)	451
Screen Input Call-Backs	451
Screens	451
Semaphores	451
Semi-Permanent Memory (Bytes)	451
Service Advertising (Instances)	451
Service Connection Task Numbers	452
Service Connections	452
Setable Parameters	452
STREAMS: Active Stream Handles	452
Tracked Resource Types	452

How to Use This Manual

Purpose

The purpose of this manual is to help you be an effective system administrator of your NetWare network. You can use *System Administration* as a reference tool and troubleshooting guide.

The manual includes general information about the file server utilities and about some tasks you can perform with them; it does not, however, give step-by-step instructions on completing all tasks.

Most utilities have online help that explains how to complete tasks. This manual discusses the installation and use of the Novell's online documentation viewer.

Also included in this manual are sections related to remote management of the network and troubleshooting hints.

To use this manual, you should be familiar with the platform you are using and with NetWare terminology and concepts.

For more information on NetWare terminology and concepts, see *Concepts*. For procedural help on some tasks, see *Utilities Reference*.

Organization

This manual is divided into four parts:

- ♦ **Chapter 1, “File Server Utilities,” on page 29**

This chapter is an alphabetical listing of server utilities, which are executed from the console prompt.

Information for each utility includes tasks you can perform with the utility, command syntax and parameters, and instructions for using the utility. Many utilities also include examples.

Three types of utilities are documented in this chapter:

- ♦ *Console commands* allow you to perform the following types of tasks: change memory allocations, monitor how the server is being used, and control the way workstations can use the server’s resources.
 - ♦ *Loadable Modules* link disk drivers, LAN drivers, name space modules, management applications, and enhancement utilities with the server’s operating system.
 - ♦ *SERVER* boots the NetWare operating system on the server.
- ♦ **Chapter 2, “Remote Management,” on page 331**

This chapter provides an overview of what remote management is, who can use it, and how it works.

Topics discussed in this chapter include:

- ♦ Different types of communication links that can be set up using remote management.
 - ♦ Hardware and software requirements for establishing connections to remote servers and workstations.
 - ♦ Using a remote console. This section addresses the purpose, activation, and use of the remote console.
- ♦ **Chapter 3, “Troubleshooting Guide,” on page 359**

This chapter gives helpful hints on some of the more common problems you may encounter while maintaining your network.

The Troubleshooting Guide is divided into three sections.

- ♦ Miscellaneous tips—intended to help you develop good system administration habits.

- ◆ Flow charts—designed to assist you in isolating possible network problems.
- ◆ Common problems—included to identify potential solutions to specific problems.
- ◆ Appendixes
 - ◆ **Appendix A, “Custom LAN Driver Statistics Shown in MONITOR,” on page 423**—lists LAN driver statistics available in MONITOR.
 - ◆ **Appendix B, “Tracked Resources Displayed in MONITOR,” on page 445**—lists the tracked resources that are displayed in MONITOR.

1

File Server Utilities

Overview

Three types of file server utilities are documented in this manual: console commands, loadable modules, and SERVER (a DOS executable file, NetWare's "kernel"). Each type of file server utility is described here.

Console Commands

You enter console commands at the file server console prompt, a colon (:). You use these commands to perform the following types of tasks: change memory allocations, monitor how the file server is being used, and control the way workstations can use the file server's resources.

Loadable Modules

NetWare Loadable Modules™ link disk drivers, LAN drivers, name space modules, management applications, and enhancement utilities with the file server's operating system. For additional information see "Loadable module" in *Concepts*.

SERVER

The executable file SERVER boots the NetWare operating system on the file server. You can execute SERVER from drive A: or from a DOS partition on drive C:. After SERVER executes, you can load disk or LAN drivers to complete the operating system configuration. Once the system is configured, you can enter console commands or load loadable modules to maintain and monitor network activity.

ABORT REMIRROR

Why Use ABORT REMIRROR?

Use ABORT REMIRROR to stop the remirroring of a logical partition.

Command Format

```
ABORT REMIRROR number
```

Command Parameter

Replace *number* with the number of the logical partition you want to stop remirroring for.

Stop Remirroring a Logical Partition

To halt the process of remirroring a logical partition, type

```
ABORT REMIRROR number <Enter>
```

For example, to stop remirroring for logical partition 2, you would type

```
ABORT REMIRROR 2 <Enter>
```

Additional Information

For more information about partition remirroring, see “[REMIRROR PARTITION](#)” on page 223.

ADD NAME SPACE

Why Use ADD NAME SPACE?

Use ADD NAME SPACE to allow non-DOS files (such as Macintosh files) to be stored on a NetWare volume. Execute this command only once for each non-DOS naming convention that you want to store on a volume.

Before you can use this command, you must load the name space module. For instructions, see “LOAD name space” on page 162.

Command Format

```
ADD NAME SPACE name [TO [VOLUME]] volume_name
```

Command Parameters

Replace *name* with the name of the variable for the name space module you loaded. (See the documentation that comes with the name space module or use ADD NAME SPACE without any variables to display the name of the loaded name spaces.)

Replace *volume_name* with the name of the volume you want to store the non-DOS files on.

Additional Information

When adding name space, you should be aware of the following special considerations:

- ◆ You will need more file server memory.
- ◆ You must run VREPAIR to reverse ADD NAME SPACE.

Calculating Extra Memory Required for the Name Space

Your file server needs extra memory for each name space you add to a volume. Unless all users on your system will be using the name space, we recommend that you have a separate volume for each non-DOS name space that you add to your file server.

IMPORTANT: It's possible that if you add name space to the volume, you might not have enough memory in the file server to mount the volume.

Before adding a name space to a volume, calculate the amount of memory that the name space will require. First, view the current volume size with `INSTALL`. Then use the formulas described in the following table to estimate the total amount of memory needed per volume.

Figure 1 Calculating extra memory required for the name space

How much memory does your server need?

1. Calculate the memory requirement for each volume.

For each DOS volume:

$$M = .023 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

For each volume with added name space:

$$M = .032 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

2. Add the memory requirements for all volumes.

$$\text{Total Volume Memory} = M_{\text{SYS}} + M_{\text{VOL1}} + M_{\text{VOL2}} + \dots$$

3. Add 2 MB for the operating system and round the figure to the next higher MB.
4. Your computer needs at least 4 MB to run NetWare. If Steps 1 through 3 have only arrived at 3 MB, assume a minimum memory requirement of 4 MB anyway.

Example:

A server has four volumes, each with a block size of 4:

SYS: an 80MB DOS volume

DOSVOL: a 100MB DOS volume

UNIXVOL: a 300MB volume with name space

MACVOL: a 100MB volume with name space

1. Memory requirement for each volume:
 $M_{\text{SYS}} = .023 \times 80 \text{ MB} \div 4 = 0.46 \text{ MB}$
 $M_{\text{DOSVOL}} = .023 \times 100 \text{ MB} \div 4 = 0.575 \text{ MB}$
 $M_{\text{UNIXVOL}} = .032 \times 300 \text{ MB} \div 4 = 2.4 \text{ MB}$
 $M_{\text{MACVOL}} = .032 \times 100 \text{ MB} \div 4 = 0.8 \text{ MB}$

2. Total volume memory requirements: $0.46 + 0.575 + 2.4 + 0.8 = 4.235 \text{ MB}$

3. Operating system memory requirements: $2 + 4.235 = 6.235 \gg 7 \text{ MB}$

4. 7 MB is higher than the 4 MB minimum; therefore, no further adjustment is needed. Your server needs at least 7 MB of memory.

Reversing ADD NAME SPACE

Once a volume is set to store non-DOS files, you can reverse the setting only by running VREPAIR and destroying all the non-DOS file data.

Set Up a Volume to Store Non-DOS Files

To set up a volume to store non-DOS files, complete the following.

Procedure

- 1 Make sure the module for the non-DOS files is loaded.

Type

```
MODULES <Enter>
```

If the module has not been loaded, see [“LOAD name space” on page 162](#) for instructions.

- 2 Configure the volume for the new name space.

For example, to add Macintosh name space to the MACVOL volume, type

```
ADD NAME SPACE MAC TO MACVOL <Enter>
```

List the Current Name Space

To see the name space support already added, type

```
ADD NAME SPACE <Enter>
```

A message similar to the following appears:

Figure 2 Name space support screen

```
Missing name space name
Syntax: ADD NAME SPACE <name space name>
       [TO [VOLUME]] <volume name>

Loaded name spaces are:
  DOS
  MAC
```

BIND

Why Use BIND?

Use BIND to link LAN drivers to a communication protocol and to a specific network board in the file server. Unless you link a communication protocol to the board, the board cannot process packets.

NOTE: You may not need to use the BIND command. The “Product Options” feature of INSTALL may automatically insert a BIND command in an .NCF file. Consult the documentation for the network products that you use with your file server.

Before you can bind the LAN driver, you must first install the network board and load the LAN driver. See [“LOAD LAN driver” on page 133](#).

Command Format

```
BIND protocol [TO] LAN_driver | board_name  
[driver_parameter...] [protocol_parameter...]
```

Command Parameters

Replace *protocol* with IPX™ or some other protocol. Consult NetWire®, your Novell Authorized ResellerCLM, or third-party dealers for other available options. If the communication protocol will not bind to the driver, see [“PROTOCOL” on page 217](#).

Replace *LAN_driver* with either the name of the driver you loaded for the network board or the *board_name* you assigned when you loaded the driver.

Driver Parameters

Include a *driver_parameter* when you have more than one network board of the same type in your file server. (You do *not* need driver parameters if you bind a protocol to a board name rather than to a LAN driver.)

Replace *driver_parameter* with one or more of the following parameters.

DMA=*number*

FRAME=*name*

INT=*number*

MEM=*number*

PORT=*number*

SLOT=*number*

Include those that make the network board unique from all other network boards of its type. If you include the driver parameter with the command, you must enclose it in square brackets.

DMA=*number*

Identifies the DMA channel the driver is using for the network board. Bind the protocol with the same DMA channel that you used when you loaded the driver for the board.

FRAME=*name*

Identifies the frame type the driver is using for the network board. Bind the protocol with the same frame type that you used when you loaded the driver for the board.

INT=*number*

Identifies the interrupt the driver is using for the network board. Bind the protocol with the same interrupt that you used when you loaded the driver for the board.

MEM=*number*

Identifies the memory address the driver is using for the network board. Bind the protocol with the same memory address that you used when you loaded the driver for the board.

PORT=*number*

Identifies the I/O port the driver is using for the network board. Bind the protocol with the same I/O port that you used when you loaded the driver for the board.

SLOT=*number*

Identifies the network board by the slot that the network board was installed in. This parameter is used with microchannel and EISA computers. Bind the protocol with the same slot number that you used when you loaded the driver for the board.

Protocol Parameters

Use *protocol_parameter* for the parameters unique to the communication protocol. IPX has one parameter: NET. (See the documentation that comes with other protocols for their specific protocol parameters.)

NET=*number*

Identifies a unique network number for the cabling system attached to the board.

- ◆ If the board is attached to an existing cabling system, use the network address of that cabling system.
- ◆ If the board is attached to a new cabling system, select a hexadecimal number that is different from all other network numbers (IPX internal network numbers and cabling systems).
- ◆ If you have loaded the driver with more than one frame type for a single board in the file server, you must select a hexadecimal number that is different from all other network numbers (IPX internal network numbers and cabling systems). Do *not* use the same number that was used for another frame type on the cabling system.

You must specify this parameter when you bind IPX. If you do not enter this parameter at the command line, the operating system prompts you for a network number.

Bind a Protocol to a Driver

The steps for binding a protocol to a driver vary with how the driver has been loaded. Select the procedure that fits your situation.

Driver Loaded Only Once

To bind a driver when the file server has only one network board of a particular type (such as an RX-Net board), complete the following steps.

Procedure

1 Type

```
BIND IPX TO TRXNET <Enter>
```

2 Enter the network number for the cabling scheme.

NOTE: To bind the driver automatically when the file server is booted, add the following line to the AUTOEXEC.NCF file. In this example, the network number is 26. The line should follow the LOAD command for the driver.

```
BIND IPX TO TRXNET NET=26
```

3 Repeat the process for each driver in the file server.

Driver Loaded More than Once for Additional Network Boards

For file servers with multiple network boards of the same type, direct the operating system to bind a specific board by completing the following steps.

Procedure

1 Complete one of the following. (Both of the examples below explain how to bind the NE2000 driver to IPX.)

- ◆ Type the command, including the driver and protocol parameters. Type

```
BIND IPX TO NE2000 [INT=4] NET=26 <Enter>
```

- ◆ Type the command and answer the prompts. Type

```
BIND IPX TO NE2000 <Enter>
```

The operating system lists the network boards installed in your file server and prompts you to enter the board number and the network number of the cabling system.

NOTE: To bind the driver automatically when the file server is booted, add the following line to the AUTOEXEC.NCF file. You must include complete configuration information in the file. In this example, network number = 26, port = 340, interrupt = 4, and frame type = Ethernet_802.3 (default). Enter the network number after *NET=*. The line should follow the command that loads the driver.

```
BIND IPX TO NE2000 PORT=340 INT=4  
FRAME=ETHERNET_802.3 NET=26
```

- 2 Repeat the process for the other boards in the server.

Driver Loaded with a Name for the Board

When a board has been given a name, as documented in [“LOAD LAN driver” on page 133](#), the operating system associates the driver parameters and the frame type with the board name. To bind the protocol to the board name, complete the following steps.

Procedure

- 1 To bind IPX to a board named BACKBONE, type

```
BIND IPX BACKBONE <Enter>
```

- 2 Enter the network number for the cabling scheme.

NOTE: To bind the driver automatically when the file server is booted, add the following line to the AUTOEXEC.NCF file. In this example, the network number is 26 and the board name is BACKBONE. The line should follow the load command for the driver.

```
BIND IPX TO BACKBONE NET=26
```

Driver Loaded More than Once for Additional Frame Types

To bind a protocol to a driver that is loaded with two or more frame types for the same network board, complete the following.

Procedure

- 1 To bind IPX to an NE2000 driver, type

```
BIND IPX TO NE2000 <Enter>
```

A list of configurations for the driver appears.

- 2 Enter the number of the configuration that you want to bind.
- 3 Enter the network number for the cabling scheme.

Each frame type must use its own unique network address for the cabling scheme. For additional information see “Network numbering” in *Concepts*.

NOTE: To bind the driver automatically when the file server boots, add the following line to the AUTOEXEC.NCF file. You must include complete configuration information. The line should follow the load command for the driver.

```
BIND IPX TO NE2000 [PORT=300 INT=3 FRAME=ETHERNET_SNAP]  
NET=26
```

- 4 Repeat the process for each frame type.

BROADCAST

Why Use BROADCAST?

Use BROADCAST to send a message to all users logged in or attached to the file server or to a list of users or connection numbers.

Command Format

```
BROADCAST "message" [[TO] username|connection number]
[[and|,] username|connection number...]
```

Command Parameters

Replace *message* with the text (up to 55 characters) you want to send.

If no user or connection number is specified, the message is sent to all attached users.

Replace *username* with the user or users you want to send the message to. Separate multiple users with a comma, a space, or *and*.

Replace *connection number* with the number of the workstation you want to send the message to. Separate multiple connection numbers with a comma, a space, or *and*. To determine the connection number, see “[Connection Information](#)” on page 180.

Additional Information

Who Receives Messages

All logged-in users except the following receive the messages:

- ◆ Users who have used the CASTOFF ALL utility.
- ◆ Users who are logged in using ACS or NACS.
- ◆ Users who are logged in on remote workstations.
- ◆ Users who are using some graphics applications. These users may still hear the beep and should press <Ctrl><Enter> to proceed. To prevent the beep, users can run CASTOFF ALL before running the graphics applications.

Where Messages Appear

The BROADCAST message appears on the 25th line of the screen. Messages do not interfere with the workstation's screen display; however, the user cannot make any entries on the screen until the message is cleared.

How to Clear Messages

To clear the message from a workstation screen and resume work, press <Ctrl><Enter> at the workstation.

How to Stop Message Displays

Use CASTOFF with the ALL option to prevent messages from being received or displayed.

Send a Console Message

Send a Message to All Users

To send a message to all users logged in or attached to the file server, type
BROADCAST *message* <Enter>

You do not need to use quotation marks when you send a message to all users.

Send a Message to a Specific User

To send a message to a user named Jack, type
BROADCAST "*message*" Jack <Enter>

Send a Message to a Specific Workstation

To send a message to workstation number 1, type
BROADCAST "*message*" 1 <Enter>

Send a Message to Users and Workstations

To send a message to users Fred, Jack, and Mary and to workstations 1 and 4, you can type

BROADCAST "*message*" to Fred, Jack, 1, 4, Mary <Enter>

CDROM

Why Use CDROM?

Use CRRROM to allow the server to use a CD-ROM disk as a read-only volume.

Command Format

```
LOAD [path] CDROM
```

Command Parameters

Replace *path* with the full path to the directory containing the CDROM module.

Using CDROM

The following sections explain these tasks that can be accomplished using the console commands associated with the CDROM.NLM:

- ◆ Display Help information.
- ◆ List the CD-ROM devices.
- ◆ List all volumes identified on the CD-ROM devices.
- ◆ Dismount a CD-ROM volume.
- ◆ Request the root directory of a volume.
- ◆ Mount a CD-ROM volume.
- ◆ Change the media in a CD-ROM drive.
- ◆ Decrease the time required to remount a volume.

Display Help Information

To display help information at the console, type

```
CD HELP <Enter>
```

NOTE: CD HELP is available only if you have loaded the CDROM.NLM.

List the CD-ROM Devices

To list the CD-ROM devices that the system knows about at the console, type

CD DEVICE LIST <Enter>

- ◆ Devices are listed in groups of 10. If you repeat the command, the next group of 10 devices is listed.
- ◆ The list includes the following for each device:
 - Device number
 - Device name
 - Media volume name (if found)
 - Volume mount status
- ◆ “Device” is the CD-ROM drive that contains the system interface and allows the CD-ROM to read the information.

List All Volumes Identified on the CD-ROM Devices

To	Type
List all the volumes identified on the CD-ROM devices that the system knows about at the console	CD VOLUME LIST

- ◆ Volumes are listed in groups of 10. If you repeat the command, the next group of 10 volumes is listed.
- ◆ The list includes the following for each volume:
 - Device name
 - Volume mount status
- ◆ The **CD VOLUME LIST** command doesn't display information for devices that do not have media present.

Dismount a CD-ROM Volume

To	Type
Dismount a previously mounted CD-ROM volume	CD DISMOUNT [<i>device number</i>] [<i>volume name</i>]

- ◆ Specify the device, the drive number of the currently mounted volume, or the volume name.
- ◆ After CD DISMOUNT is executed, all system resources are returned to the system.

Request the Root Directory of a Volume

To	Type
Request the root directory of a volume from the console	CD DIR [<i>device number</i>] [<i>volume name</i>]

- ◆ Specify the device, the drive number of the currently mounted volume, or the volume name.
- ◆ CD DIR lists directory entries in DOS format.
- ◆ CD DIR allows you to view the contents of a CD-ROM volume to verify a volume root directory.
- ◆ Each CD-ROM is treated as one volume for NetWare access. The volume does not need to be mounted to use CD DIR.

Mount a CD-ROM Volume

To	Type
Mount a CD-ROM volume	CD MOUNT [<i>device number</i>] [<i>volume name</i>]

- ◆ Specify the device, the drive number of the volume, or the volume name.
- ◆ The mounted CD-ROM volume is a NetWare read-only volume.
- ◆ Volume names must be unique.

Change the Media in a CD-ROM drive

To	Type
Change the media in a CD-ROM drive	CD CHANGE [<i>device number</i>] [<i>volume name</i>]

- ◆ Specify the device, the drive number of the currently mounted volume, or the volume name.
- ◆ The volume is dismounted and you are prompted to replace the media.
- ◆ The new media is mounted as a NetWare volume.
- ◆ During mounting or changing a CD-ROM disk, the selected device is deactivated. This is normal.

Decrease the Time Required to Remount a Volume

To	Type
Decrease the time required to remount a volume when working with several CD-ROMs that have large directories	CD MOUNT [<i>device number</i>] [<i>volume name</i>] /R

- ◆ The /R option tells the system to reuse existing data files instead of recreating or rebuilding them. This allows volumes to be remounted faster.

CLEAR STATION

Why Use CLEAR STATION?

Use CLEAR STATION when a workstation has somehow “crashed” and left open files on a file server. The file server closes the workstation’s files and erases all the server’s internal tables for the workstation (including drive mappings not saved in the login script). The communication link between the file server and the cleared workstation is broken.

Command Format

```
CLEAR STATION n
```

Command Parameters

Replace *n* with the number of the workstation you want to clear from the file server. To determine the connection number, use MONITOR at the file server console to view “Connection Information” or use USERLIST at the workstation.

IMPORTANT: If you use CLEAR STATION while the workstation is in the middle of a transaction or a file update, files might be saved with incorrect data.

Remove All File Server Resources from a Workstation

To clear a workstation, enter CLEAR STATION at the file server console, replacing *n* with the number of the workstation. (You can determine the number of the workstation by using MONITOR at the file server or USERLIST at a workstation.)

For example, to clear workstation 5, type

```
CLEAR STATION 5 <Enter>
```

Attached to one file server. If the cleared workstation is attached to only one file server when CLEAR STATION is executed, the workstation shell automatically attempts to re-establish a connection with the default file server.

The following message appears on the workstation screen:

Figure 3 CLEAR STATION message screen

```
Network error on server SPEEDY:  
Connection no longer valid.  
Abort? Retry? Fail?
```

Type “A” (for abort) to remove the file server resources from your workstation.

Attached to multiple file servers. If the cleared workstation is attached to another file server and has a drive mapped to that server, the following message appears at the workstation:

```
Current drive is no longer valid.  
Change to a valid drive.
```


CLIB

Why Use CLIB?

Use CLIB if you have a loadable module (such as PSERVER or BTREVE) that requires CLIB's library of routines and functions. Load CLIB before the loadable module that uses it.

CLIB requires the STREAMS module. If you do not load STREAMS before CLIB, the operating system will load STREAMS for you. See [“STREAMS” on page 301](#).

Command Format

```
LOAD [path] CLIB
```

Command Parameters

Replace *path* with a full path to the directory containing the CLIB module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a *path*, the operating system looks for CLIB in SYS:SYSTEM. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

CLIB sets a time zone when it loads. Since the default is Eastern Standard Time, use the console command SET TIMEZONE (see [“SET TIMEZONE” on page 293](#)) in the AUTOEXEC.NCF file to change the time zone for your location when the file server boots.

Load CLIB

To load CLIB, type

```
LOAD CLIB <Enter>
```

NOTE: To make sure that the CLIB and STREAMS load automatically when the file server boots, add the following commands to the AUTOEXEC.NCF file:

LOAD STREAMS

LOAD CLIB

For instructions on editing the AUTOEXEC.NCF file, see **"INSTALL"** on page 69, or **"EDIT"** on page 64, or see "SYSCON" in *Utilities Reference*.

CLS

Why Use CLS?

Use CLS to clear the file server console screen.

Command Format

CLS

Clear the File Server Console Screen

To clear the console screen, type

CLS <Enter>

You can also use OFF to clear the console screen.

CONFIG

Why Use CONFIG?

Use CONFIG to display the following information:

- ◆ The file server name
- ◆ The internal network number of the file server
- ◆ The loaded LAN drivers
- ◆ The hardware settings on all network boards

Use CONFIG before installing any memory boards, network boards, or host bus adapters in the file server so that you have a current list of all hardware settings on the network boards.

- ◆ The node (station) addresses of the network boards

Consult this utility to make a current list of all assigned node addresses.

- ◆ The communication protocol bound to the network board
- ◆ The network number of the cabling scheme for a network board
- ◆ The frame type assigned to the board

More than one frame type can be assigned to Ethernet and Token-Ring boards

- ◆ The board name assigned

For an explanation of internal network numbers, network numbers for cabling, and node address, see “Network numbering” in *Concepts*.

Command Format

`CONFIG`

Additional Information

Use `MODULES` and `MONITOR` to display information about loadable modules linked to the operating system.

Use `INSTALL` and `MONITOR` to display configuration information about disk drivers.

Use DISPLAY NETWORKS to list all network numbers being used by file servers on your network.

Display Configuration Information

At the file server console, type

CONFIG <Enter>

Information similar to the following appears on the console screen:

Figure 4 Configuration information screen

```
File Server name: SPEEDY
IPX internal network number: 1986ABE1

NE-2000 LAN Driver V3.10 (900308)
  Hardware setting: I/O Port 300h to 31Fh, Interrupt 3h
  Node address:00001B0280A3
  Frame type:Ethernet_802.3
  Board name: BACKBONE
  LAN protocol:IPX network 00D0C200
```

DISABLE LOGIN

Why Use DISABLELOGIN?

Use `DISABLE LOGIN` to prevent users from logging in to the file server.

Use this command when you do not want users logged in because you are making repairs, backing up files, or loading software.

Command Format

```
DISABLE LOGIN
```

Prevent Users from Logging in to the File Server

To prevent users from logging in to the file server, type

```
DISABLE LOGIN <Enter>
```

Users logged in to the file server are not affected. However, once a user logs out, the user cannot log in again until `ENABLE LOGIN` is executed.

DISABLE TTS

Why Use DISABLE TTS?

During normal operation, you do *not* need to disable TTS (Transaction Tracking System); the file server automatically disables TTS if necessary.

TTS, an integral part of the file server operating system, protects the bindery from becoming corrupted. Disabling TTS frees up very little file server memory for other loadable modules (about 40 bytes for most transactions, and at most 400KB). For a complete description, see “TTS” in *Concepts*.

DISABLE TTS is primarily a tool for application developers who need to test transactional applications with TTS disabled.

To restore TTS after you have disabled it, use ENABLE TTS or reboot the file server.

Command Format

```
DISABLE TTS
```

Disable TTS in the File Server

To disable TTS, type

```
DISABLE TTS <Enter>
```

The following message appears:

```
TTS disabled by operator.
```

TTS remains disabled until you enable it with ENABLE TTS or reboot the file server.

DISKSET

Why Use DISKSET?

Use DISKSET to do the following tasks:

- ◆ Install an ADIC/Novell DCB subsystem.
- ◆ Place identification information about external hard disks on the EEPROM chip of the host bus adapter board.
NOTE: The term “host bus adapter,” as used in this manual, includes the specific product “Disk Coprocessor Board” (DCB).
- ◆ Place configuration information about the hard disks attached to the host bus adapter on the board’s EEPROM chip.
- ◆ Format an external hard disk through the host bus adapter.
- ◆ Back up the NetWare Ready configuration information from a NetWare Ready disk to a diskette.
- ◆ Restore the NetWare Ready configuration information from a backup diskette to the NetWare Ready disk.

WARNING: If you are using a DCB disk driver for a disk subsystem, run DISKSET.EXE before installing your NetWare server.

Command Format

```
DISKSET [path]
```

Command Parameters

Replace *path* with the full path to the directory containing DISKSET.

Refer to the README.312 file on the installation diskette for information on the source diskette or directory. (On CD-ROM, the README.312 file is in each language directory under NETWARE.312)

Using DISKSET

- ◆ Refer to the ADIC manual for information on running DISKSET.EXE.
- ◆ You may need to refer to the documentation for your board.
- ◆ The configuration information allows the NetWare server to communicate with the hard disk through the host bus adapter.

DISMOUNT

Why Use DISMOUNT?

Use DISMOUNT to make a volume unavailable to users. This allows you to maintain or repair the volume and to upgrade disk drivers while the file server is up.

If you have a volume that is not used very often, you can dismount it until you need to use it again. Mounted volumes take up memory allocated for file caching and slow down the system.

Command Format

```
DISMOUNT volume_name
```

Dismount a Volume

To dismount a volume, complete the following steps at the file server console.

Procedure

- 1** Use BROADCAST to inform all users that they should close all files and not work in the volume you are going to dismount.
- 2** Dismount the volume by typing

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with the name of the volume you want to dismount.

DISPLAY NETWORKS

Why Use DISPLAY NETWORKS?

Use DISPLAY NETWORKS to list all networks and assigned network numbers that the file server router recognizes. All network numbers (internal and cabling system) are listed.

To see a list of servers on the network, use the DISPLAY SERVERS command.

Command Format

```
DISPLAY NETWORKS
```

Display a List of Networks

To display a list of networks, type

```
DISPLAY NETWORKS <Enter>
```

Information similar to the following appears on the console screen:

Figure 5 DISPLAY NETWORKS information screen

```
:display networks
 00000001 0/1      00000003 1/2      00000004 2/3
 00000056 2/3      000000AD 0/1      000000FF 3/4
There are 6 known networks
```

This screen shows the network number, the number of hops (networks that must be crossed) to reach the network, and the estimated time in ticks (1/18 of a second) for a packet to reach the network. The number of known networks is displayed at the bottom of the screen.

If a file server is running NetWare v3.1x, both the internal IPX network numbers and the cabling network numbers are displayed.

In the previous example screen display, two network numbers are zero hops away.

- ◆ One number (00000001) is the internal network number for the file server on which the DISPLAY NETWORKS command was issued.
- ◆ One number (000000AD) is the cabling system number of the file server on which the DISPLAY NETWORKS command was issued.

If the file server had more than one network board installed, more than two numbers would be zero hops away.

DISPLAY SERVERS

Why Use DISPLAY SERVERS?

Use DISPLAY SERVERS to list all servers that the file server router recognizes.

To see a list of networks, use the DISPLAY NETWORKS command.

Command Format

```
DISPLAY SERVERS
```

Display a List of File Servers

To list known file servers, type

```
DISPLAY SERVERS <Enter>
```

Information similar to the following appears on the console screen:

Figure 6 DISPLAY SERVERS information screen

```
:display servers
  REED 1    FOUR 1    PROFIT 2    ACCT 5
  PLAIN 2   SKY  0    AUDIT 3    SALES 3
There are 8 known servers
```

The list shows the known servers' names and the number of hops (networks that must be crossed) to reach each server. The number of known servers is displayed at the bottom of the screen.

NOTE: If your file server's name does not appear in the list, volume SYS: is not mounted.

DOWN

Why Use DOWN?

Use DOWN to ensure data integrity before turning off the power to the file server. DOWN ensures data integrity by writing all cache buffers to disk, closing all files, and updating the appropriate Directory and File Allocation Tables.

Command Format

DOWN

Additional Information

Changes made to data files are held in memory (cache buffers). These changes are not normally written to the disk until a minimum time has passed (the default is 3 seconds). When DOWN is used, the file server writes the file cache buffers to disk, updates the tables, and closes the files. These changes will be lost if you turn off the power without downing the file server first.

After you down the file server, the server is still connected to the network and still receives packets. You can continue to execute console commands, such as TRACK ON and TRACK OFF, that deal with packets.

Down the File Server

To down the file server, complete the following steps.

Procedure

- 1** Use BROADCAST to inform all users that they should close all files and log out.
- 2** Type
DOWN <Enter>

Information similar to the following appears:

Figure 7 DOWN server information screen

```
Notifying stations that the file server is down
Dismounting volume SYS
4/21/93 2:30pm: Bindery close requested by the SERVER
4/21/93 2:31pm: SPEEDY TTS shut down because backout
                volume SYS was dismounted.

Server SPEEDY has been shut down.
Type EXIT to return to DOS.
```

NOTE: You can use EXIT to return to DOS. However, if you have used the REMOVE DOS command prior to issuing the DOWN command, the EXIT command will reboot the server.

If files are still open, the monitor displays the files that are open, the user who opened them, and the workstation connection number. The following prompt then appears:

```
Down server anyway? n
```

Examine the list of open files and answer

- ◆ “No” if database files or word processing files are open; you should close these files from the application rather than from the file server.

Press <Enter>; then either broadcast another message or go to the workstations and close the files.

- ◆ “Yes” if the files will not be corrupted or lose data when the connection is broken.

Type “Y” and press <Enter>.

EDIT

Why Use EDIT?

Use EDIT to create or modify a text file. EDIT is particularly useful in creating .NCF batch files to execute file server commands automatically. You can use EDIT with text files on either DOS or NetWare partitions. EDIT.NLM can be used to edit files of 8 KB or less.

Command Format

```
LOAD [path] EDIT
```

Command Parameters

Replace *path* with a full path to the directory containing the EDIT module.

Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path, the operating system looks for EDIT in SYS:SYSTEM. (Use SEARCH to set up additional paths for automatic searching.)

Edit or Create Text Files

To load the EDIT.NLM and edit a text file, complete the following steps.

Procedure

- 1** Load the module by typing

```
LOAD EDIT <Enter>
```
- 2** At the “File to Edit” prompt, enter the complete directory path for the file.
For example, to edit the AUTOEXEC.NCF file in the SYSTEM directory, type

```
SYS:SYSTEM/AUTOEXEC.NCF <Enter>
```

A file or a blank screen appears, depending on whether you are editing or creating a file. The path you entered appears at the top of the screen.
- 3** After editing or creating the text file, press <Esc> to exit.
- 4** When the confirmation box appears, select “Yes” to save the file or “No” to exit without saving the changes.

ENABLE LOGIN

Why Use ENABLE LOGIN?

Use ENABLE LOGIN to re-enable the login function or to enable the SUPERVISOR's account when the account has been locked by the intruder detection function.

You do not need to use ENABLE LOGIN when you boot the file server. The login function is automatically enabled during the bootup process.

Command Format

```
ENABLE LOGIN
```

Allow Users to Log In

To allow users to log in again after you have disabled the login function, type

```
ENABLE LOGIN <Enter>
```

All login privileges are restored.

ENABLE TTS

Why Use ENABLE TTS?

Use ENABLE TTS to start the transaction tracking (NetWare Transaction Tracking System, or TTS) in the file server.

Normally transaction tracking is always enabled. However, you can disable TTS with DISABLE TTS.

The file server automatically disables TTS if one of the following happens:

- ◆ Volume SYS: gets full. (SYS: is the TTS backout volume.)
- ◆ The file server has insufficient memory to operate TTS.

After TTS has been disabled (automatically or manually), use the ENABLE TTS command to enable TTS in the file server.

Command Format

```
ENABLE TTS
```

Additional Information

For a complete description, see “TTS” in *Concepts*.

For more information on the TTS\$LOG.ERR file, see [“TTS Problems” on page 419](#).

Enable TTS in the File Server

To enable TTS in the file server, type

```
ENABLE TTS <Enter>
```

The following message appears:

```
Transactional tracking system enabled
```

If you try to enable TTS when the SYS volume is not mounted or when the file server does not have sufficient resources (disk space or memory) to enable TTS, you will receive one of the following messages.

- ◆ If you try to enable TTS when the SYS volume is not mounted, the following message appears:

```
TTS can not be enabled because the TTS work volume is not mounted.
```

Mount volume SYS: with MOUNT before you enable TTS.

- ◆ If volume SYS: is full, the following message appears:

```
TTS disabled because of error allocating more disk space for the backout file.
```

To allow sufficient space for the backout TTS file, you must free up 1 MB of disk space on volume SYS:.

- ◆ If you try to enable TTS when the file server does not have enough free memory, the following message appears:

```
TTS cannot allocate sufficient memory.
```

TTS requires about 40 bytes of memory to track a transaction. TTS can track up to 10,000 individual transactions. You should not need more than 400 KB of memory for TTS.

To increase the amount of memory available for TTS, do one or more of the following:

- ◆ Unload any file server modules that you do not need (such as INSTALL or MONITOR).

Use ENABLE TTS again to see if you have freed up enough memory for TTS. If you have, TTS will be enabled

- ◆ Dismount any disk volumes (other than SYS) that users are not currently using.

Use ENABLE TTS again to see if you have freed up enough memory for TTS. If you have, TTS will be enabled.

- ◆ Add more memory to the file server. After you have installed the memory, the file server will automatically enable TTS when it boots.

EXIT

Why Use EXIT?

Use EXIT to return to DOS after you have downed the file server. This allows you to access DOS files or rerun the SERVER.EXE file with new parameters.

Use EXIT to warm boot the file server after you have issued the REMOVE DOS and DOWN commands.

For further information, see [“DOWN” on page 62](#) and [“REMOVE DOS” on page 226](#).

Command Format

EXIT

Return to DOS after Downing the File Server

To return to DOS after you have used the DOWN command, type

EXIT <Enter>

Warm Boot the File Server

To warm boot the file server after you have used the REMOVE DOS and DOWN commands, type

EXIT <Enter>

INSTALL

Why Use INSTALL?

Use INSTALL to complete the following installation and maintenance tasks:

- ◆ Create, delete, test, or modify NetWare hard disk partitions.
- ◆ Mirror or unmirror hard disks.
- ◆ Create, delete, expand, or modify volumes.
- ◆ Create or modify the AUTOEXEC.NCF and STARTUP.NCF files.
- ◆ Copy the SYSTEM and PUBLIC files onto the file server.
- ◆ Format a hard disk.
- ◆ Execute a surface test of the hard disk for bad blocks.
- ◆ Load the NetWare diskettes.
- ◆ Install and configure products on the file server.

Command Format

```
LOAD [path] INSTALL [NH]
```

Command Parameters

Replace *path* with the path to the directory containing INSTALL. Begin with a DOS drive letter or a NetWare volume name.

If you do not specify a path and volume SYS: has been mounted, the operating system looks for INSTALL in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

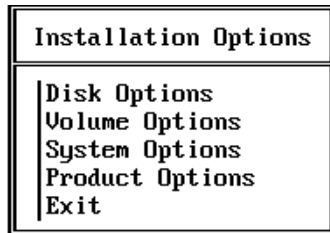
The optional NH parameter loads INSTALL without help screens, saving 16 KB. This is useful if your available cache memory is low. (Use MONITOR to view memory statistics.)

Main screen

INSTALL is a menu program. As you move through the INSTALL menus, press <F1> at any time for help.

The main menu screen for INSTALL appears below, with the tasks that relate to each menu option following.

Figure 8 **INSTALL main menu**



Install

Task	Page
Load INSTALL	"Load INSTALL" on page 72

Disk Options

Task	Page
Add a hard disk to the file server	"Add a Hard Disk to the File Server" on page 72
Replace a hard disk	"Replace a Hard Disk" on page 74
Recover volume data from an unmirrored hard disk	"Recover Volume Data from an Unmirrored Hard Disk" on page 76
Format a hard disk	"Format a Hard Disk" on page 76
Create NetWare partitions	"Create NetWare Partitions" on page 79
Delete partitions	"Delete Partitions" on page 81
Edit Hot Fix information	"Edit Hot Fix Information" on page 82
Mirror or duplex hard disks	"Mirror or Duplex Hard Disks" on page 84
Unmirror hard disks	"Unmirror Hard Disks" on page 86
Test hard disks for bad blocks	"Test Hard Disks for Bad Blocks" on page 86

Volume Options

Task	Page
Create a volume	“Create a Volume” on page 89
Delete a volume	“Delete a Volume” on page 91
Rename a volume	“Rename a Volume” on page 92
Increase the size of a volume	“Increase the Size of a Volume” on page 93

System Options

Task	Page
Copy the SYSTEM and PUBLIC files	“Copy the SYSTEM and PUBLIC Files” on page 95
Change the file server’s name	“Change the File Server’s Name” on page 95
Change the file server’s internal network number	“Change the File Server’s Internal Network Number” on page 96
Create the AUTOEXEC.NCF file	“Create the AUTOEXEC.NCF File” on page 97
Edit the AUTOEXEC.NCF file	“Edit the AUTOEXEC.NCF File” on page 98
Create the STARTUP.NCF file	“Create the STARTUP.NCF File” on page 102
Edit the STARTUP.NCF file	“Edit the STARTUP.NCF File” on page 102

Product Options

Task	Page
Install, uninstall, or configure a product on the file server	“Install, Uninstall, or Configure a Product on the File Server” on page 104

Exit

Task	Page
Exit INSTALL	“Exit INSTALL” on page 105

Load INSTALL

To load INSTALL, type

```
LOAD INSTALL <Enter>
```

If INSTALL is already loaded, the following message appears:

```
This module is ALREADY loaded and cannot be loaded more than  
once.
```

If this message appears, complete one of the following:

- ♦ Press <Alt><Esc> to move through the activated screens until the INSTALL screen appears.
- ♦ Press <Ctrl><Esc> and select “Install Screen” from the list of available screens.

Add a Hard Disk to the File Server

When a volume needs to be expanded, you can add a new hard disk to the file server and designate it as a new segment of an existing volume.

The steps for adding an internal hard disk vary from the steps for installing an external hard disk. Follow the procedure in one of the following sections that fits your situation.

Add Internal Hard Disk

To install an internal hard disk, complete the following steps.

Procedure

- 1** Use BROADCAST to inform all users that the file server is going down.
- 2** Down the file server by typing

```
DOWN <Enter>
```
- 3** Turn off the power and install the new hardware.
- 4** Boot the file server.
- 5** Load INSTALL.
- 6** Create a NetWare partition.

If you need help, see [“Create NetWare Partitions” on page 79](#).

7 Designate the partition as a new segment of an existing volume.

If you need help, see [“Increase the Size of a Volume” on page 93](#).

Add External Hard Disk in a Subsystem

Users can stay logged in to the file server while the following steps are performed, but the disk driver to the subsystem must *not* be loaded. All volumes with data stored on the subsystem must *not* be mounted.

To add a hard disk to the subsystem, complete the following steps.

Procedure

1 Dismount all volumes with data on the disks in the subsystem by typing

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with the name of the volume that needs to be dismounted. Repeat this step for each volume that has data stored on the subsystem.

2 Unload the disk driver for the subsystem by typing

```
UNLOAD driver <Enter>
```

Replace *driver* with the name of the disk driver. Repeat this step for each disk driver that controls hard disks in the subsystem.

3 Turn off the power to the disk subsystem and install the hard disk.

4 Turn on the power to the disk subsystem.

5 Load the disk drivers that you unloaded in Step 2.

6 Mount the volumes that you dismounted in Step 1.

7 (Conditional) Run DISKSET if the hard disk is connected to a host bus adapter.

If you need help, see [“DISKSET” on page 56](#).

8 Load INSTALL.

9 Create a NetWare partition.

If you need help, see [“Create NetWare Partitions” on page 79](#).

10 Designate the partition as a new segment of an existing volume.

If you need help, see [“Increase the Size of a Volume” on page 93](#).

11 Repeat Steps 9 and 10 for each new hard disk.

Replace a Hard Disk

If a hard disk becomes unreliable or unusable, follow these steps to remove the disk from the network. If you do not complete these steps, the driver will hang the system for a few minutes while it looks for the missing hard disk.

If you have been making backups of your data consistently, you will be able to reload data for the volumes affected by the disk failure.

WARNING: Deleting partitions and volumes destroys data. Make extra backups, if possible, before you begin.

Procedure

- 1 Dismount the volume at the console prompt by typing

```
DISMOUNT volume_name <Enter>
```

- 2 Load INSTALL.

- 3 If the hard disk is mirrored, unmirror it.

If you need help, see [“Unmirror Hard Disks” on page 86](#).

- 4 Delete the NetWare partition.

If you need help, see [“Delete Partitions” on page 81](#).

- 5 Complete one of the following:

- ♦ If the hard disk is located internally, press <Alt><Esc> and down the file server by typing

```
DOWN <Enter>
```

Then skip to Step 8.

- ♦ If the hard disk is located in a subsystem, dismount any other volumes that have data on hard disks in the subsystem by typing

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with the name of the volume that needs to be dismounted. Repeat this step for each volume with data stored on the subsystem.

- 6 If you are not replacing the hard disk with the same type of disk you are removing, run DISKSET (or the driver’s configuration utility) to remove the hard disk’s configuration information from the EEPROM chip.

7 Unload the disk driver for the subsystem by typing

UNLOAD driver <Enter>

Replace *driver* with the name of the disk driver. If more than one disk driver is controlling hard disks in the subsystem, repeat this step for each disk driver.

8 Turn off the system containing the disk.

9 Using the instructions that came with the hard disk, remove the hard disk and connect the replacement.

10 Complete one of the following:

- ♦ If the hard disk is located internally, run the computer's setup program. Then boot the file server and skip to Step 14.
- ♦ If the hard disk is located in a subsystem, reload the disk drivers.

11 Mount any dismounted volumes.

12 Run DISKSET (or the driver's configuration utility) and set up the configuration information on the EEPROM chip.

13 Load INSTALL.

14 Create a new partition.

If you need help, see [“Create NetWare Partitions” on page 79](#).

15 Complete one of the following:

- ♦ If the disk was not mirrored, create the volume and then restore the data from a backup. (See [“Create a Volume” on page 89](#).)
- ♦ If the hard disk was mirrored, remirror the disk. (See [“Mirror or Duplex Hard Disks” on page 84](#).)

IMPORTANT: If you replaced the “Not Mirrored” disk rather than the “Out Of Sync” disk, recover the volume data from the “Out Of Sync” disk *before* remirroring the disks. (See the following section.)

Recover Volume Data from an Unmirrored Hard Disk

Once a hard disk is unmirrored, its status is listed as either “Not Mirrored” or “Out Of Sync” on the “Partition Mirroring Status” list. When a hard disk is listed as “Out Of Sync,” the operating system does not recognize any volume information on the “Out Of Sync” hard disk.

To recover data from the “Out Of Sync” partition, complete the following steps.

Procedure

- 1** Load INSTALL.
- 2** Select “Disk Options” from the “Installation Options” menu.
- 3** Select “Mirroring” from the “Available Disk Options” menu.
- 4** Highlight the “Out Of Sync” partition and press <F3>.

The following warning may appear if another volume segment with the same name exists on another disk:

```
Warning!! The selected partition contains "volume <name>
segment <number>" and that volume is already defined.
<Press ESCAPE To Continue>
```

- 5** Press <Esc> and answer “Yes” at the “Rename the Volume Segment?” prompt.
- 6** Enter a unique name for the new volume segment.
- 7** Answer “Yes” to the prompt to salvage the volume segment.

Format a Hard Disk

Formatting is *not* a required step in NetWare v3.1x. Hard disks are usually formatted by the manufacturer.

IMPORTANT: If the manufacturer recommends that the hard disk be formatted, follow the manufacturer’s procedures. Most hard disks that require formatting have utilities (the DOS FORMAT command or a utility on a reference diskette) that must be performed *prior* to installation in the NetWare v3.1x file server.

Use INSTALL's "Format" option in the following instances:

- ◆ You have a hard disk that is unreliable and you hope to salvage the disk. (Formatting may not solve the problem.)
- ◆ The hard disk manufacturer recommends the procedure. Start with Step 3.
- ◆ You have changed the controller type on a hard disk, and the controller uses a different format for data storage. Start with Step 3.

IMPORTANT: Before you format a hard disk, make sure that all users have logged out of the file server and that no other network activity is occurring. Use BROADCAST to tell the users to log out. Use MONITOR to delete any remaining connections.

IMPORTANT: Once all connections are clear, use DISABLE LOGIN to prevent users from logging in during the procedure.

To format a hard disk, complete the following steps.

Procedure

- 1** Back up the data on the hard disk using NBACKUP or a third-party backup utility.
- 2** Dismount all volumes that have data on the hard disk you are going to format by typing

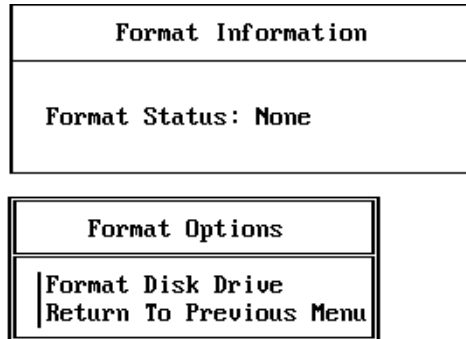
`DISMOUNT volume_name <Enter>`

Replace *volume_name* with the name of the volume that is on the hard disk. Repeat this step if you have more than one volume on the hard disk.
- 3** Load INSTALL.
- 4** Complete one of the following:
 - ◆ If the hard disk is mirrored, unmirror the disk. (See "Unmirror Hard Disks" on page 86.)
 - ◆ If the hard disk is not mirrored, delete the volumes on the hard disk. (See "Delete a Volume" on page 91.)
- 5** Select "Disk Options" from the "Installation Options" menu.
- 6** Select "Format (optional)" from the "Available Disk Options" menu.

- 7** If you have more than one hard disk, select the hard disk from the “Available Disk Drives” list.

The following screens appear:

Figure 9 INSTALL disk “Format information” and “Format Options” screens



The “Format Information” box can display the following status information:

<i>None</i>	The disk has not been formatted since INSTALL was last loaded.
<i>Formatting</i>	The disk is currently being formatted.
<i>Completed</i>	The disk has been formatted successfully.
<i>Not Supported</i>	The disk driver for the hard disk does not support the format command.
<i>Failed</i>	The disk failed the formatting process.

- 8** Select “Format Disk Drive” from the “Format Options” menu.

NOTE: If the hard disk still has NetWare information on it, you will be warned that you must delete the volumes first. Recheck the volume information to make sure you have dismounted all volumes.

If any partitions exist, you will be warned that all information on the disk will be lost. Press <Esc> to continue.

- 9** Enter the interleave factor.

The default is 2. Check the hard disk’s documentation for its interleave factor.

Once the interleave factor is entered, the formatting begins. Formatting can take a long time (from a few hours to a few days), depending on the disk's capacity.

NOTE: You cannot complete any other tasks with INSTALL while INSTALL is formatting. If you use <Esc> to return to a previous menu, INSTALL appears to be hung. Be patient. The status in the "Format Information" box will change to either "Completed" or "Failed."

- 10** If the format is successful, re-create a NetWare partition on the hard disk. See the following section.

Create NetWare Partitions

You can create a NetWare partition on any hard disk formatted at the factory or stamped as NetWare Ready. See "[Format a Hard Disk](#)" on page 76.

NOTE: If the hard disk has partitions on it that you want to delete, see "[Delete Partitions](#)" on page 81. Then continue with the following steps.

Procedure

- 1** Load INSTALL.
- 2** Select "Disk Options" from the "Installation Options" menu.
- 3** Select "Partition Tables" from the "Available Disk Options" menu.

- 4 Select the disk you need to partition from those listed on the “Available Disk Drives” menu.

Screens similar to the following appear:

Figure 10 INSTALL NetWare “Partition Type” and “Partition Options” screens

Partition Type	Start	End	Size
NetWare 386 Partition	0	635	635.9 Meg
Free Space	636	636	1.0 Meg

Partition Options
Change Hot Fix
Create NetWare Partition
Delete Partition
Return To Previous Menu

NOTE: If no partition table exists, you will see a message stating so. Press <Esc> to continue.

- 5 Select “Create NetWare Partition” from the “Partition Options” menu.

A form similar to the one below shows the total space on the hard disk and the blocks allocated to each function.

Figure 11 INSTALL NetWare “Partition Information” screen

Partition Information			
Partition Type: NetWare 386 Partition			
Partition Size:	636	Cylinders,	635.9 Meg
Hot Fix Information:			
Data Area:	160001	Blocks,	625.0 Meg
Redirection Area:	2811	Blocks,	1.7 %

NetWare automatically sets up the following configuration for the partition:

- ◆ All “Free Space” is assigned to the NetWare partition.
- ◆ The data area receives 98% of the available space.
- ◆ The Hot Fix redirection area receives 2% of the available space.

NOTE: Some NetWare-Ready hard disks leave a little free space even though you accept the defaults for using the whole disk for a NetWare partition. NetWare cannot use this free space.

- 6** To reduce the partition size, enter the new size in the “Partition Size” field.
- 7** To change the size of the Data Area or the Hot Fix Redirection Area, press <Enter> or use the arrow keys to move to either field.
- 8** Type the new number of blocks for that field and press <Enter>.

NetWare automatically assigns any remaining space to the other field.

WARNING: If you change the size of the Hot Fix area after data is stored on the hard disk, all data is destroyed. Back up data before you change the size of the Hot Fix area.

- 9** Press <Esc> and answer “Yes.”
- 10** Press <Esc> again.

If you need to create a partition on more than one hard disk, select the next hard disk from the “Available Disk Drives” list and repeat Steps 3 through 9.

Delete Partitions

You can use INSTALL to delete partitions (such as DOS, NetWare, or OS/2) on a hard disk. You may need to delete a partition for the following reasons:

- ◆ You are adding a hard disk that was previously used and you want to use the space for a NetWare v3.1x partition.
- ◆ The Hot Fix Redirection Area needs to be increased because all the blocks have been used.

WARNING: If you delete a partition, you destroy all data on the partition. If the data is important, back it up. Then continue with the following steps.

Procedure

- 1** Load INSTALL.
 - ◆ If the hard disk is mirrored, continue with Step 2.
 - ◆ If the hard disk is not mirrored, skip to Step 3.
- 2** Unmirror any hard disks associated with the partition.
See [“Unmirror Hard Disks” on page 86](#).
- 3** Complete one of the following:
 - ◆ If you are deleting the partition on the “Out Of Sync” partition, skip to Step 5.
 - ◆ If you are deleting the partition on the “Not Mirrored” partition, continue with Step 4.
- 4** Delete the volumes on the partition.
See [“Delete a Volume” on page 91](#).
- 5** Select “Disk Options” from the “Installation Options” menu.
- 6** Select “Partition Tables” from the “Available Disk Options” menu.
- 7** If you have more than one hard disk, select the hard disk containing the target partition from the “Available Disk Drives” list.
- 8** Select “Delete Partition” from the “Partition Options” menu.
- 9** If more than one partition has been created on the hard disk, select the partition you want to delete from the “Available Partitions” menu.
- 10** Answer “Yes” to the prompt to delete the partition.

Edit Hot Fix Information

WARNING: To change the size of the Hot Fix Redirection Area on a hard disk, you must dismount all volumes and *delete all volume information* on that hard disk. These steps *destroy* all data on the hard disk.

Procedure

- 1** Back up data that you want to save using a reliable backup utility.
- 2** Load INSTALL.

- 3** Complete one of the following:
 - ◆ If the hard disk is mirrored, continue with Step 4.
 - ◆ If the hard disk is not mirrored, skip to Step 6.
- 4** Unmirror any hard disks mirrored to the target hard disk.
See [“Unmirror Hard Disks” on page 86.](#)
- 5** Complete one of the following:
 - ◆ If you are changing the Hot Fix area on the “Not Mirrored” partition, continue with Step 6.
 - ◆ If you are changing the Hot Fix area on the “Out Of Sync” partition, skip to Step 7.
- 6** Delete the volumes.
See [“Delete a Volume” on page 91.](#)
- 7** Select “Disk Options” from the “Installation Options” menu.
- 8** Select “Partition Tables” from the “Available Disk Options” menu.
- 9** If you have more than one hard disk, select the target hard disk from “Available Disk Drives.”
- 10** Select “Change Hot Fix” from “Partition Options.”
A screen similar to the following appears:

Figure 12 Changing Hot Fix from INSTALL NetWare “Partition Information” screen

Partition Information			
Partition Type: NetWare 386 Partition			
Partition Size:	636	Cylinders,	635.9 Meg
Hot Fix Information:			
Data Area:	160001	Blocks,	625.0 Meg
Redirection Area:	2811	Blocks,	1.7 %

- 11** To change the size of either the Data Area or the Redirection Area, do the following:
 - 11a** Press <Enter> or use the arrow keys to move to the field.
 - 11b** Type the new number of blocks in that field, and press <Enter>. NetWare automatically assigns the remaining space to the other field.
- 12** Verify the change to the Hot Fix Redirection Area.

At least 2% of the NetWare partition should be in this area.
- 13** Press <Esc> and select “Yes” at the “Change Partition Information?” prompt.
- 14** Complete one of the following:
 - ◆ If the hard disk was not mirrored, skip to Step 17.
 - ◆ If the hard disk was mirrored, continue with Step 15.
- 15** Select the other hard disk of the pair and repeat Steps 4 through 13.
- 16** Remirror the hard disks

See [“Mirror or Duplex Hard Disks” on page 84](#).
- 17** Recreate the volumes.

See [“Create a Volume” on page 89](#).
- 18** Restore the files and directories to the volume.

Mirror or Duplex Hard Disks

NetWare v3.1x protects data from hard disk failure by letting you duplicate (mirror) one hard disk’s data on one or more other hard disks. When you mirror hard disks on different host bus adapters, this is called “duplexing.” The INSTALL processes for mirroring and duplexing are the same.

Mirrored and duplexed hard disks must have partitions of similar size (within several megabytes). In the mirroring process, NetWare makes adjustments so the mirrored partitions are exactly the same size.

Although you can mirror eight partitions together, mirroring two partitions is usually sufficient.

If a hard disk fails and cannot be accessed by the server, you can unmirror the hard disks and salvage the volume from the functional disk. See [“Recover Volume Data from an Unmirrored Hard Disk” on page 76](#).

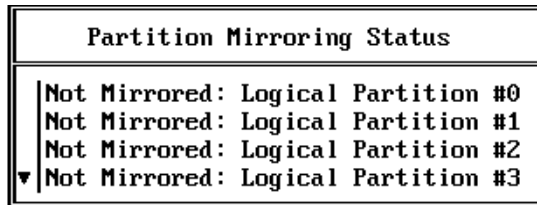
To mirror two or more disks to each other, follow these steps.

Procedure

- 1 Load INSTALL.
- 2 Select “Disk Options” from the “Installation Options” menu.
- 3 Select “Mirroring” from the “Available Disk Options” menu.

A “Partition Mirroring Status” list similar to the following appears:

Figure 13 INSTALL “Partition Mirroring Status” list



Each partition displays one of the following conditions:

Not Mirrored	The partition is not currently mirrored to another partition.
Mirrored	The partition is currently mirrored to another partition.
Out Of Sync	The partition was mirrored to another partition, but is currently unmirrored from that partition.

- 4 Select the partition you want to mirror from the “Partition Mirroring Status” list.
A “Mirrored NetWare Partitions” list appears. The hard disks that are currently mirrored to the partition you selected appear in this list.
The partition you select becomes the primary partition of the mirrored pair. For an explanation of how logical partitions relate to the installed hard disks see “Device numbering” in *Concepts*.
- 5 Press <Insert> and select a hard disk from the “Available Partitions” list.

NOTE: If you are mirroring hard disks, the status on the “Mirrored NetWare Partitions” list will show “Out Of Sync” for one of the disks. As soon as mirroring is completed, the status of both disks will be “In Sync.”

Unmirror Hard Disks

Before you can change the Hot Fix Redirection Area, delete a partition, or conduct surface tests, you must unmirror the mirrored hard disks.

Procedure

- 1** Load INSTALL.
- 2** Select “Disk Options” from the “Installation Options” menu.
- 3** Select “Mirroring” from the “Available Disk Options” menu.
- 4** Select the “Mirrored” partition to unmirror from the “Partition Mirroring Status” list.
- 5** Highlight the hard disk you want to unmirror in the “Mirrored NetWare Partitions” list and press <Delete>.

For an explanation of the device number, see “Device numbering” in *Concepts*.

- 6** Press <Esc>; then select “Mirroring” again.

The “Out Of Sync” status appears next to the disk you unmirrored.

You can now repair or replace the hard disk, format the hard disk, delete the partition on the hard disk, change the Hot Fix Redirection Area, or salvage the volume information on the “Out Of Sync” partition.

- 7** (Optional) If you want to allocate the unmirrored partition as a new volume segment:
 - 7a** Highlight the partition and press <F3>.
 - 7b** Answer “No” to the prompts.

Test Hard Disks for Bad Blocks

Use the surface test to check a hard disk you are adding to the file server. The surface test runs in the background so you can work on other hard disks during the test. You must dismount the volumes on the disk being tested. Users should log out.

IMPORTANT: Test for bad blocks when there is no activity on the file server. Otherwise, workstations connected to the file server may hang or appear to hang.

You can run two types of tests:

- ♦ *Destructive*. This test destroys all data on the hard disk as it reads and writes test patterns. After the test is over, the disk still retains the test patterns. If you decide to run a destructive test, back up all data you want to save.
- ♦ *Nondestructive*. A nondestructive test pre-reads the data on the disk, writes and reads its test patterns, and then restores the original data. The nondestructive test protects your data but takes 20% longer to run than a destructive test.

Complete the following steps to test your hard disk for bad blocks.

Procedure

- 1** At the console prompt dismount each volume on the hard disk by typing

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with a name of a volume on the disk. Repeat the step for each volume on the disk.

- 2** Load INSTALL.
- 3** Select “Disk Options” from the “Installation Options” menu.
- 4** Select “Surface Test” from the “Available Disk Options” menu.

- 5** If you have more than one hard disk on your file server, select the disk you want to check from the “Available Disk Drives” list.

Screens similar to the following appear:

Figure 14 INSTALL “Disk Surface Test Status” and “Surface Test Options” screens

Disk Surface Test Status	
Test Type: None	Blocks Tested:
Bad Blocks: 217	Total Blocks: 160001

Surface Test Options
Begin Surface Test
Stop Surface Test
Return To Previous Menu

The “Test Type” field can show the following status information:

None	The partition is not being tested.
Failed	A disk error occurred that Hot Fix could not correct.
Completed	The test was successful.
Terminated	The test was stopped. All data on the hard disk will be lost.
Nondestructive Destructive	Data on the hard disk will be preserved.

- 6** Select “Begin Surface Test” from the “Surface Test Options” menu.

- 7** Select the type of test.

- ◆ Remember, destructive destroys all data; nondestructive protects your data.
- ◆ For a complete test, let the test run several hours until the number of blocks tested is equal to the total blocks listed on the status screen.

- ◆ To end the test before it finishes, select “Stop Surface Test” from the “Surface Test Options” menu.

NOTE: To perform other file server operations while the surface test is running (such as testing other hard disks), press <Esc> to move to the other options in INSTALL, or press <Alt><Esc> to go to the console prompt.

All testing will stop if you exit INSTALL.

At the end of the test, the “Disk Surface Test Status” form displays the number of blocks tested, the number of bad blocks found, and the total blocks tested. The “Test Type” field displays “Terminated” or “Completed.”

Create a Volume

You can create a new volume on any hard disk that has a NetWare v3.1x partition. Your file server can have up to 64 volumes. The needs of your users determines how many volumes you need on your file server; the operating system requires only one volume, SYS:, to function properly. For suggestions on setting up your volumes, see “Volume” in *Concepts*.

NOTE: To reduce the size of a volume, you must delete it (and the data) first, and then recreate it with a smaller size. If your system will have more than one volume, we recommend that you leave a few megabytes unassigned to any volume. This reserve can later be assigned to the volume that is in critical need of more disk space.

Complete the following steps to create a volume.

Procedure

- 1** Load INSTALL.
- 2** Select “Volume Options” from the “Installation Options” menu.
- 3** When the “Volumes” list appears, press <Insert>.
 - ◆ *Multiple hard disks.* If you have more than one hard disk with available disk space, a “Free Space Available for Volume Segments” list appears. Select the disk you want to create the volume on. The “New Volume Information” form appears.
 - ◆ *One hard disk.* If only one hard disk has available disk space, the “New Volume Information” form appears:

Figure 15 INSTALL “New Volume Information” screen

New Volume Information	
Volume Name:	
Volume Block Size:	4 K Blocks
Initial Segment Size:	5649 Blocks
Volume Size:	21 Megs
Status:	Not Mounted

4 To name the volume, highlight the “Volume Name” field and enter the name of the new volume.

5 Press <Enter> to move to the next field; then enter the block size.

Consider the following points as you decide which block size is best:

- ♦ The default block size is 4 KB.
- ♦ Block size must be the same on all segments of a volume. Once a block size has been selected, it cannot be changed for additional segments.
- ♦ Small block sizes require more file server memory to track the File Allocation and Directory Entry Tables. Large block sizes use more disk space because small files must be assigned at least one block.
- ♦ Larger block sizes are best for large database records.
- ♦ DOS utilities may calculate the amount of free disk space incorrectly if you select large block sizes (32 KB or 64 KB).

6 Press the Down-arrow key to move to the “Initial Segment Size” field.

7 Complete one of the following:

- ♦ To assign the entire available segment to the volume, skip to Step 11.
- ♦ To calculate the number of blocks to assign to the volume, continue with Step 8.

8 Divide the size of a megabyte (1024) by the selected block size.

$$1024/4 = 256 \text{ blocks per megabyte}$$

$$1024/8 = 128 \text{ blocks per megabyte}$$

- 9** Multiply the number of blocks per megabyte by the number of megabytes you want to allocate.
 $256 \times 25\text{MB} = 6400$
 $128 \times 25\text{MB} = 3200$
- 10** Enter the number calculated in Step 9 in the “Initial Segment Size” field.
- 11** To create the volume with the configuration entered in the “New Volume Information” form, press <Esc> and answer “Yes” to the prompt to create the volume.
- 12** With the new volume name highlighted, press <Enter> to return to the “Volume Information” screen.
- 13** Highlight the “Status” field and press <Enter>.
- 14** Select “Mount Volume.”

Delete a Volume

You can delete volumes as needed. Complete these steps while the network is up.

Procedure

- 1** Use MONITOR to determine who has files opened on the volume.
Use BROADCAST to tell users to move to another volume.
- 2** Back up any data you want to save from the volume you intend to delete.
- 3** Load INSTALL.
- 4** Select “Volume Options” from the “Installation Options” menu.
- 5** Select the volume you want to delete.
- 6** Highlight the “Status” field and press <Enter>.
- 7** Select “Dismount Volume.”
- 8** Press <Esc> to return to the “Volumes” list.
- 9** Highlight the volume and press <Delete>.
- 10** Answer “Yes” to the prompt to delete the volume.

Rename a Volume

You can use INSTALL to rename a volume. To rename volume SYS;, dismount SYS;, create another volume, and name the new volume “SYS:”.

To rename a volume, complete the following steps.

Procedure

- 1** Use MONITOR to determine if users have files opened on the volume.
Use BROADCAST to tell users to move to another the volume.
- 2** Load INSTALL.
- 3** Select “Volume Options.”
- 4** Select the volume you want to rename.

The “Volume Information” form appears:

Figure 16 Renaming a volume from INSTALL “Volume Information” form

Volume Information
Volume Name: SYS
Volume Block Size: 4 K Blocks
Volume Segments: (select for list)
Volume Size: 44 Meg
Status: Mounted

- 5** Highlight the “Status” field and press <Enter>.
- 6** Select “Dismount Volume.”
- 7** Move to the “Volume Name” field.
- 8** Type the new name of the volume over the old name and press <Enter>.
- 9** Answer “Yes” at the prompt to change the volume name.

- 10** To mount the newly named volume, highlight the “Status” field and press <Enter>.
- 11** Select “Mount Volume.”

Increase the Size of a Volume

A volume can have multiple segments spanning multiple hard disks. This allows you to add a hard disk when you need to expand a given volume.

Keep the following requirements in mind as you expand volumes:

- ◆ The maximum number of segments in a volume is 32.
- ◆ The maximum number of segments you can create on one hard disk is 8.
- ◆ The maximum number of volumes is 64.
- ◆ You can add segments to a volume without destroying data, but you cannot remove the segments without destroying data.

You can increase the size of a volume in two ways:

- ◆ Add a new volume segment on the same hard disk as the volume.
- ◆ Add a new volume segment by adding a segment from a new hard disk.

To add another segment to an existing volume, complete the following steps.

Procedure

- 1** Load INSTALL.
- 2** Select “Volume Options” from the “Installation Options” menu.

- 3 From the “Volumes” list, select the volume you want to add the segment to.

A form similar to the following appears.

Figure 17 Adding volume segments from the INSTALL “Volume Information” screen

Volume Information
Volume Name: SYS
Volume Block Size: 4 K Blocks
Volume Segments: (select for list)
Volume Size: 44 Meg
Status: Mounted

- 4 Select the “Volume Segments” field.

A list of the current segments in the selected volume appears.

- 5 Press <Insert>.

One of the following happens:

- ◆ If more than one free area exists, a list of disks with free areas appears. Select the hard disk from the list. Then continue with Step 6.
- ◆ If only one disk has a free area, the disk is selected for you. Continue with Step 6.
- ◆ If no free areas exist, nothing happens. A hard disk needs to be added to the file server and a NetWare partition created on the disk before you can select a segment. See [“Add a Hard Disk to the File Server” on page 72](#).

- 6 Type the number of blocks you want in the new volume segment and press <Enter>.

The default number is the whole area. We recommend that you leave an unassigned segment of at least 6 MB on one hard disk.

- 7 Answer “Yes” at the prompt to add a new segment to the volume.

Copy the SYSTEM and PUBLIC Files

You can recopy the SYSTEM and PUBLIC utility files from diskette onto volume SYS: using INSTALL. INSTALL automatically assigns the proper attributes to the files. If you copy the files any other way, they will not be assigned the proper attributes and they might be deleted.

WARNING: Do not just rely on INSTALL to restore all files in the SYS:SYSTEM and SYS:PUBLIC directories. Use a backup utility to back up these directories. If you accidentally delete volume SYS:, the AUTOEXEC.NCF file and the system login script will be destroyed, and you will have to recreate them.

To recopy the SYSTEM and PUBLIC files, complete the following steps.

Procedure

1 Load INSTALL.

If volume SYS: is not mounted, you have to load INSTALL from the hard disk or the *System_2* diskette.

2 Select “System Options” from the “Installation Options” menu.

3 Select “Copy System and Public Files” from the “Available System Options” menu.

Insert the *System_2* diskette into drive A: as prompted.

4 Follow the system prompts to insert the remaining diskettes.

If you want to skip one or more diskettes after copying the first one, press <F7>. Then answer “Yes.” Repeat this procedure to continue skipping diskettes until you come to the one you want to copy.

NOTE: If security is a priority, copy INSTALL.NLM to another secured directory. Then delete INSTALL.NLM from the SYS:SYSTEM directory. This will prevent an intruder who has gained access to the file server console from deleting volumes and partitions.

Change the File Server’s Name

You can change the file server’s name by using the FILE SERVER NAME command in the AUTOEXEC.NCF file. The next time the server is booted, the file server will be assigned the new name.

Procedure

- 1 Load INSTALL.
- 2 Select “System Options” from the “Installation Options” menu.
- 3 Select “Edit AUTOEXEC.NCF file” from the “Available System Options” menu.
- 4 Locate the present server name in the file and type the new name over the old one.

The name can have as many as 47 characters, but only 10 will show in any of the system messages. Do not use spaces or any of the following characters:

" * + , \ / | ; : = < > ? [] .

- 5 Press <Esc> and answer “Yes” to the “Save Changes” prompt.
- 6 Press <Alt><Esc> to return to the console prompt.
- 7 Use SEND to broadcast a message to all users to log out.
- 8 Down the file server by typing

DOWN <Enter>

- 9 Reboot the file server:

The new name will be in effect once the server is up.

NOTE: You may need to change drive mappings in the system login script and the user login scripts to reflect the file server’s new name. You may also need to change the workstations’ AUTOEXEC.BAT files.

Change the File Server’s Internal Network Number

You can use the IPX INTERNAL NET command in the AUTOEXEC.NCF file to change the file server’s internal network number. The next time the file server boots, it has the new internal network number.

Procedure

- 1 Load INSTALL.
- 2 Select “System Options” from the “Installation Options” menu.
- 3 Select “Edit AUTOEXEC.NCF file” from the “Available System Options” menu.

- 4** Locate the IPX INTERNAL NET command in the file and type the new number for the server over the old number. The number must be one of these:
 - ◆ A hexadecimal number (base 16, using numbers 0 through 9 and letters A through F)
 - ◆ One to eight digits long
- 5** Press <Esc> and answer “Yes” to the “Save Changes” prompt.
- 6** Press <Alt><Esc> to return to the console prompt.
- 7** Use SEND to broadcast a message to all users to log out.
- 8** Down the file server by typing
DOWN <Enter>
- 9** Reboot the file server.

The new internal network number will be in effect once the server is brought up.

Create the AUTOEXEC.NCF File

The AUTOEXEC.NCF file is a batch file (similar to a DOS batch file) that contains commands that execute after the NetWare operating system is booted and STARTUP.NCF is executed. This file is stored in the SYS:SYSTEM directory and is executed after volume SYS: has been mounted. After AUTOEXEC.NCF executes, the file server becomes accessible from attached workstations.

The operating system uses the AUTOEXEC.NCF file to complete the boot process for the file server. More specifically, the file provides the following types of configuration information:

- ◆ The file server’s name
- ◆ The internal network number
- ◆ LOAD commands for LAN drivers
- ◆ BIND commands to bind communication protocols to the LAN drivers
- ◆ The network numbers for the LAN drivers
- ◆ LOAD commands for loadable modules such as MONITOR and PSERVER

- ◆ Commands to mount volumes
- ◆ Commands to execute console commands such as SET parameters

If the file server's AUTOEXEC.NCF file has been deleted, complete the following steps to recreate it.

Procedure

- 1** Load INSTALL.
- 2** Select "System Options" from the "Installation Options" menu.
- 3** Select "Create AUTOEXEC.NCF file" from the "Available System Options" menu.
- 4** Press <Esc> and answer "Yes" to the prompt to create the AUTOEXEC.NCF file.

For further information about creating the file during initial installation, see Chapter 2, "Install the File Server Software," in *Installation and Upgrade*.

For details on the commands that can be included in the file, see the next section, ["Edit the AUTOEXEC.NCF File" on page 98](#).

Edit the AUTOEXEC.NCF File

You can change commands in the AUTOEXEC.NCF file. However, these changes do not affect the configuration of the file server until the file server is rebooted.

Usually, you change the file server's configuration with a console command and then save the command in the file. This procedure ensures that the command executes the next time the file server is booted.

You can execute console commands, load loadable modules, change SET parameters, or execute file server batch file commands with the AUTOEXEC.NCF file.

Procedure

- 1** Load INSTALL.
- 2** Select "System Options" from the "Installation Options" menu.
- 3** Select "Edit AUTOEXEC.NCF file" from the "Available System Options" menu.

- 4 Place any of the commands discussed in the following sections at the end of the file.

NOTE: You can also use a text editor to create other file server batch files that include these commands. Add an .NCF extension to any files created this way. If the file is copied to the SYS:SYSTEM directory, the file can then be executed at the console by typing the filename.

LoadableModules

```
LOAD INSTALL
LOAD MONITOR
LOAD PSERVER
```

For more information on loadable module commands, see the documentation for the loadable module.

LAN Driver Commands

The following sample commands are preceded with a comment line that explains what the command loads.

- ◆ To load the NE2000 driver the first time:

```
LOAD NE2000 PORT=300 INT=3
```

- ◆ To load the NE2000 driver with a frame type:

```
LOAD NE2000 PORT=3000 INT=3 FRAME=ETHERNET_II
```

For more information on LAN driver commands, see [“LOAD LAN driver” on page 133](#).

BIND Commands

The following sample commands are preceded with a comment line that explains what the command binds.

- ◆ To bind a protocol to a driver that is loaded once:

```
BIND IPX NE2000 NET=26
```

- ◆ To bind to a driver that is loaded more than once:

```
BIND IPX NE2000 [PORT=340 INT=4 FRAME=
ETHERNET_802.3] NET=27
```

BIND should follow the LOAD command for the LAN driver. For more information, see [“BIND” on page 35](#).

SET Commands

The following SET commands indicate the default parameter on the first line and the parameter limits on the second line.

```
Set Minimum File Cache Report Threshold=20
```

```
#Limits: 0 to 1000
```

```
Set Minimum Directory Cache Buffers=20
```

```
#Limits: 10 to 2000
```

```
Set Minimum File Delete Wait Time=1 minute 5.9  
seconds
```

```
#Limits: 0 seconds to 7 days
```

```
Set File Delete Wait Time=5 minutes 29.6 seconds
```

```
#Limits: 0 seconds to 7 days
```

```
Set Maximum Packet Receive Buffers=100
```

```
#Limits: 50 to 2000
```

```
Set Allow Unencrypted Passwords=OFF
```

NOTE: NetWare v3.1x supports encrypted passwords. To allow NetWare v2.x users to access NetWare v3.1x file servers, set this command to ON in the AUTOEXEC.NCF file and upgrade the NetWare v2.x file servers with NetWare v3.1x utilities. For details on updating NetWare v2.x file servers, see Chapter 2, “Follow Up After File Server Software Installation,” in *Installation and Upgrade*.

For more information on parameters for SET commands, see [“SET” on page 250](#).

Console Commands

```
MOUNT
```

```
REMOVE DOS
```

```
SECURE CONSOLE
```

```
SPOOL
```

```
TRACK ON
```

```
UPS STATUS
```

For more console commands and for more information, refer to the individual commands discussed in this manual.

File Server Batch File Commands

```
#  
ECHO  
FILE SERVER NAME  
IPX INTERNAL NET
```

#. The pound sign allows you to put remarks in the file so that you can remember why a command was added to the file.

ECHO. When the file server is booting, the default for ECHO is set to OFF. The file server does not display any of the commands from the boot files. The file server does, however, display the results of the commands as they are executed.

ECHO ON allows the file server to display commands on the screen as they are executed.

Use ECHO ON to troubleshoot errors in the AUTOEXEC.NCF file. If commands are not executing properly when the file server boots, add the ECHO ON command as the first line in the file. Then, as the file is executed, the commands and the results are displayed.

The command preceding the error message is the command you need to edit.

The default is ECHO OFF.

FILE SERVER NAME. This command assigns a name to the file server as it boots.

If you need to change the name of your file server, change the name in the AUTOEXEC.NCF file; then reboot the file server. (See [“Change the File Server’s Name” on page 95.](#))

IPX INTERNAL NET. This command assigns the internal network number for the file server.

If you need to change the internal network number, change the number in the AUTOEXEC.NCF file; then reboot the file server. (See [“Change the File Server’s Internal Network Number” on page 96.](#))

Create the STARTUP.NCF File

This file, stored on either the file server boot diskette or the DOS partition, provides the file server with the commands it needs to load any disk drivers or name space modules (*.NAM). After the commands in this file execute, the server searches for the AUTOEXEC.NCF file to continue the boot process.

You created this file during the initial installation process. If the file server's STARTUP.NCF file is missing, complete the following steps to recreate it.

Procedure

- 1** Load INSTALL.
- 2** Select "System Options" from the "Installation Options" menu.
- 3** Select "Edit STARTUP.NCF file" from the "Available System Options" menu.
- 4** If the path to STARTUP.NCF is drive C:, press <Home> and change A: to C:.
- 5** Press <Enter> and then <Esc>.
- 6** Answer "Yes" to the prompt to create the STARTUP.NCF file.

For details on the commands that can be included, see the next section, "[Edit the STARTUP.NCF File](#)" on page 102.

For instructions on creating this file during initial installation, see Chapter 2, "Install the File Server Software," in *Installation and Upgrade*.

Edit the STARTUP.NCF File

You can change the STARTUP.NCF file at any time. However, these changes do not affect the configuration of the file server until the file server is rebooted.

Usually you change the file server's configuration with a console command, and then save the command in the file. This procedure ensures that the command executes the next time the file server is booted.

However, some commands cannot be entered at the console, but must be entered in the STARTUP.NCF file. Then you must reboot the file server for the new configuration to take effect.

To edit the STARTUP.NCF file, complete the following steps.

Procedure

- 1** Load INSTALL.
- 2** Select “System Options” from the “Installation Options” menu.
- 3** Select “Edit STARTUP.NCF file” from the “Available System Options” menu.
- 4** If the path to STARTUP.NCF is drive C:, press <Home> and change A: to C:.
- 5** You can place any of the commands discussed in the following sections at the end of the file.

NOTE: You can also use a text editor to create other startup files. Give the file a unique name and an .NCF extension. If the file is stored in the file server’s boot directory, you can execute this file, rather than the default STARTUP.NCF file, by using a SERVER parameter. See [“SERVER” on page 246](#).

Disk Driver Commands

In the following commands, the default parameters are given for the drivers that require parameters:

```
LOAD ISADISK INT=E PORT=1F0
LOAD PS2ESDI
LOAD DCB PORT=340
LOAD PS2MFM
LOAD PS2SCSI SLOT=1
```

For more information on the commands, see [“LOAD disk driver” on page 120](#).

Name Space Commands

```
LOAD MACLOAD NFSLOAD OS2
```

File Server Batch File Commands

```
#ECHO OFF/ON
```

For an explanation of batch file commands, see [“File Server Batch File Commands” on page 101](#).

SET Parameters

The following SET commands indicate the default on the first line and the limits on the second line. For more information on SET parameters, see [“SET” on page 250](#).

```
Set Cache Buffer Size=4096 (bytes) Limits: 4096 to  
16384
```

```
Set Display Disk Device Alerts=OFF
```

```
Set Display Relinquish Control Alerts=OFF
```

Install, Uninstall, or Configure a Product on the File Server

INSTALL's "Product Options" feature allows you to work with NetWare products like name space modules and SBACKUP. To install, uninstall, or configure a product, complete the following steps. When you use the "Product Options" feature of INSTALL, BTRIEVE and CLIB are automatically loaded.

NOTE: Information about currently installed products and their current configuration options is in SYS:SYSTEMPRODUCTS.DAT (a BTRIEVE database).

Procedure

- 1** Load INSTALL.
- 2** Select "Product Options" from the "Installation Options" menu.
The "Currently Installed Products" list appears. If no products are currently installed, the list is empty.
- 3** To uninstall a product, delete it from the list.
- 4** To install a product, press <Insert> and follow the prompts.
- 5** To set configuration options for a product, select that product from the list.

Some products may not have configuration or uninstall options. A message explaining this appears if you try to perform unsupported operations. For further installation instructions and configuration options, refer to the documentation on the product.

Exit INSTALL

You can exit INSTALL by pressing <Esc> until the exit prompt appears, or, you can exit temporarily by pressing the hot key.

Escape

This form of exit unloads INSTALL and frees up memory.

Press <Esc> until the “Exit Install” prompt appears, and then answer “Yes.” The console prompt appears.

Hot Key

INSTALL, as well as the other file server menu utilities, allows you to exit the program temporarily by pressing <Alt><Esc>.

The module is still loaded, and you can press <Alt><Esc> to return to INSTALL at any time.

IPXS

Why Use IPXS?

Use IPXS if you have an NLM that requires STREAMS-based IPX protocolservices.

Command Format

```
LOAD [path] IPXS
```

Command Parameters

Replace *path* with a full path to IPXS.NLM. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system looks for IPXS in SYS:SYSTEM. (Use SEARCH to set up more paths.)

Additional Information

IMPORTANT: Do not unload a protocol-stack NLM such as IPXS until you have unloaded all applications that are potentially using it.

To use IPXS, load these modules in the following order:

1. STREAMS
2. CLIB
3. TLI
4. IPXS

Load IPXS

To load IPXS, type

```
LOAD IPXS <Enter>
```

KEYB

Why Use KEYB?

Use KEYB to change the keyboard type for the NetWare server console.

Command Format

```
LOAD [path]KEYB [parameter]
```

Command Parameters

Replace *path* with the full path to the directory containing KEYB.NLM.

Replace *parameter* with the keyboard type you want. The following types are available:

English (United States)

French

German

Italian

Spanish

Load KEYB

To load KEYB, type

```
LOAD KEYB [parameter] <Enter>
```

NOTE: If you load KEYB without entering a keyboard parameter, a list of the available keyboards is displayed.

LIST DEVICES

Why Use LIST DEVICES?

Use LIST DEVICES to display device information for the server.

Command Format

```
LIST DEVICES
```

Display Device Information

To display device information for the server, type

```
LIST DEVICES <Enter>
```

Additional Information

A device can be a disk driver, tape driver, optical disk driver, or any other storage device driver.

LOAD

Why Use LOAD?

Use LOAD to link modules to the operating system.

IMPORTANT: Exercise caution when selecting loadable modules to allow on the file server. If you are unsure of the source or the purpose of the module, you may want to first test the module in a secure environment that you can easily recover. Loadable modules supplied by Novell have been tested prior to release.

This section describes the following tasks:

Task	Page
Load a module	“Load a Module” on page 112
Troubleshoot LOAD	“Troubleshoot LOAD” on page 113

See the following pages for each module type.

Module type	Page
Disk drivers	“Why Use LOAD disk driver?” on page 120
LAN drivers	“Why Use LOAD LAN driver?” on page 133
Name space	“Why Use LOAD name space?” on page 162
NLM utilities	“Why Use Load NLM utility?” on page 167

Command Format

```
LOAD [path]loadable_module [parameter...]
```

Command Parameters

Replace *path* with a full path to the directory containing the loadable module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: has not yet been mounted, the operating system assumes that the loadable module is located in the default DOS directory. Once volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *loadable_module* with an option from one of the four types of loadable modules:

- Disk drivers
- LAN drivers
- Name space
- NLM utilities

Each type of loadable module is described in the following sections. Each description includes a list of modules being shipped with the operating system.

Consult NetWare, your Novell Authorized Reseller, or third-party dealers for other available loadable modules.

Disk Drivers

Loadable modules for disk drivers establish communication between the operating system and the hard disks' controller boards.

For an explanation of how to load disk drivers and for a list of parameters that can be used with disk drivers, see [“LOAD disk driver” on page 120](#).

LAN Drivers

Loadable modules for LAN drivers establish communication between the operating system and the network boards installed in the file server.

For an explanation of how to load LAN drivers and for a list of parameters that can be used with LAN drivers, see [“LOAD LAN driver” on page 133](#).

Name Space

Loadable modules for name space link non-DOS naming conventions to the operating system. Once linked, the naming convention can be assigned to the volumes on the file server; those volumes can then store files created with the specific type of naming convention.

For an explanation of how to load name space, see [“LOAD name space” on page 162](#).

NLM Utilities

Loadable modules for NetWare Loadable Module (NLM) utilities link management and enhancement programs with the operating system. These utilities can include the following types of programs: installation, monitor, volume repair, backup, print server, database server, communication gateway, and diagnostic.

For an explanation of how to load these NLM utilities, see [“LOAD NLM utility” on page 167](#).

Additional Information

A loadable module links itself to the operating system and allocates a portion of the file server’s memory for its use.

Some modules, such as LAN drivers and disk drivers, need to be loaded every time the file server is booted. Other modules, such as the NLM utilities, can be loaded, used, and then unloaded. When modules are unloaded, all allocated resources are returned to the operating system.

If you want modules to be loaded automatically when the file server boots, you must store the LOAD commands in either the AUTOEXEC.NCF file or the STARTUP.NCF file. For instructions on editing the .NCF files, see [“INSTALL” on page 69](#).

When you install the SYSTEM and PUBLIC files, .NLM, .LAN, and .NAM loadable modules are copied to the SYS:SYSTEM directory. You must copy the .DSK and .NAM modules that your system uses to the boot directory of the file server. For instructions, see Chapter 2, “Install the File Server Software,” in *Installation and Upgrade*.

For a complete description of the types of loadable modules, see “Loadable Module” in *Concepts*.

Load a Module

How you load a module depends on where it is. You can copy a module to and load it from any of the following partitions:

- ◆ A diskette in the floppy disk drive of the file server
- ◆ A DOS partition on the file server
- ◆ NetWare directories on the file server

Examples of loading MONITOR from each source are in the following sections. To set up search paths to other directories, see [“SEARCH” on page 239](#).

SYS:SYSTEM directory

You can load any module that has been copied to the SYS:SYSTEM directory as long as volume SYS: is mounted.

To load MONITOR, for example, type

```
LOAD MONITOR <Enter>
```

Floppy disk drive

You can load any module on a diskette from the file server's floppy disk drive.

To load MONITOR, for example, insert a diskette with the MONITOR module into drive A: of the file server and type

```
LOAD A:MONITOR <Enter>
```

NOTE: If you have removed DOS with the REMOVE DOS or SECURE CONSOLE command, you cannot load a module from drive A:.

DOS partition

If you have set up your file server to boot from a DOS partition, you can load any module from the DOS partition that you have copied to it.

To load MONITOR, for example, type

```
LOAD C:MONITOR <Enter>
```

NOTE: If you have removed DOS with the REMOVE DOS or SECURE CONSOLE command, you cannot load a module from the DOS partition.

NetWare directory

You can load a module from any directory on the file server as long as the module has been copied to the directory.

To load MONITOR from the SYS:MODULES directory, for example, type

```
LOAD SYS:MODULES/MONITOR <Enter>
```

NOTE: If you have used SECURE CONSOLE, you cannot load modules from any network directory other than SYS:SYSTEM.

Troubleshoot LOAD

All loadable modules that you link to your operating system should be approved by Novell, Inc. If you are running third-party loadable modules, check with NetWare or ask your Novell Authorized Reseller for a list of approved modules. If you load a module that is not approved, your server may abend or data may become corrupted.

Occasionally a loadable module displays warnings as it loads, or it does not load at all. These problems and their possible solutions are described in the following sections.

Warning Messages

If you load NetWare v3.0 modules on a NetWare v3.1x file server, you will receive warning messages that the module is using old API calls. The following message is displayed on the file server console:

```
This module is using <number> old API calls Contact the module  
vender regarding the availability of a newer module
```

NetWare after v3.0 changed some API calls to include resource tagging. Resource tagging ensures that the loadable modules return all allocated resources to the operating system when unloaded.

The old API calls still work; however, they are slower than the new 3.1x API calls. Contact the vender of the module for an updated version that uses the new API calls.

Module Will Not Load

Modules will not load when one or more of the following conditions exist:

- ◆ The file server cannot find the loadable module.
- ◆ The file server does not have enough free memory to load another module.
- ◆ The loadable module depends on another loadable module.
- ◆ An invalid parameter is specified when the module is loaded from the console prompt.
- ◆ LOAD is not entered before the module name.
- ◆ An invalid command is entered in the .NCF files.

Possible solutions for these problems are described in the following sections.

The File Server Cannot Find the Module

When the operating system cannot find the module, it usually returns the message “Unable to find load file filename.”

The solution depends upon whether volume SYS: is mounted. Use VOLUMES to list the mounted volumes.

- ◆ If volume SYS: is mounted, go to “volume SYS: mounted” under [“Troubleshoot LOAD” on page 113](#).
- ◆ If volume SYS: is not mounted, go to “volume SYS: not mounted” under [“Troubleshoot LOAD” on page 113](#).
- ◆ If volume SYS: will not mount, go to “volume SYS: will not mount” under [“Troubleshoot LOAD” on page 113](#).

Volume SYS: mounted. If SYS: is mounted but the module is not in SYS:SYSTEM, use one of the following methods to change the search path of the operating system:

- ◆ Specify the path with the LOAD command. For examples, see [“Load a Module” on page 112](#).
- ◆ Use the SEARCH command to add search drives to the operating system.

The operating system’s search is limited if you have issued the SECURE CONSOLE or REMOVE DOS commands.

SECURE CONSOLE. If you have issued the SECURE CONSOLE command, the operating system looks only in the SYS:SYSTEM directory for a loadable module. To load a module that is not in the SYS:SYSTEM directory, do either of the following:

- ◆ Remove the SECURE CONSOLE command from the AUTOEXEC.NCF file (if you have added it to the file). Down the file server; then reboot the server to disable the SECURE CONSOLE command.
- ◆ Copy the module into the SYS:SYSTEM directory from a workstation.

REMOVE DOS. If you have issued the REMOVE DOS command, the operating system cannot load modules from any DOS drive. Copy the module to the SYS:SYSTEM directory; then load the module.

Volume SYS: not mounted. Loadable modules are normally kept in two areas: the SYS:SYSTEM directory and the file server boot directory.

When the operating system is first installed, all loadable modules (except disk drivers) are copied into the SYS:SYSTEM directory; the operating system automatically looks in SYS:SYSTEM for the module.

- ◆ If the module is in the SYS:SYSTEM directory, mount the SYS volume.
- ◆ If the module is not in the SYS:SYSTEM directory, For examples on how to specify a path, see [“Load a Module” on page 112](#).

Volume SYS: will not mount. If SYS: will not mount, a number of possible causes exist; however, only one is related to loadable modules. For other causes, see [Chapter 3, “Troubleshooting Guide,” on page 359](#).

The operating system needs to be able to find the necessary loadable modules to mount SYS:. For example, the operating system must be able to find the disk driver module for the disk that contains SYS:. Also, if SYS: stores non-DOS files, the operating system must be able to find the name space module.

The following conditions can prevent volume SYS: from mounting:

- ◆ The disk drivers and name space modules are not in the same directory as the file server boot files.
- ◆ An incorrect path is specified in the command to load the disk drivers or name space modules.
- ◆ The commands to load the disk drivers or name space modules are not in the STARTUP.NCF file.

Complete one or more of the following procedures:

- ◆ If you have not loaded the necessary name space and disk drivers and you have used REMOVE DOS or SECURE CONSOLE, down the file server.
Then copy the necessary modules to the boot directory and reboot the file server. (Boot the file server without the AUTOEXEC.NCF file if that file contains the REMOVE DOS or SECURE CONSOLE command. See [“SERVER” on page 246.](#))
- ◆ If your file server boots from a DOS partition, load the necessary modules from drive A:. Then use RCONSOLE to copy the modules to the DOS partition.
- ◆ If your file server boots from a floppy diskette, copy the disk drivers and name space modules to the diskette. Then load the modules.
- ◆ Edit the STARTUP.NCF file and correct the path for the disk driver or name space module.
- ◆ Enter the commands to load the disk drivers and name space modules at the console prompt, and then add the commands to the STARTUP.NCF file.

For the proper syntax for these commands, see [“LOAD name space” on page 162](#) or [“LOAD disk driver” on page 120.](#)

The File Server Does Not Have Enough Free Memory

Use MONITOR to view the memory allocations. Do one or more of the following:

- ◆ Unload some of your loaded modules.
- ◆ Use SET to change memory allocations. If the “Alloc Memory Pool” statistic (“Server Memory Statistics” window in MONITOR) is near the default of 8,000,000 bytes, increase this pool. (See [“Maximum Alloc Short Term Memory = number” on page 267.](#))

For instructions on saving the new settings in the AUTOEXEC.NCF file, see [“INSTALL” on page 69.](#)

- ◆ Add more memory to the file server. If the “Cache Buffers” statistic (“Server Memory Statistics” window in MONITOR) is near 20%, the file server needs more memory before it can load any more modules.

The Module Is Dependent on Another Module

Some modules depend on others to define some of their variables. For example, REMOTE must be loaded before RSPX because REMOTE provides variables that RSPX needs in order to work correctly.

Some modules contain instructions that tell the operating system to load another module first. This is called “Autoloading.” Other modules are not programmed with this information.

Autoloading. If autoloading has been programmed into the module, the module instructs the operating system to load the other module.

If the operating system can find the dependent module either in its search paths or in the directory from which the command to load the first module was issued, the dependent module is loaded.

A message similar to the following appears:

```
Auto-loading module <module name>
```

If the operating system cannot find the dependent module, neither module is loaded. You need to specify where the dependent module can be found. Load the dependent module with a path command. Then load the other module.

Non-autoloading. If the module is not programmed for autoloading, the following message is displayed when you try to load a module before its dependent module has been loaded:

```
Loader cannot find public symbol: <symbol name>Load file  
referenced undefined public variable.
```

When this dependency exists, the modules must be loaded in the right order. Check the documentation that came with the module to determine the correct loading order.

An Invalid Parameter Is Entered

Some modules, especially LAN drivers and disk drivers, require parameters. These modules do not load if the following conditions exist:

- ◆ The parameters you selected conflict with other drivers’ parameters.
- ◆ The parameters you entered do not match the board’s configuration.
- ◆ The board’s hardware has failed.
- ◆ None of the boards installed in the file server can use the driver you are trying to load.

Do one or more of the following:

- ♦ *LAN drivers.* Use CONFIG to view hardware configuration information about loaded LAN drivers. Write down the parameters so that you can configure the newly installed board with parameters that do not duplicate any of the displayed parameters. Bring down the file server, reconfigure the board, and reboot the server.
- ♦ *Disk drivers.* Load INSTALL and view the STARTUP.NCF file. Write down the disk driver parameters so that you can configure the newly installed controller board with parameters that do not duplicate any of the displayed parameters. Bring down the file server, reconfigure the board, and reboot the server.
- ♦ *Board configurations.* Bring down the file server. Check the board's configuration and reconfigure it (if necessary) or install a different board of the same type. Then reboot the file server.

LOAD Is Not Entered Before the Module Name

You must precede all loadable modules with LOAD. If you don't, you receive the following message:

```
??? Unknown command???
```

To load MONITOR, for example, you would type

```
LOAD MONITOR <Enter>
```

Make sure you leave a space between "LOAD" and the NLM.

An Invalid Command Is in the .NCF File

If the console displays error messages about invalid commands as the file server boots, invalid commands are probably in the AUTOEXEC.NCF or STARTUP.NCF file. Commands in the .NCF files do not execute if the following conditions exist:

- ♦ The command does not use the proper syntax.
- ♦ The command is in the wrong file.
- ♦ The command requires another command before it.

Do one or more of the following:

- ◆ Add “ECHO ON” to the top of the STARTUP.NCF and AUTOEXEC.NCF files so the console displays each command as it executes or fails to execute. This helps you determine which command is failing first.
- ◆ Check the syntax and order of your module load commands.

Module type	Page
LOAD <i>disk driver</i>	“LOAD disk driver” on page 120
LOAD <i>LAN driver</i>	“LOAD LAN driver” on page 133
LOAD <i>name space</i>	“LOAD name space” on page 162
LOAD <i>NLM utility</i>	“LOAD NLM utility” on page 167

- ◆ Make sure the commands are in the correct .NCF file. (See “[Edit the STARTUP.NCF File](#)” on page 102 and “[Edit the AUTOEXEC.NCF File](#)” on page 98.)

LOAD disk driver

Why Use LOAD *disk driver*?

Use `LOAD disk driver` to establish communication between the operating system and the hard disk controllers installed in your file server.

During the initial operating system installation, `LOAD disk driver` links a driver with your hard disk controller. Afterwards, use it to link an updated driver to your controller or to link a driver to an additional hard disk controller.

IMPORTANT: A conflict will occur if you have installed more than 16 MB of memory and the disk adapter board uses 16- or 24-bit DMA or Bus-Master DMA.

If a memory address conflict occurs, you can solve it by doing either of the following:

- ◆ Upgrade to full 32-bit bus adapters.
- ◆ Use drivers that have been modified and certified to compensate for these memory addressing limitations.

The following tasks are described in this section.

Task	Page
Load a disk driver in an ISA (AT bus) computer	“Load a Disk Driver in an ISA (AT Bus) Computer” on page 125
Load a disk driver for the internal disk controller (microchannel)	“Load a Disk Driver for the Internal Disk Controller (Microchannel)” on page 127
Load a disk driver for a disk controller board (microchannel)	“Load a Disk Driver for a Disk Controller Board (Microchannel)” on page 128
Upgrade a disk driver	“Upgrade a Disk Driver” on page 129
Troubleshoot the host-bus-adapter driver	“Troubleshooting the Host Bus Adapter Driver” on page 130

Command Format

```
LOAD [path]disk_driver [driver_parameter...]
```


Command Parameters

Replace *path* with a full path to the directory containing the loadable module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: has been mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *disk_driver* with the name of the disk driver for your disk controller. Those shipped with the operating system are found on *System_2* diskette and are listed in “Disk drivers included with the operating system” on page 122.

All disk driver names end with a .DSK extension. Consult NetWare or your Novell Authorized Reseller for a list of other certified disk drivers and controller boards.

For a list of valid parameters for the drivers, see “Driver Parameters” on page 134.

Figure 18 Disk drivers included with the operating system

Type of Architecture	Controller Type	Add-On Board Type	Disk Driver
Industry Standard Architecture (ISA)	AT	<i>built-in</i>	ISADISK
		Third-party Secondary Adapter	ISADISK
	Novell SCSI	DCB	DCB
Microchannel	ESDI	<i>built-in</i>	PS2ESDI
	MFM	<i>built-in</i>	PS2MFM
	IBM SCSI	IBM SCSI Adapter	IBMSCSI
		<i>built-in</i>	IBMSCSI
Extended Industry Standard Architecture (EISA)	AT class	<i>built-in</i>	ISADISK
		<i>See Vender</i>	ISADISK
	EISA Vender Proprietary	<i>built-in</i>	<i>See Vender</i>
		<i>See Vender</i>	<i>See Vender</i>

Additional Information

Since most controllers can be configured more than one way, you must specify parameters for the controller each time you load a disk driver. The drivers use the parameters to identify which controller they should link with. However, controllers that use the PS2ESDI disk driver or the PS2MFM disk driver do not need any parameters because they cannot be configured.

Record the configuration options for all disk coprocessor boards (adapters and controllers) on the “File Server Worksheet” in *Installation and Upgrade*.

Make sure the board settings do not conflict with other hardware settings in the computer. No other piece of hardware (COM ports, monitors, keyboards) can use the same I/O port or interrupt. (In a few cases, interrupts can be shared. If you configure hardware to share an interrupt, make sure that the hardware allows sharing.)

Drivers that can link with more than one configuration can be loaded more than once. These drivers either produce multiple copies of the driver code in memory or load re-entrantly.

When a driver loads re-entrantly, the operating system produces only one copy of the code in memory and allocates a small data block of memory each time the driver is loaded.

DriverParameters

Some drivers can read the information from the controller board installed in the file server. These types of drivers do not prompt you for any parameters. Other drivers must be told the configuration of the controller to find the controller in the file server.

Each parameter should have a unique value, different from any other boards installed in the file server. A few boards can share interrupts. Check the documentation that comes with the boards.

Each parameter is defined in this section. Following the definitions is a table for each driver which includes the supported parameters, the default value for the parameters, and all supported values. The PS2ESDI and PS2MFM drivers are not included because these drivers have no parameters.

You can enter parameters at the command line, (For configuration information, see the documentation that came with the controller board.) or you can let the operating system prompt you for them.

The driver parameters for each disk driver are unique. However, most drivers use one or more of the following:

DMA=number

INT=number

MEM=number

PORT=number

SLOT=number

DMA=number

Reserves a DMA channel for the driver.

INT=number

Reserves a hardware interrupt for the driver. The operating system uses hexadecimal values for the interrupts (10=A, 11=B, 12=C, 13=D, 14=E, 15=F).

MEM=number

Reserves a memory address for the driver.

PORT=number

Reserves an I/O port for the driver.

SLOT=number

Tells the operating system which board to link the driver to. This option is used with microchannel and bus master slots on EISA computers. The interrupts, memory addresses, and I/O ports are set with the reference diskette that comes with the computer.

DCB

The DCB driver can be loaded four times. When the driver is loaded more than once, the driver loads re-entrantly. You can specify any of the following DCB parameters.

Parameter	Default	Supported Values
PORT	340	320, 328, 340, 348, 380, 388
/s=0		/s=0

The /s=0 parameter is different from the PORT parameter. Use it the first time you load the DCB driver for a board that has been used with different hard disks and does not have current hard disk information. This speeds the load process.

You can then use DISKSET to edit the EEPROM information and add the current hard disks that are attached to the board.

Although the driver does not prompt you for an interrupt, the board uses an interrupt; the driver displays which interrupt it is using while the driver loads.

ISADISK

The ISADISK driver can be loaded twice. When the driver is loaded more than once, the driver loads re-entrantly. You can specify any of the following hexadecimal parameters.

Parameter	Default	Supported Values
INT	E	B, C, E, F
PORT	1F0	170, 1F0

The default settings are the standard values for an internal controller. Use the other supported values only if you are adding a secondary ISA adapter.

PS2SCSI

The PS2SCSI driver can be loaded four times. When the driver is loaded more than once, the driver loads re-entrantly. You can specify the following PS2SCSI parameter:

Parameter: SLOT

Default: None

Supported values: All available

Load a Disk Driver in an ISA (AT Bus) Computer

To load a disk driver in an ISA computer, complete the following steps.

Procedure

- 1 Complete one of the following, depending on the type of controller you are loading a disk driver for:
 - ◆ If the controller is internal, boot the file server and skip to Step 2.
 - ◆ If the controller is a disk controller board, complete Steps 1a through 1f.

NOTE: If you have already loaded a disk driver for a controller board and do not know its configuration, view the STARTUP.NCF file to obtain needed configuration information before downing the file server.

- 1a** Down the file server.
- 1b** Disconnect the power.
- 1c** Configure the board and install it in the file server.

Follow the instructions in the documentation that came with the board. Record all configuration information on the “File Server Worksheet” in *Installation and Upgrade*.

- 1d** Connect the hard disks to the board.
- 1e** Connect the power.
- 1f** Run the appropriate setup program.
 - ♦ If you are installing a secondary ISA adapter, use the setup program to specify the hard disk types; then boot the file server.
 - ♦ If you are installing a host bus adapter, boot the file server; then load DISKSET. For instructions, see “**DISKSET**” on page 56.

2 Insert a working copy of the *NetWare System_2* diskette into drive A:.

3 Load the disk driver at the command line with or without parameters.

- ♦ *Without driver parameters.* To load the ISADISK driver, for example, type

```
LOAD A:ISADISK <Enter>
```

Answer the configuration prompts.

NOTE: You can only select options that do not conflict with previously loaded drivers (LAN and disk). To change a default parameter, type in the number that matches your board's configuration.

- ♦ *With driver parameters.* To load the DCB driver, for example, type

```
LOAD A:DCB PORT=320 <Enter>
```

NOTE: The driver loads only if the parameters match the board's configuration and do not conflict with already loaded LAN and disk drivers.

If you have set the board to a conflicting configuration, you must down the file server, remove the board, and reconfigure the board.

- 4 Edit the STARTUP.NCF file by adding the command to load the disk driver.

For example, to load the DCB driver with an I/O port of 320, you would add the following line to the file:

```
LOAD DCB PORT=320
```

See “[Edit the STARTUP.NCF File](#)” on page 102 for more information.

- 5 Copy the disk driver file from the *System_2* diskette to the file server’s boot directory.

Use RCONSOLE to copy the file.

Load a Disk Driver for the Internal Disk Controller (Microchannel)

A microchannel computer can have three types of internal controllers: ESDI, MFM, and SCSI. Use the reference diskette that came with the computer to determine the type of controller installed in your computer.

The following steps explain how to load the PS2ESDI and PS2MFM drivers. If you have a SCSI controller, see “[Load a Disk Driver for a Disk Controller Board \(Microchannel\)](#)” on page 128.

Procedure

- 1 Boot the file server with DOS.
- 2 Run SERVER.
- 3 Enter the file server’s name and internal network number.
NOTE: See Chapter 2, “Install the File Server Software,” in *Installation and Upgrade* for more information about Steps 1 through 3.
- 4 Insert a working copy of the *System_2* diskette into drive A: of the file server.

- 5 Load a driver.

To load the PS2ESDI driver, for example, type

```
LOAD A:PS2ESDI <Enter>
```

- 6 Edit the STARTUP.NCF file by adding the command to load the disk driver.

For example, add the following line to the file for the PS2ESDI driver:

```
LOAD PS2ESDI
```

See “[Edit the STARTUP.NCF File](#)” on page 102 for more information.

- 7 Copy the disk driver file from the *System_2* diskette to the file server’s boot directory.

Use RCONSOLE to copy the file.

Load a Disk Driver for a Disk Controller Board (Microchannel)

If the controller board comes with its own instructions, please follow them. Use the following instructions for loading the PS2SCSI driver.

To load a disk driver for a controller board installed in a microchannel computer, complete the following steps.

Procedure

- 1 Down the file server.
- 2 Disconnect the power.
- 3 Install the board in the file server.
- 4 Connect the hard drives to the board.
- 5 Copy the configuration file to the reference or setup diskette for the microchannel computer.

The configuration file is usually an .ADF file on the diskette that came with the board.

- 6 Connect the power.
- 7 Complete one of the following:
 - ♦ If the controller board came with a setup program, run the setup program to select the hard disks. Then boot the file server and continue with Step 8.
 - ♦ If the controller board uses DISKSET to select the hard disks, boot the file server. Then continue with Step 8. (You select the hard disks in Step 12.)
- 8 Insert a working copy of the *System_2* diskette into drive A:.

- 9 The driver can be loaded at the command line with or without driver parameters.

Complete one of the following options:

- ◆ *Load without driver parameters.* To load the PS2SCSI driver, for example, type

```
LOAD A:PS2SCSI <Enter>
```

Enter the slot number for the board.

- ◆ *Load with driver parameters.* To load the PS2SCSI driver, for example, type

```
LOAD A:PS2SCSI SLOT=4 <Enter>
```

- 10 Edit the STARTUP.NCF file.

See [“Edit the STARTUP.NCF File” on page 102](#).

- 11 Add the command to load the disk driver.

For example, to load the PS2SCSI driver (installed in slot 4), add the following line to the file: **LOAD PS2SCSI SLOT=4**

- 12 Copy the disk driver file from the *System_2* diskette to the file server’s boot directory.

Use RCONSOLE to copy the file.

- 13 If the controller board uses DISKSET to select the hard disks, load DISKSET.

For instructions on selecting the hard disks, see [“DISKSET” on page 56](#).

Upgrade a Disk Driver

Procedure

- 1 Determine the current configuration information for the disk driver being upgraded.

View the STARTUP.NCF file in [“Edit the STARTUP.NCF File” on page 102](#).

- 2 Dismount all volumes stored on the hard disks connected to the controller board by typing

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with the name of a volume on the hard disks.
Repeat this step for all volumes stored on the hard disks.

NOTE: If you do not dismount all the volumes but still attempt to unload the disk driver, the operating system warns you that the driver is being used by mounted volumes and lists the volumes that are using the driver.

If you override the warning and unload the disk driver without dismounting the volumes, the file server automatically dismounts all volumes that are using the disk driver. Users who are logged in receive the following message:

```
Volume "volume_name" dismounted due to drive deactivation.
```

3 Unload the disk driver.

For example, to unload the ISADISK driver, type

```
UNLOAD ISADISK <Enter>
```

4 Load the updated driver.

For example, to load the ISADISK driver from a diskette into drive A:, type

```
LOAD A: ISADISK <Enter>
```

NOTE: If DOS has been removed with the SECURE CONSOLE or REMOVE DOS command, you cannot load the driver from drive A:. You have to copy the driver to the SYS:SYSTEM directory.

5 Remount the volumes.

See **“MOUNT”** on page 209.

6 Copy the updated driver to the directory containing the file server boot files.

Either down the file server or use RCONSOLE.

Troubleshooting the Host Bus Adapter Driver

Certain Host Bus Adapter (HBA) drivers reserve memory addresses between 14 MB and 16 MB. These addresses may conflict with (and corrupt) system memory if you have more than 14 MB installed. If this happens, you must remove the system memory or, if the server is an EISA machine, configure the conflicting addresses out of system memory. See the documentation that comes with your disk driver for address ranges.

The HBA cannot load unless the hard disks and controllers have been addressed, terminated, and configured properly.

The disk subsystem power must also be turned on. If the HBA driver fails to load, check the following:

- ♦ Make sure the hard disks are addressed and terminated correctly. If the controller can have two hard disks cabled to it, make sure that disk 0 is cabled and addressed as disk 0 and that it is terminated. Disk 1 needs to be cabled and addressed as disk 1, but it should not be terminated. If only one disk is attached to the controller, make it disk 0.
- ♦ Make sure the HBA is terminated if it connects to external subsystems and does *not* connect to any internal hard disks. Make sure the termination has been removed if the HBA is connected to internal hard disks.
- ♦ Make sure the last controller daisy-chained to the HBA is terminated.
- ♦ Make sure you address each controller attached to the host bus adapter according to its position in the daisy chain. For example, the controller attached directly to the Host Bus Adapter should have address 0, the controller attached to controller 0 should have address 1, etc.
- ♦ Disable parity on SCSI hard disks connected to an HBA. Most SCSI disks are shipped with parity enabled; you need to remove the jumper to disable parity. See the documentation that came with the hard disk.
- ♦ Check the power supply to the disk subsystem.
- ♦ Check interrupt conflicts. The following chart lists possible conflicts:

Hex Value Interrupts	Decimal Value Interrupts	Possible Conflicts
B	11	ISADISK.DSK
C	12	ISADISK.DSK, mouse port (COMPAQ & compatibles)
F	15	ISADISK.DSK

- ◆ Check for I/O port conflicts. The following chart lists some possible areas of conflict:

I/O port	Possible LAN driver conflicts
320	3C505,NE1000,NE2000
328	3C503 (330)
340	NE1000, NE2000
348	3C503 (350), TRXNET (350)

LOAD LAN driver

Why Use LOAD LAN driver?

Use *LOAD LAN driver* to link the appropriate drivers with the network boards installed in your file server.

IMPORTANT: Avoid memory conflicts. If you have installed more than 16 MB of memory, do *not* install a network board that uses online DMA or that is an AT bus master board. The board will corrupt the file server's memory.

If you want to use such a board, complete one of the following to remove the memory from the operating system:

- ◆ If you are using an EISA computer with memory above 16 MB, see [“Auto Register Memory above 16 Megabytes = value” on page 268](#).
- ◆ If you have a microchannel or ISA computer, remove the REGISTER MEMORY command from the AUTOEXEC.NCF file and reboot the file server.

The following tasks are described in this section:

Task	Page
Load a LAN driver in an EISA file server	“Load a LAN Driver in an EISA File Server” on page 149
Load a LAN driver in an ISA (AT bus) file server	“Load a LAN driver in an ISA (AT bus) File Server” on page 150
Load a LAN driver in a microchannel file server	“Load a LAN Driver in a Microchannel File Server” on page 152
Change an optional parameter of a loaded driver	“Change an Optional Parameter of a Loaded Driver” on page 153
Load a driver more than once	“Load a Driver More than Once” on page 155
Upgrade a LAN driver	“Upgrade a LAN Driver” on page 158
Troubleshooting LAN drivers	“Troubleshooting LAN Drivers” on page 159

Command Format

```
LOAD [path] LAN_driver [driver_parameter...]
```

Command Parameters

Replace *path* with a full path. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. Use SEARCH to set up additional paths for automatic searching.

Replace *LAN_driver* with the appropriate driver for your network board. LAN drivers shipped with the operating system are found on the *System_2* diskette. See “LAN drivers shipped with the operating system” on page 135. See NetWare or your Novell Authorized Reseller for a list of other certified LAN drivers and boards.

Driver Parameters

LAN drivers parameters may be required or optional.

- ◆ The LAN driver prompts you for required parameters if you do not specify them on the command line.
- ◆ The LAN driver does not prompt you for optional parameters; the default values are coded into the driver. To modify the default value, you must specify the new value at the command line when you load the driver.

Most drivers use one or more of the following parameters.

DMA=*number*
INT=*number*
NAME=*board name*
PORT=*number*
SLOT=*number*
FRAME=*name*
MEM=*number*
NODE=*number*
RETRIES=*number*

These driver parameters, and a few specialized TOKEN parameters, are described here. Lists and explanations of the parameters that each driver supports begin under “LAN Driver Parameters” on page 140.

Figure 19 LAN drivers shipped with the operating system

Driver	Network Board	Cabling System
TRXNET.LAN	RX-Net	Arcnet
	RX-Net II	
	RX-Net/2	
3C503.LAN	EtherLink II - ASSY 2227 (3C503)	Ethernet
3C505.LAN	EtherLink Plus - ASSY 2012 (3C505)	
3C523.LAN	EtherLink/MC	
NE2.LAN	NE/2	
NE232.LAN	NE/2-32	
NE1000.LAN	NE1000 - ASSY 950-054401 - ASSY 810-160-001	
NE2000.LAN	NE2000 - ASSY 810-149	
NE3200.LAN	NE3200	
TOKEN.LAN	PC Adapter II	Token-Ring
	16/4 Adapter	
	16/4 Adapter/A	
	PC Adapter/A	

DMA=number

Specifies the Direct Memory Access (DMA) channel the driver should use for the network board.

FRAME=*name*

Tells the Ethernet and Token-Ring drivers which type of packet header to use with NetWare. The default for Ethernet is the 802.2 standard (a length code); the default for Token-Ring is Token-Ring.

Ethernet. If you are using Ethernet drivers, replace *name* with one of the following:

Name	Explanation
Ethernet 802.3	Assigns a Novell frame. Use on a network that is using only NetWare.
Ethernet_II	Assigns a unique packet header (type code). Use on networks connected to DEC or to computers using the TCP/IP protocol.
Ethernet_802.2 (default)	Assigns the IEEE and OSI standard frame type.
Ethernet_SNAP	Use when the 802.2 SNAP extension is required.

If you select an option other than the default frame type (Ethernet_802.2), you must configure the drivers for the workstations.

Each workstation that you want to communicate with the file server needs its driver configured to the file server's frame type.

Use the following chart to determine the type of driver you can use in the workstation:

Frame type	DOS driver	DOS ODI driver
Ethernet_802.3	Yes	Yes
Ethernet_II	Yes	Yes
Ethernet_SNAP	No	Yes
Ethernet_802.2	No	Yes

For instructions on using the DOS ODI driver, see Chapter 2, "Preparing to Install Workstation Software," in *Workstation Basics and Installation*.

For instructions on configuring the DOS NET.CFG file for ODI drivers, see Workstation for DOS and Windows.

Token-Ring. If you are using Token-Ring drivers, replace *name* with one of the following:

Name	Explanation
Token-Ring	Assigns the standard packet header 802.2 (default). Use only with protocols which require 802.2 encapsulation (such as the OSI protocol suite.)
Token-Ring_SNAP	Assigns the 802.2 with SNAP header. Use with networks that need to communicate with such protocols as AppleTalk and TCP/IP.

If you select *Token-Ring_SNAP*, your workstations must use DOS ODI drivers that are configured for *Token-Ring_SNAP*. For instructions on configuring DOS ODI drivers, see *Workstation for DOS and Windows*.

INT=*number*

Reserves a unique interrupt for the driver. Some ISA (AT bus) drivers prompt for this parameter. Microchannel computers set this parameter with the reference diskette that comes with the computer.

LS=*number*

Determines the number of 802.5 link stations for the Token-Ring driver. This optional parameter can be modified at the command line only when the driver is loaded.

MEM=*number*

Reserves a unique memory address for the driver. Some ISA (AT bus) drivers prompt for this parameter. Microchannel computers set this parameter with the reference diskette that comes with the computer.

NAME=*board name*

Assigns a unique name to the board's configuration. You can use this optional parameter to identify network boards when you have more than one network board of the same type installed in the file server. The name can be 17 characters long.

NODE=*number*

Overrides the node address setting on some network boards. Use this optional parameter only if you or someone else keeps track of and assigns node addresses. The address selected must be a valid hexadecimal address for the board. Some drivers may not support this parameter.

PORT=*number*

Reserves a unique I/O port for the driver. Some ISA (AT bus) drivers prompt for this parameter. Microchannel computers set this parameter with the reference diskette that comes with the computer.

RETRIES=*number*

Instructs the driver to retry the packet transmission a specified number of times when a packet transmission fails. This optional parameter can be modified at the command line only when the driver is loaded.

SAPS=*number*

Determines the 802.2 service access point stations for the Token-Ring driver. This optional parameter can be modified at the command line only when the driver is loaded.

SLOT=*number*

Tells the operating system which board to link the driver to. This parameter is used with microchannel and EISA computers. The I/O ports, interrupts, memory addresses, and node addresses are set with the reference or setup diskette that comes with the computer.

TBC=*number*

Determines the transmit buffer count for the Token-Ring driver. This optional parameter can be modified at the command line only when the driver is loaded.

TBZ=*number*

Determines the transmit buffer size for the Token-Ring driver. The default assigns the maximum packet size allowed by either the board or the operating system. This optional parameter can be modified at the command line only when the driver is loaded.

For information on increasing the operating system's maximum packet size, see [“SET” on page 250](#).

Additional Information

Before you can load a v3.1x driver, you must do the following:

- ◆ Configure and install the network board in the file server.
- ◆ Make sure each network board is uniquely configured.
- ◆ Load (or autoload) NAGENT.

Third-party v3.0 drivers work with NetWare v3.1x. However, v3.0 drivers do not need NAGENT. System messages will be displayed about old API calls. Use the driver until an updated version is available.

If you have more than one network board of the same type in your file server, or if you need to use more than one frame type, you should understand how to load drivers more than once and how to load additional frames.

Multiple Boards

Most LAN drivers can be loaded more than once. Some drivers produce multiple copies in memory. These drivers produce the entire driver code in memory for each configuration entered with the driver.

Other drivers load reentrantly. These drivers produce only one copy of code and global data in memory and then allocate a small data block of memory for parameters each time the driver is loaded. These drivers use less memory than drivers that load the entire code in memory each time they are loaded.

Logical Boards

Ethernet and Token-Ring drivers can be configured so that the same network board can communicate using more than one frame type. When you load a driver using the same parameters except for frame type, the operating system views the second loading as another board.

For example, if two frame types are loaded for one NE2000 network board, the NE2000 board is treated as two logical boards—a board for each frame type.

LAN Driver Parameters

The LAN drivers and the parameters they support are described on the following pages.

Table 1 LAN driver parameters

LAN driver	Page
3C503	"3C503" on page 140
3C505	"3C505" on page 141
3C523	"3C523" on page 142
NE2	"NE2" on page 143
NE2-32	"NE2-32" on page 144
NE1000	"NE1000" on page 144
NE2000	"NE2000" on page 145
NE3200	"NE3200" on page 146
PCN2	"PCN2" on page 147
TOKEN	"TOKEN" on page 147
TRXNET	"TRXNET" on page 148

3C503

You can have up to four 3C503 boards in an ISA (AT) bus file server. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 16 times). This driver loads reentrantly.

Table 2 3C503 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
INT	3	2, 3, 4, 5	No
MEM	C8000*	C8000, CC000, D8000, DC000	No
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number**	Yes
PORT	300	300, 310, 330, 350, 250, 280, 2A0, 2E0	No
RETRIES	5	0—255	Yes

To change the transceiver type from BNC (thin ethernet cabling or an internal transceiver) to DIX (thick ethernet cabling or an external transceiver), load the driver with the DIX parameter by typing

```
LOAD 3C503 DIX <Enter>
```

The default is BNC. This parameter does not need to be specified. If the driver has been loaded with DIX, you can unload the driver and then reload the driver without the DIX parameter to set the driver to the default (BNC).

3C505

You can have up to three 3C505 boards in an ISA (AT) bus file server. However, the board must be installed in a 16-bit slot. You can load this driver for each board and for each frame type assigned to a board (maximum: 12 times). The driver loads reentrantly.

Table 3 3C505 driver

Parameter	Default	Supported values	Optional
DMA	5	1, 3, 5, 6, 7	No

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
INT	3	2, 3, 4, 5	No
MEM	C8000*	C8000, CC000, D8000, DC000	No
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number**	Yes
PORT	300	300, 310, 330, 350, 250, 280, 2A0, 2E0	No
RETRIES	5	0—255	Yes

IMPORTANT: This driver uses the board's DMA. Do *not* use this driver in a file server that has more than 16 MB of memory installed.

3C523

You can have up to four 3C523 boards in the microchannel file server. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 16 times). This driver loads re-entrantly.

Set the interrupts, memory addresses, I/O ports, and transceiver type with the computer's setup or reference diskette. You must also enable the board with the reference diskette. The driver reads these settings when you enter the slot number in which the board is installed.

Table 4 3C523 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes

Parameter	Default	Supported values	Optional
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number**	Yes
RETRIES	10	0—255	Yes
SLOT	None	All available	No

NE2

You can have as many as four NE/2 boards in a microchannel file server, installed in 16-bit slots. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 16 times). This driver loads reentrantly.

Set the interrupts, memory addresses, and I/O ports with the computer's setup or reference diskette. The recommended setting for memory is disabled. The driver reads the settings when you enter the slot number in which the board is installed.

Table 5 NE2 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number**	Yes
RETRIES	5	0—255	Yes
SLOT	First one found scanning from slot 1 to 8	1—8	No

NE2-32

The NE2-32 driver can be loaded for as many NE2-32 boards as can fit in a microchannel file server. If your server has only three 32-bit slots, you can install three boards. You can load this driver for each board and for each additional frame type assigned to the board. This driver loads reentrantly.

Set the interrupts, memory addresses, and I/O ports with the computer's setup or reference diskette. The driver reads these settings when you enter the slot number in which the board is installed.

Table 6 NE2-32 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
NAME	None	Any unique 17-character name	Yes
RETRIES	5	0—255	Yes
SLOT	None	All available	No

NE1000

You can have as many as four NE1000 boards in an ISA (AT bus) file server if the boards are configured so that they do not conflict with other components in the file server. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 16 times). This driver loads reentrantly.

Table 7 NE1000 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
INT	3	2, 3, 4, 5	No
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number*	Yes
PORT	300	300, 320, 340, 360	No
RETRIES	5	0—255	Yes

NE2000

You can have up to four NE2000 boards in an ISA (AT bus) file server if the boards are configured so that they do not conflict with other hardware in the file server. However, each board must be installed in a 16-bit slot. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 16 times). This driver loads reentrantly.

Table 8 NE2000 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
INT	3	2, 3, 4, 5	No
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number*	Yes

Parameter	Default	Supported values	Optional
PORT	300	300, 320, 340, 360	No
RETRIES	5	0—255	Yes

NE3200

You can have up to six NE3200 boards in the EISA (Extended Industry Standard Architecture) file server. However, the board must be installed in a 32-bit bus master slot. You can load this driver for each board and for each additional frame type assigned to the board (maximum: 24 times). This driver loads reentrantly.

Set interrupts and connector types with the *CONFIGURATION* (or similarly named) diskette. The driver reads these settings when you enter the slot number in which the board is installed.

Table 9 NE3200 driver

Parameter	Default	Supported values	Optional
FRAME	Ethernet_802.2	Ethernet_802.2 Ethernet_II Ethernet_Snap Ethernet_802.3	Yes
NAME	None	Any unique 17-character name	Yes
RETRIES	5	0-255	Yes
SLOT	None	All available	No

NOTE: The NE3200 driver uses more than one packet receive buffer. If the “No ECB available count” counter in MONITOR increments, see **“SET” on page 250** to increase the minimum and maximum number of packet receive buffers.

PCN2

You can have a maximum of two PCN2 boards in a file server, one each at the primary port addresses.

Table 10 PCN2 driver

Parameter	Default	Supported values	Optional
FRAME	PCN2_802.2	PCN2_802.2 PCN2_Snap	Yes
NAME	None	Any unique 17-character name	Yes
NODE	Board value	Any 12-digit hexadecimal number*	Yes
PORT	620	620, 628	No

TOKEN

You can use this driver in both ISA (AT bus) and microchannel file servers. You can have a maximum of two Token-Ring network boards in your file server.

All parameters are optional. You can modify parameters at the command line only when you load the driver. All users of the driver can set the NAME, NODE, MEM, and TBZ parameters. You should not set the other parameters unless you are a programmer.

IMPORTANT: The shared RAM should not be set higher than 16 KB. Even though some boards can be set to 64 KB, use 16 KB. The file server will still use all 64 KB on the board.

Table 11 TOKEN driver

Parameter	Default	Supported values	Optional
FRAME	IBM_TOKEN_RING	IBM_TOKEN_RING IBM_TOKEN_RING_SNAP	Yes
LS	0	0-255	Yes
MEM	0*	A0000-F0000	Yes
NAME	None	Any unique 17-character name	Yes

Parameter	Default	Supported values	Optional
NODE	Board value	Any 8-digit hexadecimal number**	Yes
PORT	A20	A20, A24	Yes
SAPS	0	0-255	Yes
SLOT	None	All available	Yes
TBC	2	0-2	Yes
TBZ	0***	96-65535	Yes

TRXNET

This driver can be used for both ISA (AT bus) and microchannel file servers.

- ◆ An ISA file server can have as many as four RX-Net boards installed; therefore, you can load this driver four times in an ISA file server.
- ◆ A microchannel file server can have as many as six RX-Net boards installed; therefore, you can load this driver six times in a microchannel file server.

The driver loads reentrantly.

ISA parameters. When loading the TRXNET driver in an ISA file server, select values from the following table.

Table 12 TRXNET driver

Parameter	Default	Supported values	Optional
INT	2	2, 3, 4, 5*, 7	No
NAME	None	Any unique 17-character name	Yes
MEM	D0000	C0000, CC000, D0000, DC000, E0000	No
PORT	2E0	2E0, 2F0, 300, 310, 350	No
RETRIES	100	0-255	Yes

Microchannel parameters. Select interrupts, memory addresses, and I/O ports with the computer's setup or reference diskette. When you load the driver, use the values from the chart below.

Table 13 TRXNET driver for microchannel computers

Parameter	Default	Supported values	Optional
NAME	None	Any unique 17-character name	Yes
RETRIES	100	0-255	Yes
SLOT	None	All available	Yes

Load a LAN Driver in an EISA File Server

To load a driver in an EISA file server, complete the following steps. (For a list of the configuration options supported by the driver, see the parameters listed under “LAN Driver Parameters” on page 140 through “TRXNET” on page 148.)

Procedure to Down the file server.

- 1** Make sure all power is off before installing a network board.
- 2** Install the board in the file server.
See the NetWare supplement or the documentation that came with the computer for installation instructions.
- 3** Connect the power to the file server.
- 4** Copy the .CFG file from the diskette that came with the board to the *CONFIGURATION* (or similarly named) diskette for the file server.
- 5** Configure the board with the EISA configuration utility.
- 6** Boot the file server.
NOTE: If NAGENT is not loaded, NAGENT automatically loads with the driver.

7 Load the driver.

You can load the driver at the command line with or without parameters. Do one of the following:

- ◆ *Without driver parameters.* For example, to load the NE3200 driver without driver parameters, type

```
LOAD NE3200 <Enter>
```

You are prompted to enter the board's slot number.

- ◆ *With driver parameters.* For example, to load the NE3200 driver with driver parameters and the name BACKBONE, type

```
LOAD NE3200 SLOT=3 NAME=BACKBONE <Enter>
```

8 Bind a communication protocol to the board.

See [“BIND” on page 35](#).

9 Edit the AUTOEXEC.NCF file to load and bind the driver automatically.

For example, to load the NE3200 driver automatically (configuration: slot=3, name=BACKBONE) and bind IP to the driver, add the following lines to the AUTOEXEC.NCF file:

```
LOAD NE3200 SLOT=3 NAME=BACKBONE
```

```
BIND IP TO BACKBONE NET=26
```

For instructions on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Load a LAN driver in an ISA (AT bus) File Server

To load a driver in an ISA file server, complete the following steps. (For a list of the configuration options that are supported by the driver, see the parameters listed under [“LAN Driver Parameters” on page 140](#) through [“TRXNET” on page 148](#).)

- 1 If you do not know the configuration of the boards already installed in the file server, run CONFIG.
- 2 Down the file server.
- 3 Make sure the power is off before installing a network board.

4 Configure the board and install it in the file server.

See the NetWare supplement or the documentation that came with the board for appropriate jumper settings.

Select settings that are supported by the driver and that do not conflict with the boards already installed. Record the configuration information for the new board.

5 Connect the power.

6 Boot the file server.

NOTE: If NAGENT is not loaded, the driver loads it.

7 Load the driver.

The driver can be loaded at the command line with or without driver parameters. Complete one of the following:

- ◆ *Without driver parameters.* For example, to load the NE2000 driver without driver parameters, type

```
LOAD NE2000 <Enter>
```

You are prompted to enter the configuration information.

You can select only options that do not conflict with boards already installed. To change a default parameter, type the value that corresponds to the board's configuration.

- ◆ *With driver parameters.* For example, to load the TRXNET driver with driver parameters, type

```
LOAD TRXNET INT=3 PORT=2E0 MEM=C0000 <Enter>
```

NOTE: The driver only loads if the parameters match the board's configuration and the board's configuration does not conflict with any other server hardware.

If you have set the board to a conflicting configuration, the driver will not load. You will need to down the file server, remove the board, and set the board differently before the driver can load. See the NetWare supplement or the documentation for the LAN driver board.

8 Bind a communication protocol to the driver.

See **“BIND” on page 35**.

- 9 Edit the AUTOEXEC.NCF file and add lines to load the driver and bind it to a protocol.

For example, to load the TRXNET driver (configuration: interrupt=3, I/O port=2E0, and memory address=C000) and bind it to IPX, add the following lines to the AUTOEXEC.NCF file:

```
LOAD TRXNET INT=3 PORT=2E0 MEM=C0000
BIND IPX TO TRXNET NET=26
```

For instructions on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Load a LAN Driver in a Microchannel File Server

To load a driver in a microchannel file server, complete the following steps. (For a list of the configuration options supported by the driver, see the parameters under [“LAN Driver Parameters” on page 140](#) through [“TRXNET” on page 148](#).)

- 1 Down the file server.
- 2 Turn the power off before you install a network board.
- 3 Install the board in the file server.

See the NetWare supplement or the documentation that came with the board for installation instructions.

- 4 Copy the *.ADF file from the diskette that came with the board to the setup or reference diskette for the file server.

For more information, see the instructions that came with the reference diskette.

- 5 Connect the power to the file server.
- 6 Run the setup or reference program and configure the board.

IMPORTANT: If you are using RX-Net boards and compatibles, make sure that the node address is unique and is *not* 0.

- 7 Boot the file server.

NOTE: If NAGENT is not loaded, NAGENT will automatically load with the driver.

8 Load the driver.

You can load the driver with or without parameters at the command line. Do one of the following:

- ◆ *Without driver parameters.* For example, to load the TRXNET driver without driver parameters, type

```
LOAD TRXNET <Enter>
```

You are prompted to enter the board's slot number.

- ◆ *With driver parameters.* For example, to load the NE2 driver with parameters and the name BACKBONE, type

```
LOAD NE2 SLOT=3 NAME=BACKBONE <Enter>
```

9 Bind a communication protocol to the board.

See [“BIND” on page 35](#).

10 Edit the AUTOEXEC.NCF file and add lines to load the driver and bind it to a protocol.

For example, to load the NE2 driver automatically (configuration: slot=3, name=BACKBONE) and bind it to the IP protocol, add the following lines to the file:

```
LOAD NE2 SLOT=3 NAME=BACKBONE  
BIND IP TO NE2 NET=26
```

For instructions on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Change an Optional Parameter of a Loaded Driver

You can change optional parameters for loaded drivers. (For a list of optional parameters for your LAN driver, see [“LAN Driver Parameters” on page 140](#) through [“TRXNET” on page 148](#).) Hardware configuration options *cannot* be changed following these steps.

IMPORTANT: If users are logged in and doing critical processes, do not change the driver parameters until the users have logged out.

You should be able to change an optional parameter in less than five minutes. If a logged-in user makes a call to the file server during the process, the user receives a lost connection message. If the user waits until you finish (and you finish within 15 minutes), the user can re-establish the connection by choosing to retry.

If this process takes 15 minutes or longer, users who are logged in lose their current work and their connections to the file server.

Procedure

1 Type “CONFIG” at the console and record the parameter information for the driver you are going to change.

2 Unload the driver at the console prompt.

For example, to unload the TRXNET driver, type

```
UNLOAD TRXNET <Enter>
```

3 Load the driver with the value for the optional parameter.

For example, to add a board name for the TRXNET driver, type

```
LOAD TRXNET NAME=LOCAL <Enter>
```

You are prompted to enter needed configuration information if you did not enter it with the optional parameter.

If more than one network board uses the driver, load the driver for each board.

4 Bind a communication protocol to the network board.

See “[BIND](#)” on page 35.

If the driver is used by more than one network board, bind a communication protocol to each board.

5 Edit the AUTOEXEC.NCF file and add lines to load the driver and bind it to a protocol.

For example, to load the NE2 driver automatically (configuration: slot=3, name=BACKBONE) and bind it to the IP protocol, add the following lines to the AUTOEXEC.NCF file:

```
LOAD NE2 SLOT=3 NAME=BACKBONE
```

```
BIND IP TO NE2 NET=26
```

For instructions on editing the AUTOEXEC.NCF file, see “[Edit the AUTOEXEC.NCF File](#)” on page 98.

Load a Driver More than Once

If you have installed more than one network board of the same type or if you need to use more than one frame type, you must load the same driver more than once. For more information on frame types, see “Frame” in *Concepts*.

From the procedures that follow, select the one that fits your situation.

Load the Driver for a Second Board

To load the driver a second time for an additional network board installed in the file server, complete the following steps.

Procedure

- 1 Load the driver.

For example, to load the NE2000 driver, type

```
LOAD NE2000 <Enter>
```

- 2 Answer “No” to the following prompt by pressing <Enter>:

```
Do you want to add another frame type for a previously  
loaded board? n
```

- 3 Answer the prompts for the configuration parameters.

When you have successfully added the second configuration to the driver, the following prompt appears:

```
Previously loaded module was used re-entrantly.
```

- 4 Bind a configuration protocol to this unique configuration of the network board.

See “[BIND](#)” on page 35.

- 5 Edit the AUTOEXEC.NCF file and add the commands to load and bind the driver.

For example, to load the NE2000 driver (configuration: interrupt=4, port=340, protocol=IPX, net=26) automatically, add the following lines to the AUTOEXEC.NCF file:

```
LOAD NE2000 INT=4 PORT=340
BIND IPX NE2000 NET=26
```

For more information on editing this file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Load the Driver for a Second Frame Type

To add a second frame type to a loaded driver, complete the following steps.

Procedure

- 1 Load the driver again.

For example, to load the NE2000 driver, type

```
LOAD NE2000 <Enter>
```

- 2 Answer “Yes” to the following prompt by typing “Y” and pressing <Enter>:

```
Do you want to add another frame type for a previously
loaded board? n
```

A list of supported frame types for the board appears.

- 3 Enter the number of the frame type you want to add and press <Enter>.
- 4 Bind a configuration protocol to this unique configuration of the network board.

See [“BIND” on page 35](#).

- 5 Edit the AUTOEXEC.NCF file and add the commands to load and bind the driver.

For example, to load and bind the NE2000 driver (configuration: interrupt=3, port=300, frame=ETHERNET_II, protocol=IPX, net=27) automatically, add the following lines to the file:

```
LOAD NE2000 INT=3 PORT=300 FRAME=ETHERNET_II
BIND IPX NE2000 [PORT=300 INT=3
FRAME=ETHERNET_II] NET=27
```

For instructions on editing this file, see [“Edit the AUTOEXEC.NCF File” on page 98.](#)

Add Multiple Frames to More than One Network Board

To add more than one frame type to a network board when the driver has already been loaded for more than one network board, complete the following steps.

Procedure

- 1 Load the driver.

For example, to load the NE2000 driver, type

```
LOAD NE2000 <Enter>
```

- 2 Answer “Yes” to the following prompt by typing “y” and pressing <Enter>:

```
Do you want to add another frame type for a previously  
loaded board? n
```

A list of configurations for the network board appears.

- 3 Enter the number of the configuration that you want to add the frame type to and press <Enter>.

A list of supported frame types for the board appears.

- 4 Enter the number of the frame type you want to add and press <Enter>.
- 5 Bind a configuration protocol to this unique configuration for the network board.

See [“BIND” on page 35.](#)

- 6 Edit the AUTOEXEC.NCF file and add the command to load and bind the driver with the new configuration.

For example, to load and bind the NE2000 driver (configuration: interrupt=4, port=340, frame=Ethernet_SNAP, protocol=IPX, net=30) automatically, add the following lines to the file:

```
LOAD NE2000 INT=4 PORT=340 FRAME=ETHERNET_SNAP  
BIND IPX NE2000 [PORT=340 INT=4  
FRAME=ETHERNET_SNAP] NET=30
```

For more information on editing this file, see [“Edit the AUTOEXEC.NCF File” on page 98.](#)

Upgrade a LAN Driver

If the developer of a LAN driver releases an updated version of the driver, you can load it without downing the file server.

IMPORTANT: If users are logged in and running critical processes, do not upgrade the driver until they have logged out.

You should be able to upgrade the driver in less than five minutes. If a logged-in user makes a call to the file server during the process, the user receives a lost connection message. If the user waits until you finish (and you finish within 15 minutes), the user can re-establish the connection by choosing to retry.

If the upgrade takes more than 15 minutes, users lose their current connections and their work.

To upgrade a driver, complete the following steps.

Procedure

- 1** From a workstation, log in to the file server as SUPERVISOR (or supervisor equivalent).
- 2** Copy the updated driver to the SYS:SYSTEM directory.
- 3** Run CONFIG and record the configuration settings for the network boards that will use the updated driver. Type

```
CONFIG <Enter>
```

- 4** Unload the current driver.

For example, type

```
UNLOAD TRXNET <Enter>
```

When you unload the driver, the driver unbinds all communication protocols.

- 5** Load the updated driver.

For example, type

```
LOAD TRXNET <Enter>
```

Enter the parameters that match the board's configuration. If more than one network board uses the driver, load the driver for each board.

- 6** Bind a communication protocol to the network board.

See [“BIND” on page 35](#).

If you have loaded the driver more than once, bind a protocol to each network board.

Troubleshooting LAN Drivers

Most LAN drivers cannot be loaded unless the network board has a cable attached and the cabling has been properly terminated. Check the cabling. See the appropriate NetWare supplement for your network board to set up and terminate the cabling system.

LAN drivers cannot share interrupts, I/O ports, or memory addresses with any other piece of hardware in the file server.

NOTE: The exception is the TOKEN driver, which allows you to configure two Token-Ring network boards to the same interrupt. However, the TOKEN driver cannot share the interrupt with other types of LAN drivers.

The following sections should help you prevent conflicts with other network boards, the print server, and other types of hardware in the file server.

Network Board Conflicts

If two network boards have been configured to the same parameter, the file server may display one of the following symptoms:

- ◆ The LAN driver does not initialize when loaded.
- ◆ The computer refuses to boot DOS or beeps when DOS is booted.
- ◆ If the driver loads and initializes, the conflict prevents the driver from broadcasting any packets.

Make sure you fill out the “File Server Worksheet” in *Installation and Upgrade* so that you have an accurate record of the parameters. Do not configure any network boards (except interrupts for two Token-Ring boards) to the same interrupt, I/O port, memory address, or DMA.

Another source of conflict with LAN drivers is overlapping memory addresses or I/O port addresses. Each address parameter specifies a range of bytes that begins at the parameter. (CONFIG displays the range for a loaded LAN driver.)

For example, the TOKEN driver (for a board configured to 16 KB) starts its memory address at D80000 and uses all memory from D80000 to DC0000. If you load another driver or install hardware that uses memory starting at D70000 and ending at D85000, the TOKEN driver will not initialize (because of the memory conflict).

To avoid memory address and I/O port conflicts, do either of the following:

- ◆ Map the memory ranges of all hardware I/O ports and memory addresses. Make sure that no conflicts exist. (CONFIG displays the memory range of memory addresses and I/O ports for all loaded drivers.)
- ◆ Select options as far away from each other as the software and hardware will allow. For example, if you configure the NE1000 board with an I/O port of 300, select 2E0 or 350 rather than 310 for the I/O port of the RX-Net board.

Print Server Conflicts

The network board configurations can also conflict with printers if your file server is also your print server. The printers attached to the file server can be configured to use the same interrupts as a LAN board.

To prevent conflicts with PSERVER.NLM, complete one or more of the following:

- ◆ Use PCONSOLE to display the interrupts selected for the printers attached to the file server. Do *not* configure a network board to any interrupt used by a printer.
- ◆ Change a printer so that it is polled and does not use an interrupt (see Chapter 2, “Print Server Installation,” in *Print Server*). Polling will free the interrupt so that a network board can use the interrupt.
- ◆ Reconfigure the board’s interrupt (see the NetWare supplement for the network board).

Hardware Conflicts

The following chart lists the interrupts and I/O ports of various pieces of hardware. If the hardware is installed, check the parameters to see if they conflict with the configuration you set for the network board.

Hardware	Interrupt (decimal)	I/O port (hexadecimal)
COM1	4	3F8 - 3FF
COM2	3	2F8 - 2FF
LPT1	7	378 - 37F
If LPT3 exists, then		
LPT1	7	3BC - 3BE
LPT2	5	378 - 37A
LPT3	-	278 - 27A
AT Controller	14	1F0 - 1F8 170 - 177
Floppy Controller	6	1F0 - 1F8
Tape Controller	5	280 - 28F
EGA	2	3C0 - 3CF
VGA	-	102, 46E8
Mono Adapter	-	3B0 - 3BF
Color Graphics	-	3D0 - 3DF

For example, if you configure a 3C503 network board to interrupt 2 and your file server has an EGA monitor, the network board's interrupt conflicts with the monitor's interrupt.

LOAD *name space*

Why Use LOAD *name space*?

Use LOAD *name space* if you have computers that need to store non-DOS files on your file server.

The following tasks are described in this section:

Task	Page
Load name space	“LOAD name space” on page 162
Upgrade name space	“Upgrade Name Space” on page 166

Command Format

```
LOAD [path] name_space
```

Command Parameters

Replace *path* with a full directory path to the directory containing the name space module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *name_space* with the name of the module that you need. Name space modules all end with the .NAM extension and are found on the *NetWare Operating System_2* diskette. Included with NetWare v3.12 are MAC and OS/2 name space modules.

Consult NetWare, your Novell Authorized Reseller, or third-party dealers for a list of other certified name space modules.

Additional Information

A name space module allows you to store non-DOS files on a NetWare file server. When you link the name space module to a volume with the ADD NAME SPACE command, the operating system maintains a directory table with two entries for each file—one for DOS naming conventions and information and one for non-DOS naming conventions and information. For more information, see “Name space” in *Concepts*.

IMPORTANT: Because name space support takes extra memory, be sure to leave enough memory to mount the volume.

Before adding a name space to a volume, you need to calculate the amount of memory that the name space will require. View the current volume size with INSTALL (see “[Increase the Size of a Volume](#)” on page 93). Then use the following chart, [Figure 20 on page 164](#), to estimate the total amount of memory needed per volume.

Figure 20 Calculating memory for adding name space

How much memory does your server need?

1. Calculate the memory requirement for each volume.

For each DOS volume:

$$M = .023 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

For each volume with added name space:

$$M = .032 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

2. Add the memory requirements for all volumes.

$$\text{Total Volume Memory} = M_{\text{SYS}} + M_{\text{VOL1}} + M_{\text{VOL2}} + \dots$$

3. Add 2 MB for the operating system and round the figure to the next higher MB.

4. Your computer needs at least 4 MB to run NetWare. If Steps 1 through 3 have only arrived at 3 MB, assume a minimum memory requirement of 4 MB anyway.

Example:

A server has four volumes, each with a block size of 4:

SYS: an 80MB DOS volume

DOSVOL: a 100MB DOS volume

UNIXVOL: a 300MB volume with name space

MACVOL: a 100MB volume with name space

1. Memory requirement for each volume:
 $M_{\text{SYS}} = .023 \times 80 \text{ MB} \div 4 = 0.46 \text{ MB}$
 $M_{\text{DOSVOL}} = .023 \times 100 \text{ MB} \div 4 = 0.575 \text{ MB}$
 $M_{\text{UNIXVOL}} = .032 \times 300 \text{ MB} \div 4 = 2.4 \text{ MB}$
 $M_{\text{MACVOL}} = .032 \times 100 \text{ MB} \div 4 = 0.8 \text{ MB}$

2. Total volume memory requirements: $0.46 + 0.575 + 2.4 + 0.8 = 4.235 \text{ MB}$

3. Operating system memory requirements: $2 + 4.235 = 6.235 \gg 7 \text{ MB}$

4. 7 MB is higher than the 4 MB minimum; therefore, no further adjustment is needed. Your server needs at least 7 MB of memory.

In addition to loading the name space module, you must also complete the following tasks to set up the file server for non-DOS files:

- ♦ Link the module to the volumes where you want to store the specific type of non-DOS files on. Use `ADD NAME SPACE`.
- ♦ For further instructions, see the documentation that accompanies the name space module.

Load Name Space

Procedure

- 1** To load name space, type “LOAD” and the name of the name space module.

For example, to load support for Macintosh filenames, type

```
LOAD MAC <Enter>
```

- 2** Copy the module to the appropriate directory by completing one of the following:
 - ♦ If the name space module is used with volume `SYS:`, use `RCONSOLE` to copy the module to the directory containing the file server boot files. Step 3 explains how to add the command to the `STARTUP.NCF` file.
 - ♦ If the module is not used with volume `SYS:`, do one of the following:
 - ♦ Copy the module to the `SYS:SYSTEM` directory. Step 3 explains how to add the command to the `AUTOEXEC.NCF` file.
 - ♦ Use `RCONSOLE` to copy the module to the directory containing the file server boot files. Step 3 explains how to add the command to the `STARTUP.NCF` file.

- 3** Add the following command to the appropriate `.NCF` file:

```
LOAD MAC
```

For instructions on editing this file, see “[Edit the AUTOEXEC.NCF File](#)” on page 98, or “[Edit the STARTUP.NCF File](#)” on page 102.

- 4** Configure a volume to support an additional type of name space.

See “[ADD NAME SPACE](#)” on page 31.

- 5** For further instructions, refer to the documentation that accompanies your non-DOS product.

Upgrade Name Space

If the manufacturer of the name space module produces a new version of the module, you can update the module without downing the file server.

IMPORTANT: These steps do not work if volume SYS: is using the name space module and you have used the SECURE CONSOLE or REMOVE DOS command. You will have to down the file server, copy the updated module to the file server boot directory, and then reboot the file server.

To update the module without downing the file server, complete the following steps:

Procedure

1 Back up the data on all volumes that use the name space module.

2 Dismount all volumes that use the name space module.

3 Unload the current name space module.

For example, to unload the MAC module, type

```
UNLOAD MAC <Enter>
```

If you did not dismount all the volumes using the non-DOS module, a list of volumes still using the module will appear. Answer “No” to the prompt and use DISMOUNT to dismount the remaining volumes.

4 Insert the diskette with the updated module into drive A of the file server.

NOTE: If you have used SECURE CONSOLE or REMOVE DOS, you cannot load the module from a DOS drive. Use RCONSOLE to copy the file to SYS:SYSTEM and the file server boot directory.

5 Load the updated module.

For example, to load the MAC module, type

```
LOAD A:MAC <Enter>
```

6 Mount all volumes that were using the module by typing

```
MOUNT ALL <Enter>
```

The operating system mounts all dismounted volumes. If you do not want all dismounted volumes to mount, mount individual volumes by using MOUNT with the names of the volumes.

7 Copy the updated module to the directory that has the older version of the module.

LOAD *NLM utility*

Why Use Load *NLM utility*?

Use LOAD *NLM* (NetWare Loadable Module) *utility* to link management and enhancement programs with the operating system. These programs may provide such services as installation, monitor, volume repair, backup, and diagnostics.

Some NLMs require that you load other NLMs first. Some NLMs load other NLMs automatically. Still others load from the product options menu of INSTALL. See “[Install, Uninstall, or Configure a Product on the File Server](#)” on page 104.

Command Format

```
LOAD [path]NLM_utility [parameter...]
```

Command Parameters

Replace *path* with a full directory path to the directory containing the NLM utility. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a *path* and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *NLM_utility* with the name of the module you want to load. NLMs shipped with NetWare v3.12 are on the *System-2* and *System-3* diskettes. Consult NetWare, your Novell Authorized Reseller, or third-party dealers for a list of other approved NLMs. All utilities that are loadable modules have an .NLM extension.

Replace *parameter* with the parameters supported by the module you are loading.

Load an NLM Utility

To load an NLM utility, type “LOAD” and the name of the NLM at the console prompt.

For example, to load the INSTALL utility, type

```
LOAD INSTALL <Enter>
```

IMPORTANT: Do not unload a protocol-stack NLM such as IPXS or SPXS until you have unloaded all applications that potentially depend on it.

MAGAZINE

Why Use MAGAZINE?

Use MAGAZINE to confirm that magazine requests (“Insert Magazine” and “Remove Magazine”) from the NetWare server have or have not been satisfied.

Command Format

MAGAZINE [*parameter*]

Command Parameters

Replace *parameter* with one of these four options:

Option	Explanation
Inserted	Acknowledges that the specified media magazine was inserted in response to the “Insert Magazine” console message.
Not Inserted	Acknowledges that the specified media magazine was not inserted in response to the “Insert Magazine” console message.
Not Removed	Acknowledges that the specified media magazine was not removed in response to the “Remove Magazine” console message.
Removed	Acknowledges that the specified media magazine was removed in response to the “Remove Magazine” console message.

MATHLIB

Why Use MATHLIB?

Use MATHLIB if your server has a math coprocessor (a 486 computer or a 386 computer with a math coprocessor chip). You must load STREAMS and CLIB before you load MATHLIB.

Command Format

```
LOAD [path]MATHLIB
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

The following modules need to be loaded in the order listed below:

```
STREAMS  
CLIB  
MATHLIB
```

Load MATHLIB

To load MATHLIB, type

```
LOAD MATHLIB <Enter>
```

NOTE: To make sure that the modules necessary for MATHLIB are loaded automatically when the file server is booted, add the following commands to the AUTOEXEC.NCF file. For instructions on editing the AUTOEXEC.NCF file, see ["Edit the AUTOEXEC.NCF File" on page 98](#).

```
LOAD STREAMS  
LOAD CLIB  
LOAD MATHLIB
```

MATHLIBC

Why Use MATHLIBC?

Use MATHLIBC if your file server does not have a math coprocessor (a 386 machine without the math coprocessor chip). You must load STREAMS and CLIB before you load MATHLIBC.

Command Format

```
LOAD [path]MATHLIBC
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

The following modules need to be loaded in the order listed below:

```
STREAMS  
CLIB  
MATHLIBC
```

Load MATHLIBC

To load MATHLIBC, type

```
LOAD MATHLIBC <Enter>
```

NOTE: To make sure that the modules necessary for MATHLIBC are loaded automatically when the file server is booted, add the following commands to the AUTOEXEC.NCF file. For instructions on editing the AUTOEXEC.NCF file, see ["Edit the AUTOEXEC.NCF File" on page 98](#).

```
LOAD STREAMS  
LOAD CLIB  
LOAD MATHLIBC
```

MEDIA

Why Use MEDIA?

Use MEDIA to confirm that media requests (“Insert Media” and “Remove Media”) from the NetWare server have or have not been satisfied.

Command Format

MEDIA [*parameter*]

Command Parameters

Replace *parameter* with one of these four options:

Option	Explanation
Inserted	Acknowledges that the specified media was inserted in response to the “Insert Media” console message.
Not Inserted	Acknowledges that the specified media was not inserted in response to the “Insert Media” console message.
Not Removed	Acknowledges that the specified media was not removed in response to the “Remove Media” console message.
Removed	Acknowledges that the specified media was removed in response to the “Remove Media” console message.

MEMORY

Why Use MEMORY?

Use MEMORY to display the total amount of installed memory that the operating system can address.

Command Format

MEMORY

Additional Information

NetWare v3.1x automatically addresses memory above 16 MB on EISA computers. On microchannel and ISA (AT bus) computers, NetWare can only automatically address memory up to 16 MB. Use the REGISTER MEMORY command to enable the operating system to address memory above 16 MB.

Display the Total Amount of Memory

To display the total amount of installed memory that the operating system is currently addressing, type

MEMORY <Enter>

MIRROR STATUS

Why Use MIRROR STATUS?

Use MIRROR STATUS to display all mirrored logical partitions and the status of each.

Command Format

MIRROR STATUS

Display Status of Mirrored Logical Partitions

To display the status of all mirrored logical partitions, type

MIRROR STATUS <Enter>

MIRROR STATUS displays five statuses for partitions. The following table explains each status.

Table 14 **Mirror statuses**

Status	Explanation
Not mirrored	The partition is not being mirrored.
Orphaned state	The integrity of the data in this partition is not guaranteed. Use the “Mirroring” option in the INSTALL utility to recover the partition from its orphaned state.
Fully synchronized	The mirrored partitions have the same data and are functioning correctly.
Out of synchronization	One of the servers does not have the same data and is not being remirrored.
Being remirrored	The partition is being remirrored. The percentage of remirroring completed is displayed.

MODULES

Why Use MODULES?

Use MODULES to display the following information about the modules currently loaded in the file server:

- ◆ The short name used to load the module
- ◆ A descriptive string or long name for each module
- ◆ The version number for disk and LAN drivers

Command Format

MODULES

Additional Information

A loadable module links itself to the operating system and allocates a portion of the file server's memory for its use. Some modules, such as LAN drivers and disk drivers, need to be loaded every time the file server is brought up. Other modules, particularly the NLM utilities, can be loaded, used, and then unloaded. When the module is unloaded, the module returns its allocated resources to the file server.

For additional information, see "NetWare Loadable Module" in *Concepts*.

For additional information about loading and unloading modules, see "LOAD" on page 109 and "UNLOAD" on page 312.

List the Loaded Modules

To list the loaded modules, type

MODULES <Enter>

Information similar to the following appears:

```
MONITOR.NLM NetWare 386 Console Monitor Version 1.67 February  
7, 1991 Copyright 1991 Novell, Inc. All rights reserved.
```

```
RSPX.NLM NetWare 386 Console SPX Driver Version 1.30 February  
9, 1991 Copyright 1991 Novell, Inc. All rights reserved.
```

```
REMOTE.NLM NetWare 386 Remote Console Version 1.31 February  
13, 1991 Copyright 1991 Novell, Inc. All rights reserved.
```


MONITOR

Why Use MONITOR?

Use MONITOR to lock the file server console and to see how efficiently your network is operating. Use MONITOR to view information about the following:

- ◆ Utilization and overall activity
- ◆ Cache memory status
- ◆ Connections and their status
- ◆ Disk drives
- ◆ Mounted volumes
- ◆ LAN drivers
- ◆ Loaded modules
- ◆ File lock status
- ◆ Memory usage

Command Format

```
LOAD [path]MONITOR [parameter]
```

Command Parameters

Replace *path* with a full path. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: has been mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

ns

Replace *parameter* with *ns* (no saver) to turn off the screen saver option.

NOTE: If MONITOR is not loaded with the *ns* parameter, a utilization snake appears on the screen after 1 minute of inactivity if the console is locked (after 10 minutes if it is not locked). As network usage increases, the snake moves faster and the tail (moving randomly around the screen) gets longer. To retrieve the MONITOR display, press any key.

nh

Replace *parameter* with *nh* (no help) if you do not want to load the HELP function (and use the additional memory).

-p

Replace parameter with *-p* (processor utilization) if you want the Processor Utilization option to appear on the “Available Options” menu.

Load MONITOR

To load MONITOR, type

LOAD MONITOR <Enter>

If MONITOR is already loaded, the following message appears:

This module is already loaded and cannot be loaded more than once.

If this message appears, complete one of the following:

- ◆ Press <Alt><Esc> to move through the activated screens until the MONITOR screen appears.
- ◆ Press <Ctrl><Esc> and select “Monitor Screen” from the list of available screens.

Interpret the Main MONITOR Screen

The main MONITOR screen displays the status of the network. It also displays an “Available Options” menu that you can use to access detailed information. When MONITOR is loaded, a screen similar to the following appears:

Figure 21 MONITOR main screen

Information For Server PRUFROCK			
File Server Up Time:	0 Days 21 Hours 16 Minutes 55 Seconds		
Utilization:	1	Packet Receive Buffers:	60
Original Cache Buffers:	8,680	Directory Cache Buffers:	209
Total Cache Buffers:	4,420	Service Processes:	4
Dirty Cache Buffers:	0	Connections In Use:	53
Current Disk Requests:	0	Open Files:	128

Available Options
Connection Information
Disk Information
LAN Information
System Module Information
Lock File Server Console
File Open / Lock Activity
Resource Utilization
Exit

Each item on the screen is described in the following paragraphs:

Operating System Version and Date. The version and release date of the operating system (upper-left corner of the screen).

Information For Server. The name of the file server.

File Server Up Time. The length of time the file server has been running since it was last booted.

Utilization. The percentage of time the processor is busy.

Original Cache Buffers. The number of cache buffers available when the file server is first booted. The figure represents the number of blocks installed as memory in your file server. The default block size is 4 KB.

Total Cache Buffers. The number of blocks currently available for file caching. This number decreases as modules are loaded into memory.

Dirty Cache Buffers. The number of file blocks in memory that are waiting to be written to disk.

Current Disk Requests. The number of disk requests (in a queue) that the server is waiting to service.

Packet Receive Buffers. The number of buffers available to handle station requests. Default: 10.

Directory Cache Buffers. The number of buffers allocated to handle directory caching.

Service Processes. The number of “task handlers” allocated for station requests. When the number of station requests exceeds a certain limit, the file server employs extra task handlers to execute the requests. Once memory is allocated for a service process, it remains allocated. The only way to remove this memory allocation is to down the file server.

Connections In Use. The number of stations currently attached to the file server.

Open Files. The number of files being accessed by the file server and by network stations.

Use “Available Options” Menu

The tasks that can be accomplished with each menu option in the “Available Options” menu on the main screen are listed on the following pages.

Connection Information

Task	Page
List active connections	“List Active Connections” on page 183
List physical record locks for a user	“List Physical Record Locks for a User” on page 185
Clear a connection	“Clear a Connection” on page 186
List open files	“List Open Files” on page 186

Disk Information

Task	Page
List system hard disks	“List System Hard Disks” on page 187
List volume segments per hard disk	“List Volume Segments Per Hard Disk” on page 188
Change the “Read After Write Verify” status of the hard disk	“Change the “Read After Write Verify” Status of the Hard Disk” on page 190
Flash the hard disk light	“Flash the Hard Disk Light” on page 191
Activate/deactivate a hard disk	“Activate/Deactivate a Hard Disk” on page 192
Mount/dismount a removable media device	“Mount/Dismount a Removable Media Device” on page 193
Lock/unlock a removable media device	“Lock/Unlock a Removable Media Device” on page 195

LAN Information

Task	Page
List LAN drivers and statistics	“List LAN Drivers and Statistics” on page 196

System Module Information

Task	Page
List system modules	“List System Modules” on page 198
List resources used by system modules	“List Resources Used by System Modules” on page 199

Lock File Server Console

Task	Page
Lock the file server console	“Lock the File Server Console” on page 200
Unlock the file server console	“Unlock the File Server Console” on page 201

File Open/ Lock Activity

Task	Page
Check the status of a file	“Check the Status of a File” on page 201
View mounted volumes	“View Mounted Volumes” on page 202

Resource Utilization

Task	Page
View memory statistics	“View Memory Statistics” on page 203
View tracked resources	“View Tracked Resources” on page 205

Processor Utilization

Task	Page
Check server processor utilization	“Checking a Server’s Processor Utilization” on page 207

NOTE: The “Processor Utilization” option appears on the “Available Options” menu only if you use the -P parameter when you load MONITOR.

Exit

Task	Page
Exit MONITOR	“Exit MONITOR” on page 208

List Active Connections

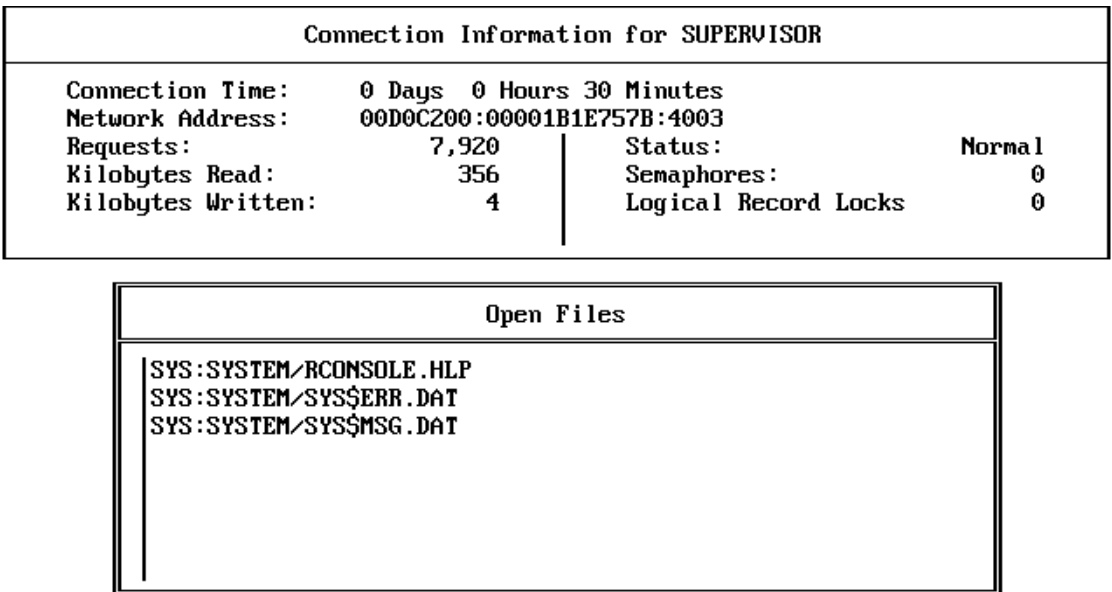
Use this option to view information about individual connections.

Procedure

- 1 Select “Connection Information” from the “Available Options” menu.
- 2 Select a username to see information about the user’s connection.

A display similar to the following appears. The top of the display gives statistics on the user; the bottom half shows the open files. In the following displays, user SUPERVISOR has SYSCON open.

Figure 22 MONITOR “Connection Information” screen



Each item in the display is described in the following paragraphs:

Connection time. Shows how long the user has been logged in to the network. Accounts can be billed for connection time.

Network address. Displays the network address (cabling network number), the station (node) address, and the socket address. The socket address is used mainly with OS/2 workstations. Network OS/2 workstations can have several socket addresses (or logical connections to the file server), enabling the workstation to perform multiple operations simultaneously.

Requests. Displays the number of requests the connection has made to the file server since the server was last booted. Accounts can be billed by the number of requests made.

Kilobytes read. Displays the number of kilobytes the connection has accessed for reading. Accounts can be billed for the number of kilobytes read.

Kilobytes written. Displays the number of kilobytes the connection has used in writing data to disk. Accounts can be billed for the number of kilobytes written.

Status. Displays one of the following messages:

<i>Normal</i>	Logged in and functioning.
<i>Waiting</i>	Waiting for a file to be unlocked so that the station can get the file and lock it.
<i>Not-logged-in</i>	Attached to the file server, but not logged in.

Semaphores. Displays the number of semaphores a connection has open. A semaphore can arbitrate the following:

- ◆ How many tasks can use a resource (bus, hard disk, network) at the same time
- ◆ How many workstations can run a program at the same time

Logical record locks. Displays the number of logical record locks a connection has. A logical record lock flags a file or application so that only one station at a time can use it.

Open files. Lists the files that are currently being accessed by the workstation.

List Physical Record Locks for a User

While accessing a database, a workstation can have records locked for its use. Other workstations cannot access these locked records. Follow these steps to see which records are locked.

Procedure

- 1 Select “Connection Information” from the “Available Options” menu.
- 2 Select the user whose information you want to see.
- 3 Select an open file to see the current record locks, if any.

A “Record Lock” screen similar to the following appears:

Figure 23 MONITOR “Record Lock Status” screen

Start	End	Record Lock Status

Each item in the screen is described below:

Start. The lock begins at this offset in the file.

End. The lock ends at this offset in the file.

Record lock. Displays one of the following messages:

<i>Locked Exclusive</i>	Locked so that no one else can read or write to the record.
<i>Locked Shareable</i>	Locked so that other stations can read, but not write to, the record.
<i>Locked</i>	Logged for future locking. The type of lock is specified when the lock is completed.
<i>TTS Holding Lock</i>	Unlocked by the application; however, file transactions are not completed, so TTS has locked it. TTS can restore original data to the record if it needs to back out the transaction.

Status. Displays one of the following messages:

Logged

A set of records is being prepared for locking. The file server logs each file before locking the set to avoid deadlock or “deadly embrace.”

Not Logged

This is the normal condition. There are no pending requests for a set of locks.

Clear a Connection

When a workstation hangs, its files are left open. Before rebooting the workstation, use MONITOR to close the files safely and clear the connection.

Procedure

- 1** Select “Connection Information” from the “Available Options” menu.
- 2** Select the user whose workstation is not functioning and press <Delete>. Use the Mark key (<F5> on most computers) to select more than one user.
- 3** Answer “Yes” to the prompt to clear the connection.

List Open Files

Determine the extent of a user’s activity on the file server by viewing such statistics as the number of requests to read from or write to a file and the number of files that the user currently has open.

Procedure

- 1** Select “Connection Information” from the “Available Options” menu.
- 2** Select the user whose activity you want to check. The user’s statistics and opened files are displayed on the screen.

NOTE: Although executable files can be displayed in the window, they are not usually listed because once the files have been read into memory, they are closed.

List System Hard Disks

To check the number and type of hard disks attached to the file server, complete the following steps.

Procedure

- 1 Select “Disk Information” from the “Available Options” menu.
- 2 Select one of the hard disks you need information about.

For an explanation of the numbers and codes, see “Device Numbering” in *Concepts*.

A screen similar to the following appears:

Figure 24 MONITOR hard disk information screen

MAXTOR	XT-8760S	AP9	Card	0	Controller	1	Drive	0	
Driver:	AHA1740.DSK							Partition Blocks:	162,812
Disk Size:	637 Meg							Data Blocks:	160,001
Partitions:	1							Redirection Blocks:	2,811
Mirror Status:	Not Mirrored							Redirected Blocks:	217
Hot Fix Status:	Normal							Reserved Blocks:	32

Drive Status
Volume Segments On Drive: (select for list)
Read After Write Verify: Disabled
Drive Light Status: Not Supported
Drive Operating Status: Active

Each item on the screen is described below. A description of the tasks that can be performed from the “Drive Status” form start under [“List Volume Segments Per Hard Disk” on page 188](#) (“List Volume Segments Per Hard Disk”).

Driver. The name of the disk driver that operates the hard disk.

Disk size. The size (in megabytes) of all partitions on the hard disk.

Partitions. The number of partitions defined on the hard disk.

Mirror Status. Status options are explained below:

<i>Mirrored</i>	Data is stored on more than one hard disk.
<i>Not mirrored</i>	Data is stored on one disk.
<i>Remirroring</i>	Data is being copied to a duplicate hard disk so that both disks have the same (mirrored) data.

Hot Fix Status. Hot Fix options are explained below:

Normal	Hot Fix is functioning.
Not-hot-fixed	Hot Fix has failed. Remove the hard disk from the file server.

Partition Blocks. The total space on the partition shown in blocks. (Default block size is 4 KB.)

Data Blocks. The space (shown in blocks) on the hard disk available to hold data.

Redirection Blocks. The number of blocks currently allocated for the Hot Fix Redirection Area.

Redirected Blocks. The number of bad blocks found by Hot Fix.

Reserved Blocks. Blocks reserved for Hot Fix tables.

IMPORTANT: When the number of Reserved Blocks plus the number of Redirected Blocks equals the number of Redirection Blocks, Hot Fix has failed on the hard disk.

List Volume Segments Per Hard Disk

If you discover errors on a particular hard disk, you can determine which volumes have segments, or parts, on the hard disk.

Procedure

- 1 Select “Disk Information” from the “Available Options” menu.
- 2 Select one of the hard disks.

For an explanation of the device codes, see “Device numbering” in *Concepts*.

A “Drive Status” form similar to the following appears:

Figure 25 “Drive Status” form

Drive Status	
Volume Segments On Drive:	(select for list)
Read After Write Verify:	Hardware Level
Drive Light Status:	Not Supported
Drive Operating Status:	Active
Removable Drive Mount Status:	
Removable Drive Lock Status:	

- 3 If the “Drive Operating Status” field lists “Inactive,” the “Volume Segments On Drive” field will be blank.
See [“Activate/Deactivate a Hard Disk” on page 192](#) and activate the disk. Then continue with Step 4.
- 4 Select the “Volume Segments on Drive” field in the “Drive Status” menu.

A window similar to the following appears. This window lists the volumes that are on the hard disk.

Figure 26 “Volume Segments” list

Volume Segments
117 Meg on Volume DOC segment 5
156 Meg on Volume DOC segment 8
19 Meg on Volume SYS segment 1
331 Meg on Volume DOC segment 6

Change the “Read After Write Verify” Status of the Hard Disk

Each driver has a default setting for verifying that the data written to disk matches the data still in memory. To change the default setting for a selected hard disk, complete the following steps.

Procedure

1 Select “Disk Information” from the “Available Options” menu.

2 Select one of the hard disks.

For an explanation of the device codes, see “Device numbering” in *Concepts*.

A “Drive Status” form appears.

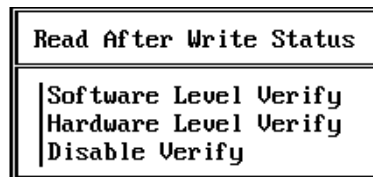
3 Complete one of the following:

- ◆ If the driver for the hard disk you selected supports the “Read After Write Verify” option, the field displays a status message (“Software Level,” “Hardware Level,” or “Disabled”). Continue with Step 4.
- ◆ If the driver displays “Not Supported,” you cannot change the default setting. Press <Esc> and select another hard disk.

4 Select the “Read After Write Verify” field.

The following menu appears:

Figure 27 “Read After Write Status menu



Each option is described here. Not all options are available for all drivers. The driver determines which options are supported.

Software Level Verify. Selects the driver to perform the read-after-write verification. Displays a “Software Level” status in the “Read After Write Verify” field in the “Drive Status” form.

Hardware Level Verify. Selects the controller to perform the read-after-write verification. Displays a “Hardware Level” status in the “Read After Write Verify” field in the “Drive Status” form.

Disable Verify. Disables both the driver and the controller from performing a read-after-write verification. Select this option if your hard disk performs a read-after-write verification internally. (Check the hard disk’s specifications.) The option displays a “Disabled” status in the “Read After Write Verify” field in the “Drive Status” form.

- 5** Select the option you want.

The “Drive Status” form reappears. If the option you selected is not displayed in the “Read After Write Verify” field, that option is not supported by the driver.

Flash the Hard Disk Light

Use the “Drive Light Status” option to physically identify which hard disk corresponds to the drive listed in the “System Disk Drives” window. This option can be set so that the disk light flashes at a timed interval.

Procedure

- 1** Select “Disk Information” from the “Available Options” menu.
- 2** Select a hard disk from the “System Disk Drives” window.

For an explanation of the device codes, see “Device numbering” in *Concepts*.

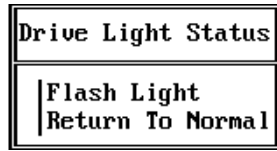
A “Drive Status” form appears.

- 3** Complete one of the following:
 - ◆ If the driver for the hard disk you selected supports the “Drive Light Status” option, the field displays a status message (“Normal” or “Flashing”). Continue with Step 4.
 - ◆ If the driver displays “Not Supported,” you cannot change the default setting. Press <Esc> and select another hard disk.

- 4 Select the “Drive Light Status” field.

The following menu appears:

Figure 28 “Drive Light Status” field



Each option is described below.

Flash Light. Flashes the hard disk light at a regular interval so that you can identify the disk. Displays a “Flashing” status in the “Drive Light Status” field in the “Drive Status” form.

Return To Normal. Returns control of the light to the hard disk. Displays a “Normal” status in the “Drive Light Status” field in the “Drive Status” form.

- 5 Select the option you want.

The “Drive Status” form reappears.

Activate/Deactivate a Hard Disk

Use the “Drive Operating Status” option to manually activate or deactivate a hard disk.

Procedure

- 1 Select “Disk Information” from the “Available Options” menu.
- 2 Select a hard disk from the “System Disk Drives” window.

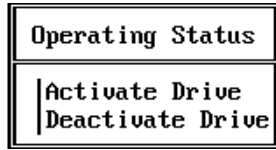
For an explanation of the device codes, see “Device numbering” in *Concepts*.

A “Drive Status” form similar to the following appears:

- 3 Select the “Drive Operating Status” field.

The following menu appears:

Figure 29 “Operating Status” menu



Each option is described below.

Activate Drive. Controls whether the “Drive Status” window displays information about the hard disk (such as Hot Fix and mirror status information). Displays an “Active” status in the “Drive Operating Status” field in the “Drive Status” form.

Deactivate Drive. Removes all NetWare information from the drive status window except for the disk size and the driver the hard disk was using. Displays an “Inactive” status in the “Drive Operating Status” field in the “Drive Status” form.

- 4 Select the option you want.

The “Drive Status” form reappears.

Mount/Dismount a Removable Media Device

Use the “Removable Drive Mount Status” option to manually mount or dismount a removable media device.

Procedure

- 1 Select “Disk Information” from the “Available Options” menu.
- 2 Select a removable media device from the “System Disk Drives” window.
A “Drive Status” form appears.

3 Complete one of the following:

- ♦ If the driver for the hard disk you selected supports the “Removable Drive Mount Status” option, the field displays a status message (“Mounted” or “Dismounted”). Continue with Step 4.
- ♦ If the driver displays nothing in the “Removable Drive Mount Status” field, the device you selected is not a removable media device. Press <Esc> and select another device.

4 Select the “Removable Drive Mount Status” field.

The following menu appears:

Figure 30 “Drive Mount Status” menu

Drive Mount Status	
	Mount Drive
	Dismount Drive

Each option is described here.

Mount Drive. Mounts the media so that information can be accessed from it. Displays a “Mounted” status in the “Removable Drive Mount Status” field in the “Drive Status” form.

Dismount Drive. Dismounts the media so that information cannot be accessed from it. Displays a “Dismounted” status in the “Removable Drive Mount Status” field in the “Drive Status” form.

5 Select the option you want.

The “Drive Status” form reappears.

Lock/Unlock a Removable Media Device

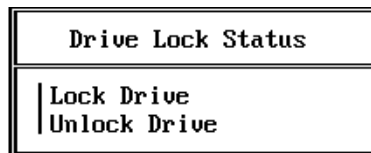
Use the “Removable Drive Lock Status” option to lock or unlock a removable media device. Locking the device prevents the media from being physically removed.

Procedure

- 1 Select “Disk Information” from the “Available Options” menu.
- 2 Select a removable media device from the “System Disk Drives” window.
A “Drive Status” form appears.
- 3 Complete one of the following:
 - ◆ If the driver for the hard disk you selected supports the “Removable Drive Lock Status” option, the field displays a status message (“Locked” or “Unlocked”). Continue with **“Select the “Removable Drive Lock Status” field.” on page 195.**
 - ◆ If the driver displays nothing in the “Removable Drive Lock Status” field, the device you selected is not a removable media device. Press <Esc> and select another device.
- 4 Select the “Removable Drive Lock Status” field.

The following menu appears:

Figure 31 “Drive Lock Status” menu



Drive Lock Status	
	Lock Drive
	Unlock Drive

Each option is described below.

Lock Drive. Locks the media so that the media cannot be removed from the device. Displays a “Locked” status in the “Removable Drive Lock Status” field in the “Drive Status” form.

Unlock Drive. Unlocks the media so that it can be removed from the device. Displays an “Unlocked” status in the “Removable Drive Lock Status” field in the “Drive Status” form.

- 5 Select the option you want.

The “Drive Status” form reappears.

List LAN Drivers and Statistics

By comparing information about the LAN drivers installed on the file server, you can tell which cabling system is handling the most traffic. If errors occur frequently on a high-traffic system, you may want to switch some of the workstations on the busy system to a new cabling system or to a less busy cabling system.

Procedure

- 1 Select “LAN Information” from the “Available Options” menu.
- 2 Select a LAN driver.

A screen similar to the following appears:

Figure 32 Sample LAN driver statistics screen

NE3200 [slot=8 frame=ETHERNET_802.3]	
Version 3.18	
Node Address: 00001B140BF5	
Protocols:	
IPX	
Network Address: 00D0C200	
Generic Statistics:	
▼ Total Packets Sent:	2,546,427

- 3 Use the Up- and Down-arrow keys or the PageUp and PageDown keys to view all available information.

The version, address, and protocol information is similar to the information you can view with CONFIG.

The generic statistics common to most of the current drivers are listed on the following pages.

NOTE: Custom statistics vary, depending on the LAN driver installed. For detailed definitions of the statistics listed by the LAN drivers that Novell currently supports, see [Appendix A, “Custom LAN Driver Statistics Shown in MONITOR,” on page 423](#). For statistical information about third-party drivers, check the documentation that comes with the driver.

Driver name. The driver name and parameters that correspond to the hardware settings on the network board.

Version. The current version of the driver.

Node address. The station or node address of the network board in the file server.

Protocols. The communication protocols bound to the driver with BIND.

Network address. The network number assigned to the cabling system the LAN driver is operating on. This address appears only if the IPX protocol has been bound to the board.

Total packets sent. The number of packets sent from the file server through this LAN driver. By comparing this figure with the figures for other LAN drivers, you can see which driver is handling the most traffic.

Total packets received. The number of packets received by the file server since it was last booted (includes file service requests, packets routed to another network, and packets sent to other IPX sockets in the file server).

No ECB available count. A counter that increments when a device sends a packet to your file server, but a packet receive buffer is not available. The file server allocates more packet receive buffers after each incident until the file server reaches its maximum limit (configurable with a SET parameter).

If you are using an EISA or microchannel bus master board (such as the NE3200 board), you probably need to increase both the minimum and maximum number of packet receive buffers. See the following SET parameters: [“Minimum Packet Receive Buffers = number” on page 264](#) and [“Maximum Packet Receive Buffers = number” on page 263](#).

Send packet too big count. A counter that increments when your file server tries to transmit a packet that is too large for your file server’s hardware to handle.

Send packet too small count. A counter that increments when a device transmits a packet that is too small for your file server’s hardware to handle.

Receive packet overflow count. A counter that increments when your file server receives a packet that is too big to store in a cache buffer. This should happen rarely, unless you are running a software program that does not negotiate packet size. Contact the vendor for an updated version of the software.

Receive packet too big count. A counter that increments when the file server receives a packet that is too big.

Receive packet too small count. A counter that increments when the file server receives a packet that is too small.

Send packet miscellaneous errors. A counter that increments when errors occur with send packets.

Receive packet miscellaneous errors. A counter that increments when errors occur with receive packets.

Send packet retry count. A counter that increments when the file server tries to send a packet but is unsuccessful because of a hardware error. Based on the number of retries in the retry counter, the file server will continue to try to send the packet until it is successfully sent or the retry setting is reached. If you are receiving a large number of these errors, use *LOAD LAN driver* to increase the maximum retry count, or check the cabling and workstation hardware.

Checksum errors. A counter that increments when the checksum byte at the end of the packet does not match the sum of the bytes contained in the packet. This indicates a data error.

Hardware receive mismatch count. A counter that increments when the packet length received by the hardware and the packet length specified by the packet do not match.

List System Modules

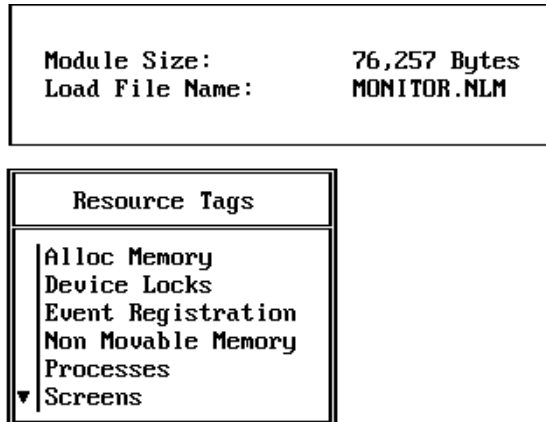
Loaded modules use memory and other types of file server resources. To see the amount of memory and the types of resources each module uses, complete the following steps.

Procedure

- 1** Select “System Module Information” from the “Available Options” menu.
- 2** Select a module.

A screen similar to the following appears:

Figure 33 System module information screen



The first screen indicates the size of the module and the name the loadable module was loaded with.

NOTE: The NetWare operating system is not a loadable module, even though it will be listed as a module in this screen. As a result, MONITOR does not track the size of its code and data.

The “Resource Tags” menu is described in the following section, “List Resources Used by System Modules.”

List Resources Used by System Modules

Procedure

- 1** Select “System Module Information” from the “Available Options” menu.

- 2** Select a module.

A system module information screen appears.

The “Resource Tags” menu lists all the resource tags defined by the module. Each tag allows the module to allocate resources from the file server.

- 3** To view how much of a resource a resource tag uses, select a tag from the menu.

A screen similar to the following appears:

Figure 34 “Resource Information” screen

Resource Information	
Tag:	Non Movable Memory
Module:	NetWare 386 Console Monitor
Resource:	Cache Non-Movable Memory (Bytes)
In Use:	42,200

Each item on the screen is described below.

Tag. The name of the resource tag that the loadable module gave to a resource.

Module. The name of the module using the tag. The NetWare operating system can be used as a module name.

Resource. The type of resource the tag is using. For a definition of each type of resource, see [Appendix B, “Tracked Resources Displayed in MONITOR,” on page 445](#).

In Use. The amount of memory, in bytes, currently used or the number of resources being used. For example, the Cache Movable Memory resource displays the total number of bytes; the Screens resource displays the total number of activated screens.

Lock the File Server Console

You can lock the file server console so that only those who know either the keyboard password or the SUPERVISOR password can unlock the keyboard and use commands and equipment associated with the file server.

To lock the console, complete the following steps.

Procedure

- 1 Select “Lock File Server Console” from the “Available Options” menu.
- 2 Type in a password to lock the keyboard.

Use either the SUPERVISOR’s password or another password of your choice.

Unlock the File Server Console

Procedure

- 1 If the console monitor is creating patterns, press any key to restore the main MONITOR display.
- 2 Type either the SUPERVISOR password or the keyboard password and press <Enter>.

Check the Status of a File

Use MONITOR to display how often a file is being used, how many connections are using a file, how a file is used, or whether a file is locked.

Procedure

- 1 Select “File Open / Lock Activity” from the “Available Options” menu.
- 2 Select the path (volume, directory, subdirectory, file), one level at a time, from the “Select an Entry” window.

When you have selected a file, screens similar to the following appear:

Figure 35 File Lock/Activity screen

LOGIN.EXE	<File>	Conn	Task	Lock	Status
Use Count:		0			
Open Count:		0			
Open For Read:		0			
Open For Write:		0			
Deny Read:		0			
Deny Write:		0			
Status:	Not Locked				

Each item in the display is described below.

Use count. The number of connections that have the file open, logged, or locked.

Open count. The number of connections that currently have the file open.

Open for read. The number of connections that currently have the file open for reading.

Open for write. The number of connections that currently have the file open for writing.

Deny read. The number of connections that have opened the file and will not allow other stations access.

Deny write. The number of connections that have opened the file and will not allow other stations to write to the file.

Status. Displays one of the following messages:

<i>Locked</i>	Other users cannot access the file.
---------------	-------------------------------------

<i>Not Locked</i>	Other users can access the file.
-------------------	----------------------------------

Conn. A list of the connections using the file.

Task. A number assigned by the shell to an application program.

Lock Status. Displays one of the following messages:

<i>Exclusive</i>	No one else can read or write to the record.
------------------	--

<i>Shareable</i>	Others may read, but not write to, the record.
------------------	--

<i>TTS Holding Lock</i>	The file was unlocked by the application; however, the transactions are not completed, so TTS has locked it. TTS can restore original data to the record if it needs to back out the transaction.
-------------------------	---

<i>Not Logged</i>	This is the normal condition. No requests for a set of locks are pending.
-------------------	---

View Mounted Volumes

You can use MONITOR to determine which volumes are currently mounted on your file server.

Select “File Open / Lock Activity” from the “Available Options” menu.

The “Select An Entry” screen lists all currently mounted volumes.

View Memory Statistics

Memory usage statistics can help you determine how the memory in your file server is being used and when to add more memory.

Select “Resource Utilization” from the “Available Options” menu.

A screen similar to the following appears:

Figure 36 “Server Memory Statistics” screen

Server Memory Statistics			
Permanent Memory Pool:	2,727,480 Bytes	7%	2,716,784 In Use
Alloc Memory Pool:	1,606,804 Bytes	4%	940,416 In Use
Cache Buffers:	18,458,280 Bytes	50%	
Cache Movable Memory:	11,989,020 Bytes	33%	
Cache Non-Movable Memory:	1,945,420 Bytes	5%	
Total Server Work Memory:	36,727,004 Bytes		

The “byte” column indicates how many bytes of memory are reserved for a particular memory pool or buffer.

The “percentage” column indicates the amount of available memory being used for a particular memory pool or buffer.

The “in use” column indicates how many of the available bytes are being used by a particular memory pool. If you run VREPAIR and the “In Use” statistics are considerably lower than the total amount in the memory pools, down the file server to return the Alloc and Permanent pools to their original amounts.

The types of memory pools and buffers are described below. For a complete description, see “Memory Pools” in *Concepts*.

Permanent Memory pool. This statistic contains both permanent and semi-permanent memory. Both pools are used for long-term memory needs such as directory cache buffers and packet receive buffers.

Once this memory is allocated as either permanent or semi-permanent memory, the memory is not returned to the regular cache buffers unless the file server is rebooted.

Alloc Memory pool. *Alloc Memory pool* is a shorter name for the Alloc Short Term Memory pool. This pool allocates memory to loadable modules for temporary or short-term use. For example, modules with pop-up windows use Alloc Memory to store previous menu information on screen.

The operating system also uses this pool for the following types of information: mappings, user connection information, and server advertising.

Once memory is allocated to this pool, it is not returned to the regular cache buffers. When the module is unloaded, the allocated memory returns to the pool for other loadable modules.

The “Maximum Alloc Short Term Memory” parameter in SET controls the size of the Alloc Short Term Memory pool. If the amount of memory allocated to this pool reaches the default of 8,000,000 bytes, increase the SET parameter by 1,000,000.

Cache Buffers. This memory pool lists the total amount of memory available for data caching. The amount is listed in bytes. When this figure reaches 20%, you need to add more memory to your file server.

You can do any of the following to temporarily increase the number of cache buffers.

- ◆ Unload loadable modules, such as INSTALL, DISKSET, or MONITOR, that are not currently needed.
- ◆ Down the file server and reboot it to recover unused blocks in the permanent and allocated memory pools.
- ◆ Use REMOVE DOS to free the file server memory being used by DOS.

Cache Movable Memory. This pool lists memory buffers that are “rotating free blocks” in a certain range of memory. The operating system can move the location of these memory blocks at any time to facilitate memory management. Hash tables are a good example of data that uses this kind of a buffer. Once a program is no longer using these buffers, it returns the buffers to the cache buffer pool.

Cache Non-Movable Memory. This pool lists memory buffers that are allocated to a program temporarily. Once the program no longer needs these buffers, it returns the buffers to the cache buffer pool.

Total Server Work Memory. This statistic displays the total number of bytes available for the server to use. This total equals the amount of installed memory minus the memory needed for SERVER.EXE, DOS, and ROM BIOS.

View Tracked Resources

Names are given to various operating system resources so that the resources can be tracked. The operating system allocates these resources to loadable modules when they are loaded, and then tracks the resources to make sure that all the resources are returned when the module is unloaded. By looking at each resource, you can see which modules are using that particular resource. For a definition of each tracked resource, see [Appendix B, “Tracked Resources Displayed in MONITOR,” on page 445.](#)

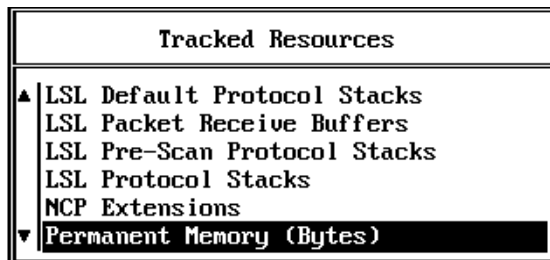
To view tracked resources, complete the following steps.

Procedure

- 1 Select “Resource Utilization” from the “Available Options” menu.

A list similar to the following appears:

Figure 37 “Tracked Resources” list

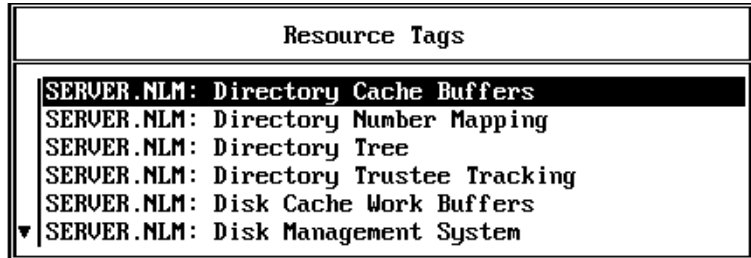


- 2 Use the Up- and Down-arrow keys or the PageUp and PageDown keys to scroll through the list.

- 3 Select the resource you want information about.

A list similar to the following appears:

Figure 38 “Resource Tags” lists

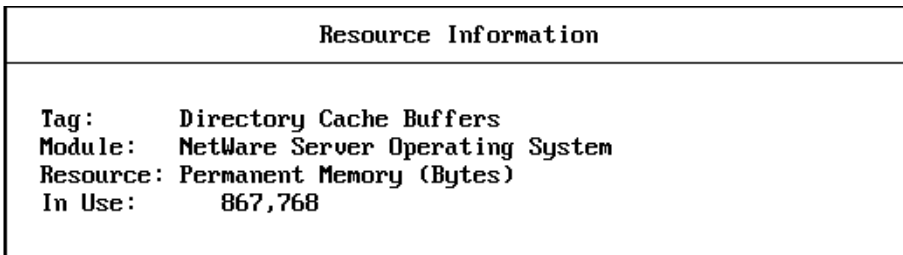


The module that assigned the resource tag is listed first, followed by the resource tag name.

- 4 From the “Resource Tag” list, select the module that you want more resource information about.

A screen similar to the following appears:

Figure 39 “Resource Information” screen



Each item on the screen is described below.

Tag. The name of the resource tag. If the module needs to allocate a resource for more than one function, it can assign a different resource tag to each function. For example, the “Resource Tags” screen in Step 3 shows SERVER.NLM with six different resource tags for the same resource (Alloc Short Term Memory).

Module. The name of the module using the tag. The NetWare operating system can be used as a module name.

Resource. The type of resource the tag is using. For a definition of each type of resource, see [Appendix B, “Tracked Resources Displayed in MONITOR,” on page 445](#).

In Use. The amount of memory, in bytes, currently used by the loadable module, or the number of resources being used. For example, the Cache Movable Memory resource displays the total number of bytes; the Screens resource displays the total number of activated screens.

Checking a Server’s Processor Utilization

One possible cause of network problems is the monopolizing of the Central Processing Unit (CPU) by a single process. This procedure helps you know which processes are using the CPU and how much load they are putting on the CPU’s time.

Procedure

- 1 Select “Processor Utilization” from the “Available Options” menu.

NOTE: The “Processor Utilization” option appears on the “Available Options” menu only if you used the -P parameter when you loaded MONITOR as in the example below:

```
LOAD MONITOR -P <Enter>
```

- 2 Press <F3> to view a list of the currently loaded processes and interrupts.

For each item on the list, notice the percentage given in the “Load” column. This percentage shows which processes are taking the most CPU time.

- 3 To balance processor utilization, unload noncritical NLMs that are taking a large percentage of CPU time.

Exit MONITOR

You can exit MONITOR by pressing <Esc> until the exit prompt appears or by pressing the hot key to exit temporarily.

Using the Escape Key

Use <Esc> to unload the MONITOR module and free up memory.

Procedure

- 1** Press <Esc> until “Exit” appears on the “Available Options” menu.
- 2** Answer “Yes” to the “Exit Monitor?” prompt.

Using the Hot Key

You can temporarily exit MONITOR by pressing <Alt><Esc>. This also works for any other loadable module with menus.

Even though the module no longer appears on the screen, it is still loaded. You can press <Alt><Esc> to return to MONITOR at any time.

MOUNT

Why Use MOUNT?

Use MOUNT to make a volume available to your users. You can mount and dismount one or all volumes while the file server is running.

Command Format

```
MOUNT volume_name
```

or

```
MOUNT ALL
```

Mount a New Volume or One that Is Not Used Often

Use MOUNT to make a newly created volume available to your users or to mount a volume that is not used very often. You may want to leave rarely used volumes dismounted since each mounted volume takes up memory and reduces the memory available for file caching.

To mount a volume, type

```
MOUNT volume_name <Enter>
```

If you try to mount a volume before creating it with INSTALL or if the file server has a problem locating all the segments in a given volume, the following message appears:

```
Volume volume_name could NOT be mounted. Some or all volume  
segments cannot be located.
```

If you try to mount a volume that is already mounted, the following message appears:

```
Volume volume_name is already mounted.
```

Mount Several Volumes

To mount several volumes at once, type

```
MOUNT ALL <Enter>
```

NAME

Why Use NAME?

Use NAME to display the name of the file server.

Command Format

NAME

Display the Name of the File Server

To view the name of the file server, type

NAME <Enter>

When you enter this command, the console displays the name of the file server in the following format:

This is Server *server_name*

NLICLEAR (Not-Logged-In CLEAR)

Why Use NLICLEAR?

NLICLEAR is an NLM that is copied from the *SYSTEM-3* diskette. NLICLEAR deletes or “clears” unauthenticated user connections. Unauthenticated connections cannot be reused until they are cleared. NLICLEAR allows you to reuse idle connections by periodically deleting them.

Command Format

```
LOAD [path]NLICLEAR [parameter...]
```

Command Parameters

Replace path with a full path to the directory containing the NLICLEAR module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path, the operating system looks for NLICLEAR in SYS:SYSTEM. (Use SEARCH to set up additional paths for automatic searching.)

Replace parameter with one or more of the following parameters.

NOTIFY

Causes a message to be written to the server console screen each time a connection is cleared.

Default: No notification

POLL=*number*

Sets the time (in seconds) for NLICLEAR to wait between checks of the user connection table. The number of seconds can be from 15 to 3600.

Default: 60 seconds

CONN=*number*

Sets the uppermost number of connections to check. Connections are assigned from 1 to the number of licensed connections. For example, on a 250-user version of NetWare v3.12, CONN=50 would only check the last 50 connections (201-250). Connections 1-200 would not be checked or cleared by NLICLEAR. NLICLEAR does not load on a one-user server if you use this parameter.

Default: Number of licensed user connections

Additional Information

Unauthenticated user connections occur when

- ♦ A user specifies a login name after a LOGIN or ATTACH command, but does not enter a password to complete the login procedure.
- ♦ A user logs out without logging in elsewhere.
- ♦ The shell establishes a connection with the file server, but no login is attempted.

In these cases, the connection is made to the server, but no authentication is granted to the user except to complete the login or to log in elsewhere.

NMAGENT

Why Use NMAGENT?

Use NMAGENT to allow LAN drivers to register and pass network management parameters. NMAGENT must be loaded before LAN drivers can be loaded. If you do not load NMAGENT before loading a LAN driver, the operating system will try to autoloading NMAGENT for you.

Command Format

```
LOAD [path]NMAGENT
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

NMAGENT registers three resources for tracking: NetWork Management Triggers, Network Management Managers, and Network Management Objects. You can view these tracked resources with MONITOR.

Load NMAGENT

To load NMAGENT, type

```
LOAD NMAGENT <Enter>
```

NUT

Why Use NUT?

Use NUT (NLM Utility User Interface) if you have a NetWare v3.11 loadable module (such as v3.11 MONITOR) that requires NUT's library of routines and functions.

NOTE: Most loadable modules that use NUT will autoload NUT before they load. Use the MODULES console command to see if you already have NUT loaded.

Command Format

```
LOAD [path] NUT
```

Command Parameter

Replace *path* with the full path to the directory containing the NUT module.

NWSNUT

Why Use NWSNUT?

Use NWSNUT (NLM Utility User Interface) if you have a NetWare v4.0 loadable module that requires NWSNUT's library of routines and functions.

NOTE: Most loadable modules that use NWSNUT will autoload NWSNUT before they load. Use the MODULES console command to see if you already have NWSNUT loaded.

Command Format

```
LOAD [path]NWSNUT
```

Command Parameters

Replace *path* with the full path to the directory containing the NWSNUT module.

OFF

Why Use OFF?

Use OFF to clear information from the file server console screen.

Command Format

OFF

Clear the File Server Console Screen

To clear the console screen, type

OFF <Enter>

You can also use the CLS command to clear the file server console screen.

PROTOCOL

Why Use PROTOCOL?

Use PROTOCOL to view the protocols registered on your file server. Use PROTOCOL REGISTER to register additional protocols and frame types.

LAN drivers automatically register only IPX. Other protocol stacks automatically register themselves. Using PROTOCOL REGISTER is only necessary for unusual cases, such as using a new media.

Command Format

PROTOCOL

or

PROTOCOL REGISTER *protocol frame id#*

Command Parameters

Replace *protocol* with the protocol name. Only IPX is automatically registered with the operating system.

Consult your Novell Authorized Reseller for approved protocol loadable modules. Check the documentation that comes with the protocol module for the protocol name.

Replace *frame* with the name representing the frame type that is to be bound to the communication protocol. LAN drivers automatically register a frame type when they are loaded. If the LAN driver supports more than one frame type, the frame type is registered when you load the driver with that frame type.

Replace *id#* with the Protocol Identification number (PID), a unique, assigned hexadecimal number that tells the file server how to recognize data coming from a certain network board through a designated communication protocol (such as IPX). You may find this number called a protocol ID or (PID), an Ethernet type (or E-type), or an SAP, although it may be called something else entirely.

View the Kinds of Protocols and Frame Types on Your Network

At the console prompt, type

```
PROTOCOL <Enter>
```

Information similar to the following is displayed:

The following protocols are registered

```
Protocol: IPX Frame type: VIRTUAL_LAN Protocol ID: 0
```

LAN drivers automatically register additional frame types when you load them with a frame type other than the default. For example, when the NE2000 driver is loaded with an Ethernet_II frame type, information similar to the following appears:

The following protocols are registered:

```
Protocol: IPX Frame type: VIRTUAL_LAN Protocol ID: 0
```

```
Protocol: IPX Frame type: Ethernet_802.3 Protocol  
ID: 0
```

```
Protocol: IPX Frame type: Ethernet_II Protocol ID:  
8137
```

Add a New Protocol or Frame to Your Network

Because the protocol (IPX) and frame types listed in “[Command Parameters](#)” on page 217 are already registered with NetWare, use the following example as a guide for loading new protocols and frames.

To add a new protocol called XYZ to an Ethernet network that is using the NE2000 LAN driver, complete the following steps.

Procedure

- 1 Check the protocol documentation for the protocol name, frame name, and protocol ID number.

For this example, assume the protocol name is XYZ, the frame name is Ethernet_Snap, and the ID number is 8137.

- 2 Load the loadable module for the protocol by typing

```
LOAD XYZ <Enter>
```

3 Register the new protocol with NetWare by typing

```
PROTOCOL REGISTER XYZ ETHERNET_SNAP 8137 <Enter>
```

4 Bind the protocol to a loaded LAN driver by typing

```
BIND XYZ TO NE2000 <Enter>
```

NOTE: The LAN driver must support the specified frame type.

PSERVER

Why Use PSERVER?

Use PSERVER to load the print server on the fileserver and to establish print services for the network.

Command Format

```
LOAD PSERVER printserver
```

NOTE: Before you load the print server, you must use PCONSOLE to set up a print server and configuration files. For more information, see Print Server.

REGISTER MEMORY

Why Use REGISTER MEMORY?

Use REGISTER MEMORY if the operating system does not recognize installed memory above 16 MB. If you have an EISA computer, see “[Auto Register Memory above 16 Megabytes = value](#)” on page 268.

IMPORTANT: If you have installed more than 16 MB of file server memory, avoid memory address conflicts. A conflict will occur if you have installed more than 16 MB of memory and the disk adapter board uses 16- or 24-bit DMA or Bus-Master DMA.

If a memory conflict occurs, you can solve it by doing either of the following:

- ◆ Upgrade to full 32-bit bus adapters.
- ◆ Use drivers that have been modified and certified to compensate for these memory-addressing limitations.

Command Format

```
REGISTER MEMORY start length
```

Command Parameters

Replace *start* with the starting hexadecimal address where the memory beyond 16 MB begins. In most instances, the starting address will be 0x1000000 (which equals 16 MB).

Replace *length* with a hexadecimal length of the memory installed beyond 16 MB. This number must be on an even paragraph boundary (a number that is divisible by 10h).

Additional Information

If the additional memory is added successfully, the message “Memory successfully added” appears and the additional memory is visible in MONITOR. Use the MEMORY command to display the total amount of memory the file server is addressing.

If the memory is not added, see the “Important” on “[Command Parameters](#)” on [page 217](#) and check for the following errors:

- ◆ An incorrect hexadecimal value was specified for *start* or *length*.
- ◆ The *length* value exceeds the total installed memory. Use the setup or reference diskette that came with the computer to determine the total amount of installed memory.

The following chart lists start and length values for standard computers that begin addressing memory above 16 MB at 0x1000000:

Total Memory	start (hex)	Length (hex)
20 MB	1000000	400000
24 MB	1000000	800000
28 MB	1000000	C00000
32 MB	1000000	1000000
36 MB	1000000	1400000
40 MB	1000000	1800000

Register Memory Above 16 MB

To add 4 MB of memory above 16 MB, type

```
REGISTER MEMORY 1000000 400000 <Enter>
```

To have the memory registered automatically when the file server is booted, add the following line to the AUTOEXEC.NCF file:

```
REGISTER MEMORY 1000000 400000
```

Add this line just after the lines for the file server name and the IPX internal network number. For instructions on editing the AUTOEXEC.NCF file, see “[Edit the AUTOEXEC.NCF File](#)” on [page 98](#), or “SYSCON” in *Utilities Reference*.

REMIRROR PARTITION

Why Use REMIRROR PARTITION?

Use REMIRROR PARTITION to start remirroring of a logical partition.

Command Format

```
REMIRROR PARTITION number
```

Command Parameter

Replace *number* with the number of the logical partition you want to start remirroring for.

Start Remirroring a Logical Partition

To start remirroring a logical partition, type

```
REMIRROR PARTITION number <Enter>
```

NOTE: The server remirrors partitions automatically. Use REMIRROR PARTITION only if you have stopped remirroring or if something else has caused your server to cease remirroring.

For example, to start remirroring for logical partition 4, you would type

```
REMIRROR PARTITION 4 <Enter>
```

Additional Information

For information about stopping a partition remirror, see “**ABORT REMIRROR**” on page 30.

REMOTE

Why Use REMOTE?

Use REMOTE to access the file server console from a workstation. After you load REMOTE, you must also load RSPX for REMOTE to function fully.

Command Format

```
LOAD [path] REMOTE [password]
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *password* with the password that you want all remote administrators of the file server to use.

Additional Information

REMOTE requires a password. If you do not enter the password with the command, REMOTE will prompt you for a password.

The password can be the same as the SUPERVISOR's password or the console password (that you enter with MONITOR), or the password can be unique. Even if a unique password is entered, the SUPERVISOR's password can still be used with the RCONSOLE utility to access the file server.

Load REMOTE

To load REMOTE without a password on the command line, type

```
LOAD REMOTE <Enter>
```

You will then be prompted to enter a password.

To load REMOTE with the password SECRET, type

```
LOAD REMOTE SECRET <Enter>
```


Set Up Autoloading of Remote Console

To make sure that the modules necessary for remote console access are automatically loaded when the file server is booted, add the following commands to the AUTOEXEC.NCF file. For instructions on editing this file, see “[Edit the AUTOEXEC.NCF File](#)” on page 98, or “SYSCON” in *Utilities Reference*.

```
LOAD REMOTE password LOAD RSPX
```

The command to load REMOTE must precede the command to load RSPX. Replace *password* with the password you want to use with RCONSOLE.

REMOVE DOS

Why Use REMOVE DOS?

Use REMOVE DOS to

- ◆ Remove DOS from the file server's memory. The memory that was used for DOS is returned to the operating system for file caching. If available memory in the file server is low, use this command to free additional memory for file caching.
- ◆ Increase file server security. With DOS removed, loadable modules cannot be loaded from the file server's DOS drives (floppy disk drives or a DOS partition on the hard disk).
- ◆ Warm boot the file server with the EXIT command.

Command Format

```
REMOVE DOS
```

Additional Information

Once this command is issued, DOS is no longer resident in the file server and loadable modules located on DOS drives are no longer accessible. These modules can be loaded only if they are copied to a network drive on the file server.

After the file server is downed, the EXIT command will no longer return you to DOS. However, the EXIT command *will* warm boot the file server. This feature allows users who are using RCONSOLE to reboot the file server remotely.

Remove DOS from the File Server

To remove DOS from the file server, type

```
REMOVE DOS <Enter>
```

The following message appears:

```
DOS removed and its memory given to the disk cache
```

See [“EXIT” on page 68](#) and [“SECURE CONSOLE” on page 242](#).

RESET ROUTER

Why Use RESET ROUTER?

Use RESET ROUTER to reset an inaccurate or corrupted router table in the file server.

For example, if several file servers or bridges on your network go down, any packets sent to or through their routers are lost. If you reset the router in each file server that is up, the router sends a request (an advertising packet) to nearby file servers to verify any other networks the servers know about. The router builds a new, accurate router table from this information.

This command cannot be used when the file server is down.

NOTE: In normal situations, the router updates its tables every two minutes to automatically handle situations in which other servers or their routers have gone down. This command speeds up the normal process of updating the router table.

Command Format

```
RESET ROUTER
```

Reset the Router Table

To reset the router table, type

```
RESET ROUTER <Enter>
```

ROUTE

Why Use ROUTE?

Use ROUTE to allow NetWare to pass frames (packets) through IBM bridges on a Token-Ring cabling system. You must load the TOKEN LAN driver before you load ROUTE.

All NetWare workstations on Token-Ring networks must use the new Token-Ring workstation driver.

If you are using ODI shells, see *ODI Shell for DOS* for instructions on setting up the workstation boot diskettes with the new driver.

NOTE: For instructions on setting up workstations and NetWare 286 file servers and bridges for source routing, see *Installation Supplement for IBM Token-Ring Network*.

The following tasks are described in this section:

Task	Page
Set up the file server for source routing	“Set Up the File Server for Source Routing” on page 232
Change a source routing parameter	“Change a Source Routing Parameter” on page 232

Command Format

```
LOAD [path]ROUTE [parameter...]
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Replace *parameter* with one or more of the following:

BOARD = <i>number</i>	REMOVE = <i>number</i>
CLEAR	RSP = <i>value</i>
DEF	TIME = <i>number</i>
GBR	UNLOAD
MBR	

Each parameter is described below.

Parameters

All the parameters described on the following pages are optional. ROUTE can be loaded re-entrantly (a second time) with a specified parameter to change ROUTE's configuration.

Most of the parameters have default values that should work with simple configurations for IBM bridges. If you have installed parallel IBM bridges, you can change some of the parameters to reduce traffic on some of the paths.

NOTE: For more information about source routing and broadcast frames, see the *IBM Token-Ring Network Architecture Reference* produced by IBM.

BOARD = *number*

Use this parameter if the Token-Ring driver is not the first driver loaded. The operating system numbers the boards, starting with the first driver loaded. That board is board number one. (Check the order in the AUTOEXEC.NCF file if you have more than one driver. See [“Edit the AUTOEXEC.NCF File” on page 98](#). Use this parameter to specify which board you want to change parameters on or load ROUTE for.

CLEAR

Use this parameter to clear the Source Routing table. This parameter forces a dynamic rebuilding of the table by sending a default frame to each specific node in the network. Use this parameter when an IBM bridge on the network has gone down and an alternate route is available.

DEF

Use this parameter to prevent frames that have unknown (Default) destination addresses from being sent across Single Route IBM bridges.

- ◆ If this parameter is specified, all frames that have addresses not currently in the file server's Source Routing table are forwarded as All Routes Broadcast frames.
- ◆ If this parameter is not specified, all frames that have addresses not currently in the file server's Source Routing table are forwarded as Single Route Broadcast frames.
- ◆ If ROUTE has already been loaded with the DEF parameter, reloading ROUTE with this parameter broadcasts all subsequent Single Route Broadcast frames as All Routes Broadcast frames.

GBR

Use this parameter to specify that all General Broadcast frames are to be sent as All Routes Broadcast frames.

- ◆ If this parameter is not specified when ROUTE is loaded, all General Broadcast frames are broadcast as Single Route Broadcast frames.
- ◆ If ROUTE has already been loaded with the GBR parameter, reloading ROUTE with this parameter broadcasts all subsequent General Broadcast frames as All Routes Broadcast frames.

MBR

Use this parameter to specify that all Multicast Broadcast frames are to be sent as All Routes Broadcast frames.

- ◆ If the parameter is not specified when ROUTE is loaded, all Multicast Broadcast frames are broadcast as Single Route Broadcast frames.
- ◆ If ROUTE has already been loaded with the MBR parameter, reloading ROUTE with this parameter broadcasts all subsequent Multicast Broadcast frames as All Routes Broadcast frames.

REMOVE = *number*

Use this parameter to remove a specified node address from the file server's Source Routing table. Use the parameter when a bridge has gone down. When you remove the node from the Source Routing table, you force the file server to determine an alternate route.

Replace *number* with a 12-digit (06-byte) hexadecimal number. If less than 9 digits are entered, ROUTE prefixes the address with 4000h. For example, REMOVE=2 is interpreted as REMOVE=400000000002

RSP = *value*

Use this parameter to specify how the file server should ReSPond to a broadcast request.

Replace *value* with one of the following:

NR	Specifies that all Broadcast Requests are to be responded to directly. A Broadcast Response is Not Required (this is the default value).
AR	Specifies that all Broadcast Requests are to be responded to with an All Routes Broadcast frame.
SR	Specifies that all Broadcast Requests are to be responded to with a Single Route Broadcast frame.

TIME = *number*

Use this parameter to specify how often the Source Routing table should be updated. This parameter forces the table to be updated with a new route if the current route has not been used during the specified time period. This parameter enables ROUTE to determine alternate routes dynamically when an IBM bridge goes down.

Replace *number* with a value from 03 to 255 seconds. The default is 03 seconds.

UNLOAD

Use this parameter after the board parameter to specify the board from which you want to remove source routing. To unload ROUTE.NLM from the file server, use UNLOAD ROUTE.

Additional Information

As frames pass through an IBM bridge, source routing information is added to the frame header at the Media Access Control (MAC) layer. NetWare's bridging is done above this layer. ROUTE.NLM enables NetWare to do the following:

- ♦ Keep track of the source routing information in the frames.
- ♦ Configure the source routing information in the frames according to the parameters with which ROUTE is loaded.

ROUTE can be loaded re-entrantly.

- ♦ If you have two Token-Ring boards in the file server, ROUTE should be loaded twice. The second time it is loaded, you must use the BOARD parameter to specify a board number.
- ♦ If you need to change the configuration, load ROUTE with the parameter that needs to be changed.

Set Up the File Server for Source Routing

Procedure

- 1** Load the TOKEN.NLM LAN driver.
See [“LOAD LAN driver” on page 133](#).

- 2** Load ROUTE by typing

```
LOAD ROUTE <Enter>
```

NOTE: To set up the workstations and NetWare v2.x file servers and bridges for source routing, see *Installation Supplement for IBM Token-Ring Network*.

Change a Source Routing Parameter

To change a parameter in ROUTE after ROUTE has been loaded, follow the procedure in the following section that fits your situation.

One Token-Ring Network Board

To clear the Source Routing table when only one driver has been loaded, type

```
LOAD ROUTE CLEAR <Enter>
```


Two Token-Ring Network Boards

To change a parameter when more than one driver has been loaded, complete the following steps.

Procedure

(This procedure shows how to change the update time for the Source Routing table from the default of 3 seconds to 10 seconds.)

1 To change the TIME parameter for the first driver, type

```
LOAD ROUTE BOARD=01 TIME=10 <Enter>
```

2 To change the TIME parameter for the second driver, type

```
LOAD ROUTE BOARD=02 TIME=10 <Enter>
```

RPL

Why Use RPL?

Use RPL to enable remote booting of IBM PC diskless workstations that have network boards installed.

Command Format

```
LOAD [path] RPL
```

Command Parameters

Replace *path* with the full path to the directory containing the RPL module.

Load RPL

To load RPL, type

```
LOAD RPL <Enter>
```

Additional Information

For information about	Refer to
Remote booting a DOS workstation	“Create a Single or Multiple Remote Boot Disk Image File(s)” in <i>NetWare Workstation for DOS and Windows</i>
Remote booting an OS/2 workstation	“Remote-Booting OS/2 Workstations” in <i>NetWare Workstation for OS/2</i>

RS232

Why Use RS232?

Use RS232 to set up a communications port for remote management. RS232 is an asynchronous communications driver that initiates the file server's communication port and transfers screen and keystroke information to and from REMOTE.NLM.

Command Format

```
LOAD [path]RS232 [comm port] [modem speed]
```

Command Parameters

If the module is in the SYS:SYSTEM directory, you do not need to specify a path. If the module is in a different directory, replace *path* with the full directory path to the directory containing RS232.NLM. Begin with a DOS drive letter or a NetWare volume name.

Replace *comm port* with the communications port number (1 or 2). If you do not enter this number when entering the LOAD command, you will be prompted to enter it.

Replace *modem speed* with the baud rate of your modem (2400, 4800, or 9600). If you do not enter the modem speed when entering the LOAD command, you will be prompted to select a baud rate.

RSPX

Why Use RSPX?

Use RSPX to allow the RCONSOLE utility to access a file server. RSPX loads the SPX driver for REMOTE and advertises the server to workstations (therefore, you should load REMOTE before you load RSPX).

Command Format

```
LOAD [path] RSPX
```

Command Parameters

Replace *path* with a full directory path to the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system looks for RSPX in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

You need two NLMs (RSPX and REMOTE) and a menu utility (RCONSOLE) to set up Remote Console. Load REMOTE; then load RSPX. Then you can use the file server console with RCONSOLE from a workstation using the IPX/SPX protocol.

RCONSOLE is in the SYS:SYSTEM directory; to use it, you must be logged in as SUPERVISOR or have Read and File Scan rights in the SYS:SYSTEM directory.

Load RSPX

To load RSPX, type

```
LOAD RSPX <Enter>
```

SBACKUP

Why Use SBACKUP?

Use SBACKUP to back up and restore data that you specify on a NetWare server, workstation, or service that you select.

Command Format

```
LOAD [path] SBACKUP SIZE=xx BUFFER=x
```

Command Parameters

Replace *path* with the full path to the directory containing SBACKUP.

For the SIZE and BUFFER parameters, use values from the following table.

Table 15 SBACKUP parameter values

Parameter	Syntax	Values
Buffer Size	SIZE = xx	16, 32, 64, 128, or 256 Default: 64 KB
Number of Buffers	BUFFER = x	2 to 10 Default: 4

Additional Information

For information about using SBACKUP, refer to “Rules for Using SBACKUP” in Chapter 1 of *Server Backup*.

SCAN FOR NEW DEVICES

Why Use SCAN FOR NEW DEVICES?

Use SCAN FOR NEW DEVICES to check for disk hardware that has been added since the NetWare server was last booted.

Command Format

```
SCAN FOR NEW DEVICES
```

Check for New Hardware Devices

To check for new hardware devices that have been added since the NetWare server was last booted, type

```
SCAN FOR NEW DEVICES <Enter>
```

SEARCH

Why Use SEARCH?

Use SEARCH to tell the file server where to look for loadable module files and .NCF files. The default search path is SYS:SYSTEM.

You can use SEARCH to add other search paths or to delete current search paths. You can also use SEARCH to view the current search paths for the operating system.

The following tasks are explained in this section:

Task	Page
Display the current search paths	“Display the Current Search Paths” on page 240
Add a search path	“Add a Search Path” on page 240
Delete a search path	“Delete a Search Path” on page 241

Command Format

```
SEARCH [ADD [number] path]
```

or

```
SEARCH DEL number
```

Command Parameters

Replace *number* with the number of the search drive you want to add or the number of the search drive you want to remove.

Replace *path* with the complete path of the directory you want searched. Begin with a DOS drive letter or a NetWare volume name.

Additional Information

IMPORTANT: If you execute SECURE CONSOLE, SEARCH is disabled. The SYS:SYSTEM search path remains in effect, but you cannot create any new search paths.

Once you execute SECURE CONSOLE, you must down the file server and reboot it in order to create additional search paths.

Display the Current Search Paths

To display the current search paths on the file server, type

```
SEARCH <Enter>
```

Information similar to the following appears:

Figure 40 Current search path information

```
Search 1: [Server Path] SYS:SYSTEM
Search 2: [DOS Path ] A:
```

Add a Search Path

If you have copied loadable modules to directories other than SYS:SYSTEM and want to load a module without specifying the path, you can add a search path. During a command to load a module, the operating system searches the path you specified for loadable modules. The following examples explain how to add a search path to the file server's local drive or to a network directory, and how to specify a search number.

To a Local Drive

To add drive A: as a search path in the list, type

```
SEARCH ADD A: <Enter>
```


To a Network Directory

To add a network directory on the file server, you must enter the path, starting with the volume name. For example, to add the SYS:MODULES directory as a search path, you would type

```
SEARCH ADD SYS:MODULES <Enter>
```

To a Specific Number

When you add a search path to the operating system, the default is to make the path last on the list. If you want to have one path searched before another, you must specify a number. To make a directory the first directory searched, use 1; second, 2; etc. For example, to have drive C: searched first, type

```
SEARCH ADD 1 C: <Enter>
```

Delete a Search Path

Procedure

- 1 Display a list of current search paths by typing

```
SEARCH <Enter>
```
- 2 From the list displayed, choose the number of the drive you want to delete and then type in the DELETE command.

For example, to delete search drive 2, you would type

```
SEARCH DEL 2 <Enter>
```

SECURE CONSOLE

Why Use SECURE CONSOLE?

Use SECURE CONSOLE to implement the following security measures:

- ♦ Prevent loadable modules from being loaded from any directory other than SYS:SYSTEM.
- ♦ Prevent keyboard entry into the OS debugger.
- ♦ Prevent anyone other than a console operator from changing the date and time.
- ♦ Remove DOS from the file server.

Command Format

`SECURE CONSOLE`

Additional Information

The SECURE CONSOLE command prevents the following types of breaches in security. For additional security tips, see “Console” in *Concepts*.

Unauthorized NLMs

An intruder could load an NLM that accesses or alters any information on the file server. In addition, these loadable modules can change user account information at the BINDERY security level. Because of this danger, we recommend using SECURE CONSOLE, especially in security-sensitive environments.

When SECURE CONSOLE has not been used, a module can be loaded from a DOS partition, a diskette drive, or any directory on a NetWare volume. If you allow modules to be loaded from all these drives, anyone who has access to the file server console can load a loadable module.

Date and Time Considerations

Some security and accounting features depend on date and time for their enforcement. These features include password expiration, time restrictions (when a user can log in to the server), intruder detection, and lockout intervals.

An intruder can change the date and time at the file server and bypass these time-dependent features. SECURE CONSOLE prevents this. Although FCONSOLE can still be used to change the date and time, the user must have console operator or supervisor rights.

DOS Considerations

If DOS remains enabled on the file server console, an intruder can down the file server and execute a DOS file developed expressly to steal or alter data. With DOS removed from the file server, the intruder must turn the file server off and then on again to access DOS.

If you have armed your file server with a power-on password, the intruder cannot access DOS. (See the documentation that comes with the computer for information on setting a power-on password. Not all computers have this feature.)

Secure the File Server from Unauthorized System Programs

To secure the file server, type

```
SECURE CONSOLE <Enter>
```

SEND

Why Use SEND?

Use SEND to send a message to all users logged in or attached to the file server or to a list of users or connection numbers.

Command Format

```
SEND "message" [[TO] username|connection number] [[and|,]
username|connection number]
```

Command Parameters

Replace *message* with the information (up to 55 characters) you want to send.

NOTE: If no user or connection number is specified, the message is sent to *all* attached users.

Replace *username* with the user or users you want to send the message to. Separate multiple users with a space, a comma, or an *and*.

Replace *connection number* with the number of the workstation you want to send the message to. Separate multiple connection numbers with a space, a comma or an *and*. To determine the connection number, see ["Connection Information" on page 180](#).

Additional Information

Who Receives Messages

All logged-in users *except the following* receive the messages:

- ◆ Users who have used the CASTOFF ALL utility.
- ◆ Users who are logged in using ACS or NACS.
- ◆ Users who are logged in on remote workstations.
- ◆ Users who are using some graphics applications. These users may hear the beep and should press <Ctrl><Enter> to proceed (even though no message appears telling them to do so). To prevent the beep, run CASTOFF in a batch file before running the graphics applications.

Where Messages Appear

All attached users receive SEND messages on the 25th line of the screen. Messages do not interfere with the workstation's screen display; however, you cannot make any entries on the screen until you clear the message.

How to Delete Messages

To delete the message from a workstation screen and resume work, press <Ctrl><Enter>.

How to Stop Message Displays

Use CASTOFF with the ALL option to prevent messages from being received and displayed. (See "CASTOFF" in *Utilities*.)

Send a Console Message

Send a Message to All Users

To send a message to all users logged in or attached to the file server, type

```
SEND "message" <Enter>
```

Send a Message to a Specific User

To send a message to a user named Jack, type

```
SEND "message" Jack <Enter>
```

Send a Message to a Specific Workstation

To send a message to workstation 1, type

```
SEND "message" 1 <Enter>
```

Send a Message to Users and Workstations

To send a message to a combination of users and workstations, you could type

```
SEND "message" to Fred, Jack, 1, 4, Mary <Enter>
```

SERVER

Why Use SERVER?

Use SERVER (SERVER.EXE) to boot NetWare on your file server. SERVER is a DOS-executable file that boots the NetWare operating system. As part of the boot process, SERVER performs the following tasks. (For complete information, see Chapter 2, “Install the File Server Software,” in *Installation and Upgrade*.)

- ◆ Executes the STARTUP.NCF file.
- ◆ Mounts volume SYS:.
- ◆ Executes the AUTOEXEC.NCF file.
- ◆ If neither of the .NCF files exists, SERVER prompts you for a file server name and an IPX internal network number; SERVER then brings up the console prompt (:).

Command Format

```
SERVER [parameter]
```

Command Parameters

Replace *parameter* with one of the following:

-S [*path*]*filename*

Include this parameter when you want to use an alternate to the STARTUP.NCF file. You can include a drive letter and/or the directory path with the filename. If you do not specify a drive or directory path, the operating system will look for the file in the current boot directory.

-NA

Include this parameter when you do not want to execute the AUTOEXEC.NCF file that you created in INSTALL. This parameter is useful if you are changing drivers or other commands in your AUTOEXEC.NCF file.

-NS

Include this parameter when you do not want to execute the STARTUP.NCF and AUTOEXEC.NCF files created in INSTALL. This parameter is useful if you want to change the boot process.

-C *cache_buffer_number*

Include this parameter if you want to change the block size of the cache buffer. Valid block sizes are 4 KB, 8 KB, or 16 KB.

Default: 4 KB

IMPORTANT: Do not use a cache buffer size larger than the block allocation size (for example, do not specify an 8 KB cache buffer with a 4 KB block allocation). The server will not mount any volume whose block allocation size is smaller than the cache buffer size.

If you are using block allocation sizes larger than 4 KB, you can improve performance in some situations by increasing the cache buffer size.

Boot the File Server

At the DOS prompt, type

```
SERVER <Enter>
```

SERVER executes the STARTUP.NCF and AUTOEXEC.NCF files, if they exist. If you have not created the .NCF files, you have to load all necessary disk and LAN drivers. See [“Edit the AUTOEXEC.NCF File” on page 98](#).

Boot with an Alternate STARTUP File

You can use an alternate STARTUP file to boot the file server. For example, if you have a file server with both an internal hard disk and a disk subsystem, you may want to boot the file server to function only from the internal disk (perhaps to do maintenance on the disk subsystem). The contents of the alternate STARTUP file would be similar to the following:

```
load ISADISK port=1F0 int=E
```

To boot the file server using a file called ALTDISK.NCF, type

```
SERVER -S ALTDISK.NCF <Enter>
```

Boot without a **STARTUP.NCF** File

You can boot the file server without a **STARTUP.NCF** file. For example, if you are doing maintenance or troubleshooting on the hard disks in the file server and you add a new disk subsystem, you might want to test the subsystem before you load the drivers for the internal disks.

To boot the file server without a **STARTUP.NCF** file, type

```
SERVER -NS <Enter>
```

Boot without an **AUTOEXEC.NCF** File

You can boot the file server without executing an **AUTOEXEC.NCF** file. For example, when you are doing maintenance or troubleshooting on the volumes or the LAN drivers, you might want to manually load the LAN drivers or mount the volumes.

If you add a new cabling system to your file server, you might want to test communication just on the new cabling. If you execute **SERVER** without the **AUTOEXEC.NCF** file, you can load only the LAN drivers and loadable modules needed for the test.

To boot the file server without executing an **AUTOEXEC.NCF** file, type

```
SERVER -NA <Enter>
```

Boot with a Different Cache Buffer Size

If you have a file server that contains mainly large files (8 KB or larger), you might increase access speed to the files by specifying a larger cache buffer size. The larger cache size allows a larger portion of the file to be read into memory with only one request.

IMPORTANT: Do not use a cache buffer size larger than the smallest block allocation size (for example, do not use an 8 KB cache buffer with a 4 KB block allocation). The server will not mount any volume whose block allocation size is smaller than the cache buffer size.

To boot the file server with an 8 KB block cache buffer, type

```
SERVER -C8KB <Enter>
```


Add the following line to the STARTUP.NCF file so that the file server automatically boots with the larger cache buffer size:

```
SET CACHE BUFFER SIZE = 8192
```

SET

Why Use SET?

Use SET to view the current operating system parameters and to configure the operating system to fit your situation. Most of the parameters do not need to be changed. They have been set to give maximum performance to most users. However, by changing some of the parameters, you may be able to increase the performance of your operating system.

The following tasks are explained on the indicated pages:

Task	Page
View current operating system configurations	“View Current Operating System Configurations” on page 260
Change an operating system parameter at the console prompt	“Change an Operating System Parameter at the Console Prompt” on page 260
Change an operating system parameter in the STARTUP.NCF file	“Change an Operating System Parameter in the STARTUP.NCF File” on page 261
Understand the operating system parameters	“Understand the Operating System Parameters” on page 262

Command Format

SET [*parameter*]

The available parameters (listed under [“Communications Parameters” on page 254](#) through [“View Current Operating System Configurations” on page 260](#)) are divided into nine categories.

The categories, along with their parameters, are explained on the following pages.

Category	Page
Communications	“Communications” on page 262
Memory	“Memory” on page 267
File caching	“File Caching” on page 269

Category	Page
Directory caching	“Directory Caching” on page 271
File system	“File System” on page 275
Locks	“Lock” on page 280
Transaction tracking	“Transaction Tracking” on page 282
Disk	“Disk” on page 284
Miscellaneous	“Miscellaneous” on page 285

Additional Information

SET can be used to display or change current settings, control memory allocations, and configure other types of operating system functions. The following sections give a brief overview of SET.

Displaying and Changing Current Settings

SET can be used both to display and change current settings.

- ◆ If you use SET without a parameter, a list of categories appears. When you select a category, the current settings for the parameters in that category are displayed.
- ◆ If you use SET with a parameter, the current setting for the parameter is displayed.
- ◆ If you use SET with a parameter and give the parameter a value, the operating system reconfigures itself according to the specified value.

Configuring Memory Allocations

SET controls how much memory can be allocated for the following items and how fast the additional memory can be allocated:

- ◆ File caching
- ◆ Directory caching
- ◆ Packet receive buffers
- ◆ Server processes

Configuring Other Types of Operating System Functions

SET also configures the following functions:

- ◆ Number of open and locked files
- ◆ Cache buffer size
- ◆ Physical receive packet size
- ◆ Warning parameters for full volumes
- ◆ Encrypted passwords
- ◆ Purging times for deleted files
- ◆ Length of time between disk writes

Entering Parameters

Most SET parameters can be executed from the console prompt and saved permanently in the AUTOEXEC.NCF file. However, some parameters can only be changed in the STARTUP.NCF file; a few others can be changed in the STARTUP.NCF file, at the console, or in the AUTOEXEC.NCF file.

At the Console Prompt

Most of the parameters can be set at the console prompt. If you try to enter a STARTUP.NCF file parameter at the console prompt, you are prompted to enter it into the STARTUP.NCF file.

When a parameter is set at the console, the operating system is immediately configured to that setting. Any setting in the AUTOEXEC.NCF file is automatically overridden until the file server is rebooted.

In the AUTOEXEC.NCF File

Any parameter set at the console prompt can be saved in the AUTOEXEC.NCF file.

- ◆ When a parameter is saved in this file, the file server automatically configures itself to the parameter when the server is rebooted.
- ◆ When the parameter is not saved in the file, the operating system returns to the default setting for the parameter when the file server is booted.

Edit the AUTOEXEC.NCF file with INSTALL.

In the STARTUP.NCF File

The following parameters must be set in the STARTUP.NCF file. They cannot be set at the console prompt or saved in the AUTOEXEC.NCF file.

Auto Register Memory Above 16 Megabytes

Auto TTS Backout Flag

Cache Buffer Size

Maximum Physical Receive Packet Size

Maximum Subdirectory Tree Depth

Minimum Packet Receive Buffers

Reserved Buffers Below 16 Meg

Concurrent Remirror Requests

The STARTUP.NCF file can be edited from within the INSTALL utility.

Console, AUTOEXEC.NCF File, or STARTUP.NCF File

The following parameters can be set in any one of either the STARTUP.NCF file, the AUTOEXEC.NCF file, or at the console.

Display Spurious Interrupt Alerts

Display Lost Interrupt Alerts

Display Disk Device Alerts

Display Relinquish Control Alerts

Display Old API Names

Maximum Packet Receive Buffers

Reply to Get Nearest Server

NCP Packet Signature Option

Maximum Alloc Short Term Memory

Enable Disk Read After Write Verify

Display Incomplete IPX Packet Alerts

Replace Console Prompt with Server Name

Allow Change to Client Rights

These parameters control the display of alert messages about hardware, loadable modules, and hard disks. The parameters can be entered as the first commands in the STARTUP.NCF file so that the alerts appear for all modules that you load and all hardware devices that you add.

Using Parameters that Control the Allocation of Services

Some SET parameters control how the operating system dynamically allocates services. Three types of parameters interact to control the actual allocation of a resource:

- ♦ *Maximum limits* control how many resources the operating system can allocate for a particular service.
- ♦ *Minimum limits* allow the operating system to allocate a minimum number of resources as soon as a request is received. Low minimum limits slow the growth of a particular service. High minimum limits allow rapid growth.

For example, if the minimum number of directory cache buffers is set to 20, the operating system immediately allocates another buffer resource as soon as a request is made until 20 cache buffers have been allocated. When 20 directory cache buffers have been allocated, the operating system waits 2.2 seconds (default) when a request comes in, and then allocates another buffer if the request is still active.

However, if the minimum number of directory cache buffers is set to 40, the operating system allocates 40 directory cache buffers before it starts slowing the growth by waiting 2.2 seconds after each request.

- ♦ *Wait time limits* control how rapidly the operating system can allocate a new resource.

Parameters

The SET categories and their associated parameters are listed in the following tables. The parameter name and default value are listed in the left column and the parameter limits are shown in the right column.

Communications Parameters

The following table lists the default value and limits for each of the Communications parameters. For an explanation of these SET parameters, see [“Communications” on page 262](#).

Table 16 Communications parameters

Parameter	Limits
Console Display Watchdog Logouts = OFF	ON, OFF
New Packet Receive Buffer Wait Time = 0.1 seconds	0.1 to 20 seconds
Maximum Physical Receive Packet Size = 1514	618 to 4202
Maximum Packet Receive Buffers = 400	50 to 2000
Minimum Packet Receive Buffers = 10	10 to 1000
Number of Watchdog Packets = 100	5 to 100
Delay Between Watchdog Packets = 59.3 seconds	9.9 seconds to 10 minutes 26.2 seconds
Delay Before First Watchdog Packet = 4 minutes 56.6 seconds	15.7 seconds to 20 minutes 52.3 seconds
NCP Packet Signature Option = 1	0 to 3
Enable Packet Burst Statistics Screen = OFF	ON, OFF
Reply to Get Nearest Server = ON	ON, OFF
Enable IPX Checksum = ON	ON, OFF
Allow LIP = ON	ON, OFF

Memory Parameters

The following table lists the default value and limits for each of the Memory parameters. For an explanation of these SET parameters, see [“Memory” on page 267](#).

Table 17 Memory parameters

Parameter	Limits
Cache Buffer Size = 4096 bytes	4096, 8192, or 16384 bytes
Maximum Alloc Short Term Memory = 8388608	50000 to 33554432
Auto Register Memory Above 16 Megabytes = ON	ON, OFF

File Caching Parameters

The following table lists the default value and limits for each of the File Caching parameters. For an explanation of these SET parameters, see [“File Caching” on page 269](#).

Table 18 File Caching parameters

Parameter	Limits
Maximum Concurrent Disk Cache Writes = 50	10 to 1000
Dirty Disk Cache Delay Time = 3.3 seconds	0.1 to 10 seconds
Minimum File Cache Report Threshold = 20	0 to 1000
Minimum File Cache Buffers = 20	20 to 1000
Read Ahead Enabled = ON	ON, OFF
Read Ahead LRU Sitting Time Threshold = 10 seconds	0 seconds to 1 hour
Reserved Buffers Below 16 Meg = 16	8 to 300

Directory Caching Parameters

The following table lists the default value and limits for each of the Directory Caching parameters. For an explanation of these SET parameters, see [“Directory Caching” on page 271](#).

Table 19 Directory Caching parameters

Parameter	Limits
Dirty Directory Cache Delay Time = 0.5 seconds	0 to 10 seconds
Maximum Concurrent Directory Cache Writes = 10	5 to 50
Directory Cache Allocation Wait Time = 2.2 seconds	0.5 seconds to 2 minutes
Directory Cache Buffer NonReferenced Delay = 5.5 seconds	1 second to 5 minutes
Maximum Directory Cache Buffers = 500	20 to 4000
Minimum Directory Cache Buffers = 20	10 to 2000

File System Parameters

The following table lists the default value and limits for each of the File System parameters. For an explanation of these SET parameters, see “[File System](#)” on page 275.

Table 20 File System parameters

Parameter	Limits
Maximum Extended Attributes per File or Path = 8	4 to 512
Immediate Purge Of Deleted Files = OFF	ON, OFF
Maximum Subdirectory Tree Depth = 25	10 to 100
Volume Low Warn All Users = ON	ON, OFF
Volume Low Warning Reset Threshold = 256	0 to 100000
Volume Low Warning Threshold = 256	0 to 1000000
Turbo FAT Re-Use Wait Time = 5 minutes 29.6 seconds	0.3 seconds to 1 hour 5 minutes 54.6 seconds
Minimum File Delete Wait Time = 1 minute 5.9 seconds	0 seconds to 7 days
File Delete Wait Time = 5 minutes 29.6 seconds	0 seconds to 7 days
NCP File Commit = ON	ON, OFF
Maximum Percent of Volume Used By Directory = 13	5 to 50
Maximum Percent of Volume Space allowed for Extended Attributes = 10	5 to 50

Lock Parameters

The following table lists the default value and limits for each of the Lock parameters. For an explanation of these SET parameters, see “[Lock](#)” on page 280.

Table 21 Lock parameters

Parameter	Limits
Maximum Record Locks Per Connection = 500	10 to 10000
Maximum File Locks Per Connection = 250	10 to 1000
Maximum Record Locks = 20000	100 to 200000
Maximum File Locks = 10000	100 to 100000

Transaction Tracking Parameters

The following table lists the default value and limits for each of the Transaction Tracking parameters. For an explanation of these SET parameters, see [“Transaction Tracking” on page 282](#).

Table 22 Transaction Tracking parameters

Parameter	Limits
Auto TTS Backout Flag = OFF	ON, OFF
TTS Abort Dump Flag = OFF	ON, OFF
Maximum Transactions = 10000	100 to 10000
TTS Unwritten Cache Wait Time = 1 minute 5.9 seconds	11 seconds to 10 minutes 59.1 seconds
TTS Backout File Truncation Wait Time = 59 minutes 19.2 seconds	1 minute 5.9 seconds to 1 day 2 hours 21 minutes 51.3 seconds

Disk Parameters

The following table lists the default value and limits for each of the Disk parameters. For an explanation of these SET parameters, see [“Disk” on page 284](#).

Table 23 Disk parameters

Parameter	Limits
Enable disk read after write verify = ON	ON, OFF
Concurrent Remirror Requests = 2	2 to 30

Miscellaneous Parameters

The following table lists the default value and limits for each of the Miscellaneous parameters. For an explanation of these SET parameters, see [“Miscellaneous” on page 285](#).

Table 24 Miscellaneous parameters

Parameter	Limits
Maximum Outstanding NCP Searches = 51	10 to 1000
Allow Unencrypted Passwords = OFF	ON, OFF
New Service Process Wait Time = 2.2 seconds	0.3 to 20 seconds
Pseudo Preemption Time = 2000	1000 to 10000
Display Spurious Interrupt Alerts = ON	ON, OFF
Display Lost Interrupt Alerts = ON	ON, OFF
Display Disk Device Alerts = OFF	ON, OFF
Display Relinquish Control Alerts = OFF	ON, OFF
Display Old API Names = OFF	ON, OFF
Maximum Service Processes = 20	5 to 40
Display Incomplete IPX Packet Alerts = ON	ON, OFF
Replace Console Prompt with Server Name = ON	ON, OFF
Allow Change to Client Rights = ON	ON, OFF

View Current Operating System Configurations

To view the current configuration for the SET parameters, complete the following steps.

Procedure

- 1 At the console prompt, type

```
SET <Enter>
```

The following information appears:

Figure 41 Current operating system configuration information

```
:set
Setable configuration parameter categories
  1. Communications
  2. Memory
  3. File caching
  4. Directory caching
  5. File system
  6. Locks
  7. Transaction tracking
  8. Disk
  9. Miscellaneous
Which category do you want to view:
```

- 2 To select a category, type the number of the category and press <Enter>.

Change an Operating System Parameter at the Console Prompt

To change a SET parameter that can be set at the console prompt, type “SET” and the parameter.

For example, to set the “Allow unencrypted passwords” parameter so that unencrypted passwords are valid, type

```
SET ALLOW UNENCRYPTED PASSWORDS = ON <Enter>
```

To set the parameter each time the file server is booted, add the following line to the AUTOEXEC.NCF file:

```
SET ALLOW UNENCRYPTED PASSWORDS = ON
```

You can modify the AUTOEXEC.NCF file with INSTALL or SYSCON.

Change an Operating System Parameter in the STARTUP.NCF File

Some SET parameters can be set only in the STARTUP.NCF file. For a list, see [“In the STARTUP.NCF File” on page 253](#).

To change one of those parameters, complete the following steps.

Procedure

1 Load INSTALL.

At the console prompt, type

```
LOAD INSTALL <Enter>
```

2 Select “System Options.”

3 Select “Edit STARTUP.NCF file.”

4 Complete one of the following:

- ◆ If the STARTUP.NCF file is on the diskette in drive A:, press <Enter>.
- ◆ If the STARTUP.NCF is on the DOS partition, delete the “A” and type “C”. Then press <Enter>.

NOTE: If the STARTUP.NCF file is located in a DOS partition directory other than C:\, verify that the proper directory path is specified following the drive letter designation.

5 Add the SET parameter to the file.

For example, to change the maximum subdirectory depth to 30, type

```
SET MAXIMUM SUBDIRECTORY TREE DEPTH = 30
```

6 Save the file with the changes.

Answer “Yes” to the exit prompts.

7 Down the file server by typing

```
DOWN <Enter>
```

8 Reboot the file server.

Understand the Operating System Parameters

The following parameters are described according to their groupings in the SET information screens.

Communications

The communication parameters determine the settings for the packet receive buffers and the watchdog packets.

- ◆ Packet receive buffers are areas in the file server's memory set aside to hold data packets. The packets remain in the buffers while the file server processes them. Use MONITOR to view the number of packet receive buffers currently allocated.
- ◆ The watchdog packets are used to make sure workstations are currently connected. If the server has not received a packet from a workstation in a certain time (set by the Delay Before First Watchdog Packet parameter), a watchdog packet is sent to the station. If the station does not respond within a certain time (set by the Delay Between Watchdog Packets parameter), another watchdog packet is sent. If the station still does not respond to a certain number of watchdog packets (the Number of Watchdog Packets parameter), the server assumes that the station is no longer connected and clears the station's connection.
- ◆ NCP packet signature levels on the server are controlled with the NCP Packet Signature Option parameter.

Console Display Watchdog Logouts = *value*

This parameter determines whether a console message is displayed when a connection is cleared.

- ◆ If your network is running smoothly and stations are not having any problems with file server connections, you do not need to display watchdog logouts.
- ◆ If your stations are having connection problems, the watchdog logout messages can help you isolate which stations are not receiving or successfully sending watchdog packets.

Supported values: ON and OFF

Default: OFF

Maximum Physical Receive Packet Size = *number*

This parameter determines the maximum size of packets that can be transmitted on any of the file server's networks. The default allows 1 KB (data with the packet header) to be transmitted.

- ◆ If you are using Token-Ring or Ethernet boards, the default is acceptable.
- ◆ If some of the network boards can transmit more than 512 bytes of data per packet, set this parameter for the largest packet size.

This parameter cannot be modified at the console prompt. To modify the default, you must include the parameter in the STARTUP.NCF file.

Supported values: 618 to 24682

Default: 1514

Maximum Packet Receive Buffers = *number*

This parameter determines the maximum number of packet receive buffers that the operating system can allocate.

Before increasing this parameter, use MONITOR to view the file server's current use of packet receive buffers and service processes.

- ◆ If the number of packet receive buffers is at its maximum, increase this value in increments of 10 until you have one packet receive buffer per workstation.
- ◆ If you have EISA or microchannel bus master boards in your file server, increase this parameter to allow for at least 5 buffers per board. Use MONITOR ("LAN Information") to determine if the board is producing "No ECB available count" errors. If you are receiving "No ECB available count" errors, increase the parameter to allow for 10 packet receive buffers per board.
- ◆ If the number of allocated service processes is at its maximum, you can increase the "Maximum number of service processes" parameter to decrease the need for more packet receive buffers.

Supported values: 50 to 2000

Default: 400

Minimum Packet Receive Buffers = *number*

This parameter determines the minimum number of packet receive buffers that the operating system can allocate. Rather than waiting for requests to come in, the operating system allocates the minimum number of buffers as soon as the file server boots.

Before increasing this parameter, use MONITOR to view the file server's current use of packet receive buffers. If the allocated number is higher than 10 and the server is slow in responding immediately after it has been booted, increase this number.

If you have EISA or microchannel bus master boards in your file server and are receiving "No ECB available count" errors (see "LAN Information" on page 181) right after the file server boots, increase this parameter. Increase the parameter so that each board can have at least 5 packet receive buffers.

This parameter can be changed only in the STARTUP.NCF file.

Supported values: 10 to 1000

Default: 100

New Packet Receive Buffer Wait Time = *time*

This parameter determines how long the operating system waits after receiving a request for another packet receive buffer before granting another buffer.

This parameter prevents the operating system from granting too many packet receive buffers during a sudden peak in usage. If you have an EISA bus master board in your file server, this parameter should never be changed.

Supported values: 0.1 seconds to 20 seconds

Default: 0.1 seconds

Number of Watchdog Packets = *number*

This is the number of watchdog packets that the server will send out, without receiving a reply from a workstation, before eliminating the workstation's connection.

Supported values: 5 to 100

Default: 10

Delay Between Watchdog Packets = *time*

This is the amount of time between watchdog packets. After the server sends out the first watchdog packet, it waits the specified time before sending out the succeeding packets if it receives no reply.

Supported values: 9.9 seconds to 10 minutes 26.2 seconds

Default: 59.3 seconds

Delay Before First Watchdog Packet = *time*

This is the amount of time the server waits without receiving a request from a workstation before it sends out the first watchdog packet to that workstation.

Supported values: 15.7 seconds to 20 minutes 52.3 seconds

Default: 4 minutes 56.6 seconds

NCP Packet Signature Option = *number*

This parameter determines the packet signature level for the server. The signature level that is set on the server works in conjunction with the signature level of the client to determine the effective packet signature.

Supported values: 0 to 3

Default: 1

This parameter can be set in the STARTUP.NCF file.

NOTE: After startup, you can only increase the packet signature level.

The following table explains each of the packet signature level options for the server.

Number	Explanation
0	Server does not sign packets (regardless of the client level)
1	Server signs packets <i>only</i> if the client requests it (client level is 2 or higher)
2	Server signs packets if the client is capable of signing (client level is 1 or higher)
3	Server signs packets and requires all clients to sign packets (or logging in will fail)

Some combinations of server and client packet signature levels may slow performance. However, low CPU-demand systems may not show any performance degradation. Network supervisors can choose the packet signature level that meets both their performance needs and their security requirements

Enable Packet Burst Statistics Screen = *value*

This parameter determines whether the NCP Packet Burst Statistics Screen is displayed.

Supported values: ON and OFF

Default: OFF

Reply to Get Nearest Server = *value*

This parameter determines if the server will respond to Get Nearest Server requests from workstations that are attempting to locate a server.

This parameter can be set in the STARTUP.NCF file.

Supported values: ON and OFF

Default: ON

Enable IPX Checksums = *number*

This parameter determines the level of IPX checksums to be performed.

Supported values: 0 to 2

Default: 1

The following table explains each of the IPX checksum level options.

Number	Explanation
0	No checksums performed
1	Checksums performed if enabled at the client
2	Checksums required

Allow LIP = value

This parameter determines if Large Internet Packet support is enabled.

Supported values: ON and OFF

Default: ON

Memory

The memory parameters control the size of the dynamic memory pool, the block size of the cache buffers, and the automatic registering of memory on EISA bus computers.

Maximum Alloc Short Term Memory = number

The Alloc Short Term Memory pool stores the following information:

- ◆ Drive mappings
- ◆ Service request buffers
- ◆ Open and locked files
- ◆ User connection information
- ◆ Messages waiting to be broadcast
- ◆ Loadable module tables
- ◆ Queue manager tables

This parameter controls how much memory the operating system can allocate to the Alloc Short Term Memory pool. The 8MB default should be sufficient for up to 1000 users, each with 26 drive mappings.

- ◆ Decrease this value if the server is allocating more memory to this pool than is usually needed, due to a temporary situation.
- ◆ Increase this value if the file server issues warnings that operations cannot be completed because this memory pool has reached its limits. Increase the limit in increments of 1 MB.

Use MONITOR to view the amount of memory allocated to the “Alloc Memory Pool” (the “Server Memory Statistics” window).

Supported values: 50000 to 33554432

Default: 8388608

Auto Register Memory above 16 Megabytes = *value*

This parameter controls the automatic registering of memory above 16 MB in EISA computers.

- ◆ Set this parameter to OFF if you have installed a network board or a disk adapter board that uses on-line DMA or AT bus mastering. Since the board uses 24-bit address lines, the board can address only 16 MB of memory correctly.

If you install one of these boards and the file server addresses more than 16 MB of memory, the board will corrupt file server memory. The board will address low memory rather than its assigned high memory and corrupt the low memory being used by the operating system.

- ◆ Set this parameter to ON if you want memory above 16 MB to be registered with the operating system.

This parameter cannot be set at the console prompt. To change the value, you must add the parameter to the STARTUP.NCF file and reboot the file server.

Supported values: ON and OFF

Default: ON

Cache Buffer Size = *number*

This parameter controls the block size of the cache buffer.

- ◆ If you are using block allocation sizes larger than 4,096 bytes (4 KB) on all volumes, you can improve performance in some situations by increasing the cache buffer size.
- ◆ If you are not using block allocation sizes larger than 4,096 bytes (4 KB), making the cache buffer larger *decreases* performance and wastes memory space. The operating system will *not* mount any volumes that have block allocation sizes smaller than the cache block size.
- ◆ If your volumes have different block allocation sizes, make your cache buffer size no larger than the smallest block allocation size.

This parameter cannot be modified at the console prompt. To change the default value, include the parameter in the STARTUP.NCF file or run SERVER with the -c parameter. See “**SERVER**” on page 246.

Supported values: 4096, 8192, and 16384 bytes

Default: 4096 bytes

File Caching

File caching allows faster access to frequently used files by holding a file (or a portion of the file) in memory. Files that are being read from or written to are kept in file cache buffers. The number of files kept in memory depends on the number of file cache buffers. The number of file cache buffers is determined by the amount of available memory and the “Minimum file cache buffers” setting.

Following are the operating system file caching parameters.

Minimum File Cache Buffers = *number*

This parameter sets the minimum number of cache buffers that the operating system can allow for file caching. All memory not allocated for other processes is given to file caching. As memory is requested for other uses, the file server gives up cache buffers. This limit specifies when the file server should stop giving file cache buffers to other processes.

If you set the minimum too high, other server processes may not be able to allocate necessary memory resources. For example, a loadable module could fail to load because the file server has run out of available memory.

Supported values: 20 to 1000

Default: 20

Maximum Concurrent Disk Cache Writes = *number*

This parameter determines how many write requests for changed file data can be put in the elevator before the disk head begins a sweep across the disk.

- ◆ A *high* number makes the servicing of *write* requests more efficient.
- ◆ A *low* number makes the servicing of *read* requests more efficient.

You should monitor the number of dirty cache buffers on the information screen of MONITOR. If this number is above 70% of the total cache buffers, you can optimize the write speed by increasing the limit for “Maximum concurrent disk cache writes.”

Supported values: 10 to 1000

Default: 50

Dirty Disk Cache Delay Time = *time*

This parameter determines how long the operating system will keep a write request (that does not fill a cache buffer) in memory before writing the request to disk.

If your users are making many small write requests, you can increase the time to make disk writing more efficient. If you decrease the time, you only slightly reduce the chances of losing data and you can drastically reduce performance.

Supported values: 0.1 seconds to 10 seconds

Default: 3.3 seconds

Minimum File Cache Report Threshold = *number*

This parameter sets a threshold so that the operating system warns you when it has allocated all available cache buffers within a specified number greater than the minimum. (Use SET to view the “Minimum file cache buffers” parameter for your system.)

For example, if the minimum number of cache buffers is set to 20 and the “Minimum File Cache Report Threshold” is set to 20, the operating system warns you when all but 40 cache buffers have been allocated for other processes (directory caching, server processes, loadable modules, volume FATs). When the threshold has been reached, you receive the following message:

```
Number of cache buffers is getting too low.
```

Regardless of how this parameter is set, the operating system warns you when the operating system’s memory allocation resources reach the minimum number of cache buffers. When this threshold is reached, you receive the following message:

```
Cache memory allocator exceeded minimum cache buffer left  
limit
```

Supported values: 0 to 1000

Default: 20

Read Ahead Enabled = *value*

When set to ON, and while sequential file access is taking place, background reads are done in advance to get blocks that are to be put into the cache.

Supported values: ON and OFF

Default: OFF

Read Ahead LRU Sitting Time Threshold = *time*

This parameter determines the time after which the read ahead will occur. If the cache LRU sitting time is below the threshold setting, the read ahead will not take place.

Supported values: 0 seconds to 1 hour

Default: 10 seconds

Reserved Buffers Below 16 Meg = *number*

This parameter determines the number of cache buffers to be kept for certain device drivers which are unable to access memory above 16 MB.

This parameter can be set only in the STARTUP.NCF file.

Supported values: 8 to 300

Default: 16

Directory Caching

Directory caching allows fast access to frequently used directories. A directory cache buffer is a portion of file server memory that holds entries from the directory table.

A directory entry stays in a cache buffer as long as it is being accessed frequently (the default setting is 33 seconds). When the directory entry is not being accessed frequently, the operating system can overwrite the entry if all the allocated directory cache buffers have been accessed more frequently.

When the file server boots, the operating system allocates a minimum number of directory cache buffers (the default is 20). The operating system creates these buffers immediately when it receives a request for a new directory cache buffer.

When the minimum number of directory cache buffers has been allocated and another one is needed, the operating system must wait a specified amount of time (the default is 1.1 seconds) before allocating another buffer. If necessary, the operating system keeps allocating directory cache buffers until the maximum number is reached.

If a sufficient number of directory cache buffers have been allocated and enough memory is available for directory caching, the complete directory tables can be cached in memory.

As directory cache buffers increase, file cache buffers decrease. Thus, a trade-off exists between directory caching and file caching. If you adjust the system to use too much memory for directory caching, you can leave too little memory for file caching, and vice versa. Directory caching and file caching need to be carefully balanced for maximum performance.

Six directory caching parameters control the allocation of directory cache buffers. Usually, only the first three parameters listed below need to be changed.

Directory Cache Buffer NonReferenced Delay = *time*

This parameter sets how long a directory entry must be cached before it can be overwritten by another directory entry.

- ♦ If you *increase* the time, the operating system allocates more directory cache buffers. The longer time quickens directory access because a directory is more likely to be cached in memory.
- ♦ If you *decrease* the time, directory access can slow down because a directory is less likely to be in memory. But decreasing the time reduces the need for directory cache buffers since the operating system waits less before it reuses a cache buffer.

Supported values: 1 second to 5 minutes

Default: 5.5 seconds

Maximum Directory Cache Buffers = *number*

This parameter sets the maximum cache buffers used for directory cache buffers. When the operating system allocates a directory cache buffer, the allocation is permanent until the file server reboots; the buffers do not return to file caching when the need for directory cache buffers decreases.

This parameter keeps the operating system from allocating too many directory cache buffers so that memory is available for other file server processes.

- ◆ Increase this limit if the file server responds slowly to directory searches.
- ◆ Decrease this limit if too much memory is being allocated for directory caching. If users are alerted by the operating system that the server is low on memory, this parameter should be one of the first to be reduced. However, you must reboot the file server to return the memory to the cache buffer memory pool.

Supported values: 20 to 4000

Default: 500

Minimum Directory Cache Buffers = *number*

This parameter determines the minimum number of cache buffers that the operating system can allocate for directory caching. The parameter needs to be high enough that directory searches can be done quickly, but no higher than necessary.

- ◆ If the operating system does not need the minimum number of directory cache buffers, the buffers cannot be reallocated to file caching. The unneeded portion remains unused.
- ◆ If the file server responds slowly to directory searches after it has been booted, monitor the number of directory cache buffers usually allocated for directory caching. If the number is significantly higher than this limit, consider increasing the limit to remove the delay time that would normally occur while the file server is self-configuring. Use MONITOR to view the current statistics.

Supported values: 10 to 2000

Default: 20

Dirty Directory Cache Delay Time = *time*

This parameter determines how long the operating system keeps a directory table write request in memory before writing it to disk.

- ◆ If you *increase* the delay time, the operating system gives slightly quicker performance, but the change also increases the probability of the directory tables becoming corrupted.

- ♦ If you *decrease* the delay time, you slightly reduce the chance of directory tables becoming corrupted, but the added number of disk writes can also slightly reduce performance. A zero setting dramatically reduces performance.

Supported values: 0 to 10 seconds

Default: .5 seconds

Maximum Concurrent Directory Cache Writes = *number*

This parameter determines how many write requests from directory cache buffers can be put in the elevator before the disk head begins a sweep across the disk.

- ♦ If you *increase* the number, the servicing of *write* requests becomes more efficient and the servicing of read requests becomes less efficient.
- ♦ If you *decrease* the number, the servicing of *read* requests becomes more efficient and the servicing of write requests becomes less efficient.

Supported values: 5 to 50

Default: 10

Directory Cache Allocation Wait Time = *number*

This parameter determines how long the operating system must wait after allocating a new directory cache buffer before it can allocate another buffer. During this time, all requests for a new directory cache buffer are ignored.

- ♦ If the wait time is too low, peak usage requests will cause more resources to be allocated to directory caching than needed.
- ♦ If the wait time is too high, the operating system will be very slow in allocating the directory cache buffers necessary to service the usual number of directory requests.

If directory searches seem slow even after the file server has been running for 15 minutes, you may want to decrease this time.

Supported values: 0.5 seconds to 2 minutes

Default: 2.2 seconds

File System

File system parameters are used to control the following:

- ◆ File purging
- ◆ Warnings about volumes that are almost full
- ◆ Re-use of turbo FATs

The file-purging parameters influence other parameters which, in turn, control warnings about almost-full volumes. All deleted files remain on the disk for a specified minimum amount of time. The operating system calculates a volume's remaining space by subtracting the following from the total space:

- ◆ Actual files
- ◆ Salvageable files that cannot be purged because their "Minimum file delete wait times" have not expired

Immediate Purge Of Deleted Files = *value*

This parameter controls the salvageable file feature.

- ◆ If this parameter is set to OFF, files can be salvaged with the SALVAGE utility. See "SALVAGE" in *Utilities Reference*.
- ◆ If this parameter is set to ON, all files are immediately purged when they are deleted. The ON setting disables all NetWare salvage features.

Supported values: ON and OFF

Default: OFF

Volume Low Warn All Users = *value*

This parameter controls whether the operating system warns users when a volume is almost full. If you choose not to warn your users, monitor the volume statistics at least daily with CHKVOL or VOLINFO.

Supported values: ON and OFF

Default: ON

Volume Low Warning Reset Threshold = *number*

This parameter controls how much disk space must be freed up before a second warning is issued. (The first warning is controlled by the "Volume Low Warn All Users" parameter.)

When a volume is almost full, it can hover at its warning threshold. As users delete files and the files become candidates for purging, the space on the volume can move slightly above the warning threshold; then, as they create new files, the space on the volume can dip below the threshold. If a volume is hovering at its threshold, you do not want to warn users each time the volume dips below the threshold.

This parameter controls the minimum amount of space that must be available above the threshold before users will again be warned that the space on the volume has dipped below the threshold.

For example, suppose the following conditions exist:

- ◆ The volume block size is 4 KB.
- ◆ The “Volume low warning reset threshold” parameter is 256.
- ◆ The “Volume low threshold” parameter is set to 256.
- ◆ The volume has less than 1 MB of free space.

Given these conditions, the volume must gain at least 1 MB of free space (for a total of 2 MB of free space) and then dip below 1 MB before the operating system sends a second warning that the volume is almost full.

Supported values: 0 to 100000 blocks

Default: 256 blocks

Volume Low Warning Threshold = *number*

This parameter controls how little free disk space can remain on a volume before the operating system issues a warning. The parameter is set by entering the desired number of blocks. (A block is the minimum space allocated to a file; a file can only grow in multiples of the block size.)

The block’s physical size is determined when the volume is created. A volume can be assigned a 4KB, 8KB, 16KB, 32KB, or 64KB block size. For example, if you enter 256 blocks and the volume’s block size is 4 KB, the operating system warns you that the volume is full when about 1 MB of space is left.

If your volumes have been assigned different block sizes, each volume will have a different amount of free space when the warning is issued.

Supported values: 0 to 100000 blocks

Default: 256 blocks

Minimum File Delete Wait Time = *time*

This parameter determines how long a deleted file must stay in a salvageable state on the volume. Deleted files that have not met this minimum time limit will not be purged automatically even if the volume is full and users are unable to create new files.

Supported values: 0 seconds to 7 days

Default: 1 minute and 5.9 seconds

File Delete Wait Time = *time*

This parameter determines when a salvageable file can be purged to create free space on the volume. The operating system tries to keep at least a minimum of 1/32 of the available space on the volume free for new files.

When a file has been deleted for a greater time than the “File delete wait time,” the operating system marks the file as a candidate for purging. When the volume becomes full of files that can be purged and needs free space to maintain the minimum amount, the operating system begins deleting the oldest files that can be purged.

Set this parameter as high as is useful for your users, but remember that this parameter does not guarantee that the file will remain in a salvageable state. The parameter only guarantees that the file will not be purged to maintain the volume’s minimum amount of free disk space (1/32 of the volume’s size).

Files that have not met this time limit will still be purged if the volume is full and the operating system needs space for a user to create a new file.

Supported values: 0 seconds to 7 days

Default: 5 minutes 29.6 seconds

Maximum Percent Of Volume Used By Directory = *percentage*

This parameter limits the portion of a volume that may be used as directory space.

Supported values: 5 to 50

Default: 13

Maximum Percent Of Volume Space Allowed For Extended Attributes = *percentage*

This parameter limits the portion of volume space that may be used for extended attribute storage. This setting only takes effect when the volume is being mounted.

Supported values: 5 to 50

Default: 10

Maximum Extended Attributes Per File or Path = *number*

This parameter sets a limit to the number of extended attributes that can be assigned to a file or path (subdirectory). This limit is for all the volumes on the server.

Supported values: 4 to 512

Default: 8

NCP File Commit = *value*

This parameter controls whether applications can flush all pending file writes to disk. When a File Commit NCP is issued and the flag is set to ON, a file is flushed from the cache to disk immediately, instead of waiting for the cache manager to flush it to disk some time later.

Supported values: ON and OFF

Default: ON

Maximum Subdirectory Tree Depth = *number*

This parameter determines how many levels of subdirectories the operating system supports. Some DOS applications cannot support more than 10 levels if the subdirectories have eleven-character names.

- ◆ Increase the number if your applications support trees deeper than 25.
- ◆ Decrease the number if your applications support only shallow tree structures.

This parameter cannot be set at the console prompt. To change the value, you must add the parameter to the STARTUP.NCF file and reboot the file server.

Supported values: 10 to 100

Default: 25

Turbo FAT Re-Use Wait Time = *time*

This parameter determines how long a turbo FAT buffer remains in memory after an indexed file is closed. Once the wait-time value has passed, the operating system can allocate the buffer to another indexed file.

The NetWare v3.x operating system automatically indexes any randomly accessed file that has 64 entries in the FAT. When a program starts randomly accessing a file that contains more than 64 FAT entries, the operating system automatically builds a turbo FAT index for the file so that the information can be accessed quickly.

Since a turbo FAT index takes time to build, the operating system does not immediately delete the index from its buffer when the file is closed. Having the turbo FAT index already in memory makes reopening the file and accessing the information faster.

- ◆ Increase the wait time if you want the turbo FAT index to remain in memory for long periods of time, even when the file is closed.
- ◆ Increase the wait time if you frequently reopen the same file after a specific delay and know that another file opened during that delay will reuse the index.
- ◆ Decrease the wait time if you want the memory immediately released to service the next file that needs to be indexed.

Supported values: 0.3 seconds to 1 hour 5 minutes 54.6 seconds

Default: 5 minutes 29.6 seconds

Lock

The lock parameters control how many open files each station can have and how many total open files the operating system can handle. They also control how many record locks each connection can have and how many total record locks the operating system can handle. These parameters control three types of locks: file, physical, and logical.

- ♦ A *file lock* secures the entire file and prevents other stations from accessing the file.
- ♦ A *physical record lock* controls data access by multiple users. It prevents other users from accessing or changing a range of bytes (a record) in a file. A physical record lock is enforced by the operating system. If another user attempts to access a range of bytes that is physically locked, the user receives an “Access Denied” error message.
- ♦ A *logical record lock* also controls data access by multiple users. The application assigns a name to each section of data that needs to be locked. The application then locks this name whenever it accesses the data. A logical lock is not enforced by the operating system; it is enforced only to the extent that the application checks the name each time it needs access to data.

Maximum Record Locks Per Connection = *number*

This parameter controls how many record locks a station can use at one time.

- ♦ Increase this parameter when an application cannot lock enough records and fails.
- ♦ Decrease this parameter if workstations are using too many file server resources. Use MONITOR to view how many record locks a workstation is using.

Supported values: 10 to 10000

Default: 500

Maximum File Locks Per Connection = *number*

This parameter controls how many opened and locked files a station can use at one time.

- ◆ Increase this parameter when an application cannot open enough files and fails. An OS/2 workstation might need a higher default than 250. You may also need to increase the number of file handles in the workstation's NET.CFG file.
- ◆ Decrease this parameter if workstations are using too many file server resources. Use MONITOR to view how many opened and locked files a workstation is using.

Supported values: 10 to 1000

Default: 250

Maximum Record Locks = *number*

This parameter controls how many record locks the operating system can handle.

- ◆ Increase this parameter if users are having problems running applications and are receiving messages indicating that not enough record locks are available.
- ◆ Decrease this parameter if users are using too many file server resources. Use MONITOR to view how many record locks a workstation is using.

Supported values: 100 to 200000

Default: 20000

Maximum File Locks = *number*

This parameter controls how many opened and locked files the operating system can handle.

Use MONITOR to view the number of files that are open during peak usage.

- ◆ Increase this parameter if the current number of open files is near or equal to the default.
- ◆ Decrease this parameter if you want to restrict the number of available file server resources.

Supported values: 100 to 100000

Default: 10000

Transaction Tracking

The transaction tracking parameters control the Transaction Tracking System (TTS). A transaction is a set of write operations that must be completed together in order to maintain file and database integrity. Write operations consist not only of data and data records, but also of changes to the index and the key structures that are important to an application's continual operation.

TTS guarantees that a transaction will be either written to disk in its complete form or backed out if incomplete. This ensures database integrity in the event that the workstation, the file server, or the LAN fails before a transaction has been completed. Most of these parameters should not be changed.

Auto TTS Backout Flag = *value*

This parameter determines whether a crashed file server with transactional files can automatically back out any incomplete transactions when the file server is booted.

- ◆ When this parameter is set to ON, the file server automatically backs out any incomplete transactions during its bootup procedures.
- ◆ When the parameter is set to OFF, the file server waits for you to answer the following prompt before it finishes its bootup procedures.

```
Incomplete transaction(s) found. Do you wish to back them  
out?
```

You can only set this parameter in the STARTUP.NCF file, not at the console prompt.

Supported values: ON and OFF

Default: OFF

TTS Abort Dump Flag = *value*

This parameter controls whether a file will be created to log transactional backout data. When the file server fails during a data write to a file that is flagged transactional, the operating system can back out the incomplete write.

- ◆ If this parameter is set to ON, the information that is backed out is written to the TTSS\$LOG.ERR file located in volume SYS:. To read the file, either print the file or view it with a text editor.
- ◆ If this parameter is set to OFF, the information that is backed out is not saved.

Supported values: ON and OFF

Default: OFF

Maximum Transactions = *number*

This parameter determines how many transactions can occur at the same time.

Supported values: 100 to 10000

Default: 10000

TTS UnWritten Cache Wait Time = *time*

This parameter determines how long a block of transactional data can be held in memory. Some blocks of transaction data wait for other transactional blocks to be written first. If one of these blocks reaches its maximum time limit, other write requests are held up and this block is written to disk.

Supported values: 11 seconds to 10 minutes 59.1 seconds

Default: 1 minute 5.9 seconds

TTS Backout File Truncation Wait Time = *time*

This parameter determines the minimum amount of time that allocated blocks remain available for the TTS backout file when these blocks are not currently being used.

Supported values: 1 minute 5.9 seconds to 1 day 2 hours 21 minutes 51.3 seconds

Default: 59 minutes 19.2 seconds

Disk

The disk parameters control read-after-write verification and the number of remirror requests per logical partition.

The disk parameter Enable Disk Read After Write Verify controls one part of Hot Fix redirection. Hot Fix redirection can occur during a write request, a read request, or a read-after-write verification.

- ♦ *Write redirection* occurs when the disk reports an error during a write request. The operating system marks the block as bad and redirects the data to a different block.
- ♦ *Read redirection* occurs when a disk error occurs during a read request. If the hard disk is mirrored, the operating system retrieves the data from the mirrored disk and redirects the data on the primary disk. If the hard disk is not mirrored, the data is lost, but the block is marked as bad so that future data will not be stored there.
- ♦ *Read-after-write verify redirection* occurs after the data is written to disk. The data on disk is then read and compared to that in memory. If the two do not match, the operating system marks the block as bad and redirects the data to a different block.

Enable Disk Read After Write Verify = *value*

This parameter controls whether information written to disk will be compared with that in memory. Normally, you would not want to disable this portion of Hot Fix. However, if your disks are mirrored and reliable and you need extra speed on disk writes, disabling read-after-write verify can almost double the speed of disk writes.

Supported values: ON and OFF

Default: ON

Concurrent Remirror Requests = *number*

This parameter determines the number of remirror requests per logical partition.

This parameter can be set only in the STARTUP.NCF file.

Supported values: 2 and 30

Default: 4

Miscellaneous

The miscellaneous parameters control the following:

- ◆ Encrypted passwords
- ◆ Alerts
- ◆ NCP searches
- ◆ Server processes
- ◆ Changes to client rights

Normally, you will only need to change the setting for encrypted passwords.

Allow Unencrypted Passwords = *value*

This parameter controls the use of unencrypted passwords. An ON setting allows users to use both unencrypted and encrypted passwords. An OFF setting allows users to use only encrypted passwords.

If file servers on your network are running versions of NetWare earlier than NetWare v3.0 and you leave the default to OFF, your users may have problems logging in.

- ◆ If your network has file servers running NetWare v2.12 and later but none running v2.0a, you can copy the NetWare v3.1x utilities to these file servers and set this parameter to OFF.
- ◆ If you do not copy the NetWare v3.1x utilities to the NetWare v2.x file servers, set the parameter to ON.
- ◆ If all file servers are running NetWare v3.1x, set this parameter to OFF.
- ◆ If you have file servers running NetWare v2.0a, set this parameter to ON.

Supported values: ON and OFF

Default: OFF

Display Spurious Interrupt Alerts = *value*

This parameter controls the alerts about spurious interrupts. A message is sent to the file server console whenever the hardware in the file server creates an interrupt that has been defined and reserved for another device. Such interrupts, which are labeled spurious, generate the following type of message:

```
Spurious hardware interrupt <number> detected
```

This message indicates a serious error in the hardware.

If your file server console displays this message, remove all add-on boards and run SERVER. If the message does not appear, add the boards one at a time until you have discovered which piece of hardware is creating the spurious interrupt. Then contact the vender. (Set the parameter to OFF while you are waiting for a resolution.)

Supported values: ON and OFF

Default: ON

Display Lost Interrupt Alerts = *value*

This parameter controls the alerts about lost interrupts. A message is sent to the file server console whenever a driver or board requests a service with an interrupt call and then drops the request before the CPU can respond to the request. Such interrupts, which are labeled lost, generate the following message:

```
Interrupt controller detected a lost hardware interrupt
```

This message indicates a hardware or driver problem that could degrade performance. Unload all the drivers, and then reload them one at a time to determine which driver has the problem. Then contact the vender of the driver. (Set the parameter to OFF while you are waiting for a resolution.)

Supported values: ON and OFF

Default: ON

Display Disk Device Alerts = *value*

This parameter controls the informational messages about hard disks. A message is generated each time a hard disk is added, activated, deactivated, mounted, or dismounted. For example, if the parameter is set to ON, the following types of messages appear:

```
Device # 0 (20000) ISA Type 043 added
```

```
Device # 0 (20000) ISA Type 043 activated.
```

```
Device # 0 (20000) ISA Type 043 deactivated due
```

Set this parameter to ON if you want such messages displayed when a disk driver is loaded or unloaded, when the file server is booted or downed, or when you are trying to isolate a problem with a disk driver or a hard disk.

Set this parameter to OFF if you are not experiencing any hard disk problems.

Supported values: ON and OFF

Default: OFF

Display Relinquish Control Alerts = *value*

This parameter controls messages about CPU control. If an NLM uses the processor for more than .4 seconds without relinquishing control to other processes, the following types of messages appear:

```
<process name> Process did not relinquish control frequently.
```

```
Module: <module name>
```

```
Code offset in module: <memory address>
```

This parameter controls whether the generated messages are sent to the file server console.

Set this parameter to ON if you are writing your own NLMs.

Set this parameter to OFF if you are not writing your own NLMs.

Supported values: ON and OFF

Default: OFF

Display Old API Names = *value*

This parameter controls messages about NetWare v3.0 API calls. NetWare v3.1x renamed some of the APIs as additional resources were tracked. (Resource tracking protects your file server from loadable modules that try to use more than their share of resources. In addition, resource tracking forces the loadable modules to relinquish all their resources when unloaded.)

The following types of messages appear when a module that uses the old APIs is loaded:

```
Module is using old API: SetInterruptVector
```

```
Module is using old API: ReturnPermanentMemory
```

```
Module is using old API: AllocateReturnablePermMemory
```

The old APIs work, but more slowly than the new APIs. If you receive these messages, contact the vendor of the module.

Set this parameter to ON if you are writing your own NLMs and you are upgrading NetWare v3.0 NLMs to the new v3.1x APIs.

Set this parameter to OFF if you are not upgrading NLMs to NetWare v3.1x.

Supported values: ON and OFF

Default: OFF

Pseudo Preemption Time = *time*

This parameter is available for certain NLMs to keep an NLM process from using too much CPU time. Set this parameter only as your NLM documentation recommends.

Supported values: 1000 to 10000 (raw CPU time, approximately .84 seconds each.)

Default: 2000

Maximum Outstanding NCP Searches = *number*

This parameter determines the maximum number of NetWare Core Protocol (NCP) directory searches that can be processed at the same time.

Normally, only one NCP directory search occurs at a time. Increase this default only if you are using applications that support multiple outstanding directory search operations at the same time and you have problems with corrupted or invalid directory information.

Supported values: 10 to 1000

Default: 51

New Service Process Wait Time = *time*

This parameter determines how long the operating system waits after receiving a request for another service process before making the allocation.

Supported values: 0.3 seconds to 20 seconds

Default: 2.2 seconds

Maximum Service Processes = *number*

This parameter determines the maximum number of service processes that the operating system can create. The number that have currently been allocated can be viewed in MONITOR.

- ◆ Decrease this number temporarily if the file server is low on memory. If the file server is always low on memory, add memory.
- ◆ Increase this number if the service processes number is at the maximum. File servers supporting many users and heavy usage may need more than the default of 20 service processes. However, increasing this number will help only if more than 20 requests are being delayed simultaneously for a disk I/O to be completed.

Supported values: 5 to 40

Default: 20

Display Incomplete IPX Packet Alerts = *value*

This parameter determines if alert messages are displayed when IPX receives incomplete packets.

This parameter can be set only in the server's STARTUP.NCF file.

Supported values: ON and OFF

Default: ON

Replace Console Prompt with Server Name = *value*

This parameter determines if the console prompt should be replaced with the server name.

This parameter can be set in the server's STARTUP.NCF file.

Supported values: ON and OFF

Default: ON

Allow Change to Client Rights = *value*

This parameter determines whether a server can assume the rights of a client. For example, when this parameter is set to ON, a print on the job server is allowed to assume the rights of the submitter of the queue job as it is being submitted.

This parameter can be set in the server's STARTUP.NCF file.

Supported values: ON and OFF

Default: ON

NOTE: The default is for this parameter ON, because certain job servers and third-party applications cannot function without changing to client rights. If the parameter is set to OFF, some of these third-party applications may not function.

SET TIME

Why Use SET TIME?

Use SET TIME to set the date and time kept by the file server.

Command Format

```
SET TIME [month/day/year] [hour:minute:second]
```

Replace the variables with the appropriate information.

Time Format

Enter the time in either standard or military format:

- ◆ 1:15:32 (standard time)
- ◆ 13:15:32 (military time)

Separate the hours, minutes, and seconds with colons (hours:minutes:seconds). You can omit the minute and second entries, but you must include the colon after the hour.

You can also specify AM or PM (for example, 7:14:32 AM). If you do not specify AM or PM, the file server supplies this information for you, based on usual working hours.

The file server always displays the time in the standard format (1:15:32 PM).

Date Format

Enter the date in any of these formats:

- ◆ 11/28/93
- ◆ November 28, 1993
- ◆ 28 November 1993

Additional Information

You can set both the date and the time in the same command, or you can set each one separately. You can enter either the date or the time first. If you replace only one variable, the other variable remains unaffected.

If you do not enter either the date or the time, the file server console displays the current date and time recorded in the file server's clock.

Set the Date and Time on the File Server

Example

For example, to set the date and time on your file server to December 19, 1993 at 2:15 PM, type

```
SET TIME 12/19/93 2:15:00 PM <Enter>
```

or

```
SET TIME December 19, 1993 14:15:00 <Enter>
```

or

```
SET TIME 19 December 1993 2:15:00 <Enter>
```

SET TIMEZONE

Why Use SET TIMEZONE?

Use SET TIMEZONE to configure time zone information in CLIB. This information is used by NLMs that make calls to CLIB. This command does *not* automatically change the file server from standard time to daylight time.

The default value is EST5EDT (Eastern Standard Time, 5 hours from Greenwich Mean Time, Eastern Daylight Time).

Command Format

```
SET TIMEZONE
```

or

```
SET TIMEZONE zone[hours[daylight]]
```

Command Parameters

Replace *zone* with a three-letter abbreviation for the name of the time zone. For example, in the continental United States, one of the following would be used:

Time zone	Zone
Eastern Standard Time	EST
Central Standard Time	CST
Mountain Standard Time	MST
Pacific Standard Time	PST

Replace *hours* with the number of hours west of Greenwich Mean Time (GMT). Use a plus in front of the number if your time zone is east of the GMT time zone line. For example, in the continental United States, you would use one of the following:

Time zone	Hours from GMT
EST	5
CST	6
MST	7
PST	8

Replace *daylight* with a three-letter abbreviation for the daylight saving code. This parameter is optional. If you do not enter this parameter, CLIB assumes that you are on standard time.

For example, in the continental United States, one of the following would be used during the daylight saving months:

Time zone	Daylight zone
EST	EDT
CST	CDT
MST	MDT
PST	PDT

Display the Time Zone Information

To display the time zone, type

```
SET TIMEZONE <Enter>
```

A message similar to the following appears:

```
Timezone is set to: EST5EDT
```

Change the Time Zone Information

To change the time zone to Mountain Standard Time, type

```
SET TIMEZONE MST7 <Enter>
```

To change the time zone to California Pacific Daylight Time, type

```
SET TIMEZONE PST8PDT <Enter>
```

If you live east of London, you enter the hours with a plus, meaning later than Greenwich Mean Time. For example, to set the time zone for Germany, type

```
SET TIMEZONE MEZ+1 <Enter>
```

SPEED

Why Use SPEED?

Use SPEED to display the speed at which the processor is running.

Command Format

SPEED

View the Processor Speed

To view the processor speed, type

SPEED <Enter>

The processor speed rating is determined by the following:

- ◆ CPU clock speed (16 MHz, 20 MHz, 25 MHz, etc.)
- ◆ CPU type (80386SX, 80386, 80486, etc.)
- ◆ Number of memory wait states (0, 1, 2, etc.)

An 80386SX CPU running at 16 MHz should get a rating of about 95. An 80386 CPU running at 16 MHz should get a rating of about 120. If your computer has a slower rating than you expected, check the CPU speed setting.

Some computers have an AUTO or COMMON CPU speed mode that can reduce the clock speed to as little as 6 MHz.

Check your computer's documentation and set the CPU speed setting to the highest setting.

SPOOL

Why Use SPOOL?

Use SPOOL to create, change, or display spooler mappings.

These mappings are necessary to set up default print queues for NPRINT and CAPTURE. They also support applications that make calls to printer numbers rather than to queues.

Command Format

```
SPOOL n [TO] [QUEUE] name
```

For a complete explanation of SPOOL, see *Print Server*.

SPXCONFIG

Why Use SPXCONFIG?

Use SPXCONFIG to configure certain parameters of SPX. You may use SPXCONFIG in an .NCF file, as a console command, or as an interactive menu utility.

Command Format

```
LOAD [path] SPXCONFIG [option[=value]] [option[=value]]
```

Command Parameters

Replace *path* with a full path to the directory containing the SPXCONFIG module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path, the operating system looks for SPXCONFIG in SYS:SYSTEM. (Use SEARCH to set up additional paths for automatic searching.)

If you do not specify a parameter, a menu of parameters appears. You can then select parameters to change interactively. The available options and values are as follows:

Option	Explanation
A=	SPX Watchdog Abort timeout (in ticks)
V=	SPX Watchdog Verify timeout (in ticks)
W=	SPX Ack wait timeout (in ticks)
R=	SPX Default Retry count
S=	Maximum concurrent SPX sessions
Q=1	Quiet mode (suppresses display of changed settings)
H	Displays SPXCONFIG help screen

Set SPX Parameters in a Single Command or in an .NCF File

You may set SPX parameters in a single console command, or add the command to an .NCF file. To do so, use SPXCONFIG *with* the desired parameters. For instructions on editing or creating an .NCF file, see “**EDIT**” on page 64 or “**INSTALL**” on page 69. Following is a sample usage:

```
LOAD SPXCONFIG A=1000 Q=1 <Enter>
```

Use SPXCONFIG Interactively to Change SPX Parameters

Procedure

- 1 To load SPXCONFIG, type

```
LOAD SPXCONFIG <Enter>
```

A menu similar to the following menu appears:

Figure 42 “SPX Configuration Control Program” menu

```
SPX Configuration Control Program (Aug 12 1993)

A.  SPX Watchdog Abort timeout      540
B.  SPX Watchdog Verify timeout     54
C.  SPX Ack wait timeout             108
D.  SPX Default Retry count         10
E.  Maximum concurrent SPX sessions 1000

Enter a command or ESCAPE to exit:
```

The numbers on the right of the parameters are the current settings.

- 2 Press the letter of the parameter you want to change.

Minimum, maximum, and default values for the parameter are shown in parentheses.

- 3 Type in the value you want.

The screen returns to the main menu displaying the value you selected.

Repeat Steps 2 and 3 if you want to change other parameters.

- 4 When you are finished setting SPX parameters, press <Esc> to exit.

SPXS

Why Use SPXS?

Use SPXS to provide STREAMS-based SPX protocol services.

Command Format

```
LOAD [path] SPXS
```

Command Parameters

Replace *path* with a full path to the directory containing the SPXS module. Begin with a DOS drive letter or a NetWare volume. If you do not specify a path and volume SYS: is mounted, the operating system assumes SPXS is in the SYS:SYSTEM directory. (Use SEARCH to set up paths for automatic searching.)

Additional Information

IMPORTANT: Do not unload a protocol-stack NLM such as SPXS until you have unloaded all applications that may use it.

If your module needs STREAMS-based SPX protocol services, load the following modules in the order listed:

1. STREAMS
2. CLIB
3. TLI
4. SPXS

Load SPXS

To load SPXS, type

```
LOAD SPXS <Enter>
```

STREAMS

Why Use STREAMS?

Use STREAMS if you have a loadable module that requires the CLIB loadable module or uses STREAMS-based protocol services. STREAMS must be loaded before CLIB is loaded.

Command Format

```
LOAD [path] STREAMS
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Load STREAMS

To load STREAMS, type

```
LOAD STREAMS <Enter>
```

TIME

Why Use TIME?

Use TIME to display the date and time kept by the file server's clock.

Command Format

TIME

Additional Information

To reset the file server's date or time, use SET TIME.

View the File Server's Date and Time

To view the date and time kept by the file server, type

TIME <Enter>

A message similar to the following appears:

September 3, 1993 3:11:25 PM

TLI

Why Use TLI?

Use TLI to provide TLI communication services. TLI requires STREAMS and CLIB, so TLI loads them automatically if you haven't loaded them. You also need to load one or more protocol service NLMs, such as SPXS or IPXS.

Command Format

```
LOAD [path] TLI
```

Command Parameters

Replace *path* with a full directory path to the directory containing the module. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is located in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

Additional Information

After loading TLI, load the protocol service modules.

Load TLI

To load TLI, type

```
LOAD TLI <Enter>
```

TRACK OFF

Why Use TRACK OFF?

Use TRACK OFF to prevent the file server from displaying network advertising packets that are received or sent on the Router Tracking Screen. This command turns off the Router Tracking Screen.

Command Format

TRACK OFF

Turn Off the Router Tracking Screen

To turn off the Router Tracking Screen, first get to the console prompt by typing <Alt><Esc>. Then type

TRACK OFF <Enter>

See [“TRACK ON” on page 305](#).

TRACK ON

Why Use TRACK ON?

Use TRACK ON to display the Router Tracking Screen and to make it the *active* screen. This command signals the router to display all server and network advertising packets that are received or sent.

Command Format

TRACK ON

Signal the Router to Display Packets

To turn on the Router Tracking Screen, type

TRACK ON <Enter>

See [“TRACK OFF” on page 304](#); [“DISPLAY NETWORKS” on page 59](#); [“DISPLAY SERVERS” on page 61](#); and [“RESET ROUTER” on page 227](#).

Additional Information

TRACK ON displays three types of information:

- ◆ Server
- ◆ Network
- ◆ Connection requests

This information is formatted according to whether the file server is receiving the information (IN), broadcasting the information (OUT), or receiving a connection request.

Incoming Information

Incoming information looks similar to the following:

Figure 43 Router Tracking Screen incoming information

IN	[00D0C200:00001B026C09]	10:53:01am	BILLYBOB	5
IN	[00D0C200:00001B026C09]	10:53:01am	00001EEE	2/3

Each item in the display is described below.

IN	Indicates that the message is incoming.
00D0C200	Indicates the network number of the file server sending the packet. NetWare v3.1x file servers broadcast on their internal and cabling network numbers.
0001B026C09	Indicates the node address of the file server sending the packet.

Either server or network information follows the node address.

Server Information

BILLYBOB	Indicates the name of a file server known by the sending file server.
5	Indicates the number of hops from the sending file server to this file server.

Network Information

00001EEE	Indicates the network number of a network known by the sending file server.
2/	Indicates the number of hops from the sending file server to this network.
/3	Indicates the number of ticks (1/18th of a second) that a packet would take to reach this network from the sending file server.

Outgoing Information

Outgoing information looks similar to the following:

Figure 44 Router Tracking Screen outgoing information

```
OUT [1986DAD0:FFFFFFFFFFFF] 11:25:47am  A-SOURCE____ 3
      GILA          3  SAGUARO____ 3  BACK7          3
      ARCserve@BAC  4
OUT [00D0C200:FFFFFFFFFFFF] 11:25:47am  ROCK          1
```

Each item in the display is described below.

OUT	Indicates that the message is outgoing.
1986DAD0	Indicates the network number of the file server sending the packet. NetWare v3.1x file servers broadcast on their internal and cabling network numbers.
FFFFFFFFFFFF	Indicates that the message is for all nodes on the network.

Either file server or network information follows the node address.

Connection Request

When a workstation boots and loads the NETx file, a “GET Nearest Server” request is broadcast on the network to which the workstation is cabled. Any file server that is connected can receive the message and respond to the workstation with a “Give Nearest Server” response. The workstation initially attaches to the first file server to respond to the “Get Nearest Server” request.

UNBIND

Why Use UNBIND?

Use UNBIND to remove a communication protocol from the LAN driver of a network board or to change the network number. Use UNBIND to disable communication on a specific board.

The following tasks are described in this section:

Task	Page
Unbind a protocol from a driver	“Unbind a Protocol from a Driver” on page 310
Change the network number for the cabling	“Change the Network Number for the Cabling” on page 311

Command Format

```
UNBIND protocol [FROM] LAN_driver [driver_parameter...]
```

Command Options

Replace *protocol* with *IPX*. If you have bound protocols other than *IPX*, replace *protocol* with the name of the protocol you want to unbind.

Replace *LAN_driver* with a driver you are currently using. The following drivers ship with NetWare:

3C503
3C505
3C523
NE2
NE2-32
NE1000
NE2000
NE3200
PCN2
TOKEN
TRXNET

Specify a *driver_parameter* only when you have more than one network board of the same type in your file server. You must tell the operating system which board to unbind the communication protocol from.

- ♦ If you have multiple boards, you must unbind each one separately.
- ♦ If you do not include *driver_parameter* at the command line, the operating system prompts you for the appropriate network board.

Replace *driver_parameter* with one or more of the following parameters. Include the parameters that make the network board unique from all other installed network boards of its type. When the driver parameter is included with the UNBIND command, the driver parameter must be enclosed in square brackets.

DMA=number

Identifies the DMA channel the driver is using for the network board. Use the same DMA channel that you used when you loaded the driver.

INT=number

Identifies the interrupt the driver is using for the network board. Use the same interrupt that you used when you loaded the driver.

MEM=number

Identifies the memory address the driver is using for the network board. Use the same memory address that you used when you loaded the driver.

PORT=number

Identifies the I/O port the driver is using for the network board. Use the same I/O port that you used when you loaded the driver.

SLOT=number

Identifies the network board by the slot that the network board was installed in. This parameter is used by microchannel and EISA computers. Use the same slot number that you used when you loaded the driver.

Unbind a Protocol from a Driver

The steps for unbinding a protocol from a driver vary with how the driver has been loaded. Select the example that fits your situation.

Driver Loaded Only Once

To unbind a protocol when the driver has only been loaded once, type

```
UNBIND IPX FROM LAN_driver <Enter>
```

Replace *LAN_driver* with the name of the LAN driver you want to unbind.

NOTE: To prevent the driver from binding automatically when the file server is booted, delete the following line from the AUTOEXEC.NCF file:

```
BIND IPX TO LAN_driver NET=number
```

For instructions on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Driver Loaded More Than Once

When you have loaded the driver more than once, you need to tell the operating system which board you want to unbind the protocol from.

Specify the board by including parameters or by selecting the board from a list. Complete one of the following (these examples show how to unbind the NE2000 driver from IPX):

- ◆ Type the command and include the driver parameters in brackets:

```
UNBIND IPX FROM NE2000 [INT=4] <Enter>
```

- ◆ Type the command without the driver parameters:

```
UNBIND IPX FROM NE2000 <Enter>
```

The operating system will list the network boards installed in your file server. Enter the number of the board.

NOTE: To prevent the driver from binding automatically when the file server is booted, delete the following line from the AUTOEXEC.NCF file:

```
BIND IPX TO NE2000 [INT=4] NET=26
```

For instructions on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

Change the Network Number for the Cabling

Procedure

- 1** At the console prompt of the file server, type
`UNBIND IPX FROM LAN_driver <Enter>`
Replace *LAN_driver* with the name of the LAN driver whose network number you want to change.
- 2** Type
`BIND IPX TO LAN_driver <Enter>`
Replace *LAN_driver* with the name of the LAN driver you used in [Step 1](#).
- 3** When prompted for the network number, type in the new network number.
- 4** Load INSTALL and edit the network number in the AUTOEXEC.NCF file.
For information on editing the AUTOEXEC.NCF file, see [“Edit the AUTOEXEC.NCF File” on page 98](#).

UNLOAD

Why Use UNLOAD?

Use UNLOAD to unload a loadable module that was previously loaded with the LOAD command. When the module is unloaded, all resources are returned to the operating system.

Use UNLOAD to unload old drivers so that updated drivers can be loaded.

IMPORTANT: Read [“Additional Information” on page 312](#) before unloading any modules.

The following tasks are described in this section:

Task	Page
Unload a loadable module	“Unload a Loadable Module” on page 314
Troubleshooting UNLOAD	“Troubleshooting UNLOAD” on page 314

Command Format

```
UNLOAD loadable_module
```

Replace *loadable_module* with the name of the module you want to unload.

Additional Information

Read the following information *before* unloading LAN drivers, name space, or disk drivers.

LAN Drivers

When you unload a LAN driver, the driver is automatically unbound from all communication protocols and removed from all network boards to which the driver has been linked. If the driver has been loaded more than once and you want to disable the communication on only one board, use the UNBIND command instead of the UNLOAD command.

Once the LAN driver is unloaded, logged-in users who have been using the network boards to communicate with the server will lose their connections when they attempt to access the server. They will receive the following network error:

```
Network error on Server <fileserver>: Error receiving from
network. Abort, Retry?
```

These users should retry once to see if an alternate bridge to the file server is available on another network.

If the retry produces another network error, they should wait until the LAN driver is reloaded and bound to the communication protocols. Then they should retry.

These users must establish a connection within 15 minutes. If the connection is broken for more than 15 minutes, the file server watchdog will terminate the workstation's connection.

NOTE: If you plan to have the LAN driver unloaded for 15 minutes or longer, you should have users log out before unloading the LAN driver.

Name Space

Before unloading name space modules, dismount all volumes that are using the module. These volumes cannot be remounted until the module is loaded again.

Disk Drivers

Before unloading a disk driver, dismount all volumes stored on the hard disks connected to the controller or host bus adapter. If you fail to dismount all the volumes, the operating system will warn you that the driver is being used by mounted volumes and will list the volumes that are using the driver.

NOTE: If you override the warning and unload the disk driver without dismounting the volumes, the file server will automatically dismount the affected volumes. Users who are logged in will receive the following message:

```
Volume "volume names" dismounted due to drive deactivation.
```

Unload a Loadable Module

Before unloading a loadable module, read the cautions about unloading disk driver, LAN driver, and name space modules in [“Additional Information” on page 312](#). Never unload a module that other modules depend on.

To unload a module, type “UNLOAD” and the name of the module. For example, to unload MONITOR type

```
UNLOAD MONITOR <Enter>
```

See [“LOAD” on page 109](#) and [“MODULES” on page 175](#).

Troubleshooting UNLOAD

When a module is unloaded, sometimes you see a warning message, the module refuses to unload the module, or the system abends. Possible causes and solutions are described here.

Warning Messages are Displayed

If the loadable module did not return all its resources when it unloaded, a message similar to the following appears:

```
<module name> -Alloc Memory <resource tag> did not release  
  <number> Alloc Short Tern Memory <resource> Bytes
```

Contact the vender for an updated version of the module.

Module Will Not Unload

Some modules depend on other modules to define variables. For example, RSPX depends on REMOTE. If you try to unload REMOTE before unloading RSPX, the following message appears:

```
Unable to unload module REMOTE.NLM (error 2)
```

RSPX must unload before REMOTE can load. Check with the documentation that came with the loaded modules. (Use MODULES to list the currently loaded modules.) Determine which module is using the module you are trying to unload.

File Server Abends

If the file server abends when you unload a module, do not load that module again. The module failed to return allocated resources correctly to the operating system. Check with the developer for an upgraded version of the module.

UPS

Why Use UPS?

Use UPS when you attach an uninterruptible power supply (UPS) to your file server. UPS is the software link between the file server and the UPS device connected to the file server.

NOTE: The UPS loadable module must be loaded to activate UPS monitoring.

Command Format

```
LOAD [path]UPS [type port discharge recharge]
```

Command Parameters

Replace *path* with a full path. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: is mounted, the operating system assumes that the loadable module is in the SYS:SYSTEM directory. (Use SEARCH to set up additional paths for automatic searching.)

The parameters are explained here. If you do not enter the parameters at the command line, you will be prompted for them.

type= name

Replace *name* with the name of the interface board for your UPS:

DCB

EDCB

STANDALONE

KEYCARD

MOUSE

OTHER

Default: DCB

NOTE: If you enter STANDALONE and the software does not accept the name, try entering KEYCARD. If you allow the software to prompt you for the parameters, follow the instructions on the screen.

port = number

Replace *number* with a hexadecimal number corresponding to the jumper setting on the board.

DCB—346, 34E, 326, 32E, 286, 28E

EDCB—380, 388, 320, 328

Keycard—230, 238

Mouse (no port number required)

Other (see accompanying board documentation)

Standalone—240, 231

discharge = number

Replace *number* with an estimate of the number of minutes the network can operate on battery power before depleting the battery.

Consult the battery's documentation for time estimates. You may need to reduce the discharge time as your UPS becomes older.

recharge = number

Replace *number* with an estimate of the minutes the battery will need to recharge after the network has been on battery power.

You may need to increase the recharge time as your UPS becomes older.

Add an Uninterruptible Power Supply (UPS)

Procedure

- 1** Install the UPS hardware (board and power supply) and connect the power.

See the documentation that comes with the UPS and the board for appropriate jumper settings.

2 Load the UPS module and enter the parameters in one of these two ways:

- ◆ Type the command, including the parameters:

```
LOAD UPS TYPE=DCB PORT=346 DISCHARGE=20  
RECHARGE=120 <Enter>
```

- ◆ Type the command and answer the screen prompts for type, I/O port, discharge time, and recharge time:

```
LOAD UPS <Enter>
```

NOTE: To load UPS automatically whenever the file server is booted, add the command to the AUTOEXEC.NCF file. For example, to load UPS with a DCB, add the following line:

```
LOAD UPS TYPE=DCB PORT=346 DISCHARGE=20 RECHARGE=120
```

Troubleshooting UPS

You must configure the controller to match the UPS that you have. If the configuration does not match the UPS hardware, the driver may either fail to load or function incorrectly when loaded. One of the following could cause the driver to fail or to function incorrectly:

- ◆ The controller's configuration is different from the configuration you entered as you loaded UPS. Check the configuration of the controller and enter the correct port.
- ◆ The jumpers controlling online and offline status do not agree with the configuration on the UPS. For example, if the jumpers are set incorrectly, the UPS will signal the file server that it is on battery power when commercial power is still on. Change the jumpers on the controller to match the UPS.

We recommend that you test the UPS functionality by unplugging the power and waiting 20 seconds to see if the commercial "power off" message appears.

IMPORTANT: This test should be run only after all users have logged out and all LAN and disk drivers have been unloaded. Unloading the LAN and disk drivers protects your data from corruption if the UPS fails to function correctly.

UPS STATUS

Why Use UPS STATUS?

Use UPS STATUS to check the uninterruptible power supply (UPS) attached to the file server.

NOTE: If the UPS module has not been loaded, executing UPS STATUS gives you the error “??? Unknown command???”

Command Format

```
UPS STATUS
```

Check Power Supply Status

To check the status of your uninterruptible power supply, type

```
UPS STATUS <Enter>
```

A screen similar to the following appears:

Figure 45 “UPS Status” screen

```
UPS Status for Server SPEEDY
Power being used: Commercial
Discharge time requested: 20 min.   Remaining: 20 min.
Battery status: Recharged
Recharge time requested: 160 min.   Remaining: 0 min.
Current network power status: normal

NOTICE: If your battery is over 6 months old, you may need to
lower the discharge time. (Consult the UPS
documentation for details.)
```

Each of the lines on the screen is explained here. To change the time parameters, see “UPS TIME” on page 321.

Power being used. The UPS is using either commercial power or battery power.

Discharge time requested/remaining. The first number is an estimate of the time that the network can run safely on battery power.

The second number is the safe time remaining if the network is currently on battery power. If the network is running on commercial power and the battery is charged, this number is the same as the first number.

Battery status. The battery is either recharged, low, or being recharged.

If the battery status is low, the battery should be repaired or replaced.

Recharge time requested/remaining. The first number is an estimate of the time that the battery needs to recharge after the battery has been totally discharged.

The second number is an estimate of the time needed to recharge the battery.

- ♦ If the network is running on commercial power, the time needed to recharge the battery is 0 if the battery is fully charged.
- ♦ If the network is running on battery power, this number increases as the battery is discharged. The number indicates the time the battery needs to recharge.

Current network power status. This field shows one of the following:

<i>Normal</i>	Running on commercial power.
<i>Server down</i>	Running on battery power.
<i>Server going down</i>	Running on battery power; enough in __ minutespower is left to run the network for the indicated number of minutes.

UPS TIME

Why Use UPS TIME?

Use UPS TIME to change the amount of time you want to allow the network to function on battery power and the time you estimate the battery needs to fully recharge.

This command is only valid if the UPS loadable module has been loaded.

NOTE: If the UPS module has not been loaded, executing UPS TIME gives you the error “??? Unknown command???”

Command Format

```
UPS TIME [discharge recharge]
```

Command Parameters

discharge = n

Replace *discharge* with an estimate of the number of minutes the network can operate on battery power before depleting the battery.

Consult the battery’s documentation for time estimates. You may need to reduce the discharge time as your UPS grows older.

recharge = n

Replace *recharge* with an estimate of the minutes needed to recharge the battery after the network has been on battery power.

Consult the battery’s documentation for time estimates. You may need to increase the recharge time as your UPS grows older.

Change the UPS Discharge and Recharge Times

Enter the parameters for the discharge and recharge times in one of the following ways:

- ◆ Type the command and include the parameters:

```
UPS TIME DISCHARGE=20 RECHARGE=120 <Enter>
```

- ◆ Type the command and answer the prompts for discharge time and recharge time:

```
UPS TIME <Enter>
```

VERSION

Why Use VERSION?

Use VERSION to display the file server's version information and copyright notice.

Command Format

`VERSION`

View Version Information and Copyright Notice

To view the file server version information and copyright notice, type

`VERSION` <Enter>

A message similar to the following appears:

```
Novell NetWare 386 v3.12 9/3/93(c) Copyright 1988, 1993
  Novell, Inc.
```

```
All rights reserved.
```

VOLUMES

Why Use VOLUMES

Use `VOLUMES` to list the volumes currently mounted on the file server.

Command Format

```
VOLUMES
```

View Mounted Volumes

To view a list of volumes on the file server, type

```
VOLUMES <Enter>
```

A message similar to the following appears:

```
The following volumes are mounted:
```

```
SYSMAC
```

VREPAIR

Why Use VREPAIR?

Use VREPAIR to correct volume problems or to remove name space entries from File Allocation Tables and Directory Entry Tables.

IMPORTANT: If you upgrade to NetWare v3.12 from another version and then need to return to that version, make sure you use the version of VREPAIR that matches the operating system.

The following tasks are described on the pages indicated:

Task	Page
Repair a volume or remove name space entries	“Repair a Volume or Remove Name Space Entries” on page 327
Set VREPAIR options	“Set VREPAIR Options” on page 329

Command Format

```
LOAD [path]VREPAIR
```

Command Parameters

Replace *path* with a full path to the directory containing VREPAIR. Begin with a DOS drive letter or a NetWare volume name. If you do not specify a path and volume SYS: has been mounted, the operating system assumes that the VREPAIR loadable module is located in the SYS:SYSTEM directory.

Additional Information

VREPAIR comes on the *NetWare Operating System-2* diskette. Copy VREPAIR.NLM and the VREPAIR name space support modules (V_namespace.NLM) to the boot partition of your file server. Then, if volume SYS: fails to mount, you can load VREPAIR and run it from the boot directory.

Minor problems can occur if the *primary* File Allocation Table (FAT) or Directory Entry Table (DET) becomes corrupted. VREPAIR compares the primary tables with their *mirrored* counterparts. (The operating system keeps two copies of all tables. If hard disks are mirrored, then four copies are kept.)

VREPAIR checks the sets of tables for errors and uses the most correct table entry as the corrected entry. VREPAIR then writes the *corrected* entry to both the primary and mirrored tables. VREPAIR may have to delete some corrupted files or tables.

Use VREPAIR in these situations:

- ◆ A hardware failure has either prevented a volume from mounting or caused a disk read error.
- ◆ A power failure has corrupted a volume.
- ◆ The file server console displays a mirroring error when the server boots.
- ◆ The file server displays memory errors and cannot mount a volume after a name space (such as Macintosh) has been added to the volume. You must either add more memory to the file server or remove the newly added name space. For instructions, see “[Set VREPAIR Options](#)” on page 329.

The following kinds of errors in FATs or DETs signal bad blocks:

Data mirror mismatch errors

Fatal DIR errors

Read errors

Multiple allocation errors

Write errors

VREPAIR can run on a bad volume that you have dismounted while other file server volumes are functioning. After you finish running VREPAIR, you can mount the repaired volume (in most cases).

Repair a Volume or Remove Name Space Entries

Typically, you cannot mount a volume if it has had even minor damage. Occasionally the volume mounts but causes an error in the process. Complete these steps to repair the volume.

Procedure

- 1 If the volume you want to repair is mounted, refer to “Connection Information” on the “Available Options” screen in MONITOR to check for users who have open files on the volume you need to dismount.

Use BROADCAST or SEND to warn these users to close their files and move to another volume.

- 2 Dismount the volume.

```
DISMOUNT volume_name <Enter>
```

Replace *volume_name* with the volume you need to repair.

- 3 Do one of the following:

- ♦ If volume SYS: is mounted, type

```
LOAD VREPAIR <Enter>
```

- ♦ If volume SYS: is not mounted, set a path to VREPAIR.NLM and the name space support modules. (See “SCAN FOR NEW DEVICES” on page 238.)

- 4 Check the VREPAIR options.

You can use these options to control whether name space information is deleted and how FAT and DET information is written to disk. (See “Set VREPAIR Options” on page 329.)

- 5 Select “Repair A Volume” from the “Options” menu.

- 6 If more than one volume is not mounted, select the volume to be repaired from those listed.

If only one volume has been dismounted, a screen similar to the following appears:

Total errors:

Current settings:

Pause after each error

Do not log errors to a file

Press F1 to change settings

- 7 If VREPAIR seems to be finding a large number of errors, you may want to change one or both of the current settings.

These settings can be changed while the program is running. To set either option, press <F1>.

- ◆ Select Option 1 if you do not want VREPAIR to pause after each error.

A screen appears, describing the error that was corrected. Press any key to continue.

- ◆ Select Option 2 if you want VREPAIR to log errors in a text file.

Any errors found will be written to a file you specify. The repaired files may no longer be valid and may need to be restored from a backup.

- ◆ Select Option 3 to stop the repair of the volume.

The size of the volume determines the time it takes to complete VREPAIR. If the volume is over 1000 MB, the process can take at least 30 minutes.

- 8 When VREPAIR has finished running, the screen displays information similar to the following:

Figure 46 VREPAIR information screen

```
Done checking volume.  
Number of FAT repairs: 3  
Number of directory repairs: 1  
Write repairs to the disk? (Y/N): Y
```


Answer “Yes” to the prompt to write repairs to the disk.

- 9** Press any key to return to the “Options” menu.
- 10** Type “0” to exit.
- 11** If you are unable to mount the volume after running VREPAIR, you must delete the volume, recreate the volume using INSTALL, and restore the data from a backup file.

Set VREPAIR Options

To change an option, complete the following steps.

Procedure

- 1** Load VREPAIR by typing
`LOAD VREPAIR <Enter>`
If volume SYS: is not mounted, include a path to VREPAIR.NLM.
- 2** Type the number for “Set VREPAIR Options” and press <Enter>.
- 3** Type the number of the option you want to change and press <Enter>.
See [“Available Options” on page 329](#) for a description.
- 4** Answer the confirmation prompts.
The new setting is displayed in the “Current Vrepair Configuration” list. For instructions on how to repair a volume, see [“Repair a Volume or Remove Name Space Entries” on page 327](#).

Available Options

This section describes the options available in VREPAIR.

Remove Name Space Support from the Volume/ Quit if aVREPAIR Name Space Support NLM Is Not Loaded

These options control whether name space support for non-DOS files is retained in the volume tables. If you have added a name space to a volume and the operating system no longer has enough memory to mount the volume, select “Remove Name Space support from the volume.” Then select the name space you want to delete. To be successful in deleting the name space entries, VREPAIR must be able to find the name space support module (V_namespace.NLM).

If you remove a name space, the accompanying extended file information is destroyed. For example, if you remove Macintosh name support, the Macintosh long names, the finder icons, and the resource forks are destroyed. (The DOS name and its data file are kept and are accessible from DOS workstations.)

Default: Quit If a Vrepair Name Space Support NLM Is Not Loaded

Write Only Changed Directory and FAT Entries Out to Disk/ Write All Directory and FAT Entries Out to Disk

These options control the changes that are made to the FATs and Directory Entry Tables. The first time you attempt to repair a volume, write only the changes to disk.

If the first attempt fails to repair the volume and the volume resides on mirrored disks, select “Write All Directory and FAT Entries Out to Disk” to force the tables on both hard disks to be updated. *Do not* use this option if the file server crashed during the updating of important files. Instead, for other possible solutions, see [“A Volume Cannot Be Mounted Because of Corrupted Directory Entry Tables or FATs” on page 391.](#)

Default: Write Only Changed Directory and FAT Entries Out to Disk.

Keep Changes in Memory for Later Update / Write Changes Immediately to Disk

When only a few errors need to be corrected, VREPAIR runs faster by saving all changes in memory and then writing them to disk at the end. However, VREPAIR runs very slowly when more than 1,000 changes have to be kept in memory. The memory needed to store the changes can also cause the file server to run out of memory.

- ◆ Select “Keep Changes in Memory for Later Update” if the volume problem occurred when only a few users were updating files.
- ◆ Select “Write Changes Immediately to Disk” if the volume problem occurred during peak usage or if you are removing name space entries.

Default: Keep Changes in Memory for Later Update.

2

Remote Management

Overview

The information in this section has been organized into the following sections:

- ◆ **“Introduction” on page 332.** This section explains what remote management is, who can use it, and how it works. It also explains the different types of communication links that can be set up using remote management.
- ◆ **“Setting Up Remote Management” on page 339.** This section explains the hardware and software requirements of remote management and gives procedures for the following:
- ◆ **“Adding Remote Capability to a NetWare v3.1x File Server” on page 341.**
- ◆ **“Adding Remote Capability to a Standalone PC” on page 343.**
- ◆ **“Using a Remote Console” on page 343.** This section discusses activating and using the remote console. Menus and function keys specific to the remote console program are explained. This section also contains instructions for remote administration tasks that can be completed from the remote console’s “Available Options” menu.

Introduction

NetWare's remote management capability was developed as the NetWare Remote Management Facility (RMF). Remote management allows you to manage all of your NetWare file servers (v3.1 and later) from one location. It gives you easier access to and greater control of the file servers, no matter where those servers are located.

After setting up a remote console at a workstation, you can see and control all the file servers that have the appropriate remote management software loaded.

You have greater control of file server security when you use remote management. Because a workstation can act as a file server console, you can remove the keyboard and monitor from your file server, or you can lock the file server in an area where you can control access.

Remote management works with NetWare v3.1x operating system software. It can cross all NetWare links and work with all certified NetWare platforms and DOS workstations.

When you establish a communication link to a file server, you can perform the following functions:

- ◆ Use console commands as you would at the file server console.
- ◆ Scan directories and edit text files in both DOS and NetWare partitions on a remote file server.
- ◆ Transfer files to (but not from) a remote file server.
- ◆ Add an existing NetWare v3.1x file server to an established remote management network.
- ◆ Reboot a file server from a remote console.

Who Can Use Remote Management?

For security reasons, *only NetWare supervisors and remote console operators* can use remote management.

These users must have appropriate rights and must pass password security checks before they can access a file server from a remote console. The remote console does not disable or bypass the MONITOR keyboard lock. If this lock is set, you must enter the password to gain access.

A *remote console operator* uses a remote password to open a communication session with a file server. The remote console operator must have File Scan and Read rights in SYS:SYSTEM. After successfully passing security checks, the operator can perform the tasks described in this manual and execute console commands.

A *NetWare supervisor* can open a remote console session using either the remote or the supervisor password. However, volume SYS: must be mounted in order for the supervisor password to work. Although the supervisor password allows remote access to a file server, only remote management tasks can be performed. A NetWare supervisor cannot create users or assign rights from a remote console.

How Does Remote Management Work?

Remote management establishes a communication link with a file server. This enables a workstation or standalone PC to act as a file server console, or “remote console.”

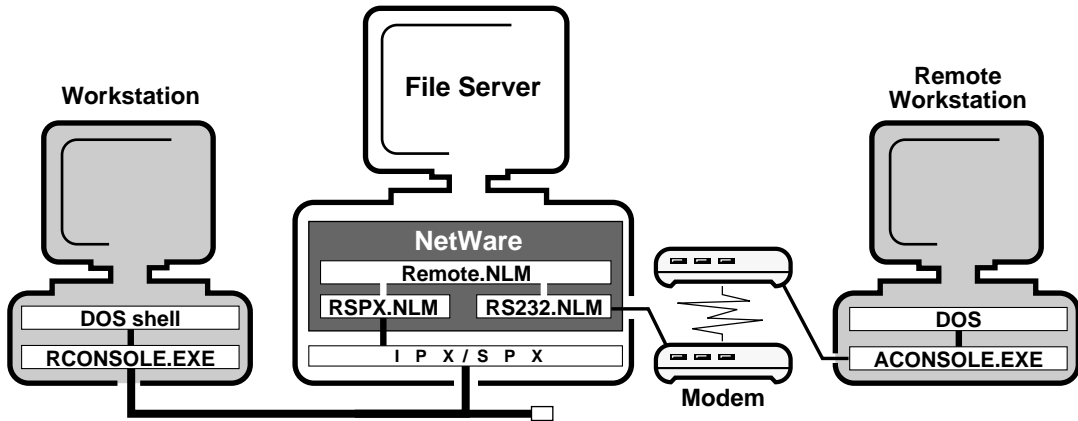
The software that manages the remote console does not disable the regular console keyboard. Remote management supports concurrent connections to a file server. This feature is helpful for training both inexperienced file server supervisors and managers. It is also helpful for troubleshooting.

For example, a remote console operator can open a communication session with a file server and enter commands to help a local supervisor. Both users can enter keystrokes, and both the file server screen and the remote console screen display file server information.

The remote console does not need to remain dedicated until a process is completed. After a server process is initiated, the remote console can terminate the session without affecting the process.

Figure 47 shows the software needed for remote management. Following the figure are more detailed descriptions of the software.

Figure 47 Software necessary for remote management



File Server Software for Remote Management

Both file server and workstation software are needed for remote management. Files with an .NLM extension are loaded from the file server.

- ♦ *REMOTE.NLM*. This loadable module manages the reception and transmission of keyboard and monitor information to and from the communications drivers.
- ♦ *RSPX.NLM*. This loadable module is a media-specific communications driver that provides SPX support for REMOTE.NLM. This module also advertises that the file server is available for remote access.
- ♦ *RS232.NLM*. This loadable module is an asynchronous communications driver that initiates the file server's communication port and transfers screen and keystroke information to and from REMOTE.NLM.

Workstation Software for Remote Management

Files with an .EXE extension are loaded from the workstation.

- ♦ *ACONSOLE.EXE*. This utility works like many standard communication programs in that it allows control of a client modem (to dial, hang up, etc.). This utility also controls the transfer of screen and keystroke information to and from the remote file server.
- ♦ *RCONSOLE.EXE*. This utility is a communication program that turns a workstation into a remote console. This utility also controls the transfer of screen and keystroke information to and from the remote file server.

What Types of Communication Links Can I Set Up?

You can establish three types of connections with file servers on local and wide area networks:

- ♦ *Direct link*. Set up a direct link to file servers physically attached to your network through an internetwork cable or T1 line.
- ♦ *Asynchronous link*. Attach asynchronously to a file server at a remote location, such as a wide area network, using a modem.
- ♦ *Redundant link*. Establish redundant links, which are both direct and asynchronous connections to the same file server.

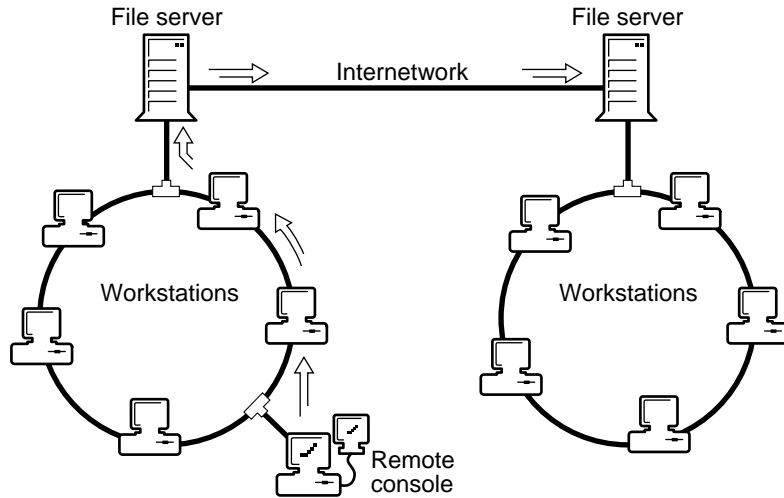
These connections are explained in further detail in the following sections.

Direct Link

One way to establish a remote session with a file server is by using a direct connection link. This works for file servers on a local or wide area network, where the servers are connected by cabling or by a T-link using IPX/SPX protocol.

In **Figure 48**, the file servers are part of an internetwork connected by cabling. The workstation acting as a remote console can log in to a file server on a LAN and then open a communication session with a remote server across the internetwork.

Figure 48 Remote session using a direct link

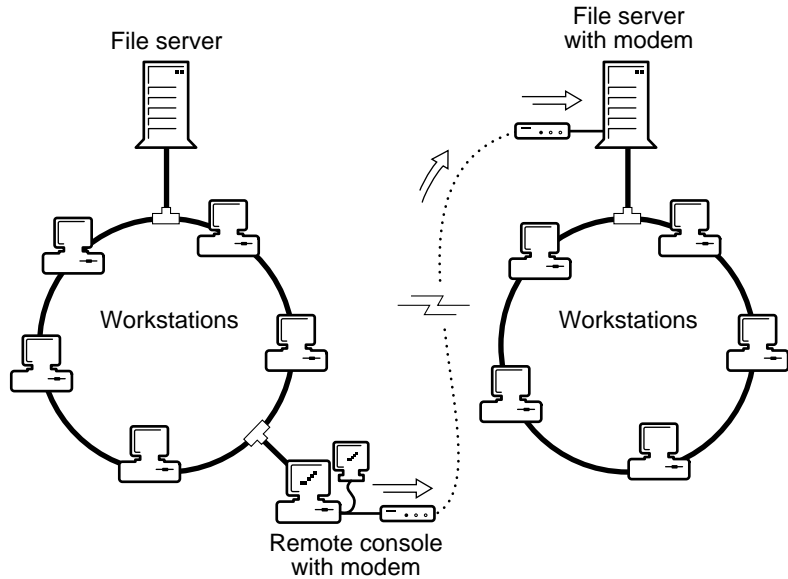


Asynchronous Link

Another way of establishing a remote session is through modems. You can use this type of connection to open a communication session with a file server on a different internetwork.

In [Figure 49](#), the workstation acting as a remote console can log in to the file server on the LAN and then dial the remote file server modem.

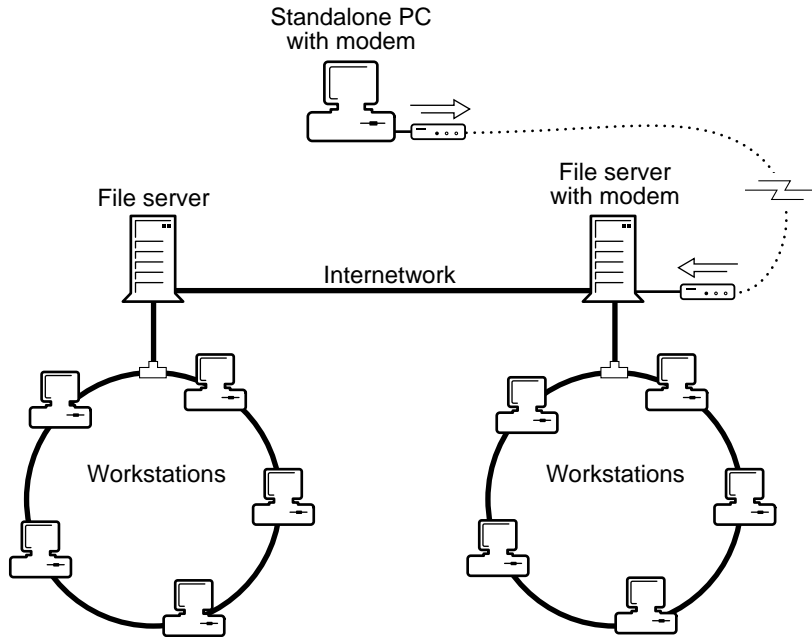
Figure 49 Remote session using an asynchronous link (via a file server)



You can also establish an asynchronous session using a standalone PC. You do not have to connect through a file server on a LAN.

In [Figure 50](#), a standalone PC with a modem has an asynchronous connection to a file server with a modem.

Figure 50 Remote session using an asynchronous link (via a standalone PC)



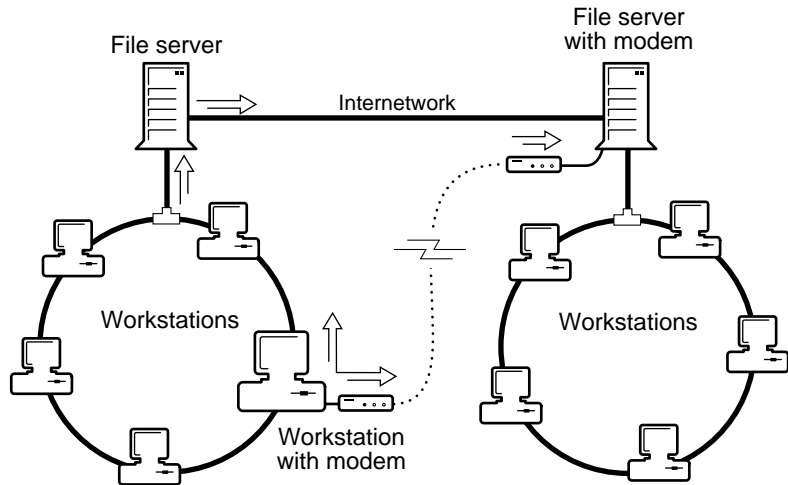
Redundant Link

You also have the option of setting up redundant communication links to a file server. The term *redundant link* means that you set up both direct and asynchronous connections to a file server. Redundant links are possible because the software for a direct link and a modem link can coexist on a file server.

This type of setup has certain advantages. For example, if a LAN driver or disk driver is unloaded, or if volume SYS: is dismounted, a direct communication link will be lost. The network supervisor or remote console operator can open an asynchronous session with the file server and reboot the server.

In [Figure 51](#), the remote console can open either a direct or an asynchronous communication session with the file server.

Figure 51 Remote session using a redundant link



Setting Up Remote Management

Before you set up remote management, be sure your hardware and software meet the requirements listed in this section. To use a remote console to manage a network, you must load appropriate software on a workstation or standalone PC and on the file servers you want to access.

To prevent unauthorized access to file servers, you should keep remote management software, particularly RCONSOLE.EXE and ACONSOLE.EXE, in your SYSTEM directory.

Two setup options are described in this section. Review the choices carefully and follow the instructions for the situation that applies to you.

- ♦ [“Adding Remote Capability to a NetWare v3.1x File Server”](#) on page 341
- ♦ [“Adding Remote Capability to a Standalone PC”](#) on page 343.

Hardware and Software Requirements for Remote Management

In order to run remote management software, file servers and workstations or standalone PCs must meet the following requirements.

File Server Requirements

The hardware requirements for a file server include the following:

- ♦ 386- or 486-based microcomputer
- ♦ 48 KB of available memory to run NLMs
- ♦ A Hayes-compatible modem capable of communicating at 2400, 4800, or 9600 baud (for asynchronous connections)

Software requirements for the file server include the following:

- ♦ NetWare v3.0 or later
- ♦ IPX/SPX network protocols

Workstation Requirements

Hardware requirements for workstations or standalone PCs include the following:

- ♦ Novell-tested-and-approved computer type
- ♦ Novell-tested-and-approved network adapter boards
- ♦ At least 200 KB of memory
- ♦ A Hayes-compatible modem capable of communicating at 2400, 4800, or 9600 baud (for asynchronous connections)
- ♦ Workstation or standalone PCs must be running DOS 2.x or later.

Adding Remote Capability to a NetWare v3.1x File Server

These instructions are for adding remote management capability to a file server running NetWare v3.1x. *They do not apply to new file servers or to file servers running v3.0 or earlier.*

In order for you to load the modules discussed in this section, they must be on the file server to which you want to add remote capability. If you have not already done so, copy the appropriate files to the server. For file server security, you should keep remote management files in the SYS:SYSTEM directory.

NOTE: If you want the modules for remote console access to be loaded automatically each time the file server is booted, place the commands discussed in this section in an AUTOEXEC.NCF file. The only condition is that the AUTOEXEC.NCF file must load REMOTE.NLM first.

Load REMOTE.NLM

For all types of connection links, you must load REMOTE.NLM.

Type

```
LOAD [path]REMOTE [password] <Enter>
```

If REMOTE.NLM is in the SYS:SYSTEM directory, you do not need to specify a path. If the module is in a different directory, replace *path* with the directory path where the module is located. Begin with a DOS drive letter or a NetWare volume name.

Replace *password* with a unique password to be used by the remote console operator (up to 47 characters). If you do not enter a password, you will be prompted for one.

Load RSPX.NLM

If you want to access a file server by a direct communication link, you must load RSPX.NLM after you load REMOTE.NLM.

Type

```
LOAD [path]RSPX <Enter>
```

If RSPX.NLM is in the SYS:SYSTEM directory, you do not need to specify a path. If RSPX.NLM is in a different directory, replace *path* with the directory path where the module is located. Begin with a DOS drive letter or a NetWare volume name.

Load RS232.NLM

If you want the file server to be accessible to asynchronous connection links, you must load RS232.NLM after you load REMOTE.NLM.

Type

```
LOAD [path]RS232 [comm port] [modem speed] <Enter>
```

If RS232.NLM is in the SYS:SYSTEM directory, you do not need to specify a path. If RS232.NLM is in a different directory, replace *path* with the directory path where the module is located. Begin with a DOS drive letter or a NetWare volume name.

Replace *comm port* with the communications port number (1 or 2). If you do not enter this number when entering the LOAD command, you will be prompted to enter it.

Replace *modem speed* with the baud rate (2400, 4800, or 9600). If you do not enter the modem speed when entering the LOAD command, you will be prompted to select a baud rate.

Where to Go from Here

The file server can now be accessed using a remote console. For instructions, see [“Using a Remote Console” on page 343](#).

Adding Remote Capability to a Standalone PC

You can use a standalone PC as a remote console if the required software is copied to a directory on the PC.

Create a directory on the standalone PC's hard disk and copy the following files to that directory:

ACONSOLE.EXE
RCONSOLE.HLP
IBM\$RUN.OVL
CMPQ\$RUN.OVL
\$RUN.OVL
SYSS\$ERR.DAT
SYSS\$HELP.DAT
SYSS\$MESS.DAT

With these files on your standalone PC, you can activate a remote console and open an asynchronous communication session with a file server by following the instructions in [“Activating ACONSOLE from a Network Station” on page 345](#).

Using a Remote Console

The tasks described in this section apply to file servers with remote console software loaded. If you have not yet set up your remote system, read the information in [“Setting Up Remote Management” on page 339](#).

This section explains how to activate a remote console session and how to access and use the remote console menus and screens.

The following tasks are explained:

- ◆ [“Activating RCONSOLE from a Network Workstation” on page 344](#)
- ◆ [“Activating ACONSOLE from a Standalone PC” on page 347](#)
- ◆ [“Exiting the Remote Console” on page 347](#)

Activating RCONSOLE from a Network Workstation

To open a connection using RCONSOLE, you must first log in to a file server on your network. Then you use RCONSOLE to connect to the remote file server.

NOTE: RCONSOLE also works through communication servers such as the Novell Access Server.

Procedure

- 1** From a workstation, log in to the local network file server as SUPERVISOR.
- 2** If you do not have a search drive mapped to the directory containing the remote console files (usually SYS:SYSTEM), type

```
MAP S16 :=SYS:SYSTEM <Enter>
```

- 3** Activate RCONSOLE by typing

```
RCONSOLE <Enter>
```

The “Available Servers” list appears, showing the file servers on your network that have REMOTE and RSPX loaded.

- 4** Select the file server you want from the “List of Available Servers” window and press <Enter>.
- 5** When the “Password” window appears, log in to the remote server in one of the following ways:
 - ◆ Enter the remote password for the remote file server.
 - ◆ Enter the SUPERVISOR password.

This will work only if volume SYS: is mounted.

After a few moments, one of the following appears:

- ◆ The MONITOR screen (if MONITOR is loaded on the file server with the keyboard lock option)
 - ◆ An active file server screen
 - ◆ The remote system console screen (:)
- 6** If the “Keyboard Lock Password” prompt appears, enter the MONITOR password and press <Enter>.

The remote console session is now open. You can see file server screens and use the remote console options as specified in [“Using the Remote Console for Administrative Tasks” on page 348](#).

Activating ACONSOLE from a Network Station

Both the workstation and file server must have modems connected to either a COM1 or COM2 port.

You open this connection by logging in to a file server on your network. Then you use ACONSOLE to connect to the remote file server.

Procedure

- 1** From a workstation, log in to the local network file server as SUPERVISOR.
- 2** If you do not have a search drive mapped to the directory containing the remote console files (usually SYS:SYSTEM), type

```
MAP S16:=SYS:SYSTEM <Enter>
```

In order for remote management to operate properly, you must map a search drive to the directory containing the remote console files.

- 3** Activate ACONSOLE by typing
`ACONSOLE` <Enter>
- 4** When the “Main Menu” appears, select “Connect to Remote Location” to access your phone list.

If you have not configured the modem, or if you want to change the current modem configuration, go to [“Configuring the Modem” on page 356](#) and then continue here with [Step 5](#).

- 5** Select the appropriate file server from the phone list by pressing <Enter>. If you have not created a phone list, or if you want to change your phone list, go to [“Configuring the Modem” on page 356](#) and then return to this step.

A “Modem Result Codes” screen appears.

Messages appear on the screen to inform you of the progress of the connection attempt.

When the connection is established, the “Available Servers” screen appears showing the name of the server you called.

NOTE: ACONSOLE does not provide a guaranteed packet delivery transport. When trying to send packets to or receive packets from a file server with extensive disk or LAN activity, ACONSOLE may “time out” when sending data to the file server or waiting for a response from the server. If so, one of the following messages will appear in the “Modem Result Codes” message screen:

Unable to Send Request to Server

No Response from Server

If either message appears, press <Esc> and continue or retry the operation.

- 6** Select the server and press <Enter>.
- 7** When the “Password” window appears, enter one of the following passwords:
 - ◆ The REMOTE password for the remote file server.
 - ◆ The SUPERVISOR password. This will work only if volume SYS: is mounted at the remote server.

After a few moments, one of the following screens or prompts appears:

- ◆ The keyboard lock password prompt (if MONITOR is loaded on the file server and the keyboard lock option has been selected)
 - ◆ An active file server screen
 - ◆ The remote system console screen (:)
- 8** If the keyboard lock password prompt appears, type the password and press <Enter>.

The ACONSOLE session is now open. You can see file server screens and use the remote management console options as explained in [“Using the Remote Console for Administrative Tasks” on page 348](#).

Activating ACONSOLE from a Standalone PC

To establish a standalone PC as a remote console and open an asynchronous connection, the PC and the remote file server must be set up as follows:

- ◆ Both the standalone PC and the file server must have modems.
- ◆ The standalone PC must be set up as explained in [“Adding Remote Capability to a Standalone PC”](#) on page 343.
- ◆ The file server must be running NetWare v3.1 or later.
- ◆ The file server must have the REMOTE and RS232 modules loaded.

After the standalone PC is set up, use ACONSOLE to open a communication session. At this point, you can perform tasks in the same way as a workstation with an asynchronous link does.

Exiting the Remote Console

You can exit a remote console session from the “Available Options” menu or from the remote system console prompt.

Exit from the “Available Options” Menu

Procedure

- 1** Select “End Remote Session With Server.”
- 2** Press <Enter>.
- 3** Answer “Yes” at the “Quit Remote Console Session” confirmation box.

Exit from the Remote System Console Prompt

Procedure

- 1** Press <Shift><Esc>.
- 2** Press <Esc>.
- 3** Answer “Yes” at the “Exit Remote Console” confirmation box.

Using the Remote Console for Administrative Tasks

This section describes how to use the remote console and how to perform administrative tasks. The tasks in this section are not in chronological order. This is a reference section to help you complete routine, isolated tasks.

If you have not opened a remote console session, follow the instructions in [“Using a Remote Console” on page 343](#) before proceeding.

The following tasks are explained in this section:

- ◆ How to use remote console screens and menus ([“Use Remote Management Screens and Menus” on page 349](#))
- ◆ How to scan file server directories in a floppy drive or on a NetWare or DOS partition ([“Scan File Server Directories” on page 350](#))
- ◆ How to reboot a file server from a remote console ([“Reboot a File Server from a Remote Console” on page 350](#))
- ◆ How to transfer files to a remote file server ([“Transfer Files to a Remote File Server” on page 351](#))
- ◆ How to add or upgrade a LAN or disk driver on a remote file server ([“Upgrade a LAN or Disk Driver” on page 354](#))
- ◆ How to configure a modem ([“Modify the Modem Configuration” on page 356](#))

Use Remote Management Screens and Menus

Use the “Available Options” Menu

Task	Procedure
Access the menu	Press <*> on the number pad.
Move down through menu levels	Press <Enter>.
Move up through menu levels	Press <Esc>.
Exit the menu	Press <Esc> or <Alt><F10>.

Move through Active Screens

Task	Procedure
Display the “Available Options” menu	Press <*> on the number pad.
Move between active file server screens	Press <-> or <+> on the number pad (does not work in the “Available Options” menu).
Terminate a session with a file server	Press <Shift><Esc> until the “List of Servers” screen reappears.
See a list of active file server screens	Press <*> on the number pad to access the “Available Options” menu, and then select “Select a Screen to View.”
View an active file server screen	Select “Select a Screen to View” from the “Available Options” menu, and then select the screen to view from the list of active screens.

Scan File Server Directories

Procedure

- 1** From the “Available Options” menu, select “Directory Scan.”
- 2** Enter the directory you want to scan by completing one of the following:
 - 2a** To scan a network drive, enter the path for the directory you want to see and then press <Enter>. For example, to scan the directories in the SYSTEM directory, type
SYS:SYSTEM <Enter>
 - 2b** To scan a DOS drive, enter the drive letter and then press <Enter>. For example, to scan the DOS directories on drive C, type
C: <Enter>
IMPORTANT: If the file server has only one floppy drive, do not attempt to scan directories on drive B. Specifying a logical drive will cause the workstation to hang until a keystroke is entered at the file server console.
- 3** To scroll through directories, use the <PgUp> and <PgDn> keys.

Reboot a File Server from a Remote Console

You can reboot a file server from a remote console by executing an .NCF file containing the appropriate commands.

Procedure

- 1** If the EDIT.NLM is not loaded, type
Load EDIT <Enter>
- 2** Do one of the following:
 - 2a** Create an .NCF file and include the following commands in the order given:
REMOVE DOS
DOWN
EXIT
 - 2b** If you have already created a reboot file, go to **Step 4**.
- 3** Save the file in the SYS:SYSTEM directory.

- 4 At the system console prompt, enter the name of the .NCF file you created to reboot the file server.

The keyboard will be disabled for a few minutes while the file is processed.

- 5 When a prompt appears telling you that the connection is lost, press <Esc>.
- 6 When the “List of Servers” screen appears, exit from the remote console.
- 7 Open a new remote console connection with the file server.

Transfer Files to a Remote File Server

You can transfer files from a workstation (acting as a remote console) to a file server in several ways. Follow the procedure which best serves your needs.

IMPORTANT: When reading the instructions for any of the file transfer methods, keep in mind that *source* means the current location of the files that you want to transfer (where the files are being copied from), and *target* means the destination of the files (where the files are being copied to). Both network drives and local hard drives can be used as sources *or* targets.

Transfer Specific Files

Use this method to transfer individual files or all files in a directory to a remote file server. For example, you can transfer customized files or update selected SYSTEM, PUBLIC, or LOGIN files.

This transfer method works with both asynchronous and direct communication sessions.

To transfer files from a remote console to a target file server, open a remote console session, and then complete the following steps.

Procedure

- 1 From the “Available Options” menu, select “Transfer Files to Server.”
- 2 Enter the source directory path (including wildcard characters if applicable) for the files you want to transfer.

2a To transfer files from a diskette, type the drive letter followed by the source directory path.

For example, to transfer all of the files from the *System_1* diskette, insert the diskette into drive A: and type

```
A: \ <Enter>
```

2b To transfer files from a network drive, type the drive letter followed by the source directory path.

If the remote console has a drive mapped to the source directory, enter the drive letter and the filename or a wildcard character.

For example, to transfer the RCONSOLE.EXE file from the SYS:ADMIN\UTILS directory which is mapped to drive G:, type

```
G: RCONSOLE . EXE <Enter>
```

If the workstation does not have a drive mapped to the source directory, enter the complete directory path.

For example, to transfer the file described above, type

```
SYS:ADMIN\UTILS\RCONSOLE . EXE <Enter>
```

3 Enter the directory path on the target file server.

3a To transfer files to a diskette at the file server, enter the target drive letter followed by the directory path.

For example, to transfer the RCONSOLE.EXE file to drive A: in the SYSTEM directory, type

```
A: \SYSTEM\RCONSOLE <Enter>
```

IMPORTANT: If the file server has only one floppy drive, do not attempt to transfer files to a logical drive (such as drive B:). Specifying a logical drive will cause the workstation to hang until a keystroke is entered at the file server console.

3b To transfer files to a network drive, enter the target directory path.

For example, to transfer the SYSTEM files to the target SYSTEM directory, type

```
SYS:SYSTEM <Enter>
```

As each file is transferred to the target file server, it is listed on the remote console screen.

If you want to verify that the files were transferred, follow the procedures in “[Scan File Server Directories](#)” on page 350

Transfer All SYSTEM and PUBLIC Files

Use this method to automatically transfer all NetWare system files from a network drive located on one file server to a remote (different) file server.

NOTE: This transfer method works with both asynchronous and direct communication sessions. However, it is not recommended for asynchronous connections because ACONSOLE does not provide a guaranteed packet delivery transport.

When trying to send packets to or receive packets from a file server with extensive disk or LAN activity, ACONSOLE may “time out” when sending data to the file server or while waiting for a response from the server.

This option automates the process of transferring NetWare operating system files to remote file servers. Once the appropriate source directories and files are created on a source network drive, the “Transfer System and Public Files” option on the remote management “Available Options” menu automatically copies the files to the correct directories on the target file server.

Procedure

- 1** If the source directory is already set up, skip to [Step 3](#).
- 2** Create subdirectories on the *source* network drive that match the names of their respective NetWare v3.12 diskettes, for example, *SYSTEM_1*, *SYSTEM_2*, etc.
- 3** Use the NCOPY command to copy the files from the NetWare system diskettes to the respective network subdirectories with the same names.

For example, to copy files from a diskette in drive A: at the workstation to a network directory called “SYSTEM_1” on drive G:, type

```
NCOPY A:*. * G:\SYSTEM_1 /S <Enter>
```

Once the source directories and files are created on the source file server, the files can be transferred to the SYSTEM, PUBLIC, and LOGIN directories on the target file server.

- 4** From a workstation, log in as SUPERVISOR to the file server on which you created the source files.

If you do not have a search drive mapped to the directory containing the remote console files (usually SYS:SYSTEM), type

```
MAP S16:=SYS:SYSTEM <Enter>
```

For remote management to operate properly, you must map a search drive to the directory containing the remote console files.

- 5** From the drive or directory containing the source subdirectories, activate a remote console (as explained in [“Using a Remote Console” on page 343](#)).

Activate the remote console using this directory as your default directory.

- 6** Access the “Available Options” menu and select “Copy System and Public Files.”

The remote console scans the default directory for a SYSTEM_2 subdirectory with a FILEDATA.DAT file. If the file is found, a window appears and each file is listed as it is copied to the target file server. If the file is not found, you will be prompted to insert installation diskettes into the target file server or to press <F7> to cancel.

Upgrade a LAN or Disk Driver

Using a remote console, you can add a new LAN driver or disk driver to a file server, or upgrade an existing LAN or disk driver.

Add or Upgrade a LAN driver

Procedure

- 1** Activate a remote console (as explained in [“Using a Remote Console” on page 343](#)).
- 2** From the “Available Options” menu, select “Transfer Files to Server.”
- 3** Enter the source directory path of the LAN driver you want to transfer.
- 4** Enter the target directory path for the LAN driver.

5 Enter the following commands according to the type of session you have opened.

5a For ACONSOLE sessions, enter the commands at the system console prompt (:).

5b For RCONSOLE sessions, create an .NCF file and enter the commands in the file.

Enter the commands in this order:

```
UNLOAD old_driver <Enter>
```

```
AUTOEXEC <Enter>
```

6 For RCONSOLE sessions, save and execute the .NCF file.

If you have opened a connection using RCONSOLE, the commands must be placed in an .NCF file because the RSPX connection will be terminated when the old LAN driver is unloaded.

Add or Upgrade a Disk Driver

Procedure

1 Activate a remote console (as explained in [“Using a Remote Console” on page 343](#)).

2 Make sure all users are logged out.

You can use the MONITOR utility to do this.

3 Disable logins to the file server by typing

```
DISABLE LOGIN <Enter>
```

4 Dismount all volumes on drives that are serviced by the controller whose driver you will unload.

5 Use the UNLOAD command to unload the old disk driver by typing

```
UNLOAD old_driver <Enter>
```

6 Access the remote console “Available Options” menu and select “Transfer Files to Server.”

7 Enter the source directory path of the new disk driver and press <Enter>.

8 Enter the target directory path for the new disk driver and press <Enter>.

9 Exit the “Available Options” menu and go to the system console prompt.

- 10** Use the LOAD command to load the new disk driver by typing
`LOAD new_driver <Enter>`
- 11** Type “MOUNT ALL” at the prompt.
- 12** Enable logins to the file server by typing
`ENABLE LOGIN <Enter>`

Configuring the Modem

Modify the Modem Configuration

Procedure

- 1** From the ACONSOLE “Main Menu,” select “Configure Modem.”
- 2** When the “Current Modem Configuration” screen appears, select the field you want to modify and make changes as follows.
IMPORTANT: We recommend that you do not change the modem Reset, Initialization, Dial, or Hangup commands. The default settings are recommended for these commands.
 - 2a** To modify SELECT COMM PORT, press <Enter> and select the communications port to which you have connected your modem.
 - 2b** To modify SELECT BAUD RATE, press <Enter> and select the baud rate from the list.
 - 2c** To modify USER CONNECTION ID, press <Enter> and enter a name for the modem user (up to 40 characters).

This field must contain an ID name before the modem will attempt a call.

Create or Modify the Modem Phone List

Phone list entries can be up to 40 characters long. The purpose of the “Location” field is to help you remember which phone number is associated with a particular file server. For example, you can enter the name of a file server or the name of a department or city.

When you enter a phone number for a remote server, you must include any necessary dial modifiers. (See your modem user’s guide for this information.)

The modifiers must be entered because the number is appended to the dial command being sent to your local modem.

Procedure

- 1** From the ACONSOLE “Main Menu,” select “Connect to Remote Location.”
- 2** When the phone list appears, you can change your phone list in any of the ways explained in the following table.

Task	Procedure
Add a number	Press <Insert>; then enter the phone number and a name for the remote server. Press <Esc> to save the entry.
Modify a number	Select the number to be modified. Press <F3> and enter the new information. Press <Esc> to save the entry.
Delete a number	Select the number to be deleted. Press . When the confirmation box appears, select “Yes.”

3

Troubleshooting Guide

Overview

This is a guide to some of the most common problems you may encounter while maintaining your network. It is not intended to be exhaustive. If you need more help, contact your Novell Service Representative. This guide is divided into the following sections:

- ♦ “Maintenance Tips” on page 360—designed to help you develop habits that prevent problems
- ♦ “Flow Charts” on page 368—designed to isolate the source of the problem
- ♦ “Common Problems” on page 382—designed to identify possible solutions to specific problems

The following sections in Chapter 1 also contain helpful troubleshooting ideas: INSTALL, LOAD, LOAD *disk driver*, LOAD LAN *driver*, MONITOR, SET, UPS, UNLOAD, and VREPAIR.

The following workstation utilities, found in *Utilities Reference*, also contain troubleshooting information: BINDFIX, BINDREST, and NBACKUP.

Appendix D in *Installation and Upgrade* contains troubleshooting information for remote booting of diskless workstations.

Maintenance Tips

This section explains some tips on managing your file server and its resources. These tips are not intended to be inclusive, but only to get you started in setting up a routine maintenance schedule that will keep the file server and its resources functioning effectively.

Table 25 Maintenance tips

Memory maintenance	“Memory Maintenance” on page 360
Disk maintenance	“Disk Maintenance” on page 363
Security maintenance	“Security Maintenance” on page 365
Bindery maintenance	“Bindery Maintenance” on page 366
Volume maintenance	“Volume Maintenance” on page 367

Memory Maintenance

NetWare has been configured so that your system can grow as your organization grows. Many of the resources that use memory can allocate additional memory as required. The NetWare operating system warns you when memory is getting low. The operating system warns you again when it cannot allocate additional memory for a resource.

If you monitor how fast available memory is being used by growing resources, you can plan for future needs. We suggest that you monitor the following statistics:

- ◆ Cache buffers
- ◆ Alloc Short Term Memory
- ◆ Service processes
- ◆ Packet receive buffers

Cache Buffers

You can view the percentage of memory available for cache buffers in MONITOR (“Server Memory Statistics” window). Cache buffers are used to store frequently used files (for fast access) and to allocate memory to other memory pools.

As memory is allocated to other pools (for example, to the Non-Movable Memory pool to load loadable modules), the number of available cache buffers decreases. The number of cache buffers will naturally decrease as you add additional hard disks and as the number of files and their size increase.

If the cache buffers get too low, performance decreases. Frequently used files can no longer be cached because not enough cache buffers are available. The files will have to be read from the hard disk (a process that is considerably slower than reading them in from memory).

The number of buffers you need depends on your system (the number of users and the tasks that they are performing). By monitoring the rate of the decrease of available cache buffers, you can plan to add more memory to the file server. When the percentage of available cache buffers reaches 20%, you need to add more memory. However, you may need to add more memory at 30% (or even at 40% or 50%) for your system.

Alloc Short Term Memory

You can view the percentage of memory allocated for the Alloc Short Term Memory pool in MONITOR (“Server Memory Statistics” window). A SET parameter (“Maximum Alloc Short Term Memory”) controls the maximum size of this pool. The default size is 8 MB. As the pool grows close to 8,000,000 bytes, increase the SET parameter by 1 MB.

You should also view the resource tags for Alloc Short Term Memory and track which modules are using more and more of this type of memory. Most modules should not need a growing amount of this memory. If a loadable module is the source of growth for this memory pool, contact the vendor of the module.

Service Processes

You can view the number of service processes created to handle requests in MONITOR (“Information for Server *servername*” window).

The number of service processes increases as the number of outstanding disk I/Os increases. A SET parameter (“Maximum Service Processes”) controls the number of service processes that the operating system allocates. The default is 20.

IMPORTANT: If your file server is low on cache buffers (see [“MONITOR” on page 177](#)), do not increase the number of service processes. If you decrease the cache buffers, you increase the likelihood that a service process has to wait for a disk I/O rather than being able to service the request immediately from the cache buffers.

If your system approaches the default number of server processes and your file server has sufficient memory, you can either increase the default by 5 or use the following suggestions to increase disk I/O:

- ◆ Use the SPEED command to check the speed of the CPU. Make sure that the jumpers have been set for the highest speed (check the computer's documentation).
- ◆ Add a host bus adapter and attach some of the hard disks to it.
- ◆ Turn off the driver's automatic read-after-write verify function if your hard disks do a read-after-write verification automatically. (See the documentation for the hard disks.) This function is controlled under the "Disk Information" option in MONITOR.
- ◆ Configure your volumes so that they span more than one hard disk. See "INSTALL" on page 69.
- ◆ Increase the number of cache buffers by adding more memory to the file server. If you increase the available cache buffers, you increase the likelihood that the file will be in memory and decrease the likelihood that an existing service process will have to wait for a disk I/O.
- ◆ Upgrade to a computer that has a higher CPU speed.
- ◆ Upgrade to a microchannel or EISA computer and use either microchannel or EISA bus master boards.

The number of packet receive buffers also influences the need for service processes. See the next section, "Packet receive buffers."

Packet Receive Buffers

You can view the number of allocated packet receive buffers in MONITOR ("Information for Server *servername*" window). A SET parameter ("Maximum Packet Receive Buffers") determines how many of these buffers can be allocated. As your server approaches the default of 100, increase the parameter in increments of 20 until you have one packet receive buffer per station.

If you have bus master boards in either an EISA or microchannel computer, you may need more than one packet receive buffer per station. The NE3200 driver, for example, can use 41 packet receive buffers when under maximum load.

If you are not using bus master boards and MONITOR shows that the operating system is using a packet receive buffer for each connected workstation, your file server cannot process disk I/Os fast enough. You can decrease the need for more packet receive buffers by increasing the number of service processes and implementing the suggestions for improving disk I/O. See “[Service Processes](#)” on page 361.

Disk Maintenance

NetWare has many features that help protect your data from corruption or loss. Hot Fix, mirroring, duplexing, and the salvageable file system all help, but an application can still corrupt the data files or two mirrored hard disks can fail at the same time.

For maximum security against loss of data, do the following:

- ◆ Back up your data regularly.
- ◆ Check your hard disks regularly for warning signs.

Back Up the Data

Current and valid backups are essential for maintenance. Every administrator, sooner or later, experiences a hardware or software failure that requires data from a backup.

NOTE: If your system uses backup devices that are attached to your file server, or if you have name spaces other than DOS and MAC, you should use SBACKUP for your backups. If your backup device is attached to a workstation and you have only DOS or MAC file types, you can use NBACKUP.

We recommend the following types of backups:

- ◆ A backup of modified files. You should have enough backup storage for two weeks (one set for the current week and an archived set for the past week).
- ◆ A complete backup of everything. This makes a mirror image of the file server. Then, if you lose everything, you can at least return to this point and use the modified file backups to bring the server to a more current state.

- ◆ A backup of the bindery. Most backup software programs that are NetWare compatible back up the bindery, but some third-party programs do not.

If you have never restored a bindery with the hardware and software you are currently using, use SBACKUP to back up the bindery.

- ◆ A backup of the trustee assignments. Most backup programs that are NetWare compatible back up the trustee assignments, but some third-party programs do not.

If you have never restored trustee assignments with the hardware and software you are currently using, use SBACKUP to back up the trustee assignments. Set the “Backup Subdirectories” and “Backup Trustees” options to “Yes” and use the “Files to exclude” option with *.* as the filename to exclude all files. The directory structure with its trustee assignments will be backed up.

Check the Hard Disks

You need to check the status of each hard disk at least weekly. An increase in redirected blocks can indicate that a hard disk is having problems and may need to be repaired or replaced. You can view the number of redirected blocks in MONITOR (use the “Disk Information” option).

When the number of “Redirected Blocks” plus the number of “Reserved Blocks” reaches half the total number of “Redirection Blocks,” Hot Fix is close to failing on the disk. Back up the data on the disk. Then use INSTALL (“Available Disk Options”) to run either a destructive or nondestructive surface test on the hard disk. If the disk fails the surface test, you will have to remove the disk and repair or replace it.

When blocks are redirected or when mirroring or Hot Fix fails, warning messages are displayed on the file server console and recorded in the File Server Error Log that can be read in SYSCON. Scan this error log at least weekly for disk messages. If you suspect problems, view the log daily.

Security Maintenance

If you need a secure system, use the security features of NetWare. Then set up a schedule to test your security. The more secure your system needs to be, the more frequently you should test it for violations. Test for general violations in the security setup, monitor your users' login habits, and monitor the effective rights in sensitive directories.

General Violations

Use the SECURITY command to list the weakest points in your security system. SECURITY lists the following types of potential security problems:

- ◆ Users who have been made supervisor equivalent
- ◆ Users who have insecure passwords or no passwords
- ◆ Users who have trustee assignments at the root directory of any volume
- ◆ Users who have rights to the SYS:SYSTEM directory

Use SYSCON to view the File Server Error Log. This file records the following kinds of information that can indicate a breach in security:

- ◆ The node addresses of stations connecting to the file server console with RCONSOLE
- ◆ The date and time when the file server is downed, TTS enabled or disabled, login enabled or disabled, and the bindery opened and closed

Login Habits

Monitor your users' login habits to ensure that they are not leaving the system open.

- ◆ Run USERLIST to make sure users are logging out when they leave for lunch and for the night. Teach them to use a keyboard lock or to log out whenever they leave a workstation unattended.
- ◆ Run USERLIST to monitor who is logged in as SUPERVISOR, how long the user has been logged in, and from which workstation the user has logged in. A user should never leave a workstation unattended when logged in as SUPERVISOR.

Effective Rights

Regularly check the security of the directories that need to be protected to ensure that only those users who should have rights to the directories do. As users move to new assignments in your department or business, their trustee assignments should also change.

Check effective rights by completing the following:

- ◆ Use the FILER “Who has rights here” option to view users’ effective rights in the directories and files that need to be secure. (This option is more complete than the TLIST command that lists only the trustee assignments given to the directory.) The FILER option scans the directory structure and reports all users who can exercise rights in the directory.
- ◆ Use SYSCON to review group member lists and delete users who have new assignments that no longer require them to be members of a particular group.
- ◆ Use NBACKUP or SBACKUP to back up directory trustee assignments whenever you have made significant changes to these assignments.

Bindery Maintenance

- ◆ Use SYSCON to delete users who are no longer using the file server.
- ◆ Check the TTSS\$LOG.ERR file. Transaction Tracking System (TTS) protects the bindery database from corruption. If the operating system shuts down TTS because of system problems, your bindery could become corrupted.

The TTSS\$LOG.ERR file, which is located in the root directory of the SYS volume, records all significant TTS events. The file can be read with any text editor program.

For more information, see [“TTS Problems” on page 419](#) or see “TTS” in *Concepts*.

- ◆ Keep a backup copy of the bindery files in a secure place. Record the SUPERVISOR’s password or back up the bindery with no password for user SUPERVISOR.
- ◆ Keep a current copy of the .OLD bindery files. To create these files, run BINDFIX. From the SYS:SYSTEM directory, copy the NET\$OBJ.OLD, NET\$PROP.OLD, and NET\$VAL.OLD files to a diskette. Then delete the .OLD files from the SYS:SYSTEM directory. Record the SUPERVISOR’s password and store the diskette in a secure place.

If you lose your bindery and cannot restore it from a regular backup, copy the .OLD files into the SYS:SYSTEM directory. Run BINDREST. The .OLD files will be restored as the file server's bindery.

Volume Maintenance

- ◆ Use NBACKUP, SBACKUP, or third-party software regularly to back up the data on the volume.
- ◆ Use CHKVOL, CHKDIR, and VOLINFO to monitor the growth of directories and files. By determining how fast a volume is growing, you can plan for adding hard disks or removing files and directories that are no longer used.
- ◆ Check the VOL\$LOG.ERR file for each volume. This file is located in the root directory of the volume. For example, the file for volume SYS: is located in SYS:. This file records all system alerts for the volume. See *NetWare System Messages* for an explanation of the alerts. Use a DOS text editor to view the file.
- ◆ Use CHKVOL to monitor the amount of disk space being used by deleted files. If you need the space, use the SET parameters (“Immediate Purge of Deleted Files,” “Minimum File Delete Wait Time,” and “File Delete Wait Time”) to increase available space. Log in as SUPERVISOR and use PURGE at the volume level to free the space immediately.
- ◆ Use LISTDIR /S at the root directory of a volume to view subdirectory depth. A SET parameter (“Maximum Subdirectory Tree Depth”) controls how many levels of subdirectories the operating system will support. The default is 25. If your structure approaches the default, either move some of the directories to a level closer to the root (see “FILER” in *Utilities Reference*) or change the limit with the SET parameter.

Flow Charts

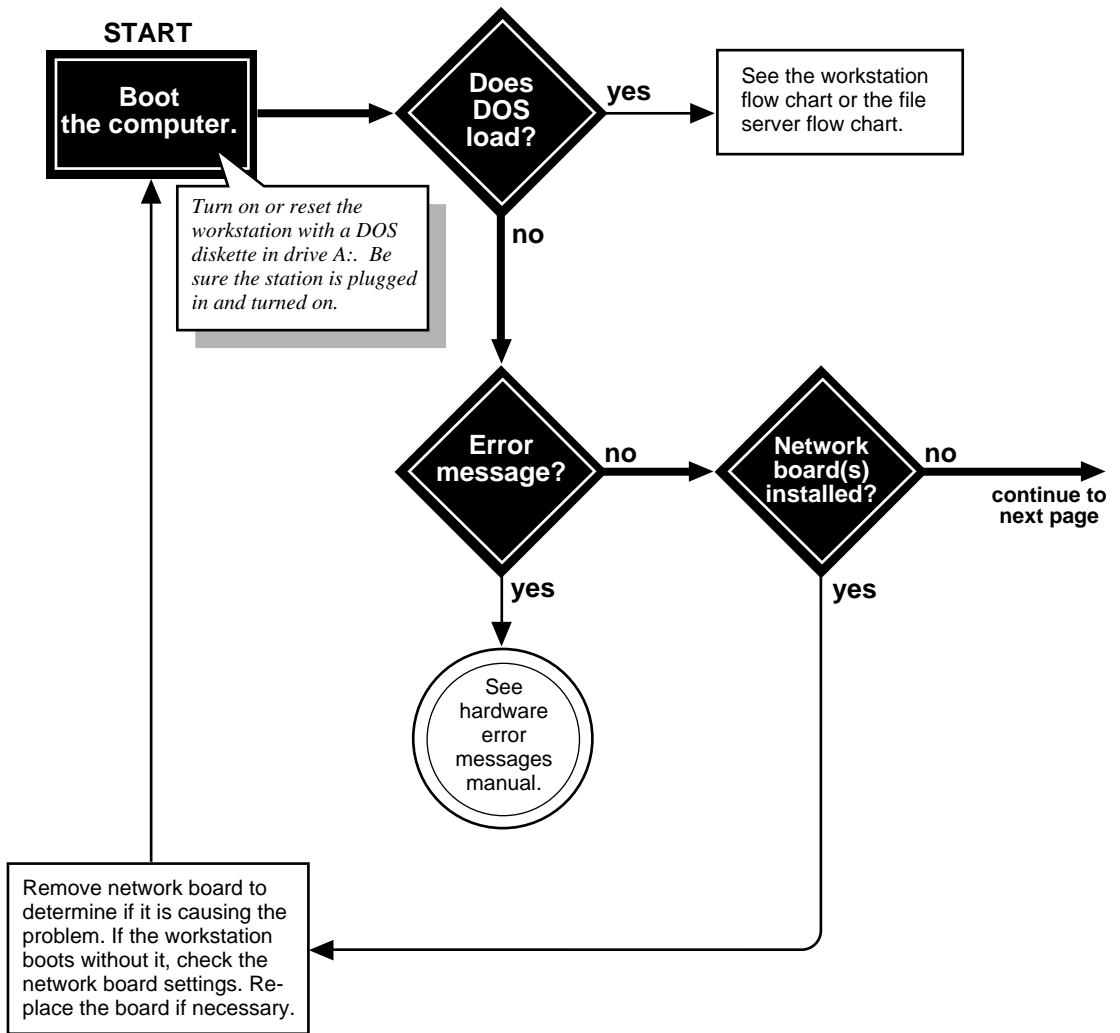
The following flow charts are designed to help isolate most problems on NetWare v3.1x networks. They also point you to specific suggestions in [“Communication Problems” on page 393](#).

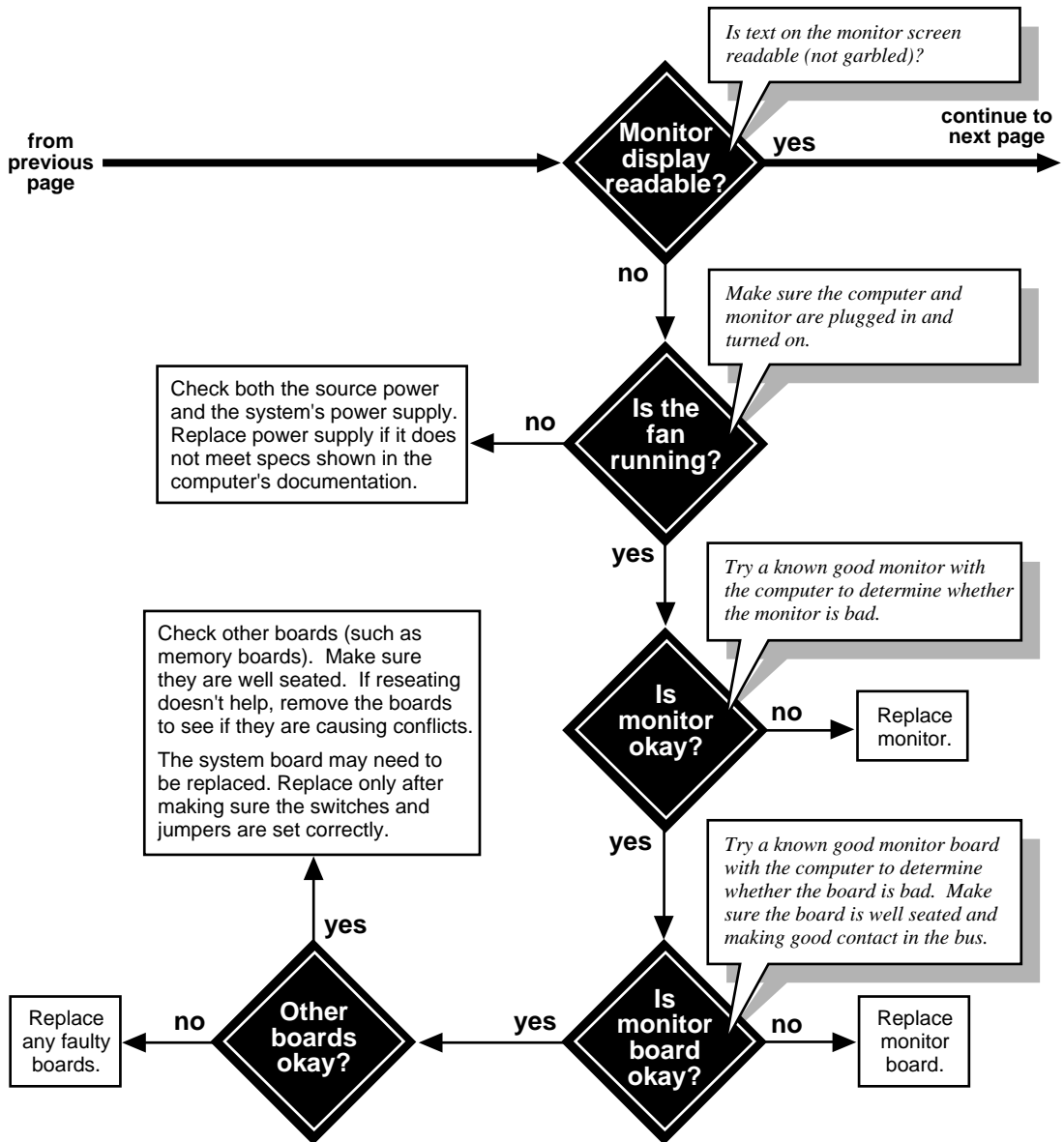
Table 26 Troubleshooting flow charts

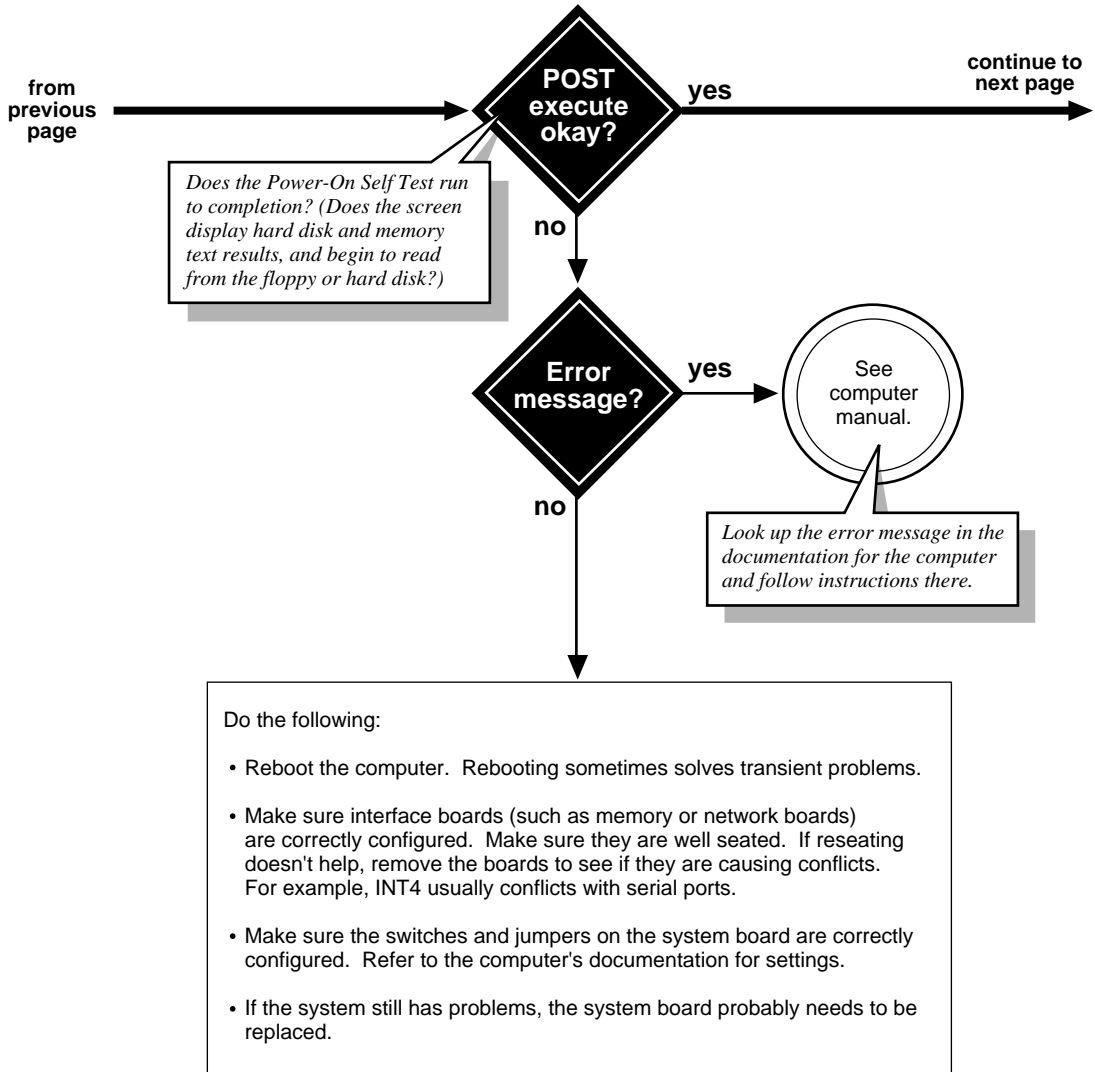
Chart	Purpose	Page
Hardware	Designed to isolate hardware problems that prevent DOS from loading.	“Hardware flow chart” on page 369
File Server	Designed to isolate problems that prevent the file server from booting after DOS has been loaded.	“File server flow chart” on page 374
Workstation	Designed to isolate problems that prevent the workstation from logging in to a file server after DOS has been loaded.	“Workstation flow chart” on page 379

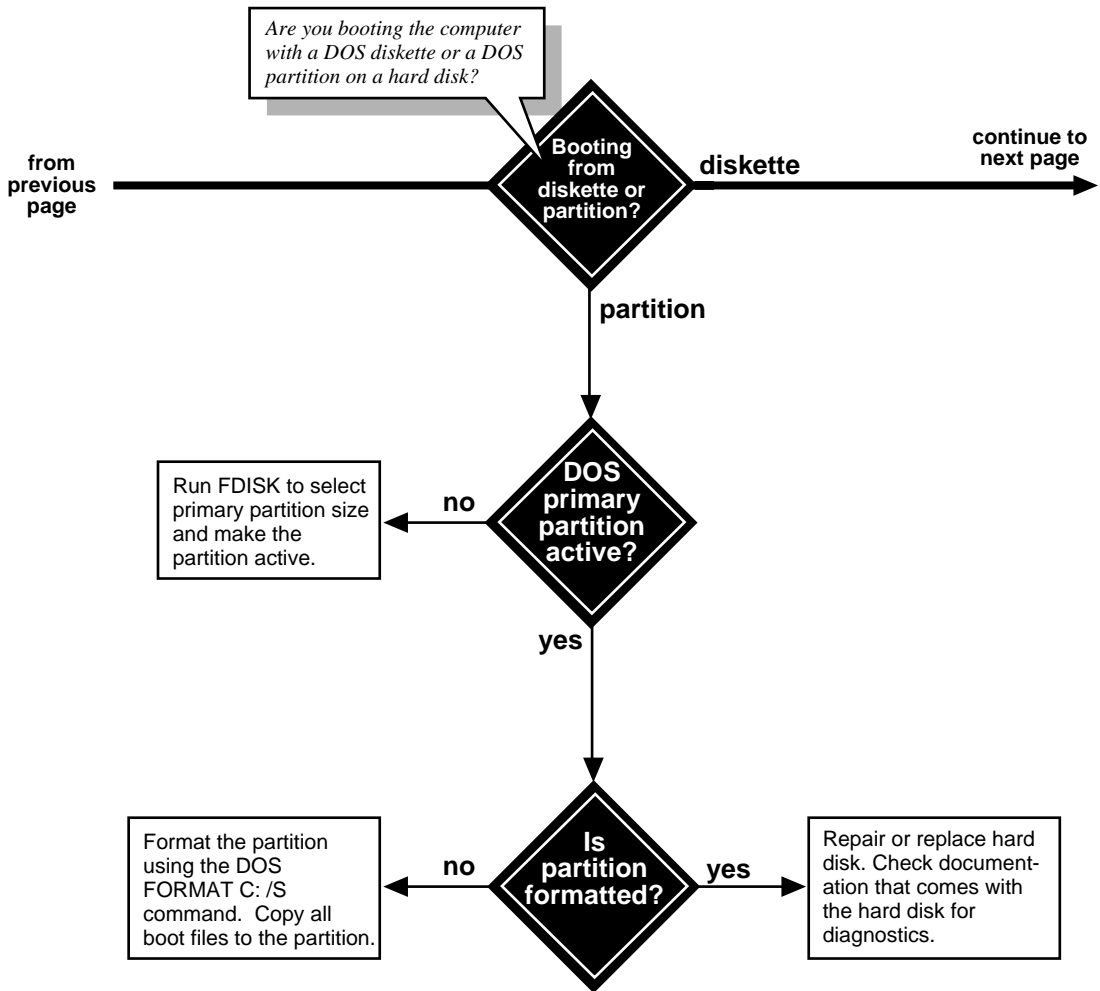
Figure 52 Hardware flow chart

Hardware









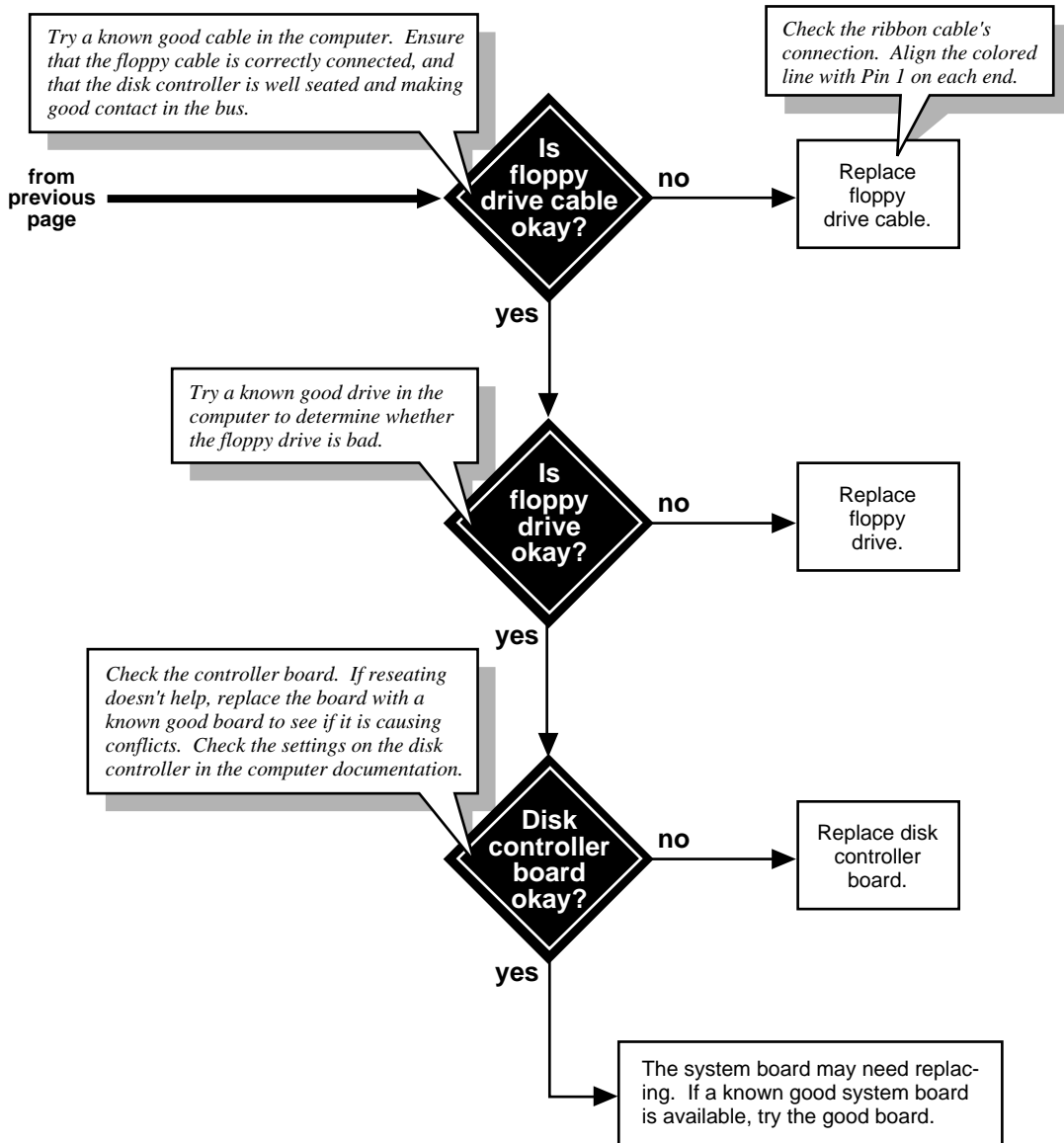
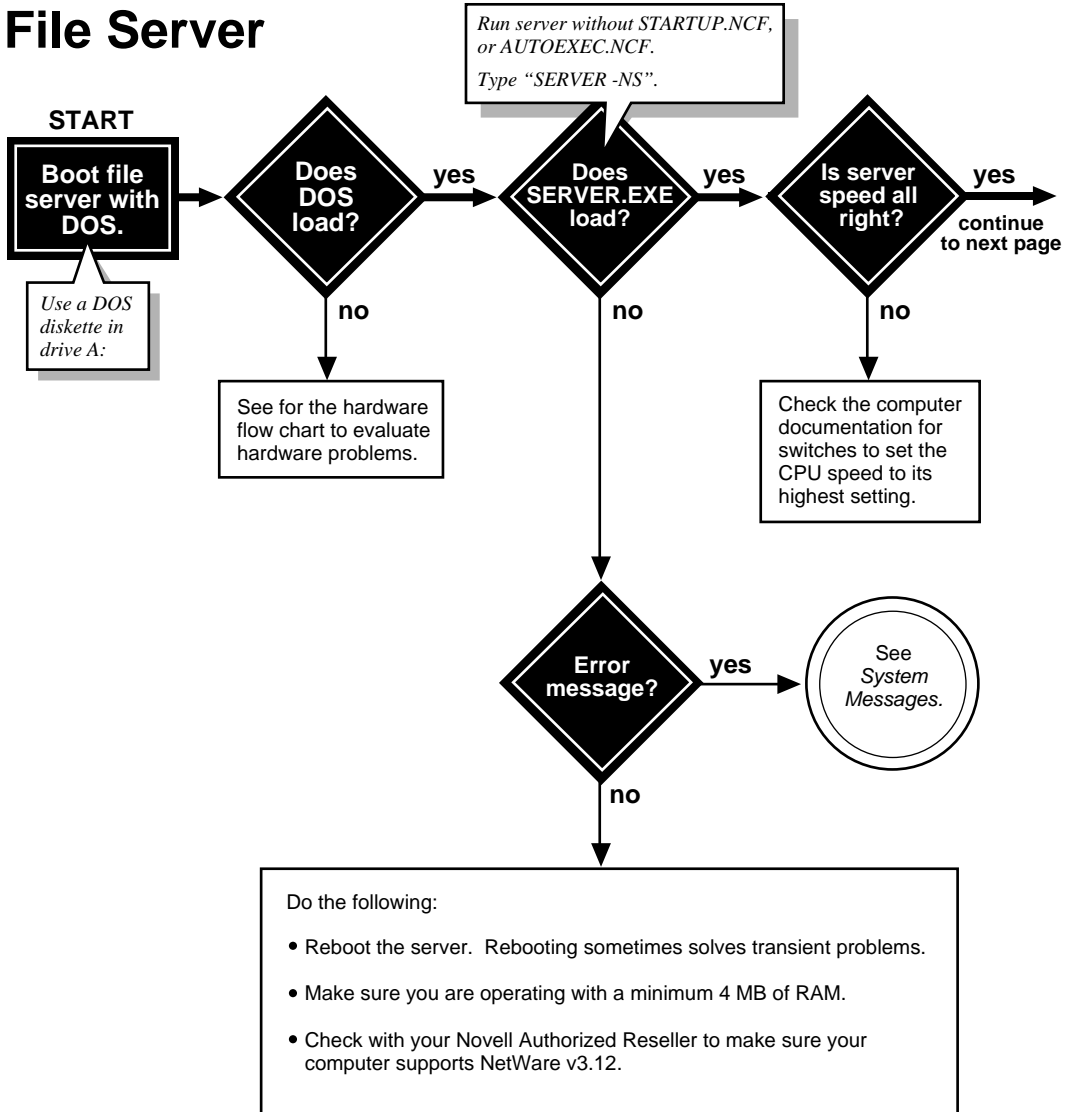
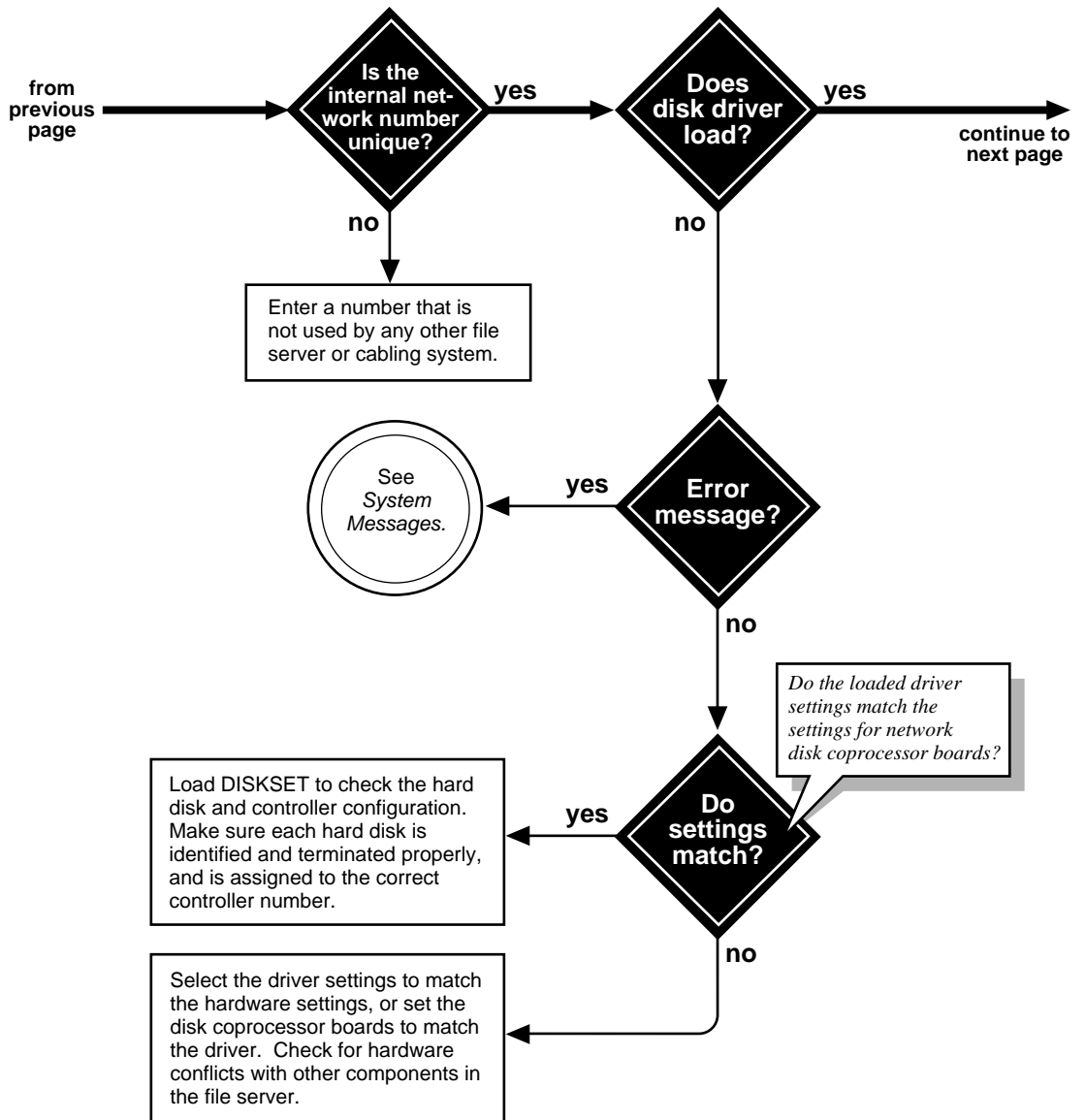
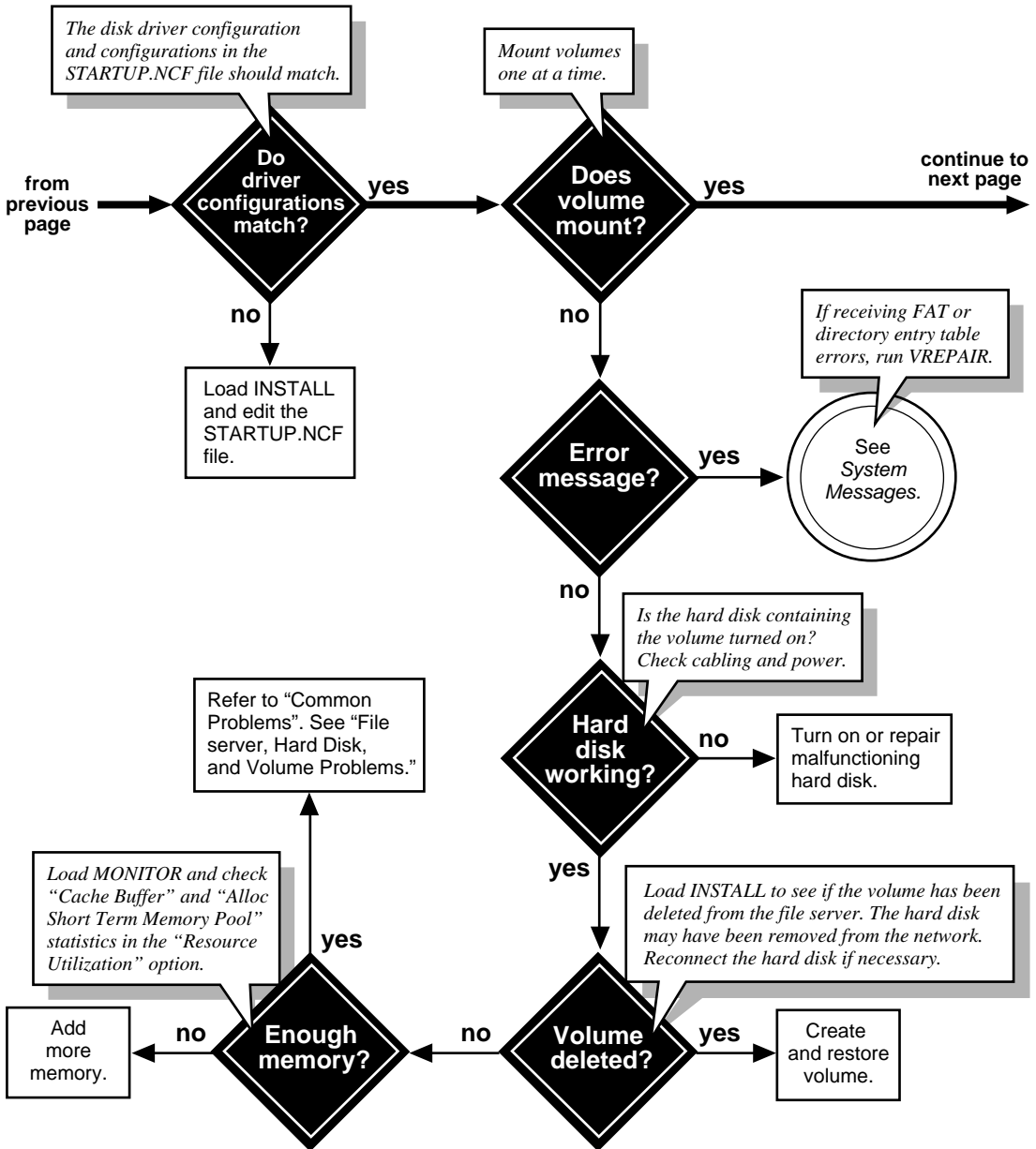


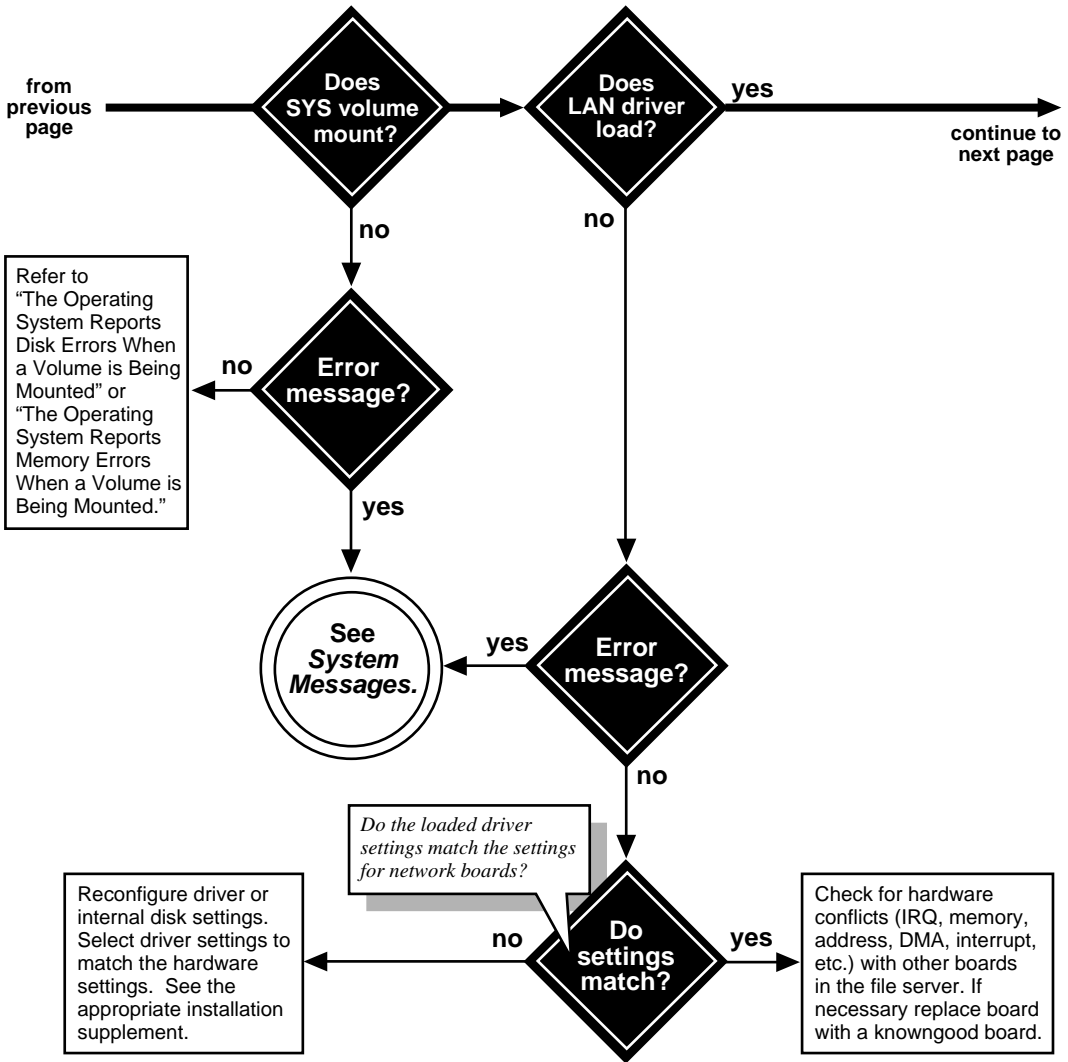
Figure 53 File server flow chart

File Server









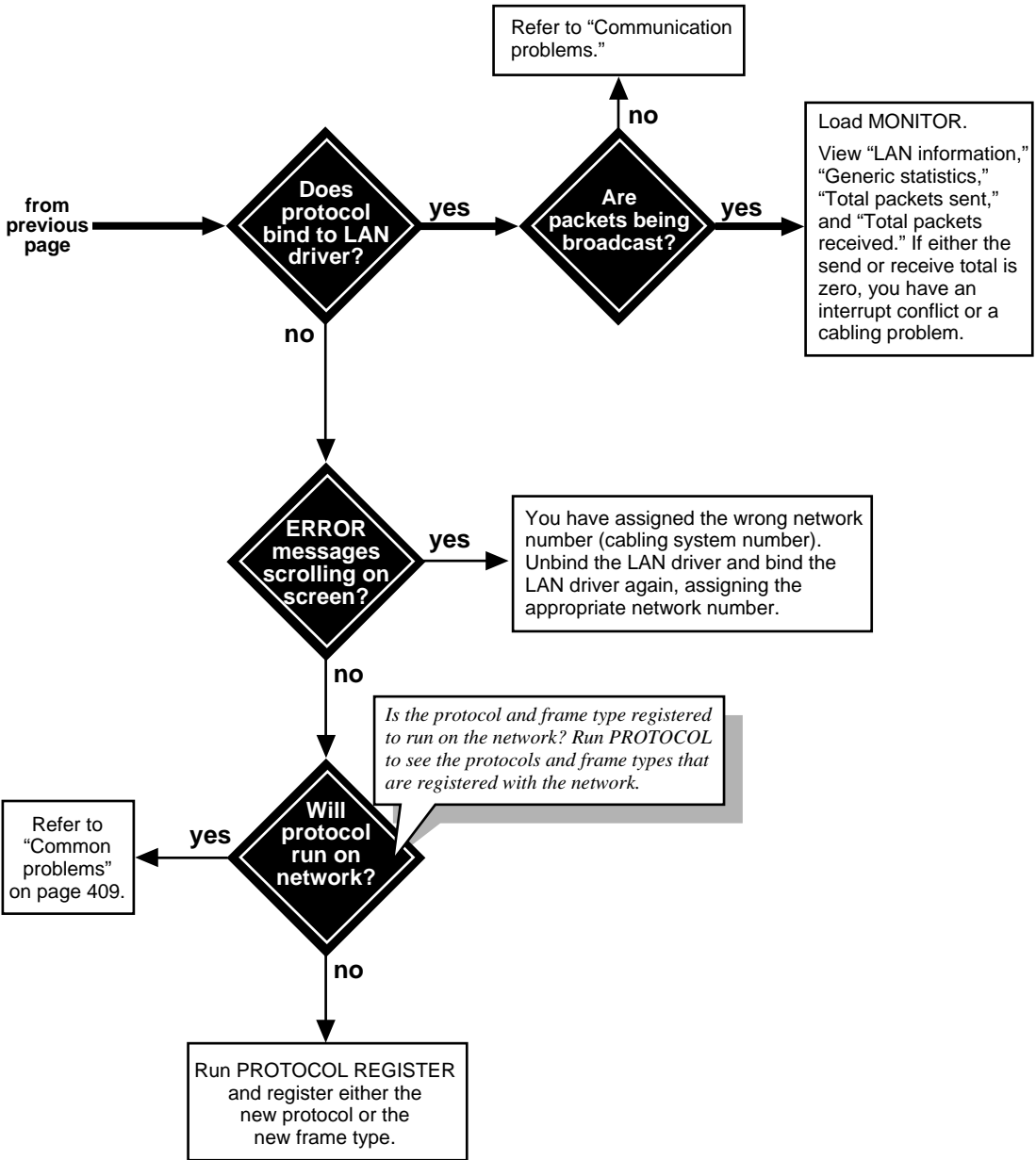
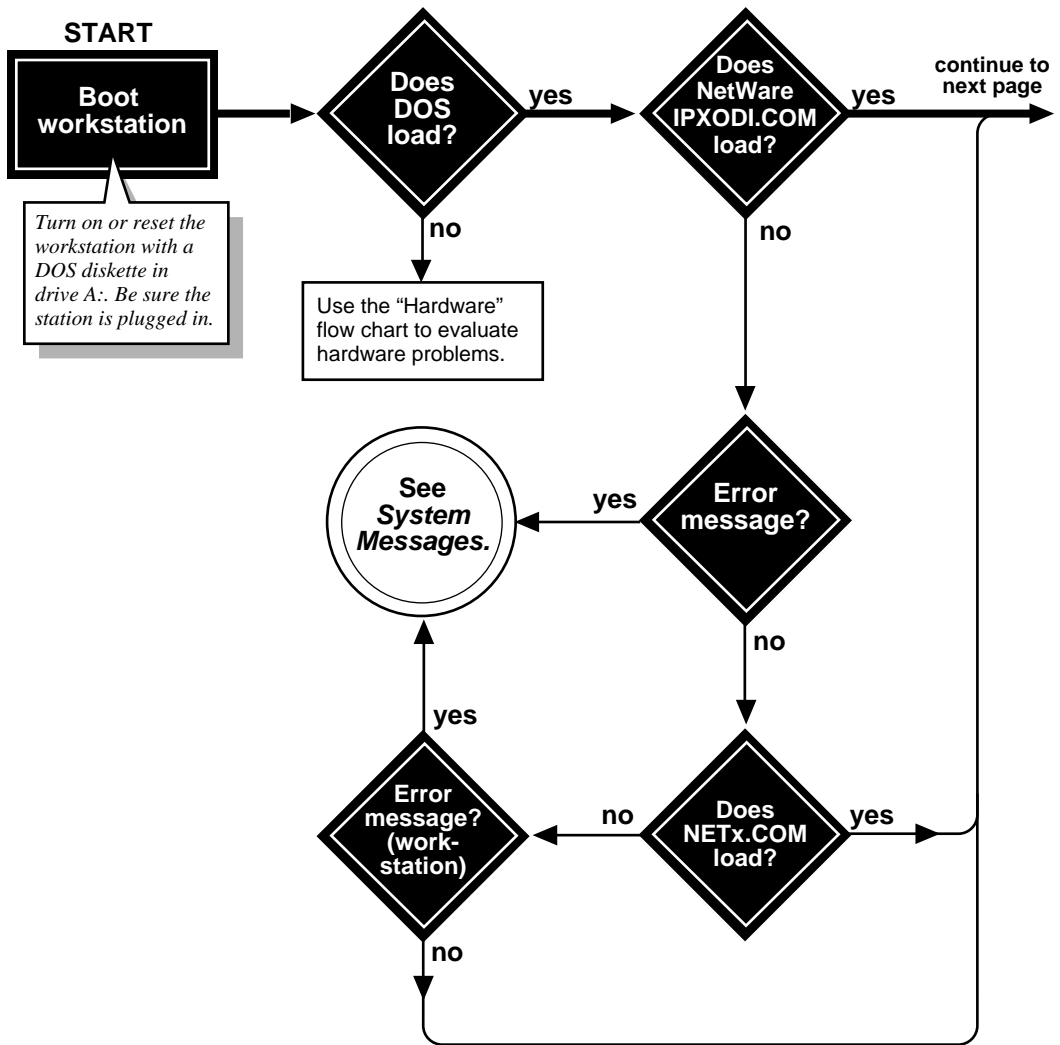
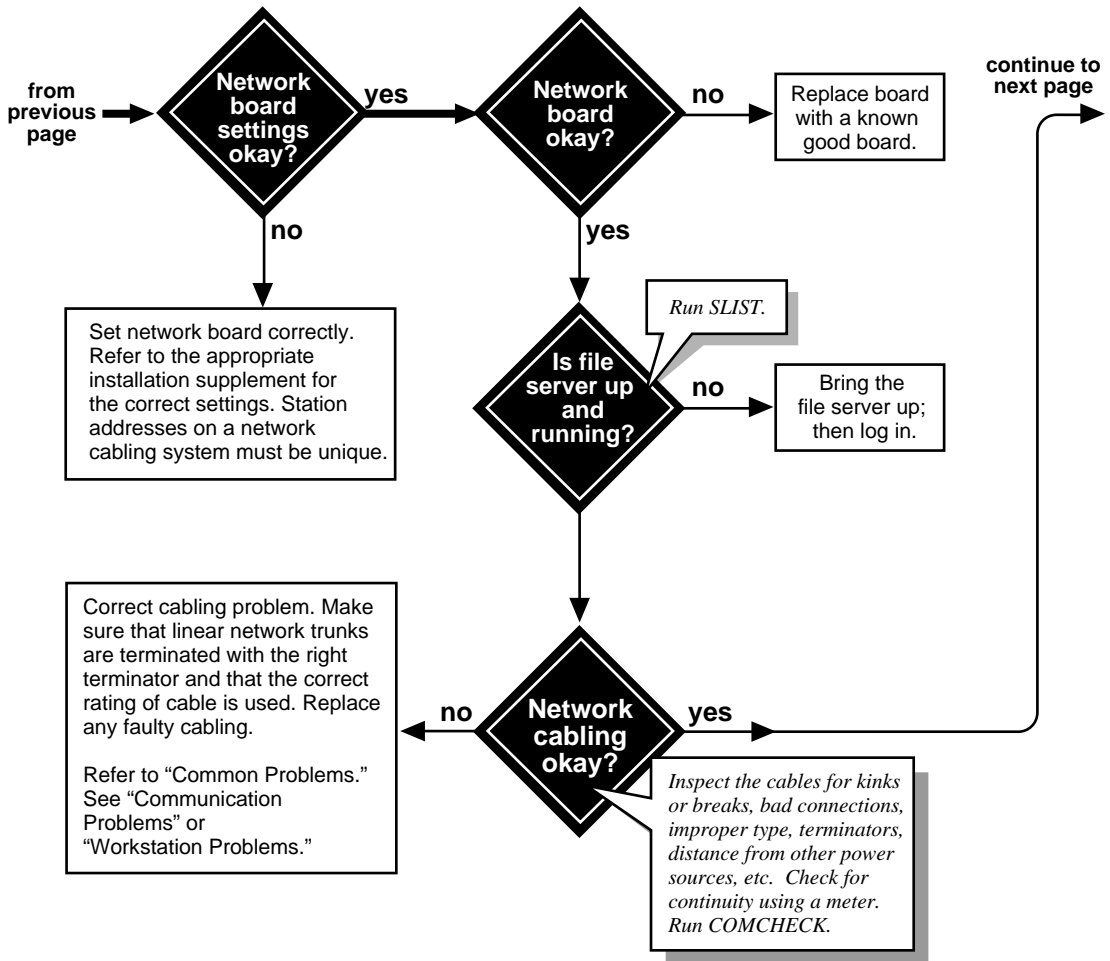
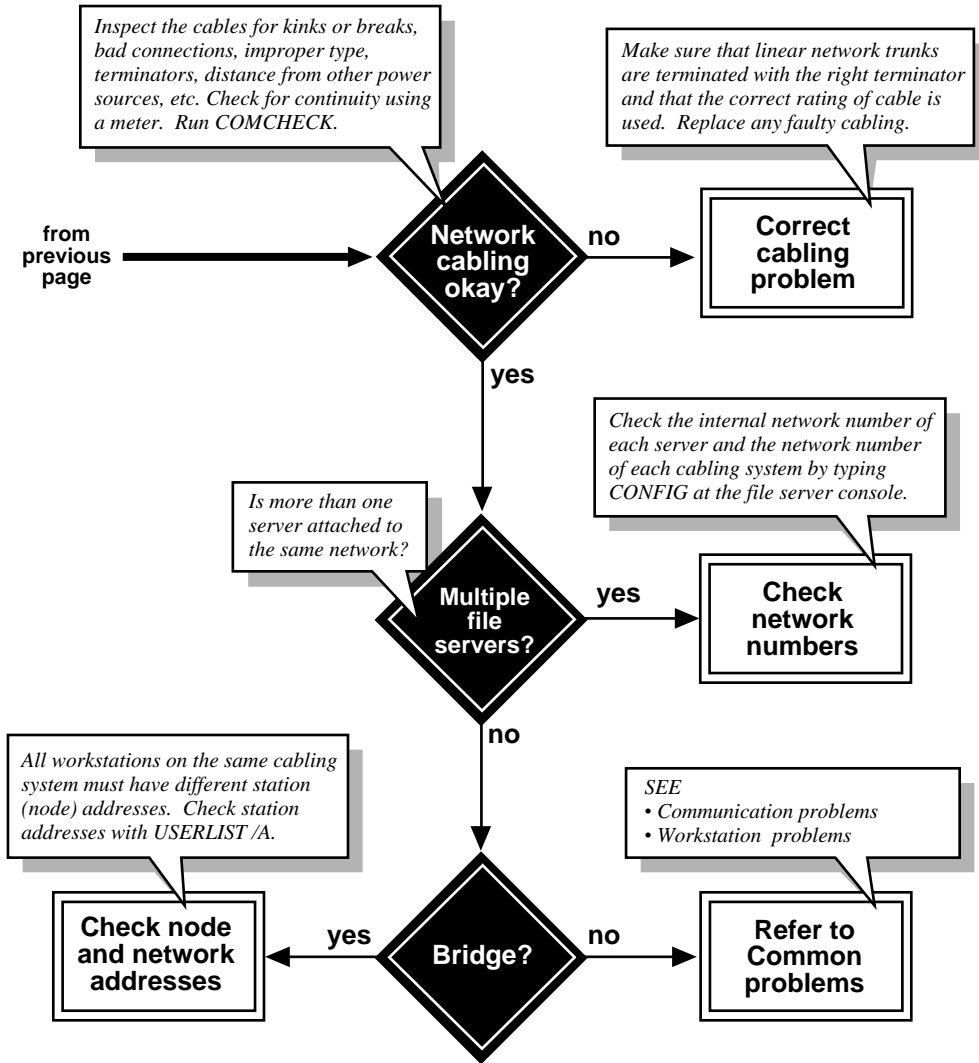


Figure 54 Workstation flow chart

Workstation







Common Problems

This portion of the troubleshooting section lists a number of solutions to specific problems that may be isolated by the flow chart. The solutions are organized into the following sections:

Section	Page
File server, hard disk, and volume problems	“File Server, Hard Disk, and Volume Problems” on page 382
Communication problems	“Communication Problems” on page 393
Workstation problems	“Workstation Problems” on page 403
Application problems	“Application Problems” on page 405
TTS problems	“TTS Problems” on page 419
If you need more help	“If You Need More Help” on page 421

File Server, Hard Disk, and Volume Problems

File server and hard disk problems commonly appear during installation or upgrade. The conditions are explained on the following pages.

Section	Page
General solutions	“General Solutions” on page 383
Console commands cannot be entered at the file server console, or they do not function correctly	“Console Commands Cannot Be Entered at the File Server Console, or They Do Not Function Correctly” on page 384
The file server does not keep track of time correctly	“The File Server Does Not Keep Track of Time Correctly” on page 385
The file server “hangs” after mounting the last volume	“The File Server “Hangs” After Mounting the Last Volume” on page 385
The operating system reports FAT errors when the file server is first booted after the installation of an RX-Net network board	“The Operating System Reports Fat Errors When the File Server is First Booted After the Installation of an RX-Net Network Board” on page 386

Section	Page
A hard disk cannot be accessed	“A Hard Disk Cannot Be Accessed. (The Format or Surface Test Options in Install Will Not Run, for Example)” on page 386
None of the volumes, including SYS: , were mounted	“None of the Volumes, Including SYS:, Were Mounted” on page 387
The operating system reports disk errors when a volume is being mounted	“The Operating System Reports Disk Errors When a Volume is Being Mounted” on page 388
The operating system reports memory errors when a volume is being mounted	“The Operating System Reports Memory Errors When a Volume is Being Mounted” on page 388
A volume cannot be mounted because of corrupted directory tables or FATs	“A Volume Cannot Be Mounted Because of Corrupted Directory Entry Tables or FATs” on page 391
A volume cannot be mounted because a name space module was not loaded first	“A Volume Cannot Be Mounted Because a Name Space Module Was Not Loaded First” on page 392

General Solutions

If the problem occurred after installation, it may indicate that the network was installed incorrectly. Do the following first:

- ◆ Check all network boards for possible conflicting address and I/O settings. See [“Troubleshooting LAN Drivers” on page 159](#).
- ◆ Each component should be able to work as a standalone system. Remove all network boards in the file server and boot DOS. Add each board and make sure that DOS still boots. Make sure that all cables are fastened securely to all network boards and network connectors and that terminating resistors are installed correctly.

Console Commands Cannot Be Entered at the File Server Console, or They Do Not Function Correctly

Possible Causes

- ◆ The NetWare operating system may be configured incorrectly.
- ◆ You are not looking at the command screen.
- ◆ The SERVER.EXE file is corrupted.
- ◆ The server has been downed.
- ◆ The server has hung.

Possible Solutions

- ◆ Check your file server records of network board configurations. Then check the actual hardware configuration on each network board in the file server to ensure that the two match.
- ◆ If your recorded network board configurations do not agree with the actual hardware configurations, reload the LAN driver with the correct parameters or change the hardware settings to match the LAN driver parameters.
- ◆ Check all network board settings for possible interrupt and I/O port conflicts. You can set an interrupt on a network board incorrectly and still have the file server boot up initially. The most common conflict occurs when a network board is set to interrupt 4 and a printer is connected to the file server's serial port, which also uses interrupt 4.
- ◆ Make sure all cables are fastened securely to all network boards and network connectors. Check the cabling for proper termination.
- ◆ From a backup, copy a new version of SERVER.EXE to the file server boot directory and reboot the file server.
- ◆ Have all users close their files and log out. Down the file server, if possible. If not, wait a few minutes after all users have logged out; then reboot the file server.

The File Server Does Not Keep Track of Time Correctly

Possible Causes

When the file server is booted initially, the NetWare operating system gets the date and time from the internal clock. After that, the operating system keeps track of time by counting the computer's clock "ticks." If the oscillator on the main system board is fast or slow, the system time is fast or slow accordingly.

Possible Solutions

- ◆ If the file server only loses time when the server is off, the battery may be low or dead. Replace the battery.
- ◆ If replacing the battery does not help, replace the main system board.

The File Server "Hangs" After Mounting the Last Volume

Possible Causes

- ◆ The file server network board may not be initializing when the file server is brought up because the board is not installed or seated correctly.
- ◆ The file server network board may not be configured correctly.

Possible Solutions

- ◆ Run CONFIG at the file server console to see what settings appear on the screen. Check the network board configurations. Make sure the settings match.
- ◆ Make sure that all file server and workstation network boards are seated properly and that cabling and connections are attached securely.
- ◆ Make sure that the terminators on cables have the right ohm rating and are installed correctly. The IBM PC Cluster sends a broadcast message during initialization and hangs if the network is not cabled or terminated properly.
- ◆ Check the network boards in all workstations for correct station address settings.

The Operating System Reports Fat Errors When the File Server is First Booted After the Installation of an RX-Net Network Board

Possible Cause

The network board was not connected to an active hub or to a workstation that was powered on.

Possible Solution

An RX-Net system using third-party network boards must be connected to an active hub (powered on) or another workstation (powered on) when the server is booted.

A Hard Disk Cannot Be Accessed. (The Format or Surface Test Options in Install Will Not Run, for Example)

Possible Causes

- ◆ The disk driver has not been loaded.
- ◆ A hard disk is not installed or cabled correctly.
- ◆ The communication channel between the controller interface board, the host bus adapter, and the hard disk is not functioning.
- ◆ The hard disk controller interface board is not terminated or addressed correctly.
- ◆ The hard disk has not been partitioned.

Possible Solutions

- ◆ Make sure the disk driver is loaded. Run MODULES to view the loaded disk drivers. Use DISKSET if you have loaded the host-bus-adapter driver more than once.
- ◆ Check the cables between the hard disks and the controller interface boards. Be sure Pin 1 of each cable is attached to Pin 1 of each connector.
- ◆ Check the power cables and make sure they are seated correctly in the power sockets on the hard disks and on the controller interface boards.
- ◆ Check the jumper settings on the host bus adapter, the controller interface board, and the hard disk. See the hardware documentation for correct jumper settings.

- ◆ Run DISKSET to make sure the hardware configurations contained on the EEPROM chip on the host bus adapter match the hard disks in your file server.
- ◆ Run DOS FDISK for internal hard disks.
- ◆ Load INSTALL to check the NetWare partition and volume information on the hard disk.
- ◆ Make sure that each controller interface board connected to the same host bus adapter has its own valid address.

None of the Volumes, Including SYS:, Were Mounted

Volume SYS: is the backout volume for TTS. It also contains the bindery files and NLMs. If this volume does not mount when the file server is booted, the AUTOEXEC.NCF file will not execute, LAN drivers will not load, the bindery cannot be opened, and TTS will not be enabled.

Possible Causes

- ◆ Volume SYS: is corrupted.
- ◆ The hard disk containing volume SYS: has failed.
- ◆ The cable or power to the external hard disks has malfunctioned.

Possible Solutions

- ◆ Run VREPAIR on volume SYS:.
- ◆ Check the cabling and power to the external hard disks. Replace any faulty components.
- ◆ Replace the hard disk containing volume SYS:.
- ◆ If you install a new hard disk type to replace the hard disk in a disk subsystem, be sure to run DISKSET.
- ◆ Load INSTALL to create the partitions and volume SYS:.
- ◆ Restore the data from a backup copy.

The Operating System Reports Disk Errors When a Volume is Being Mounted

Possible Causes

- ◆ The file server does not have enough memory to mount the volume.
- ◆ The operating system is experiencing directory sector mismatching. This mismatching can be caused if the media is defective or if the file server is turned off without the DOWN command.

Possible Solutions

- ◆ Load MONITOR and check the status of the available cache buffers. If the cache buffers are less than 20%, add more memory to your file server.
- ◆ Minor will correct themselves through normal network use. For example, if a FAT entry is wrong, the entry is updated and corrected the next time it is written to. If errors do not correct themselves, run VREPAIR.
- ◆ Some problems may be corrected automatically with TTS.

The Operating System Reports Memory Errors When a Volume is Being Mounted

Possible Causes

- ◆ Volumes take more memory to mount than they require after being mounted because the mounting process performs consistency checks (for example, the duplicate copies of all the tables are checked).
- ◆ Volumes and directory entries grow dynamically. Therefore, if your file server is using most of the memory (file cache buffers are close to 20% of the memory) and you dismount a volume, you may not be able to remount the volume unless additional memory is available.
- ◆ Each additional name space support that you add to a volume increases the size of the FATs and Directory Tables. Adding name space support can cause the tables to grow so large that the file server does not have enough memory to mount the volume.

Possible Solutions

- ◆ Load MONITOR and check the status of the available cache buffers. If the cache buffers are less than 20%, add more memory to your file server.
- ◆ Free up memory by unloading resources.
- ◆ Streamline the directory structure. Every subdirectory takes at least one directory block (a 4KB block of memory). Therefore, subdirectories with only one file require as much memory as directories with 32 files. If you combine directories so that most directories have about 32 files and purge the deleted subdirectories and files, you can free up memory.
- ◆ Remove the recently added name space support. This is a destructive step and destroys all the extended file information. Before taking this step, try to free enough memory so that the volume mounts and you can back up the data.

Have all users log out, and then unload all modules except the volume's disk drivers. Dismount any mounted volumes. Down the file server and reboot it to return memory from the Permanent and Alloc pools to the Cache Buffer pool.

To remove the name space, load VREPAIR and select the "Remove All Name Space Entries" and "Write Changes Immediately To Disk" options. Then run VREPAIR on the volume that will not mount.

- ◆ Calculate how much memory you need and add memory to the file server. View current volume size with INSTALL "INSTALL" on page 69. Then use the following chart to estimate the total amount of memory needed per volume.

Figure 55 Calculating memory needed for added name space

How much memory does your server need?

1. Calculate the memory requirement for each volume.

For each DOS volume:

$$M = .023 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

For each volume with added name space:

$$M = .032 \times \text{Volume Size (in MB)} \div \text{Block Size (default is 4)}$$

2. Add the memory requirements for all volumes.

$$\text{Total Volume Memory} = M_{\text{SYS}} + M_{\text{VOL1}} + M_{\text{VOL2}} + \dots$$

3. Add 2 MB for the operating system and round the figure to the next higher MB.

4. Your computer needs at least 4 MB to run NetWare. If Steps 1 through 3 have only arrived at 3 MB, assume a minimum memory requirement of 4 MB anyway.

Example:

A server has four volumes, each with a block size of 4:

SYS: an 80MB DOS volume

DOSVOL: a 100MB DOS volume

UNIXVOL: a 300MB volume with name space

MACVOL: a 100MB volume with name space

1. Memory requirement for each volume:
 $M_{\text{SYS}} = .023 \times 80 \text{ MB} \div 4 = 0.46 \text{ MB}$
 $M_{\text{DOSVOL}} = .023 \times 100 \text{ MB} \div 4 = 0.575 \text{ MB}$
 $M_{\text{UNIXVOL}} = .032 \times 300 \text{ MB} \div 4 = 2.4 \text{ MB}$
 $M_{\text{MACVOL}} = .032 \times 100 \text{ MB} \div 4 = 0.8 \text{ MB}$

2. Total volume memory requirements: $0.46 + 0.575 + 2.4 + 0.8 = 4.235 \text{ MB}$

3. Operating system memory requirements: $2 + 4.235 = 6.235 \gg 7 \text{ MB}$

4. 7 MB is higher than the 4 MB minimum; therefore, no further adjustment is needed. Your server needs at least 7 MB of memory.

A Volume Cannot Be Mounted Because of Corrupted Directory Entry Tables or FATs

Possible Causes

The following can cause mismatches in the duplicate copies of the FAT and Directory Entry Table:

- ◆ A power failure occurs and the file server is not downed with the DOWN command.
- ◆ A hard disk fails.
- ◆ A disk channel error occurs.
- ◆ A volume is not dismounted with the DISMOUNT command.
- ◆ Directory information in cache is not completely written to disk.

Possible Solutions

Complete one or more of the following:

- ◆ Run VREPAIR.
- ◆ Add a UPS system so that the file server is automatically downed when a commercial power failure occurs.
- ◆ Replace faulty disks or controllers.
- ◆ If the volume resides on mirrored hard disks, salvage the data on one of the drives. Use INSTALL to unmirror the hard disks (highlight the hard disk you think is least reliable and delete that disk from the mirroring list). Then run VREPAIR on the volume and mount the volume. If the volume will not mount or the data shows some corruption, read the next suggestion before remirroring the hard disks.
- ◆ If the volume resides on mirrored hard disks, salvage the data on both hard disks. Use INSTALL to unmirror the hard disks and to salvage the orphaned (“Out Of Sync”) hard disk as a new volume. Run VREPAIR on both the old and the new volumes. Mount both volumes and compare the files. Use INSTALL to delete the volume that has the least useful information; rename the salvaged volume, if necessary. Then use INSTALL to remirror the hard disks.

A Volume Cannot Be Mounted Because a Name Space Module Was Not Loaded First

Possible Causes

Once a volume has been configured to support more than the DOS naming convention, the loadable name space module must be loaded before the volume can be mounted. One of the following has probably occurred:

- ◆ The command to load the name space module is not in the STARTUP.NCF file.
- ◆ The module to load the name space has not been copied to the boot directory of the file server.

Possible Solutions

- ◆ Load the name space module; then mount the volume. Copy the name space module to the file server boot directory (C: or A:), and add the load command to the STARTUP.NCF file. The module then loads automatically whenever the file server is booted.
- ◆ Delete the name space configuration from the volume. *This is a destructive step and destroys all the extended file information.* Back up all non-DOS files. Then load VREPAIR and select the “Remove All Name Space Entries” and “Write Changes Immediately To Disk” options. Then run VREPAIR on the volume.

Communication Problems

Communication problems are related to network boards, LAN drivers, network performance, and file server/workstation communications, as well as to internetwork communications. The problems are treated on the following pages:

Section	Page
General solutions	“General Solutions” on page 393
The file server does not boot after a network board is installed	“The File Server Does Not Boot After a Network Board Is Installed” on page 395
The file server could not be found by the workstations on the network	“The File Server Could Not Be Found by the Workstations on the Network” on page 395
File servers do not recognize each other on the network	“File Servers Do Not Recognize Each Other on the Network” on page 397
Responses from the file server are noticeably slow	“Responses from the File Server Are Noticeably Slow” on page 398
Workstations can log in, but periodically lose their connections to the file server	“Workstations Can Log In, But Periodically Lose Their Connections to the File Server” on page 399
ARCnet-specific problems	“ARCnet-Specific Problems” on page 400
Ethernet-specific problems	“Ethernet-Specific Problems” on page 401
Token-Ring-specific problems	“Token-Ring-Specific Problems” on page 402

General Solutions

If the problem occurred simultaneously on several workstations, it is probably a result of one of the following:

- ◆ The file server network board is not seated or configured correctly.
- ◆ The network board cable from the file server is faulty.
- ◆ Cabling on the network is faulty.
- ◆ The connector closest to the file server is faulty.
- ◆ The RX-Net active hub is off.
- ◆ The repeater is off or nonfunctional.

- ♦ The cabling is not terminated.
- ♦ Volume SYS: is not mounted.

Possible Solutions

- ♦ Run VOLUMES at the file server console. If SYS: is not mounted, mount it. The file server does not broadcast to the network until SYS: is mounted.
- ♦ Run CONFIG at the file server console to check the configuration of the network boards. Then down the file server, turn off the power, and check the actual network board settings:
- ♦ Make sure all settings agree with the settings used to load the driver. If you load the driver with an interrupt that conflicts with the board's setting, the network board cannot broadcast on the network.
- ♦ Make sure the node (station) address on the board is a legal address. Addresses 0 and FFFFFFFF are reserved for NetWare, so do not use them.
- ♦ Run CONFIG at the file server console to make sure that each network board has a LAN protocol bound to it. Network boards cannot broadcast without a protocol.
- ♦ Run USERLIST /A at a workstation, if possible, to check node (station) addresses. Each station address on the network should be unique. Sometimes you can find the problem by turning off all workstations and bringing them up one at a time.
- ♦ Check all hubs and repeaters to make sure they are on.
- ♦ Check the cables for proper termination.
- ♦ Make sure the file server network board is seated properly.
- ♦ Replace the file server network board with a board that works correctly. Make sure it has the same jumper settings.
- ♦ Have a user log in to the network from a workstation. Load MONITOR and select "Connection Information" from the "Available Options" menu. If the "Active Connections" list shows the user's login name, the file server is receiving and responding to the workstation shell's request.

If the workstation receives a "File server cannot be found" error, continue replacing segments of cable and cabling connections until communication is restored.

The File Server Does Not Boot After a Network Board Is Installed

Possible Causes

- ◆ The network board is not attached properly to the cable.
- ◆ The hardware conflicts with other boards, the monitor, or ports in the file server.

Possible Solutions

- ◆ Cable the network board to at least one workstation and check the termination.
- ◆ Make a list of all I/O ports, interrupts, and memory addresses used by the equipment. Use the “File Server Worksheet” in *Installation and Upgrade* to record the information. Also do the following to identify potential conflicts.
- ◆ Check the documentation that comes with the computer and all installed hardware components.
- ◆ Make sure no two pieces of hardware are using the same I/O port, interrupt, or memory address.
- ◆ Make sure that the memory range for the I/O ports and memory addresses do not overlap.
- ◆ Reconfigure the equipment so that no conflicts exist.
- ◆ For additional information, see [“Troubleshooting LAN Drivers” on page 159](#).

The File Server Could Not Be Found by the Workstations on the Network

Possible Causes

- ◆ The network board may not be initializing when the file server is brought up because it is not configured correctly or it has failed.
- ◆ The file server may be anticipating the wrong frame type.
- ◆ Address or interrupt conflicts may exist between two boards within the file server or between a board and the computer’s hardware.
- ◆ The file server may not have enough packet receive buffers.

- ♦ A protocol (IPX) may not have been bound to the network board.
- ♦ The cabling may be too close to sources of interference.
- ♦ Volume SYS: may not be mounted.

Possible Solutions

- ♦ Run CONFIG at the file server console to see what settings appear on the screen. Then check network board configurations in the file server. Be sure the network board configurations match the settings that appear when you run CONFIG.
- ♦ Run VOLUMES at the file server console to ensure that SYS: is mounted. SYS: must be mounted before the file server can advertise its name to the network.
- ♦ Make sure all network connectors (including transceivers and repeaters) are installed and the cable is attached securely.
- ♦ Check node (station) address settings on all file server and workstation network boards. Each address should be unique.
- ♦ Check all network numbers (internal and cable). Each file server and cabling system should have a unique network number.
- ♦ Make sure no two boards in the file server are using the same I/O port, memory address, or interrupt.
- ♦ Make sure all network boards are seated firmly and the cabling connections are in place.
- ♦ Bind the driver (TRXNET, NE1000, TOKEN, etc.) to IPX (or another communication protocol).
- ♦ Make sure the network cable is terminated properly. Many network boards send a broadcast message during initialization and hang if the network is not cabled or terminated properly.
- ♦ If you have a lot of network interaction, increase the maximum number of packet receive buffers. See **“SET” on page 250**.
- ♦ Check cabling for interference from fluorescent lights, microwaves, radar, x-rays, and copy machines. Either move the cable or shield it from the source of interference.

File Servers Do Not Recognize Each Other on the Network

Possible Causes

- ◆ The hardware settings in the file server are incorrect.
- ◆ The network or internetwork addresses conflict.
- ◆ The bindery is corrupted.

Possible Solutions

- ◆ Run CONFIG at the file server console to see what settings appear on the screen. Then check network board configurations in the file server. Be sure the network board configurations match the settings that appear when you run CONFIG.
- ◆ Check the internal network number for the file server and the network number for the cabling.

When multiple file servers share the same cabling system (called a multiserver network), all file servers must have the same cabling network number. However, the file servers must have unique file server internal network numbers and unique station addresses.

When network cabling systems are connected through bridges (internal or external), each cabling system must have a unique network number. NetWare v3.1x file servers must also have a unique *internal* network number apart from the cabling. The unique network address is the first item read in a packet sending/receiving interaction.

- ◆ Run BINDFIX if you suspect a corrupted bindery.
- ◆ Reset the router with the RESET ROUTER console command.
- ◆ Check the cabling system for faulty termination.
- ◆ Down all file servers except one. Reset its router with RESET ROUTER. Bring up each file server, one at a time, establishing communications with it before bringing up the next one. Run DISPLAY NETWORKS to check for duplicate network addresses as each file server is booted.

Responses from the File Server Are Noticeably Slow

Possible Causes

- ◆ The workstation network board is slow or faulty.
- ◆ Network cabling is faulty.
- ◆ The file server network board is slow or faulty.
- ◆ Too many users are using the network.
- ◆ The file server speed is not set to the highest speed.
- ◆ The file server hard disk is slow or faulty.
- ◆ The file server is low on memory.
- ◆ The volume has too many deleted files.
- ◆ Network traffic is extremely high.
- ◆ The cabling system is experiencing too much interference.
- ◆ A hard disk has failed or is failing.
- ◆ Insufficient directory buffers, cache buffers, or packet receive buffers have been allocated.

Possible Solutions

- ◆ Check the computer's documentation for switch information. Set the CPU speed to its highest setting. Use SPEED to verify that the CPU is running at the appropriate speed.
- ◆ If a workstation or the file server seems slow, insert a new network board into the slow computer to check performance. If the speed is still below normal, reinstall the original network board and replace the cable attaching the workstation or file server to the network.
- ◆ Load MONITOR to check the status of the memory. If the Cache Buffers pool is near 20%, install more memory in the file server. If the Alloc Memory pool is near 8,000,000 bytes, use the "Maximum Alloc Short Term Memory" parameter in SET to increase the pool by 1MB.

- ◆ Load MONITOR to check the status of packet receive buffers and service processes. Compare their values to the maximum allowable. Use SET to increase the values for the following parameters if your system is at the maximum value: “Maximum Service Processes” and “Maximum Packet Receive Buffers.” For additional ideas, see [“Memory Maintenance” on page 360](#).
- ◆ Load MONITOR and check the Hot Fix status of all hard disks. Check the mirroring status of all mirrored disks.
- ◆ Run PURGE to eliminate deleted files.
- ◆ Load MONITOR and check the LAN driver statistics. If you have more than one network board, compare the boards’ “Total packets sent” statistics. If one board is receiving most of the traffic, recable the network so that the boards have equal loads.
- ◆ If you are on a multiserver network or an internetwork, recable the system with a backbone to reduce network traffic. See “Bridges” in *Concepts* for a description of a backbone.
- ◆ Check the cabling for interference from fluorescent lights, microwaves, radar, x-rays, and copy machines. Either move the cable or shield it from the source of interference.

Workstations Can Log In, But Periodically Lose Their Connections to the File Server

Possible Causes

- ◆ A network board in either the file server or a workstation is faulty.
- ◆ A user on the network is using an old shell file.
- ◆ Two workstations have the same node (station) address.
- ◆ The cabling system is not terminated properly.

Possible Solutions

- ◆ Run USERLIST /A. Make sure all node (station) addresses are unique.
- ◆ Check all boot files. Make sure everyone is using the latest version of the shell files.
- ◆ Check the cabling for improper termination, loose connections, and faulty components.

- ◆ Use a LAN analyzer product to check the network boards, cables, and packets. (NetWare Care and a LANalyzer are available from Novell.) Replace faulty boards and cables.
- ◆ Use the appropriate NetWare installation supplement to review the cabling specifications for your cabling system. Make sure your system is in compliance with all the specifications.
- ◆ Set the console to display all workstation connections cleared by the watchdog. See **“SET” on page 250**.
- ◆ If workstations are being cleared by the watchdog, check all network boards and the entire cabling system between the workstations and the file server. Check for faulty cables, improper termination, and faulty hubs.

ARCnet-Specific Problems

Possible Causes

- ◆ The passive or active hubs are faulty.
- ◆ The network boards are faulty.
- ◆ Receive buffer sizes conflict.
- ◆ Node addresses are illegal or conflicting.
- ◆ The monitor board conflicts with the network board.
- ◆ Improper cable lengths connect to passive or active hubs.
- ◆ Two passive hubs are connected together.
- ◆ A passive hub is terminated improperly.

Possible Solutions

- ◆ Run USERLIST /A. Make sure that all node (station) addresses are unique and that no station uses 0.
- ◆ Check the fuses in all active hubs. Replace faulty fuses.
- ◆ If active hub lights blink, bad packets are being sent on the network. Check for conflicting node addresses, bad network boards, and improperly terminated passive hubs.
- ◆ Check all passive hubs for proper termination.

- ◆ Check the cable lengths connecting active and passive hubs to ensure that they are within specifications. (See the appropriate NetWare installation supplement to review the cabling specifications for your network board.)
- ◆ If the monitor is blank when the network board is in the workstation, the monitor could be using interrupt 2. Try setting the network board to an option that does not use interrupt 2. (See the appropriate NetWare installation supplement for a list of supported options for your board.)
- ◆ Check the cabling system for loopbacks, such as a cable from an active hub that attaches back to the active hub rather than to a workstation. Make sure that two passive hubs are not cabled to each other.

Ethernet-Specific Problems

Possible Causes

- ◆ T-connectors are not terminated properly.
- ◆ The network board is set up for one type of cabling, but it is connected to a different type (such as thick Ethernet instead of thin Ethernet).
- ◆ Hardware conflicts exist between the workstation and the network board.
- ◆ The workstation and the file server are using two different Ethernet frame types.

Possible Solutions

- ◆ Check for faulty termination. Each T-connector that has only one cable attached to it must be terminated. Each trunk must be terminated with a grounded terminator.
- ◆ Check the network boards. Make sure that the board is set for the type of cabling (thick or thin) you are using.
- ◆ Some VGA boards use interrupt 3. If the monitor is blank when the network board is installed, set the network board to an option that does not use interrupt 3. (See the appropriate NetWare installation supplement for a list of supported options for your network board.)
- ◆ Make sure that the file server LAN drivers and the workstation LAN drivers have been configured for the same Ethernet frame type. For information on frame types, see “Ethernet configuration” in *Concepts*. Configure the workstations for the appropriate frame type.
- ◆ For instructions on configuring DOS ODI drivers, see *ODI Shell for DOS*.

- ◆ For the parameter you need to configure the Ethernet LAN driver in the file server, see “LOAD LAN driver” on page 133.
- ◆ Check terminators with an ohm meter for a resistance of 48 to 52 ohms. Replace any terminators that do not fall within the specified range.
- ◆ If you have used DOS ODI drivers or specialized software that sets the node address of the network boards, run USERLIST /A to make sure that each network board has a unique node address.

Token-Ring-Specific Problems

Possible Causes

- ◆ A MAU is faulty.
- ◆ A MAU has been set improperly.
- ◆ A faulty Token-Ring adapter has been installed in a workstation or file server.
- ◆ TOKREUI/LAN Support has not been loaded at the workstations.

Possible Solutions

- ◆ Reset the MAU.
- ◆ Check the MAU for faulty fuses, power problems, and bad ports.
- ◆ Check for faulty Token-Ring adapters by running the DXMAID program found on the IBM *LAN SUPPORT PROGRAM* diskette.
- ◆ Check for breaks in the daisy-chained MAUs.
- ◆ Check for duplicate node addresses if you have used DOS ODI drivers or specialized software to set the node addresses.
- ◆ Run DXMAID at each workstation and set LAN Support to load automatically when the workstation is booted. The DXMAID program is on the IBM *LAN SUPPORT PROGRAM* diskette.

Workstation Problems

The workstation problems discussed here are for problems that occur on only one network workstation. If the problems occur on more than one workstation simultaneously, see [“Communication Problems” on page 393](#).

If the problem occurred on only one workstation, it can probably be traced to one of the following sources:

- ◆ The workstation itself is not operating properly.
- ◆ The network shell is corrupted.
- ◆ The network board is faulty.
- ◆ The network board is not set correctly.
- ◆ The cabling attached to the workstation is faulty or connected improperly.
- ◆ The network shell’s configuration does not match the network board’s configuration.

Possible Solutions

- ◆ Boot the workstation with DOS only. Then run the computer’s diagnostics utility to make sure that the computer can recognize all internal components. (For example, run the IBM PC AT Diagnostic for an IBM PC AT or IBM PC AT compatible.)
- ◆ If DOS cannot load, refer to the manufacturer’s hardware installation or maintenance manual for your particular computer.
- ◆ Recopy the NetWare boot files to the boot diskette. If the files were generated with SHGEN, copy the files from the master shell diskette or rerun SHGEN. If the files are DOS ODI files, copy the files from a working copy of the NetWare ODI Shell for DOS diskette.
- ◆ Load MONITOR and select “Connection Information” from the “Available Options” menu. If the “Active Connections” list shows the user’s login name, the file server is receiving and responding to the workstation shell’s request.
- ◆ Set the “Console Display Watchdog Logouts” parameter to ON. See [“SET” on page 250](#).

- ♦ Check the interrupt, I/O, and base memory address of the board in question and make sure that the board settings match the shell you generated for that board. (Type “IPX I” to view the configuration information for the shell.) Make sure that the configuration does not conflict with any other hardware installed in the workstation. Reinstall the board and try again.
- ♦ Replace the network board with a board that you know works properly. Be sure the shell you are using is specific to the network board you are using. If the new network board does not work, replace the old board and check the cabling and the network connectors.
- ♦ Make sure that the cable is attached firmly to the network board and network connectors, and boot the workstation again.
- ♦ Install a cable you know works properly and reboot.
- ♦ Replace any network connectors (such as T-Connectors) and reboot the workstation.
- ♦ Log in when all other users are logged out. If you can log in from the workstation when you are the only user, you probably have a node address conflict.

Application Problems

Some application problems can occur when a NetWare utility and a software application perform the same tasks. Other network problems occur only when a particular software application is used. These problems are discussed on the following pages.

Section	Page
General installation problems	“General Installation Problems” on page 405
Compatibility problems (problems installing copy-protected applications; problems installing incompatible software)	“Application Problems: Compatibility” on page 407
File I/O problems (problems accessing files from the hard disk, caused by NetWare security or the workstation’s environment)	“Application Problems: File I/O” on page 408
File and record locking problems (problems using multiuser applications)	“Application Problems: File and Record Locking” on page 411
DOS utilities (problems using certain DOS utilities on NetWare)	“Application Problems: DOS Utilities” on page 413
General failure (problems causing the workstation to “hang” or be unresponsive)	“Application Problems: General Failure” on page 414
Miscellaneous problems (problems with archiving/backup, asynchronous communication, screen display, and search paths)	“Application Problems: Miscellaneous” on page 416

General Installation Problems

Possible Causes

- ◆ Insufficient rights were granted to the users in trustee assignments.
- ◆ Insufficient rights were granted to the user installing the application.
- ◆ The application was installed too deep in the directory structure.
- ◆ The application files were copied to the network rather than installed with the application’s installation program.
- ◆ All the application files were flagged SRO.

- ◆ The workstations' CONFIG.SYS files were not modified.
- ◆ Conflicts exist between the application's interrupt and the network boards installed in the workstations and the file server.
- ◆ Conflicts exist between the NET.CFG parameters and the CONFIG.SYS parameters.
- ◆ Search drives were not mapped in the users' login scripts or in the system login script.
- ◆ A single-user version of the software was installed.

Possible Solutions

- ◆ If you can run the application when you are logged in as SUPERVISOR, but cannot run it when you are logged in as a user, you have not granted the right trustee assignments to the users.
- ◆ Create a group for the application and grant the group all rights to the application's directory. Delete one right from the trustee assignment, log in as a member of the group, and try to run the application. Users need at least Read, Create, Delete, Write, Modify, and File Scan rights if they are going to write to files.
- ◆ Some applications create temporary files. Map a search drive to the application and have users try running the application from a directory to which they have all rights.
- ◆ Some applications create the temporary files in the same directory as the data files. Users need at least Create, Delete, File Scan, and Read rights at the directory level for these types of applications.
- ◆ Some applications check for rights at the root directory when they are installed. You must log in as SUPERVISOR to install these types of applications.
- ◆ Not all application files can be flagged SRO. If the user needs to write to the file, flag the file SRw.
- ◆ Use the MAP ROOT command to make the application's current directory a root directory. Then try to run the application. (You may have to reinstall the application after you change the directory to a root directory.)
- ◆ If the MAP ROOT command does not solve the problem, try installing the application in a directory below the volume level.

- ◆ Install the application using the application's installation program. Some applications' files cannot just be copied to the network. They must be installed using the application's installation program.
- ◆ Read the application's installation documentation. Modify all workstation CONFIG.SYS files to handle the application's requirements (such as number of open files or additional memory required for the DOS environment).
- ◆ Make sure that the NET.CFG parameters do not conflict with the CONFIG.SYS parameters. If your application needs 50 open files, the CONFIG.SYS parameter (files = 50) and the NET.CFG parameter (file handles = 50) must be changed.
- ◆ Add search mappings to the user or system login script. If you create groups for your applications, use the IF...THEN command in the system login script to set up the search mappings for the users accessing the application.
- ◆ Contact the vender for a multiuser version of the software.

Application Problems: Compatibility

This section covers problems with copy-protected applications and incompatible applications running on NetWare.

NOTE: Novell does not condone the use of single-user applications in a network environment. Most applications have multiuser versions that should be purchased to avoid copy-protection violations and environment problems inherent in single-user applications.

The Application Is Copy Protected and Cannot Be Installed on the File Server's Hard Disks

Possible Cause

Absolute DiskRead-INT 25h or Absolute DiskWrite-INT 26h are not valid function calls on NetWare. These interrupts transfer control directly to the DOS device driver. Since there are no local DOS device drivers for the file server's hard disks, the application will return errors when used on drives mapped to network hard disks.

Possible Solution

The application may require a “key diskette” to be placed in the workstation’s local hard disk in order to run, or you may need to buy a multiuser version of the application.

The Application Is Supposed to Work on DOS v3.1 and Later, But It Does Not Recognize NetWare

Possible Causes

Some applications use the Get Machine Name function call (5E00h Interrupt 21h) to check for the IBM PC Network Program and to ensure that all workstations on the LAN have a unique call number.

- ◆ Some applications use the PC LAN Network Program’s LAN Installation Check (B800h Interrupt 2Fh) or the SHARE Installation Check (INT 2F) to see if the application is running on a LAN.

Possible Solutions

- ◆ If the application uses the Get Machine Name function call, give the user’s workstation a machine name in each login script, using the `MACHINE="NAME"` command. Replace *NAME* with a unique name (in all capitals) for each user. For example, add the following line to the user’s login script:

```
MACHINE="HARRY'S STATION"
```

- ◆ If the application uses an installation check, load either `SHARE.COM` or `INT2F.COM` (Rev 2). `INT2F.COM` is located on the *DOS / DOS ODI Workstation Services* diskette.

Application Problems: File I/O

Possible Cause

When accessing a file from the file server’s hard disk, you may encounter problems with NetWare’s security or the workstation’s environment. See “Security” in *Concepts*.

Possible Solutions

- ◆ NetWare's default flag settings for a file are Non-Shareable/Read Write. This default cannot be changed; however, you can modify a file's flag by using the FLAG command. For more information, see "FLAG" in *Utilities Reference*.
- ◆ You can also set and modify flags using some applications.

A File Has Been Flagged Shareable and Now It Is Non-Shareable

Possible Causes

- ◆ The file has been overwritten by a program that recreates the file. Often a file is read into a temporary working file for modification. When the modification is done, the application deletes the original file and renames the temporary file to the original filename. The original file attributes are lost and the modified file takes on the attributes of the temporary file.
- ◆ The application is setting the file attributes.

Possible Solutions

- ◆ Flag the file Read Only to prevent the file from being recreated or overwritten. Also, you can contact the software developer, who can create the temporary file with a Shareable flag.
- ◆ If the application is setting the file attributes, you may not be able to share the file.
- ◆ Increase the trustee rights to the file.

An Application Cannot Find Files

Possible Causes

- ◆ The user does not have sufficient rights to a directory.
- ◆ The file is being used by another workstation.
- ◆ The application cannot find the files because the search drives have been set up improperly.
- ◆ The user may not have adequate security rights given at the root directory for the application to find and open the file.

Some applications look for a file in the default directory, and then start a search at the root directory. In DOS, the application goes to the root of the default hard disk (such as H:\), and then searches down repetitively.

Possible Solutions

- ◆ Log in as SUPERVISOR. If SUPERVISOR can run the program, the user does not have sufficient trustee rights to the directory. For an explanation of a directory's Inherited Rights Mask and trustee assignments, see *Concepts*.

Give the user sufficient trustee rights to the directory. You may need to change the Inherited Rights Mask for the directory, giving the user sufficient effective rights to use a file in this directory.

- ◆ Load MONITOR; then determine if the file is open and being used by another workstation. Some applications return an error of "file not found" when the file is being used by another workstation.

No set directive exists on how low-level error codes should be handled by applications. Some applications have their own way of handling and interpreting DOS critical errors or NetWare's interrupt signals. This means that a DOS "file lock" may be interpreted by an application as a "file not found."

Read the application's documentation concerning error messages. If you need more assistance, contact the application vendor and ask how the low-level system error code is handled.

- ◆ Map a search drive to the directory containing the files the application will use. If the mapping solves the problem, add a search drive mapping to the login script.
- ◆ Run the program as SUPERVISOR. If you can run the application as SUPERVISOR, change the user's rights to include the entire directory path. Please note, however, that this solution sacrifices network security.
- ◆ Use SMODE to set a different search mode for the application. See *Utilities Reference*.

You Are Denied Writing Access to a File While Having Rights in the Directory

Possible Causes

- ◆ The file has been flagged as Read Only and cannot be written to.
- ◆ You do not have sufficient rights in the directory. If the file does not exist on the hard disk you are using, the shell may find the file in one of the search drives. If the file is found on a network drive, NetWare checks for appropriate rights. If you do not have sufficient rights in that directory, you cannot write to the file.
- ◆ Some applications may expect the NetWare v2.x rights convention. Since NetWare v3.1x rights are different, the application may not work correctly.

Possible Solutions

- ◆ Change the file's flag to Read Write.
- ◆ If you supply the filename to the application, preface the filename with a directory path. This shuts off the shell's search drive capability. If, on the other hand, you are not required to supply the filename to the application, you must copy the file into your current directory.
- ◆ Contact the application manufacturer for an upgraded version of the application that is compatible with NetWare v3.1x.

Application Problems: File and Record Locking

Because file sharing must be regulated in a multiuser environment, file and record locking attributes control users' access to information. This section lists some of the file and record locking problems you may encounter while running software applications on a NetWare network.

The File or Record Locking Is Not Working

Possible Causes

- ◆ The application is using DOS 3.1 or later file locking functions. However, the workstation did not boot with DOS 3.1 or later; therefore, the application cannot use this locking method.
- ◆ The application is using the logical record lock or semaphore-locking function, but the application is being accessed from an attached file server.

Possible Solutions

- ◆ If the application requires DOS 3.1 or later to perform its record-locking functions, be sure that the workstation is booted with DOS 3.1 or later.
- ◆ Check with the application vendor to see if the application can be run in a network environment.
- ◆ Do not use the application from a search drive if you are attached to other file servers. Log in directly to the file server rather than attaching to the file server across an internetwork. All workstations using the application must be logged in to the file server in order to use logical record locking.
- ◆ If the application is *not* written for a multiserver environment, do *not* map network search drives to the application's directory. Have each user map a regular drive to the application and execute the application from that drive.

You Have a Contaminated Database

Possible Causes

- ◆ The hard disk may be physically damaged.
- ◆ A power failure or spike may have occurred.
- ◆ The application uses a record/file locking algorithm that does not take into consideration a multiple file server environment.

Possible Solutions

- ◆ Use VREPAIR to find and repair inconsistencies in the FATs. You may also need to run BINDFIX to fix the bindery problems. See “VREPAIR” on page 325 and “BINDFIX” in *Utilities Reference*.
- ◆ If VREPAIR and BINDFIX do not solve the problem, make sure you have a recent backup copy of the entire hard disk. Run the surface test option in INSTALL. You can run a nondestructive test (which preserves all data) or a destructive test (which destroys all data). See “INSTALL” on page 69.
- ◆ Make sure all workstations execute the program from the same default drive on the same file server.
- ◆ If the database does not have its own protection against incomplete updates, use TTS to protect the database files. For information, see “TTS” in *Concepts*.

Application Problems: DOS Utilities

This segment lists some of the problems you may encounter while using DOS commands on a NetWare network.

The DOS v3.1 and Later BACKUP Command Will Not Back Up Files Flagged Shareable

Possible Cause

The DOS BACKUP command in DOS 3.1 and later is not compatible with the Shareable flag in NetWare.

Possible Solution

Flag files Non-Shareable or use NetWare's NBACKUP utility to back up data.

When You Are on a Hard Disk (Local or Network) and Type "DIR *volume name*", the Hard Disk Becomes Mapped to the Volume

Possible Cause

When you use the DOS DIR command with a volume name, the drive you are on is automatically mapped to the root, or volume, name.

Possible Solutions

- ◆ Use MAP to remap the drive.
- ◆ Do not use volume names in the DIR command.

When Path Is Used, All the Search Drives Are Lost

Possible Cause

The DOS PATH command deletes and overwrites NetWare search drives.

Possible Solutions

- ◆ Use the NetWare MAP command instead of PATH.
- ◆ Reboot the workstation or use MAP to set up the search drives again.

RENAME Will Not Work on NetWare Directories, But It Will Work on Files

Possible Cause

The RENAME command is a DOS command.

Possible Solution

Use the NetWare RENDIR utility to rename NetWare directories.

You are Receiving Error Messages Telling You to Load SHARE.COM

Possible Cause

You have not loaded SHARE.COM. Some data synchronization primitives (extended opens and DOS record locking) require that SHARE.COM be loaded.

Possible Solution

Under NetWare, it is not necessary to load SHARE.COM. Instead, load a much smaller program called INT2F.COM (Rev 2). This program simulates the presence of SHARE.COM in memory and supports the SHARE installation check. INT2F.COM is located on the *DOS /DOS ODI Workstation Services* diskette.

CHKDSK Does Not Function When Used on a Network Hard Disk

Possible Cause

CHKDSK is a DOS command.

Possible Solution

CHKDSK works only on a DOS hard disk (local hard disk). Use NetWare VOLINFO or CHKVOL to check the status of a NetWare volume.

Application Problems: General Failure

General failure problems occur when the application or workstation hangs or when the computer does not respond to a request made from the application.

The Application Hangs

Possible Cause

The application uses a software interrupt that is also used by NetWare.

Possible Solution

If you have an interrupt conflict, call your local vender or Novell for assistance. No industry policies exist to prevent interrupt conflicts.

The Program Hangs After a Netware Message Is Sent to the Workstation

Possible Causes

- ♦ The application takes over the keyboard and monitor, but the <Ctrl><Enter> prompt from the NetWare message is not displayed.
- ♦ The monitor is in graphics mode.

Possible Solution

Press <Ctrl><Enter> to free up the keyboard. If this does not work, reboot. Then use CASTOFF to prevent messages from being sent when you are using that application. Use CASTON when you exit the application and want to receive messages again. See “CASTOFF” and “CASTON” in *Utilities Reference*.

Several Users Are Working in an Application, But Another User Is Denied Access

Possible Causes

- ♦ The application programmer is limiting the number of users through the use of semaphores. For example, if an application has a limit of five users, the semaphore limit will prevent a sixth user from accessing the application.

Sometimes the workstation hangs because of the sixth user’s attempt to access the application. Sometimes the application appears to hang until the fifth user exits the application, making room for the sixth; then the sixth workstation can enter the application, and the application continues working.

- ♦ A communication resource limitation may exist if the application requires NetBIOS or NetWare’s NetBIOS emulator. This problem does not occur very often, because NetBIOS usually has enough resources.

Possible Solutions

- ◆ Make sure you have a site license for the application and stay within the limit of that license. If a site license is not available, the application may have a user limitation. Contact the application vendor about user limitations; and, if necessary buy an extended license.
- ◆ Check with the application developer for information on resource limitations with NetBIOS.

An Application Periodically Hangs for a Time Before It Continues; This Occurs at Different Times with No Apparent Pattern

Possible Causes

- ◆ The application may wait until the record or file is released from use. Instead of returning an error, the application waits until the record or file is free. This wait could be any amount of time.
- ◆ Most applications try to read a locked file a certain number of times before sending an error message. This, too, can give the impression that the workstation is hanging.
- ◆ The network is not installed properly. The operating system may not have enough memory for file caching. Inadequate file caching can make the file server appear to hang for a time.

Possible Solutions

- ◆ Contact the application developer and ask how the application handles locked files. Ask the developer for a solution.
- ◆ Load MONITOR and check the amount of memory available for the cache buffer pool. If the pool is near 20%, install more memory in the file server.
- ◆ Load MONITOR and check “Connection Information.” If the user is waiting for a record or file, the connection status should be “Waiting.”

Application Problems: Miscellaneous

Additional applications-related problems that may occur on a file server are listed here.

Trustee Rights Are Lost in the Backup or Restore Process

Possible Cause

You may be using a backup program not written for NetWare. The backup program may be written for either a single-user environment or a non-NetWare system environment.

Possible Solution

Use a NetWare-compatible program. If the backup program is not written for NetWare, the bindery and other essential security features will be lost, and the backup program will not be able to restore NetWare.

Characters Coming into the Serial Port Are Being Lost

Possible Cause

The baud rate is too high. The characters are coming into the serial port faster than they can be picked up. When a character arrives at the port, the operating system gives an interrupt to pick up the character. All characters not picked up immediately are overwritten by the next incoming character.

This problem occurs when the operating system turns off the hardware interrupts, thereby not allowing the CPU full control. Because the interrupts are turned off, incoming characters are not acknowledged. Interrupts are turned off whenever the operating system handles other requests from the network interface board, or when it handles interrupts from within the system.

Possible Solutions

- ◆ Slow the baud rate to 2400 baud. This should be enough to avoid interrupts and prevent incoming character loss.
- ◆ Purchase serial port buffers. Serial port buffers allow incoming characters to wait until the operating system can handle them. Port buffers can be purchased from various software vendors.

The File Server Screen Displays Garbage Characters

Possible Causes

- ◆ Two workstations have the same station (node) address. All file servers and workstations on the same cabling system must have unique station addresses.
- ◆ The data being accessed is corrupted.

Possible Solutions

- ◆ Check the cabling system for bad connections.
- ◆ Check the file server and workstation addresses for duplicate address numbers.
- ◆ Check the workstation records to ensure that no two workstations have the same station address. If you do not have a record of workstation station addresses, log in all workstations and execute the `USERLIST /A` command on one workstation to see the station address listings.
- ◆ If the data is corrupted, run `VREPAIR`. *Before using VREPAIR, back up all file server data.* You may also want to keep the most recent backup that was made before the data was corrupted. See [“VREPAIR” on page 325](#).

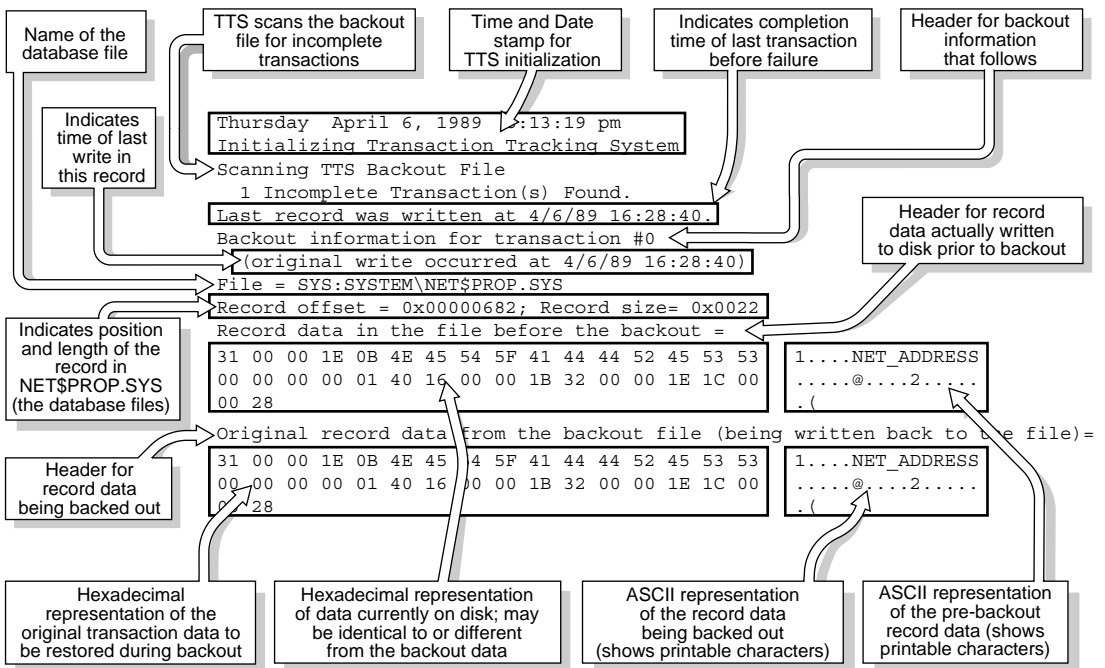
TTS Problems

TTS keeps backout information in a special system file, used only by the NetWare operating system. (For an explanation of how TTS works, see “TTS” in *Concepts*.)

TTS events are logged in TT\$LOG.ERR, a file located in the root directory of volume SYS:. The TT\$LOG.ERR file contains information about what happened with particular transactions when a failure occurred; however, TTS does not actually use this file for backing out data.

This file shows when TTS was enabled or disabled; it also gives pertinent dates, times, file offsets, record sizes, record data before the backout, and record data from the original copy of the data (see the following figure).

Figure 56 TT\$LOG.ERR file information



By holding workstation record locks until the end of a transaction, TTS avoids database corruption that can occur when workstation applications release record locks before transactions are complete. However, holding workstation record locks until the end of a transaction allows for the possibility of deadlocks between workstations using some applications.

If the application uses records that can be unlocked in the middle of transactions to avoid deadlocks, then TTS introduces the possibility of deadlocks for that application (by holding record locks until the end of a transaction). A deadlock means that the two workstations involved hang.

To fix this problem, reboot both workstations; TTS can still maintain database integrity by backing out the transactions that were in process. Although rebooting the workstations is not desirable, it allows TTS to maintain the integrity of the database.

If TTS is automatically disabled because volume SYS: (the TTS backout volume) is full, you must free up disk space on SYS:. Under normal conditions, TTS requires only 1 MB of disk space to track all transactions. If you are adding or deleting large database records (of more than 1 MB each), you need to have free space on SYS: equal to the size of the largest added or deleted record.

Once you have freed up sufficient disk space on SYS:, you can enable TTS with `ENABLE TTS`. If you want to receive a warning when the free space on SYS: is less than you need for TTS, refer to the volume parameters described under “SET” (beginning with “[Parameters](#)” on page 254).

If TTS is automatically disabled because the file server does not have enough free memory, you must increase the memory available to TTS in one of the following ways:

- ◆ Unload file server modules you do not need currently (such as `INSTALL` or `MONITOR`). You can also dismount volumes to free up file server memory. Use `ENABLE TTS` again to see if you have freed up enough memory for TTS. If enough free memory is available, TTS enables; if not, it remains disabled.
- ◆ Add more memory to the file server. TTS requires about 40 bytes to track each transaction. TTS can track up to 10,000 transactions; at peak transaction load, the file server would require no more than 400 KB of memory to track transactions. After you have installed sufficient memory, the file server enables TTS automatically when it boots.

If TTS is disabled then the file server fails before all transactions have been written to disk, the information in the TTS backout file is unreliable. You should *not* back out any transactions. If TTS is shut down, the file server cannot track when transactions are made. If TTS is allowed to back out any transactions (after being enabled), it could incorrectly overwrite information that was changed after TTS was disabled. You can reduce the risk of this situation by attaching a UPS to your file server and disk subsystems.

If the file server fails, incomplete transactions are backed out when the file server comes up again. However, transactions started before the file server failed may have been written to file server cache memory and not to disk. Since a transaction is not marked “completed” by the operating system until it has been written to disk, the file server would back out the transaction, even though the workstation application considered it “completed.”

If the “TTS Abort Dump Flag” (see “**SET**” on page 250) is set to ON, a copy of the original data from the transaction is written to the TTS\$LOG.ERR file in the root directory of SYS:. You can compare this information (which would have been restored to the database) with what was entered at the workstation to determine whether the information needs to be re-entered from the workstation.

If You Need More Help

If you cannot find the solution to a network problem in this section, call your Novell Authorized Reseller. Before calling for assistance, make sure you have the configuration information from the “File Server Worksheet” and the “Workstation Configuration Worksheet” available. Be prepared to describe the problem and the details of each attempt you have made to solve the problem.

NOTE: If you receive a solution from a source other than your Novell Authorized Reseller, please inform Novell of the problem and solution. This will assist us in updating this manual and offering timely answers to others with similar problems.

A

Custom LAN Driver Statistics Shown in MONITOR

MONITOR enables you to monitor your network activity, even down to counters that are set every time something occurs.

You can use the LAN driver statistics to monitor network traffic, hardware conditions, and errors. Use SET (see “[SET](#)” on page 250) to reconfigure the file server to handle network traffic more efficiently.

Generic LAN driver statistics are discussed in “[MONITOR](#)” on page 177. As you view the statistics on the LAN driver information screen, use the arrow keys, <PgUp>, <PgDn>, <Ctrl><PgUp>, or <Ctrl><PgDn> to view all available information. Custom LAN driver statistics are discussed on the following pages.

LAN driver	Page
3C503	“ 3C503 Custom Statistics ” on page 424
3C505	“ 3C505 Custom Statistics ” on page 426
3C523	“ 3C523 Custom Statistics ” on page 428
NE2	“ NE2 Custom Statistics ” on page 430
NE2-32	“ NE2-32 and NE2000 Custom Statistics ” on page 435
NE1000	“ NE1000 Custom Statistics ” on page 433
NE2000	“ NE2-32 and NE2000 Custom Statistics ” on page 435
NE3200	“ NE3200 Custom Statistics ” on page 437

LAN driver	Page
PCN2	“PCN2 Custom Statistics” on page 437
TOKEN	“TOKEN Custom Statistics” on page 439
TRXNET	“TRXNET Custom Statistics” on page 442

3C503 Custom Statistics

3C503ResetCount

Increments when a Hard Transmit Error, Bad Network Error, or a Hardware Receive Mismatch occurs and the network board is reset to a known state.

CarrierSenseLostCount

Increments when the transmitter on the card loses the carrier (indicating the cable connection is lost).

EnqueuedSendsCount

Increments when the driver is unable to transmit a packet and must put the packet in a queue until the transmitter is available. Use this counter to track congestion on the network board.

ExcessCollisionsCount

Increments when packets collide on a network board or in the cabling. Since Ethernet does a random “back off,” packets should not collide the second time they are sent. However, two network boards could have node addresses that are too close, or the traffic on the network may be too heavy for Ethernet to handle. Solve the problem by installing a new network board or by splitting the network.

GotNothingCount

Increments when the file server receives an interrupt from a network board that is not transmitting or receiving anything. This is not serious.

ReceiveFIFOOverrunErrorCount

Increments when an incoming packet causes an overflow because FIFO (first-in, first-out memory) was not serviced.

ReceiverMissedPacketCount

Increments when a packet goes to a network board that cannot accept the packet because its receive buffers are full.

RxPagingErrorCount

Increments when errors occur because internal buffers on the card are corrupted.

TotalCollisionsCount

Increments with each collision. A rapidly growing number in this count does not mean something is wrong, but rather that there is heavy traffic on the network.

TransmitTimeoutCount

Increments when a network board interrupts the file server with the message that the “send bit” is lost. This is a hardware problem caused by faulty cabling, a bad network board, or a missing terminator.

UnderrunErrorCount

Increments when the RAM buffer on the network board is full; the board cannot accept any more packets until the RAM buffer is cleared.

UnsupportedFramePacketCount

Increments when the driver receives a packet with a frame type that the driver does not support or has not been registered for.

UnsupportedMulticastCount

Increments for each multicast packet received by the card that is not registered with the driver.

3C505 Custom Statistics

of Ethernet 802.2 Packets Received

Increments when the driver successfully receives a packet with an Ethernet_802.2 frame type.

of Ethernet 802.3 Packets Received

Increments when the driver successfully receives a packet with an Ethernet_802.3 frame type.

of Ethernet_II Packets Received

Increments when the driver successfully receives a packet with an Ethernet_II frame type.

of Ethernet_SNAP Packets Received

Increments when the driver successfully receives a packet with an Ethernet_SNAP frame type.

of Unsupported Frame From Packets Received

Increments when the driver receives a packet with a frame type that the driver does not support.

GetNICCommandTimeOut

Increments during initialization when the network board sends the driver a timeout.

NICCmdLengthMismatch

Increments during initialization when the network board sends the driver commands of unexpected different lengths.

NICCmdRequestDMSIsActive

Increments when the driver receives a command from the network board in the interrupt routine, but the DMA is active.

NICCmdRequestInvalid

Increments when the driver receives unexpected commands from the network board.

NICCommandTooBig

Increments during initialization when the network board sends the driver a command that is too big.

NICCommandTooLarge

Increments during initialization when the network board sends the driver an excessive number of commands.

NICCommandTooSmall

Increments during initialization when the network board sends the driver a command that is too small.

NotDoingDMACount

Increments when DMA is inactive and the driver receives a request to service DMA in the interrupt routine.

ResetNICCount

Increments when an error occurs and the network board is reset to a known state.

3C523 Custom Statistics

EnqueuedSendsCount

Increments when the driver is unable to transmit a packet and must put the packet in a queue until the transmitter is available. Use this counter to track congestion on the network board.

RBD_act_cnt Not Set

Increments when the received packet's size is not set in the receive buffer descriptor (RBD).

Recv Buffer Two Bytes Off

Increments when the received packet is moved two bytes to the right in the receive buffer. Sometimes this counter increments when a packet is trashed because of packet size or frame type.

Reset82586

Increments when an error occurs and the network board is reset to a known state.

RxDMAOverrun

Increments when DMA overruns while receiving a packet.

RxFailedTestsSoltWasTrashed

Increments when a received packet is trashed because it failed one or more of the reception tests.

RxMediaMismatch

Is not used.

RxPacketsMisalignedAndCRCError

Increments when a packet with a CRC error and a misaligned error is received.

RxPacketsWithCRCError

Increments when a packet with a CRC error is received.

RxTrashedNoNICRxBuffers

Increments when a packet is trashed because no receive buffers are available for the packet. Use SET to increase the number of packet receive buffers.

TxCollisions

Increments when packets collide on the network. You may need to install another network board or split the network to reduce traffic.

TxDefer

Increments when a transmission is deferred.

TxDMAUnderrun

Increments when DMA is underrun during a transmission.

TxLostClearToSend

Increments when a transmission fails because the clear to send signal was lost during the transmission of the packet. This usually indicates a hardware problem with faulty cabling, a bad network board, or a missing terminator.

TxNoCarrierSense

Increments when a transmission fails because the carrier sense was lost during the transmission of the packet.

TxQueuedNoTB

Increments when no transmit buffers are available and a packet has to be put in a queue. Use this counter to monitor network traffic.

TxTrashedMaxRetriesReached

Increments when a packet is trashed because the file server could not transmit the packet in the preset number of times.

TxTrashedNoCommandBlocks

Increments when a packet is trashed because no command blocks are available to use for transmission. Use SET to increase the number of packet receive buffers.

TxTrashedTooManyCollisions

Increments when a packet is trashed because of packet collisions. You may need to reduce traffic by adding another network board or by splitting the network.

UnsupportedFramePacketCount

Increments when the driver receives a packet with a frame type that the driver does not support or has not been registered for.

NE2 Custom Statistics

BackToBackSends

Increments each time the driver can buffer a send packet onto the network board while the board is sending a previous buffer. Use this counter to track congestion on the network board.

CarrierSenseLostCount

Increments when the transmitter on the card loses the carrier (indicating that the cable connection is lost).

ExcessCollisions

Increments once each time packets have collided sixteen times. Since Ethernet does a random “back off,” packets should not collide the second time they are sent. However, two network boards could have node addresses that are too close and thus be “In Sync,” or you may have a hardware problem. Solve the problem by installing a network board with a different node address or by finding and fixing the hardware problem (faulty board, missing terminator, faulty cable).

OverflowReSends

Increments when a transmission fails because of an overflow. The driver sends the packet again. If you receive too many of these, you may want to reconfigure your network to reduce traffic.

Overrun

Increments when the RAM buffer on the network board is full and cannot accept any more packets. Packets will be accepted when the RAM buffer is cleared.

PagingError

Increments when the operating system detects a pointer error on the network board’s RAM. The system reinitializes the pointers on the network board and discards any packets in the RAM buffer. Paging errors can occur during normal operation.

PageZeroErrors

Increments when the operating system detects that a pointer has a value of zero. The system reinitializes the pointers on the network board. Page zero errors can occur during normal operation.

ReceiveError

Increments when the network board gets an error receiving a packet. Receive errors can occur during normal operation.

RxMulticastPacket

Increments every time the file server receives a multicast packet. (Ethernet can designate multiple recipients for one packet of information.)

RxPagingErrorCount

Increments when errors occur because internal buffers on the card are corrupted.

TotalCollisionsCount

Increments with each collision. A rapidly growing number in this count does not mean something is wrong, but rather that there is heavy traffic on the network.

TransmitFailed

Increments when the driver is unable to transmit a packet a preset number of times.

TransmitTimeoutCount

Increments when a network board interrupts the file server with the message that the “send bit” is lost. This is a hardware problem caused by faulty cabling, a bad network board, or a missing terminator.

UnderrunErrorCount

Increments when an incoming packet causes an overflow because FIFO (first-in, first-out memory) was not serviced.

UnsupportedMulticastCount

Increments for each multicast packet received by the card that is not registered with the driver.

NE1000 Custom Statistics

CarrierSenseLostCount

Increments when the transmitter on the card loses the carrier (indicating that the cable connection is lost).

EnqueuedSendsCount

Increments when the driver is unable to transmit a packet and must put the packet in a queue until the transmitter is available. Use this counter to track congestion on the network board.

ExcessCollisionsCount

Increments when packets collide on a network board or in the cabling. Since Ethernet does a random “back off,” packets should not collide the second time they are sent. However, two network boards could have node addresses that are too close, or the traffic on the network may be too heavy for Ethernet to handle. Solve the problem by installing a new network board or by splitting the network.

GotNothingCount

Increments when the file server receives an interrupt from a network board that is not transmitting or receiving anything. This is not serious.

In32BitModeCount

Increments if a network board is ever found in 32-bit mode. (Currently, workstations run in 8-bit mode.) Occasionally, older NE1000 boards have bad chips that make the boards go into 32-bit mode. If you ever see this counter incremented, you probably have one of those older boards on the network.

NE1000ResetCount

Increments when a Hard Transmit Error, Bad Network Error, or Hardware Receive Mismatch occurs and the network board is reset to a known state.

ReceiveFIFOOverrunErrorCount

Increments when an incoming packet causes an overflow because FIFO (first-in, first-out memory) was not serviced.

ReceiverMissedPacketCount

Increments when a packet is sent to a network board that cannot accept the packet because all its receive buffers are full.

RxPagingErrorCount

Increments when errors occur because internal buffers on the card are corrupted.

TotalCollisionsCount

Increments with each collision. A rapidly growing number in this count does not mean something is wrong, but rather that there is heavy traffic on the network.

TransmitTimeoutCount

Increments when a network board interrupts the file server with the message that the “send bit” is lost. This is a hardware problem caused by faulty cabling, a bad network board, or a missing terminator.

UnderrunErrorCount

Increments when the RAM buffer on the network board is full; the board cannot accept any more packets until the RAM buffer is cleared.

UnsupportedFramePacketCount

Increments when the driver receives a packet with a frame type that the driver does not support or has not been registered for.

UnsupportedMulticastCount

Increments for each multicast packet received by the card that is not registered with the driver.

NE2-32 and NE2000 Custom Statistics

BackToBackSendCount

Increments each time the driver can buffer a send packet onto the network board while the board is sending a previous buffer. Use this counter to track congestion on the network board. See [“EnqueuedSendsCount” on page 424](#).

CarrierSenseLostCount

Increments when the transmitter on the card loses the carrier (indicating that the cable connection is lost).

EnqueuedSendsCount

Increments when the driver is unable to transmit a packet and must put the packet in a queue until the transmitter is available. Use this counter to track congestion on the network board. See [“BackToBackSendCount” on page 435](#).

ExcessCollisionsCount

Increments when packets collide on a network board or in the cabling. Since Ethernet does a random “back off,” packets should not collide the second time they are sent. However, two network boards could have node addresses that are too close, or the traffic on the network may be too heavy for Ethernet to handle. Solve the problem by installing a new network board or by splitting the network.

GotNothingCount

Increments when the file server receives an interrupt from a network board that is not transmitting or receiving anything. This is not serious.

NE2000ResetCount

Increments when a `HardTransmitError`, `BadNetworkError`, or `HardwareReceiveMismatch` occurs and the network board is reset to a known state.

ReceiveFIFOOverrunErrorCount

Increments when an incoming packet causes an overflow because FIFO (first-in, first-out memory) was not serviced.

ReceiverMissedPacketCount

Increments when a network board cannot accept packets sent to it because all of its receive buffers are full.

RxPagingErrorCount

Increments when errors occur because internal buffers on the card are corrupted.

TotalCollisionsCount

Increments with each collision. A rapidly growing number in this count does not mean something is wrong, but rather that there is heavy traffic on the network.

TransmitTimeoutCount

Increments when a network board interrupts the file server with the message that the “send bit” is lost. This is a hardware problem caused by faulty cabling, a bad network board, or a missing terminator.

UnderrunErrorCount

Increments when the RAM buffer on the network board is full; the board cannot accept any more packets until the RAM buffer is cleared.

UnsupportedFramePacketCount

Increments when the driver receives a packet with a frame type that the driver does not support or has not been registered for.

UnsupportedMulticastCount

Increments for each multicast packet received by the card that is not registered with the driver.

NE3200 Custom Statistics

Transmit Retry Failure

Increments when the driver is unable to transmit a packet a preset number of times. This may indicate a hardware problem.

No Nic Board Receive Buffers

Increments when the driver does not have enough packet receive buffers on the NE3200 board to hold all the packets it needs to service. If this counter increments, the NE3200 board has a hardware problem. Replace the board.

Number Of Resets To Nic

Increments when the software corrects itself for minor problems. Under normal conditions, more of these errors should occur during idle time than when the driver is busy. For this counter to warn you of potential hardware problems, you must receive thousands of these errors when the network is busy.

PCN2 Custom Statistics

802.2PacketsReceived

Increments for each PCN_802.2 packet received.

BadTransmitCompleteInterruptCount

Increments for each complete transmission with no transmit active.

CurrentEnqueuedCount

Increments as the current number of packets waiting in the queue increases (until the transmitter is available).

EnqueuedSendsCount

Increments when the driver is unable to transmit a packet and must put the packet in a queue until the transmitter is available. Use this counter to track congestion on the network board.

GotNothingCount

Increments when the driver receives an interrupt from the card indicating that it has completed a receive but there is no data in the card's receive buffer. This is not serious.

HotCarrierInterruptCount

Increments when the board detects a carrier longer than expected without a transmit. This generally indicates that some board on the network has failed or is starting to go bad.

No82588InterruptCount

Increments each time it receives an interrupt from the card but not the 82588 chip. This should never happen.

PCN2ResetCount

Increments when an error occurs and the driver resets the board to a known state.

ReceivedShortPacketCount

Increments when a packet of less than 17 bytes is received.

ReceiveUnderrunErrorCount

Increments when the driver finds less data in the card's buffer than the card said was there.

SNAPPacketsReceivedCount

Increments when the driver successfully receives a packet with an Ethernet_SNAP frame type.

TotalTransmitErrorCount

Increments each time the file server is unable to transmit a packet, even if it eventually succeeds.

UnsupportedFramePacketCount

Increments for each unregistered frame received.

WeirdInterruptCount

Increments when the file server has received an interrupt from the card, but the card claims not to have sent one. This should never happen.

TOKEN Custom Statistics

Much of this information for Token-Ring custom statistics is condensed from the *IBM Token-Ring Network Architecture Reference* produced by IBM.

Abort Delimiters

Increments when a ring station transmits an abort delimiter. An abort delimiter is transmitted when a ring station receives a frame in which the token bit of the access control field is set to show "Token" and not "Frame." A ring station can also transmit an abort delimiter if an internal hardware error has occurred.

A/C Errors

Increments when a ring station receives a “Standby Monitor Present” MAC frame with the A/C bits in the Frame Status field equal to zero without first receiving an “Active Monitor Present” MAC frame.

Bad Correlator Count

Increments when a network board responds with a request for data from the file server that the file server does not have. The ECB or some other code may be corrupted. Eventually, this type of error will down the server. If this counter is non-zero, you should try to find the software that is corrupting the data.

Burst Errors

Increments when a ring station detects the absence of “five half-bit times” (a burst-five error). Other stations will detect a burst-four error followed by idles.

Frame Copied Errors

Increments when a ring station receives or repeats a frame that appears to have a duplicate address.

Frequency Errors

Increments when a ring station detects a frequency error.

Internal Errors

Increments as a ring station has recoverable internal errors, which means a ring station is probably marginal.

Last Ring Status

Changes each time the ring status changes. Status codes, their function, and meaning are listed on the next page. If you receive errors not listed in the chart, see the *IBM Token-Ring Network Architecture Reference* produced by IBM.

Line Errors

Increments when a frame or token is repeated by the ring station. A frame is repeated when a “Frame Check Sequence” error occurs or a code violation exists between the starting and ending delimiters of the frame.

Lost Frames

Instances when a ring station transmits a frame that does not return to the station. The active monitor sends a new token.

Receive Congestion Errors

Increments when a ring station recognizes a frame addressed to it but has no buffer space available for the frame.

Token Error

Increments when an active monitor cannot send a token. Circulating priority tokens, circulating frames, or lost tokens can prevent tokens from being transmitted.

Unknown ARB Request

Counts bad ARBs (Adapter Request Blocks). Normally the network board (adapter) uses one of four known commands to communicate with the driver. If a network board sends a command that is *not* one of the four, the driver does not recognize the request. This is not a catastrophic error. Sometimes old adapters send bad ARB requests because of software problems resident on the board. NetWare responds to the network board so that the board will not hang.

Table 27 Unknown ARB Request codes

Code	Function	Meaning
8000	Signal loss	No received signal detected.
4000	Hard error	Beacon frames were transmitted or received.
2000	Soft error	The adapter has transmitted a soft error report MAC frame.
1000	Transmit beacon	The adapter transmitted beacon frames.

Code	Function	Meaning
0800	Lobe wire fault	An open or short circuit was detected in the lobe data path. (The adapter will be closed.)
0400	Auto-removal error1	An adapter hardware error occurred following the beacon auto-removal process.
0200	Reserved	
0100	Remove received	A remove MAC frame was received. The adapter is closed.
0080	Counter overflow	One of the adapter error log counters has been incremented from 254 to 255. (Issue the DIR.READ.LOG command.)
0040	Single station	The adapter has opened and is the only station on the ring. (The bit will be reset when another station is detected.)
0020	Ring recovery	The adapter is transmitting or receiving Monitor Contention MAC frames. This bit will be reset upon receipt of a Ring Purge MAC frame.

TRXNET Custom Statistics

Fatal Retransmissions

Increments when the file server reaches the limit for retry transfers in sending a packet. You can increase the number of retry transfers with a driver parameter (see [“LOAD LAN driver” on page 133](#)). Retries, however, slow down the system.

First Halves Cancelled

Increments when the TRXNET driver splits a data buffer and starts sending the packets in the sequence, but only the first few packets of the sequence arrive because someone turned off the driver before all the packets could be sent.

Number of Orphaned Packets

Increments when the TRXNET driver breaks a data buffer (on a send) into a sequence of smaller packets and sends them out in order but a packet in the sequence is received before a preceding packet in the sequence; then all packets in the sequence are dropped and the “Number of Orphaned Packets” counter increments once for the sequence.

Raw Transmissions

Increments when the driver sends a packet without attaching a NetWare header and split flags.

Sends Cancelled

Increments when someone unloads the driver from the network while the driver is functioning. The send commands are waiting to be sent. Since there is no driver, the commands are eliminated and the counter is incremented.

Sends Ignored—Driver Shut Down

Increments when a workstation sends a packet intended for a driver that has been unloaded.

Spurious Interrupts

Increments when the TRXNET driver in the file server receives an interrupt in the middle of an interrupt service routine. The hardware interrupt should be turned off during an interrupt service routine to allow the interrupt service routine to complete its task. This counter increments, and the hardware is polled before the interrupt service routine exits.

Timed Out Receive ECBs

Increments when all of the packets in a sequence do not arrive in a specified amount of time. The TRXNET driver split a data buffer and started sending packets, but only the first few packets of the sequence arrived on time. This should be a rare occurrence unless you have heavy network traffic on your cables.

Timed Out Sends

Increments when the file server sends a packet to the network board, but the board does not respond during a preset amount of time. (The board should acknowledge each packet it receives.) This is not a serious problem.

B

Tracked Resources Displayed in MONITOR

NetWare v3.12 tracks many operating resources. It does this tracking so that when you unload an NLM, the resources return to the operating system and become available for other NLMs.

An NLM, as you load it, requests resource tags. The operating system assigns each resource tag a resource tag name, and then grants resources to each resource tag.

For example, when you load MONITOR it requests an “Alloc Memory” resource tag. The operating system grants MONITOR the resource tag and allocates some “Alloc Short Term Memory” to the resource tag.

The operating system also uses resource tags to track its own use of memory. It uses “Alloc Short Term Memory” for a number of functions, and gives each function its own tag. For example, the operating system uses the following resource tags for the “Alloc Short Term Memory” resource:

- Broadcast System
- Connection User Information
- Disk Management System
- Event Notification
- File Locks

Loadable modules can also add resources to be tracked. For example, NMAGENT adds the following resources:

- Network Management Filters
- Network Management Managers
- Network Management Objects

This appendix defines all resources tracked by the operating system and those tracked resources added by the NMAGENT module. See the documentation for third-party NLMs for any tracked resources they add.

You can view the tracked resources two different ways from MONITOR's "Available Options" menu. You can view them from the "System Module Information" option or from the "Resource Utilization" option.

- ♦ "System Module Information" shows you which types of resources a particular module uses.
- ♦ "Resource Utilization" shows you which module uses how much of a particular resource.

Improperly implemented NLMs can cause file server resources (memory, service processes, and buffers) to reach their limits quickly. For example, if nothing new has been added to the system, permanent memory should not grow at a rate of 2 MB a day. Use the statistical information gathered from tracked resources to identify loadable modules that use more resources than they need.

The function of each resource is described in the following sections.

AES Process Call-Backs

AES stands for asynchronous event service. This resource allows an NLM to schedule a future event. For example, when the power fails, UPS schedules a delayed down command for the file server. The command then executes a specified number of minutes before the battery's power is depleted.

Alloc Short Term Memory (Bytes)

NetWare v3.1x has five memory pools. It uses Alloc Memory for short-term memory requests. Loadable modules with pop-up windows use Alloc Memory to store previous menu information on the screen. When the user escapes back to the previous menu, the memory returns immediately to the operating system. The "Server Memory Statistics" window ("Alloc Memory Pool" option) displays the total amount of memory used for this resource.

C Library BSD Sockets

Tracks the number of Berkeley UNIX sockets.

Cache Movable Memory (Bytes)

NetWare v3.1x has five memory pools. It uses the Cache Movable Memory pool for system tables such as directory tables and FATs that grow dynamically. Name space modules also use this resource. The “Server Memory Statistics” window (“Cache Movable Memory”) displays the total amount of memory used by this resource.

Cache Non-Movable Memory (Bytes)

NetWare has five memory pools. It uses the Cache Non-Movable Memory pool to load modules into memory and to allocate large memory buffers. The “Server Memory Statistics” window (“Cache Non-Movable Memory”) shows the total amount of memory used by this resource.

Console Command Handlers

NetWare uses this resource to track console command resources. Loadable modules can add console commands to the operating system as you load them. For example, UPS adds two console commands (UPS STATUS and UPS TIME) when you load it.

Disk Adapter Locks

Tracks loadable modules that need to know about disk adapters, controllers, or host bus adapters.

Disk Drive Locks

Tracks loadable modules that need to know about the hard disks that you have added to the operating system. It then informs these modules when you remove the hard disk.

Disk File System Partition Locks

Tracks loadable modules that register a need to access information about logical partitions. For example, INSTALL uses this resource when it mirrors two drives.

Disk Raw Partition Locks

Tracks access to disk partitions. For example, INSTALL uses this resource when it installs Hot Fix on a partition.

Event Notification Call-Backs

Allows modules to detect when system events occur. For example, MONITOR uses it to detect when you mount or dismount a volume.

Hardware Interrupt Handlers

Tracks which loadable modules and hardware use which interrupts. LAN drivers and disk drivers that require the interrupts also use this resource.

Interrupt Time Call-Backs

Tracks NLMs that have processes which occur at regularly timed intervals. For example, MONITOR uses this resource to update the statistics in its windows every second.

IPX Sockets

Tracks NLMs that establish a socket connection between two devices. A different socket handles each type of communication. For example, the operating system uses one socket for workstation communication. The RSPX module establishes another socket for RCONSOLE communication.

LSL AES Event Call-Backs

(AES stands for asynchronous event service.) Allows LAN drivers to schedule a future event.

LSL Default Protocol Stacks

Tracks protocol NLMs that register to receive all packets that no other protocol claims. By default, the operating system discards any unclaimed packets. However, when a protocol NLM registers, the default is overridden.

LSL Packet Receive Buffers

Tracks which LAN driver is using a particular packet receive buffer so that the buffers can be freed when the LAN driver is unloaded.

LSL Pre-Scan Protocol Stacks

Tracks protocol NLMs that register to pre-scan all incoming packets to see if the packets belong to them. Each board can have only one pre-scan protocol.

LSL Protocol Stacks

Tracks NLMs that register as protocol stacks. The operating system registers the IPX protocol stack automatically.

NCP Extensions

Tracks loadable modules that define their own NCPs (NetWare Core Protocols).

Network Management Managers

Tracks the number of network management managers the NMAGENT loadable module has allocated.

Network Management Objects

Tracks the number of network management objects the NMAGENT loadable module has allocated.

Network Management Triggers

Tracks the number of network management triggers the NMAGENT loadable module has allocated.

Permanent Memory (Bytes)

NetWare has five memory pools. The Permanent Memory pool is used as a source of memory for the Semi-Permanent Memory pool and Alloc Short Term Memory pool. The Permanent Memory pool is used by the operating system for permanent tables. Loadable modules cannot use this memory.

Poll Procedure Call-Backs

Tracks loadable modules that have processes executing at defined intervals.

Processes

Tracks loadable modules that start processes. The resource makes sure that the process is deleted when the module is unloaded.

Processor Exception Handlers

Tracks exceptions to the rules that hardware detects. For example, if the CPU determines that an NLM is trying to divide by zero, the operating system notifies the NLM that it has broken the rules. The NLM then sends a message to the console or workstation. (These messages are documented by the NLM's vendor.)

Registered Disk Adapters

Tracks the configuration options of disk drivers (interrupts, DMA, memory addresses, I/O ports, and slots).

Registered Hardware Options

Tracks LAN drivers that request interrupts, DMA, memory addresses, I/O port addresses, and slots.

Registered MLID Boards

Tracks the number of LAN drivers that have been loaded and ensures that a LAN driver's resources are returned to the operating system when the driver is unloaded.

Remote Server Sessions (Instances)

Tracks the number of remote servers that have at least one remote connection.

Screen Input Call-Backs

Tracks NLMs that use an alternate method for key input from a console screen. TRACK ON uses this resource.

Screens

Tracks how many screens an NLM has created or opened on the file server console. Most NLMs with menus (such as MONITOR) will activate a screen. NLMs without menus (such as LAN drivers and disk drivers) do not activate any screens.

Semaphores

Tracks NLMs that use semaphores. Semaphores control multiple access to a resource that can be used by only one user at a time.

Semi-Permanent Memory (Bytes)

NetWare v3.1x has five memory pools. Semi-Permanent Memory is used for small amounts of memory that a loadable module expects to use for a long time. LAN drivers and disk drivers use this type of memory.

Service Advertising (Instances)

Tracks the number of times an NLM advertises itself over the network. Normally this is 1 or 0.

Service Connection Task Numbers

Tracks the task numbers that are assigned to an NLM for use on a connection. (An NLM can log in and use a connection slot.)

Service Connections

Tracks the file server to workstation connections. This resource tracks all attached and logged-in users.

Setable Parameters

Tracks NLMs that add parameters to the SET command. It ensures that, when the NLM is unloaded, the SET parameters are also unloaded.

STREAMS: Active Stream Handles

Tracks the number of communication streams that are currently in use.

Tracked Resource Types

Tracks NLMs that add tracked resources to the operating system. The resource ensures that, when the NLM is unloaded, the resource types are also unloaded. For example, the operating system tracks NMAGENT with this resource. When NMAGENT is unloaded, NMAGENT's three tracked resources ("Network Management Filters," "Network Management Managers," and "Network Management Objects") are also unloaded.