Novell NetWare® 6

www.novell.com

SERVER OPERATING SYSTEM
ADMINISTRATION GUIDE

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 © 1993-2001 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.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Server Operating System Administration Guide
October 2001
103-000148-001

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

Novell Trademarks

Appnotes is a registered trademark of Novell, Inc.

ConsoleOne is a trademark of Novell, Inc.

DeveloperNet is a registered trademark of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.

Hot Fix is a trademark of Novell, Inc.

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

LANalyzer is a registered trademark of Novell, Inc. in the United States and other countries..

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

NE3200 is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Core Protocol and NCP are trademarks of Novell, Inc

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

NetWare Peripheral Architecture is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Distributed Print Services is a trademark of Novell, Inc., and NDPS is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Support Connection is a registered trademark of Novell, Inc.

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

Transaction Tracking System is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

Server Operating System 9
Documentation Conventions 10

1 Learning about the NetWare Server 11
Overview of the NetWare Server 11
NetWare Integrated Kernel 12
The Run Queue 13
Load Balancing 14
Concurrency and Parallelism 15
Pre-emption 16
Platform Support Module 17
The Server Console 18
NetWare Is Self-Tuning 20
Java-Based Components of NetWare 21
The Novell JVM for NetWare and the Just In Time Compiler 21

2 Setting Up the NetWare Server 23
Changing the Server's Software Configuration 24
Installing, Uninstalling, and Configuring a Server or Other Products 25
Changing the Language NetWare Uses 26
Code Pages 26
Using Unicode 27
Changing Code Pages 29
Changing Server Message Files 30
Changing NLM Message Files 31
Changing the Server Keyboard Type 32

3 Optimizing the NetWare Server 33
Applying Patches 34
Matching Performance Capabilities 34
Setting the Load Balancing Threshold 37

Setting Server Parameter Values . . . 38
Understanding Server Defaults . . . 38
Finding Current Parameter Values . . . 40
Printing Current Parameter Values to a File . . . 41
Checking Current Parameter Values with DISPLAY ENVIRONMENT . . . 42
When to Modify Defaults . . . 42
When Not to Modify Defaults . . . 43
Restoring Default Values with RESET ENVIRONMENT . . . 43
Monitoring Dynamic Statistics . . . 43
Using Optional Commands in Startup Files . . . 44
Using SET Commands in Startup Files . . . 44
Minimizing Replication Traffic . . . 45

4 Managing the NetWare Server . . . 47

Starting and Stopping the Server . . . 48
Starting the Server . . . 48
Bringing Down the Server . . . 49
Viewing and Accessing Server Console Screens . . . 50
Starting and Stopping Processors . . . 52
Displaying Processor Information . . . 52
Stopping Processors . . . 53
Starting Processors . . . 54
Using Server Batch Files . . . 55
Using EDIT to Create and Edit Text and Batch Files . . . 56
Using NWCONFIG to Create and Edit Startup Batch Files . . . 57
Making a Command Optional in a Server Batch (.NCF) File . . . 58
Changing Server Name and Internal Address in AUTOEXEC.NCF . . . 59
Using Server Utilities and Console Commands . . . 60
How to Access Help for Utilities and Console Commands . . . 60
Using NetWare Loadable Modules . . . 61
Loading and Unloading NetWare Loadable Modules . . . 62
Using Java on the Server . . . 63
Environment Variables for Java . . . 63
Managing NetWare Server GUI . . . 65
Securing the Server Console . . . 67
Why Should I Use SECURE CONSOLE? . . . 68
Using the SECURE CONSOLE Command . . . 68
Using SCRSAVER to Lock the Server Console . . . 69
Unlocking the Server Console . . . 70
Using NCP Packet Signature . . . 70
Why Should I Use Packet Signatures? . . . 71
NCP Packet Signature Options . . . 72
Effective Packet Signature . . . 72
Recommended Signature Levels . . . 73
Implementing NCP Packet Signature . . . 73

Using the Transaction Tracking System . . . 77
How TTS Works . . . 78
Enabling and Activating TTS . . . 78
Using an Uninterruptible Power Supply (UPS) . . . 81
Preventing Virus Infection . . . 82
Monitoring the NetWare Server . . . 82
Accessing MONITOR . . . 83
What to Monitor and Why . . . 83
Displaying Server Alerts . . . 87
Managing Workstation Connections . . . 89
Performing Connection Management Tasks . . . 89
Monitoring Workstation Connections to the Server . . . 89
Sending Console Messages to Workstations . . . 91
Clearing a Workstation Connection . . . 92
Disabling and Enabling Logins . . . 93
Clearing a Connection That Uses Auto Reconnect . . . 93
Controlling Resource Allocation with Locks . . . 94
Performing Common Maintenance Tasks . . . 96
Backing Up Server Data . . . 96
Checking Server Error Logs . . . 97
Checking Disk Drives . . . 97
Reviewing Server Cache Statistics . . . 97
Checking Free Space on Server Disks and Volumes . . . 98
Reviewing User Accounts . . . 98
Testing the Uninterruptible Power Supply . . . 98
Documenting the Network . . . 99
Performing Preventive Maintenance Tasks . . . 101
Preventing Memory Problems . . . 101
Preventing Power Supply Errors . . . 101
Preventing Static Electricity Problems . . . 102

5 Troubleshooting the NetWare Server . . . 105

Using a Troubleshooting Methodology . . . 105
Keeping Your Servers Patched . . . 106
Eliminating Obvious Causes . . . 107
Gathering Information . . . 107
Simplifying the System . . . 109
Using Troubleshooting Resources . . . 109
Developing Hypotheses and Performing Tests . . . 111
Looking for Additional Help . . . 111
Documenting the Solution . . . 112
Creating a Core Dump . . . 112
Performing a Core Dump to a Local Drive . . . 113
Sending the Core Dump to Novell . . . 114

Troubleshooting Hardware and Network Problems 114
Identifying Problems after Installation 114
Resolving Hard Disk Access Problems 114
Making Computer Memory Available for Network Drivers 115
Troubleshooting the NetWare Server 115
Resolving Abends 116
Insufficient Packet Receive Buffers, No ECB Available Count Errors 121
Resolving Slow Server Response 121
Server Console Hangs 124
High Utilization Statistics 125
Disk Errors 132
Resolving Server Memory Problems 136
Resolving Locked Device Errors 143
Resolving Event Control Block Allocation Errors 143
Resolving Server Console Command Problems 144
Resolving Keyboard Locking Problems When Copying Files from CD-ROM 145
Monitoring and Resolving Communication Problems 147
Suspected Multiprocessing Problems 149
Unable to Communicate with Server, -625 Errors 150
Workstations Can’t Communicate with Server 153
Errors Reading from and Writing to Network, Server Cannot Be Found Errors 153
Connections Dropped Periodically 156
Tips for Resolving General Communication Problems 156
Admin Account Has Been Deleted or Admin Password Is Unknown 158
Preventive Maintenance Tasks 158

Server Operating System

Welcome to the *NetWare® Server Operating System Guide*. This guide contains the following chapters:

- Chapter 1, “Learning about the NetWare Server,” on page 11
- Chapter 2, “Setting Up the NetWare Server,” on page 23
- Chapter 3, “Optimizing the NetWare Server,” on page 33
- Chapter 4, “Managing the NetWare Server,” on page 47
- Chapter 5, “Troubleshooting the NetWare Server,” on page 105

For additional information about the server operating system, see the following table.

If you want to	Refer to
Begin installing the server	*NetWare 6 Overview and Installation Guide*
Use a multiprocessing computer as your server and you want more information on the higher level of support for multiprocessing	NetWare Integrated Kernel
Decide which protocol to use	*Server Communications Administration Guide*
Learn about how the Novell® eDirectory™ database and eDirectory tree are the foundation for convenient network administration	eDirectory Concepts in the *Novell eDirectory 8.6 Administration Guide*

If you want to	Refer to
Decide which file system to use	*Novell Storage Services Administration Guide*
Learn more about use of memory by NetWare	*Server Memory Administration Guide*

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Learning about the NetWare Server

This chapter contains the following information:

To learn about	See
NetWare Server Operating System basics	“Overview of the NetWare Server” on page 11
NetWare integrated kernel	“NetWare Integrated Kernel” on page 12
Server console security and interfaces	“The Server Console” on page 18
How the NetWare server optimizes its own performance	“NetWare Is Self-Tuning” on page 20
Java*-based components of NetWare	“Java-Based Components of NetWare” on page 21

Overview of the NetWare Server

Although it is frequently more convenient to refer to the computer where NetWare® resides as the server, the NetWare server is the network operating system that is installed on a server class computer. NetWare turns the computer into a high-performance network platform that provides connectivity between workstations, printers, mass storage devices, and other networks such as the Internet. NetWare also provides network users with a server platform for hosting Java applications.

The NetWare server manages the transmission of data among the network devices, stores and retrieves data from hard disks, manages one or more file systems, ensures data integrity, manages printers and printing, and allocates and manages memory. The NetWare server is designed to operate on either a uniprocessing or multiprocessing computer.

The principal executable for NetWare, SERVER.EXE, includes *bound-in* modules, such as those for Media Manager, NetWare Peripheral Architecture™ (NWPA), and the Link Support Layer™ (LSL™). When SERVER.EXE is executed, the NetWare server is loaded into memory, takes control of the hardware resources, and begins to load its component modules.

NOTE: NetWare uses DOS as a cold boot loader. It does not run on top of DOS.

Because the system is modular, individual modules can be updated without replacing SERVER.EXE. A new module simply replaces the previous version.

NOTE: The directory in which SERVER.EXE is stored is called the startup directory or the boot directory. By default, SERVER.EXE is stored in the C:\NWSERVER directory. Updated modules can be copied to the STARTUP directory where they will overwrite previous versions or the bound-in versions of the same modules.

NetWare 6 is based on an integrated kernel. The multiprocessing kernel (MPK) is completely multithreaded, supports pre-emption, and—as an integrated kernel—runs on both multiprocessor and uniprocessor systems. NetWare supports as many as 32 processors.

Although NetWare 6 has minimum hardware requirements (see System Requirements in the *NetWare 6 Overview and Installation Guide*), we recommend that you provide a high-performance hardware platform so you can get the full benefit of the power and scalability that NetWare 6 offers.

To ensure that no component of your system hampers the performance of any other, see also "Matching Performance Capabilities" on page 34.

NetWare Integrated Kernel

The core of the NetWare operating system is the integrated kernel. MPK (multiprocessing kernel) manages threads, schedules processor resources, handles interrupts and exceptions, and manages access to memory and the I/O subsystems.

For explanations and descriptions, see the following:

- "The Run Queue" on page 13
- "Load Balancing" on page 14
- "Concurrency and Parallelism" on page 15
- "Pre-emption" on page 16
- "Platform Support Module" on page 17

The Run Queue

A *thread* is a stream of control that can execute its instructions independently. A simpler definition is that a thread is a unit of execution. It is not the code itself.

HINT: For more information on threads, see Bil Lewis and Daniel J. Berg's *Threads Primer: A Guide to Multithreaded Programming* © Sun Microsystems, Inc. Their definition of "thread" has been quoted above.

The kernel maintains a data structure called the *run queue* which contains threads that are in a state of readiness. In a uniprocessor system, there is only one run queue from which the processor can pick up threads for execution.

In a multiprocessing system where more than one processor is available, there is more than one possible solution. The distribution of threads to multiple processors could be handled by a global run queue (all processors sharing a single run queue) or by per-processor run queues (known also as local run queues or distributed run queues). Or by some combination of both.

To compare the two approaches:

- **Global run queue.** This approach to distributing threads has the advantage of automatic load balancing. The reason is that no processor remains idle as long as the run queue has threads ready. However, the global solution has the drawback of becoming a bottleneck as the number of processors increases in a system, although under certain scheduling policies (such as a real time scheduling policy), a global queue might be necessary.
- **Per-processor run queue.** This approach has the advantage of being able to exploit cache affinity—where threads are preferentially scheduled on the processor on which they last ran. In addition, this approach does not have the bottleneck problem associated with the global run queue approach.

  With local queues, however, it becomes necessary to ensure that the load on the processors—the number of threads in the queue—does not become severely imbalanced. A load balancing mechanism is required to handle load imbalances so that threads do not pile up at one processor while another processor remains idle.

The NetWare kernel uses the per-processor run queue. As implemented, a processor can pick up threads for execution only from its local run queue. This makes the NetWare scheduler highly scalable compared to an implementation using a global run queue. To address load imbalance, NetWare uses a sophisticated load balancing algorithm.

Load Balancing

Two important requirements of any load balancing scheme are stability (*not* overreacting to small load imbalances) and the ability to distribute the processing load quickly.

The NetWare scheduler handles the stability requirement by using a threshold. The threshold determines how much load imbalance is permitted in the system before the load balancing mechanism kicks in.

Because a low threshold value would have less tolerance for load imbalances than a higher value, the *lower value* could lead to excessive thread movement due to frequent load balancing. A *higher value* would have more tolerance for load imbalances, with the result that the load balancing mechanism would be triggered less often. However, an *optimum value* of the threshold would prevent excessive thread migration while addressing load imbalance only as needed.

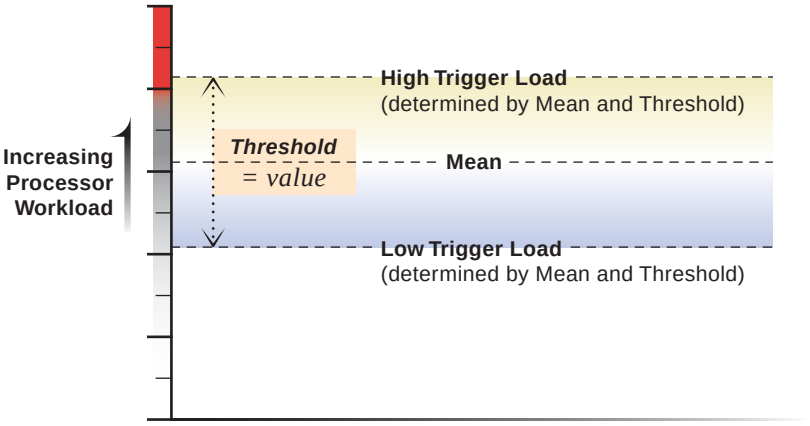
The NetWare scheduler periodically calculates the system-wide load and the mean load and uses the latter to compare loads and to determine whether an individual processor is overloaded or underloaded.

The load balancing threshold and the calculated mean load are then used to determine the high and low trigger loads.

- A processor is overloaded when its load exceeds the *high trigger load*.
- A processor is underloaded when it is below the *low trigger load*.

In this situation, the scheduler then moves threads from the overloaded processor to the underloaded processor with the result that the loads are balanced. See the following figure for an illustration of the relationship between the mean load, the load balancing threshold, and the high and low trigger loads.

Figure 1 Mean Load, Threshold, and High and Low Trigger Loads



Without the margin provided by the threshold, threads would constantly move from one processor to another, thereby compromising the productivity of the system.

WARNING: Although the threshold is configurable, we strongly recommend that you retain the preset optimum value. If after careful consideration, you decide to modify the threshold, test it in an isolated system before modifying the value for a production environment. If you modify the threshold, remember that you can always reset it at the optimum value.

You can modify the threshold through NetWare Remote Manager. For details, see "Setting the Load Balancing Threshold" on page 37.

Concurrency and Parallelism

NetWare has always had threads (typically referred to as *processes*) but until NetWare 6 has not exploited the potential for parallelism in multithreaded code. Multithreading enables multiple paths of parallel execution through the code path. A software developer identifies tasks that can be performed concurrently, that are not dependent on being performed in a fixed sequence, and provides the mechanisms for assigning tasks to multiple threads and for appropriate synchronization to protect data shared by the threads.

In a uniprocessor environment, multithreaded code allows threads to run concurrently. This means that one or more threads are active on the same processor. The threads appear to run at the same time—although they do not actually do so. One thread, for example, can be blocking while another thread

is executing code. They are perceived as executing simultaneously because processors are very fast and time quanta are very small.

On the other hand, it is the availability of hardware systems with multiple processors that makes it possible to have multiple threads actually running at exactly the same time on different processors. When threads execute simultaneously on multiple processors, they are running in parallel. Multithreaded code allows more efficient processor utilization by exploiting parallelism.

With NetWare 6, applications can be written to exploit the parallelism available in multiprocessor (MP) hardware and the support for parallelism in the server operating system, and your system will benefit from the performance gains and scaling that server applications such as GroupWise® provides.

NOTE: A single binary supports both uniprocessor and multiprocessor systems precisely because the NetWare kernel is multithreaded.

Pre-emption

NetWare allows for pre-emption of threads, within constraints. New NetWare modules can be written to be pre-emptible.

NOTE: Earlier versions of NetWare implemented a nonpre-emptible round-robin (First-in, First-out) scheduling policy where threads were scheduled to run in the order that they entered the run queue. On a uniprocessor system, NetWare is fast and very efficient.

For an application to exploit pre-emption, the code must be explicitly written to be pre-emptible. Critical section boundaries might be marked by calling scheduler API functions that signal a critical code section. Critical sectioning is used to keep program data in a consistent state and to prevent code that doesn't lend itself to concurrent execution from executing concurrently. A thread cannot be pre-empted when it is in a critical section.

By default, if an application thread is running, it will not be pre-empted until the following conditions are met.

- The code where the thread is running must be pre-emptable. This is indicated by a flag set in the module's NLM™ file format. When the code is loaded into memory, the memory pages are flagged as pre-emptible.
- The thread cannot be in a critical section of the code.
- The thread has run long enough to qualify for pre-emption. The scheduler checks the elapsed time with every tick.

Support for pre-emption provides

- An execution environment that allows simplified application development. Developers can rely on the scheduler to handle pre-emption.
- A mechanism that prevents ill-behaved modules from monopolizing the processor.

The kernel itself is not pre-emptible.

Platform Support Module

Besides NetWare, all that is necessary to enable multiprocessing on a multiprocessor computer is the Platform Support Module (PSM) for your specific hardware platform and NetWare. No other modules are required.

NOTE: Use the PSMs that load during installation. The PSMs for NetWare 4.11 SMP.NLM do not work for NetWare 5 or later.

The PSM is an interrupt abstraction for multiple processors. As a device driver for the processors, it shields NetWare from hardware-dependent or platform-specific details. It enables secondary processors to be brought online and taken offline.

During installation, NetWare detects multiple processors by reading the MP configuration table in BIOS and then determines which of the available NetWare Platform Support Modules (PSMs) matches the MP hardware platform.

The network administrator then has the option to load the PSM or to run NetWare on Processor 0 only. The installation program will modify the STARTUP.NCF file to load the PSM whenever the server is started.

Novell® provides MPS14.PSM, which supports any hardware platform that complies with the Intel* Multiprocessor Specification 1.1 and 1.4. Compaq* also provides a PSM for its system requirements. Contact Tricord* for information on their PSM for NetWare.

In addition to scalability, NetWare multiprocessing offers these benefits:

- Backward compatibility for applications written for NetWare 4.11 SMP.NLM. In fact, NetWare supports everything written to CLIB in previous releases. Older application code is simply funneled to Processor 0.

- An integrated multiprocessing kernel (MPK) that also supports uniprocessing. One binary runs on both uniprocessor and multiprocessor hardware platforms.
- Kernel support for pre-emption. (Applications must be explicitly enabled by their developers to take advantage of the kernel's pre-emption support.)
- Platform support for MPK in a single platform support module.

The Server Console

The server console includes the monitor and keyboard where you view and control NetWare server activity. From the server console, you can

- Shut down and restart the server
- Load and unload NLM programs
- Monitor server performance
- View network traffic
- Set configuration parameters
- Edit configuration and other batch files
- Send messages

The server console also supports more than one interface:

- **Command line.** Commands can be entered at the System Console prompt, with or without options and parameters. The prompt is indicated by the server name followed by a colon (:). LOAD is an example of a server console command.
- **Character-based menuing.** Utilities use menus, lists, and portals. The key utility for monitoring the server—MONITOR—is an example of this interface.
- **Java-based GUI**. The X Server--Graphical Console lets you access several Java* applications from the server.

  From the Desktop menu of the X Server--Graphical Console application, you can:

  - Run Java utilities such as ConsoleOne™, Install, RConsoleJ, Console Log, Editor, File Browser, NetWare Remote Manager, and Server Console.

- Control settings for the Java environment and GUI backgrounds.
- Run any console command.
- Close the X Server--Graphical Console application.

  To restart the Graphical Console, enter **STARTX** at the System Console prompt.

When NetWare is installed, the server console defaults to the Graphical Console screen. However, you can toggle between screens when you need access to the command line or if you choose to keep MONITOR loaded. For the procedure for toggling between console screens, see "Viewing and Accessing Server Console Screens" on page 50.

HINT: For information on bypassing the server splash screen or replacing it with a screen of your own choice, see "Starting the Server" on page 48 and SERVER in *Utilities Reference*.

Be aware of the following console security issues:

- Unauthorized access of the server console. Control keyboard access by requiring the use of a password. See "Securing the Server Console" on page 67.

  Use the SECURE CONSOLE command to secure your console against breaches of security. (See SECURE CONSOLE in *Utilities Reference*.)

  You can also use the screen saver and console-locking features in SCRSAVER. (See SCRSAVER in *Utilities Reference*.)

- **Software tampering.** An expert could use the built-in debugger to disable or bypass the security system. To prevent this, use SECURE CONSOLE.

- **Hardware tampering.** Keep your server in a secure location. An intruder could disable the power-on password or remove hard disks to access data.

NetWare Is Self-Tuning

In many ways, NetWare is a self-tuning system. It allocates resources according to need and availability.

Typically, new resources are not immediately allocated when a request is received. The operating system waits a specified amount of time to see if existing resources become available to service the request. If resources become available, no new resources are allocated. If they do not become available within the time limit, then new resources are allocated.

The time limit ensures that sudden, infrequent peaks of server activity do not result in permanently allocating unneeded resources.

For example, when the server is started, all free memory is assigned to file caching. However, as demand increases for other resources (such as directory cache buffers), the number of available file cache buffers decreases.

The following parameters are dynamically configured by the operating system:

- Directory cache buffers
- File locks
- Kernel processes
- Kernel semaphores
- Load balancing for multiple processors
- Maximum number of open files
- Memory for NLM programs
- Router/server advertising
- Routing buffers
- Service processes
- TTS™ transactions
- Turbo FAT index tables

In addition to the parameters configured by NetWare, you can adjust the value of many server parameters to optimize the server for your network. See “Setting Server Parameter Values” on page 38.

Java-Based Components of NetWare

NetWare includes the The Novell JVM for NetWare and the Just In Time Compiler, along with the Java Naming Directory Interface (JNDI) and Java Class Libraries (NJCL) for Novell, that enable you to run Java-based applets and applications on the server.

The Java-based components are installed automatically when you install NetWare. To use Java-based components, you must use TCP/IP. Instructions for using Java-based components are found in "Using Java on the Server" on page 63 and in ConsoleOne in *Utilities Reference*.

The Novell JVM for NetWare and the Just In Time Compiler

The Novell JVM for NetWare is comprised of several NLM programs that let the NetWare server run Java-based applications and applets, including multi-threaded applications and applications that use a graphical interface.

The JVM can run any application certified as 100% Pure Java, as described by JavaSoft*. However, applications that are not 100% Pure Java must be ported to NetWare.

NetWare includes the Symantec* Just In Time Compiler (JIT) to improve the performance of Java-based applications.

NetWare also includes drivers for popular video cards and a utility that automatically recognizes and configures your video card during NetWare installation.

To run the Novell JVM, you need a minimum of 48 MB RAM and at least 128 MB to run graphical applications. The more memory your server has, the more Java-based applications it can run.

For information about Java Class Libraries for Novell and the Java Naming Directory Interface (JNDI), see the Novell Class Libraries for Java documentation at the Novell DeveloperNet Web site (http://developer.novell.com/ndk/doc/njcl/njcl_enu/data/ha88dsny.html).

2 Setting Up the NetWare Server

For information about installing a NetWare® server, including hardware and software requirements and installation instructions, see the *NetWare 6 Overview and Installation Guide*.

For information about migrating from IPX™ to TCP/IP, see Migrating IPX to IP in the *Server Communications Administration Guide*.

After installation, you might want to use these setup procedures:

- "Changing the Server's Software Configuration" on page 24
- "Installing, Uninstalling, and Configuring a Server or Other Products" on page 25
- "Changing the Language NetWare Uses" on page 26

  The server's default language is English, but the server and the clients can use different languages. For information about the various localized components and procedures for changing them, see

  - "Code Pages" on page 26
  - "Changing Code Pages" on page 29
  - "Changing Server Message Files" on page 30
  - "Changing NLM Message Files" on page 31
  - "Changing the Server Keyboard Type" on page 32

Changing the Server's Software Configuration

After installing NetWare, you can make several changes, including

- "Installing, Uninstalling, and Configuring a Server or Other Products" on page 25
- "Setting Server Parameter Values" on page 38
- Changing time synchronization

  For more information on changing time synchronization, see Configuring Timesync on Servers in the *Network Time Management Administration Guide*.

- Adding or changing volumes

  For information about creating logical or traditional volumes, see Creating a Logical Volume or Creating a Traditional Volume in the *Novell Storage Services Administration Guide*.

- Modifying the eDirectory™ tree

  For information on designing and modifying the Novell eDirectory, see Designing the eDirectory Tree in the *Novell eDirectory 8.6 Administration Guide*.

Before changing the server's configuration, view the current configuration by entering **CONFIG** at the System Console prompt or by viewing and printing the configuration report in NetWare Remote Manager.

The CONFIG command displays the following information:

- Server name, internal network number, and server uptime.
- Hardware settings, node (station) addresses, external network number of the cabling scheme, board name, frame type, and communication protocol for each network board.
- The server's eDirectory tree and bindery context.
- On some systems, **CONFIG** might display information about NetWare Loadable Module™ (NLM™) programs. The kind and amount of NLM program information depends on the system.

For more information about running **CONFIG**, see CONFIG in *Utilities Reference*.

The configuration report in NetWare Remote Manager is much more complete and extensive. Printing or saving a copy of this report is a quick and easy method for documenting your server before you make any changes. For information about and instructions for creating this report, see Running and Viewing the Server Configuration Report in *NetWare Remote Manager Administration Guide*.

Installing, Uninstalling, and Configuring a Server or Other Products

The NWCONFIG utility lets you install, uninstall, and configure other products such as name space modules and NLM programs.

If you have questions during the installation or configuration of a product, refer to the documentation that came with the product.

Some products might not have configuration or uninstall options. A message explaining this is displayed if you try to perform unsupported operations.

1. At the System Console prompt, enter

   `[LOAD] NWCONFIG`

2. Select Product Options > View/Configure/Remove Installed Products.

   The list of Currently Installed Products appears. If no products are currently installed, the list is empty.

3. Do one of the following:

   - To install a product, press Insert and follow the prompts.
   - To uninstall a product, select the product from the list and press Delete.
   - To set configuration options for a product, select the product from the list and follow the prompts.

For more information, see NWCONFIG in *Utilities Reference*.

Changing the Language NetWare Uses

The default language for NetWare is English, but other languages are available. To change the language of your NetWare server and its NLM programs, see the following sections:

- "Code Pages" on page 26
- "Changing Code Pages" on page 29
- "Changing Server Message Files" on page 30
- "Changing NLM Message Files" on page 31
- "Changing the Server Keyboard Type" on page 32

Code Pages

A code page is a table storing a character set that supports one or more language scripts. When you press any key on a keyboard, the computer receives a numeric code that represents that keystroke. Code pages store these numeric codes. Many personal computer operating systems support multiple code pages and allow you to switch among them.

For example, DOS uses code page 437 for several languages that use Roman alphabetical characters, including English, French, and German, but requires code page 850 for Portuguese. DOS code page 850 (Portuguese) removes the symbol for f (franc) and inserts an O (acute). Different computer operating systems use different code pages for the same language. For example, DOS uses code page 437 for English, but Windows* 95 uses code page 1252.

In a single-byte code page, up to 256 codes are available to represent lower- and uppercase letters, numbers, punctuation marks, and all the mathematical symbols on your keyboard.

However, 256 codes are not sufficient to represent all the letters and characters used in the writing systems of every language. Some nonalphabetic writing systems, such as Chinese, Japanese, and Korean, contain thousands of characters and require a double-byte code page.

Differences between single-byte and double-byte code pages usually cause display and readability problems. For example, a document created with Windows 95 in Japan is probably created with code page 932. The same document will not look the same when displayed on a Windows 95 computer using code page 1252 in the United States. Unrecognized characters will be

replaced with a symbol such as a heart. In the past, these substituted characters might have caused a database such as Novell eDirectory to fail to recognize objects.

To help resolve these problems, a convention called Unicode* has been adopted.

Using Unicode

Unicode is a 16-bit character representation, defined by the Unicode Consortium, that supports up to 65,536 unique characters. Unicode allows the characters for multiple languages to be represented using a single Unicode representation.

Any character that your code page does not understand is substituted in your display by the 4-digit hexadecimal value of the Unicode character, surrounded by square brackets, for example: [00FF]

Because eDirectory supports Unicode, substituted characters do not prevent eDirectory from recognizing an object. For example, your company's European office might create an Organizational Unit object to represent Finance in western Europe. They might use DOS code page 852 to make the generic currency symbol a part of the object name (OU=¤W-Euro).

When this object is accessed in the United States, using DOS code page 437 or Windows 95 code page 1252, the currency symbol (¤) is replaced by square brackets surrounding the Unicode number for the currency symbol, [00A4]. eDirectory recognizes the Unicode number, so the object can still be opened and accessed.

However, the object name (containing the square brackets and unicode number) will be difficult for users to understand. If the name is too difficult to interpret, the only solution is to determine which code page was used to create the object and then view the object using that code page. Changing code pages can be troublesome; see "Changing Code Pages" on page 29 for guidelines.

The following table shows ranges of Unicode numbers, with a description of each range and a list of code pages that might be used to view the character correctly. However, switching to one of the suggested code pages does not guarantee that you will see the correct results. For example, characters in the range 4E00-9FFF (Han Ideographs) are used in Japan, China, and Korea. But switching to code page 932 (Japanese) does not display the character correctly if the character is used only in China.

The most reliable way to determine the character is to refer to the Unicode Standard, Version 2.0. Access the Unicode Web site (http://www.unicode.org) for more information. The Web site also includes charts of Unicode characters.

Table 1 Unicode Ranges, Descriptions, and Code Pages

Unicode Range	Description	Geographical Region	Windows Code Pages	DOS Code Pages
0080 - 00FF	Extended Latin	Western Europe		437, 850,860, 863, 865
0100 - 01FF	Extended Latin	Central Europe	1250, 1257	852, 775
0300 - 03FF	Greek	Greece	1253	737
0400 - 04FF	Cyrillic	Russia	1251	855, 866
0590 - 05FF	Hebrew	Israel	1255	862
0600 - 06FF	Arabic	Middle East	1256	864
2500 - 26FF	Line Drawing and Graphics	N/A	N/A	Most DOS code pages
4E00 - 95FF	Han Ideographs	Far East	932, 936, 949, 950	932, 936, 949, 950
AC00 - D7FF	Hangul Syllables	Korea	949	949
FE70 - FEFF	Arabic Presentation Forms	Middle East	N/A	864
FF00 - FFEF	Full- and Half-Width Variants	Far East	932, 936, 949, 950	932, 936, 949, 950

Changing Code Pages

Changing code pages on the NetWare server or on DOS can usually be done while the computer is operating. However, changing code pages on a Windows 3.1*x* or a Windows 95 workstation might require installing additional software and restarting Windows. For background information about Unicode and other code pages, see "Code Pages" on page 26.

To change the code page on	Do the following
NetWare Server	At the System Console prompt, type **CHARSET CP*xxx*** where *xxx* is the number of the code page you want to load. The following code pages are supported: 437, 737, 850, 852, 855, 857, 860, 861, 863, 865, 866, 869.
DOS	Follow instructions that come with the DOS operating system.
Windows 3.1*x*, Windows 95, Windows NT	Follow instructions that come with the operating system. You might be required to install a new set of Unicode translation tables, found on the NetWare product CD. You will need the following: ◆ UNI_*newpage#.platform*: Translates the new code page to Unicode and Unicode to the new code page ◆ UNI_MON.*platform*: Converts characters to lower case to facilitate comparisons ◆ UNI_UPR.*platform*: Handles uppercase characters The following platform extensions are included: .W16 (Windows 3.1*x*) .W32 (Windows 95, Windows NT*) .DOS (DOS)

For more information on changing code pages using the CHARSET command, see CHARSET in *Utilities Reference*.

Changing Server Message Files

English is the default language for both the NetWare operating system and its NLM programs and utilities.

You specified a language for the server when you installed it. To change the server language later, you must first copy new language files to the server and then set the server to the new language and restart the server as follows.

IMPORTANT: This procedure requires you to restart the server because executing SERVER.EXE sets the server language.

1. (Conditional) If you are copying the files from the NetWare installation CD-ROM, insert the CD.
2. At the System Console prompt, enter

   [LOAD] NWCONFIG
3. Select Product Options > Choose an Item or Product Listed Above > Add Additional Language to the Server.

   The screen displays a box containing the path from which you last installed files. Make sure this path is to the language files. The language files on the NetWare CD are located at

   drive or volume*:\NW60\INSTALL\NLS*language_id

   To get a list of language IDs, enter the following at the System Console prompt:

   LANGUAGE LIST
4. If the path is correct, press Enter; if the path is incorrect, press F3 and type in the correct path to the language files.

   If you are installing the files from another server, type the path to that server; the system might prompt you for a username and password. Follow the prompts.

   The system displays a window listing groups of language files.
5. Use the arrow keys to move the cursor to the language you want to install and press Enter.

   The system marks the selected language with an X. You can specify several languages, if desired.

   To deselect a language, move the cursor to the language and press Enter again.

6. When you have finished selecting languages, press F10.

   The system copies the selected language files.

7. Press Esc until the Other Installation Items/Products menu is displayed.

8. Select Change Server Language.

   The screen displays a box containing the path from which you last installed files.

9. Press Enter to accept the path.

   The system displays a menu listing the available languages.

10. Select the desired language from the menu.

    If this is the first time you have changed the language, the system displays a prompt specifying the default destination where the language files are to be placed. The location is the default boot directory, C:\NWSERVER.

    The language files must be placed in your boot directory.

11. Accept the default or type the path to your boot directory.

    After you specify the boot directory, the system loads the language files.

12. Restart the server for the change to take effect.

Changing NLM Message Files

To change the language for subsequently loaded NLM programs, use the LANGUAGE command at the System Console prompt. The LANGUAGE command does not change the language for currently loaded modules.

IMPORTANT: If you change the NLM language without changing the server language, the NLM still displays some character strings and screen titles in the server language. For consistent language display, you should also change the server language as explained in the section, "Changing Server Message Files" on page 30.

1. At the System Console prompt, enter

   LANGUAGE LIST

   The server displays a list of languages and their ID numbers. Not all languages in the list are currently supported.

2. Note the name or number of the language you want to use.

3. At the System Console prompt, enter

   LANGUAGE *Language_name* |*number*

Any subsequently loaded NLM programs will be displayed in the new language.

For more information, see LANGUAGE in *Utilities Reference*.

Changing the Server Keyboard Type

NetWare allows you to use keyboard types other than U.S. English by loading the KEYB utility. The language you specify with KEYB must match the language of your keyboard, not language of the server. The keyboard type can be changed without restarting the server.

IMPORTANT: Changing the keyboard type causes some of the keys on your keyboard to represent different characters. Do not use this command unless you have the appropriate keyboard for the language you are specifying and you are familiar with the keyboard's use. Otherwise, you might not know which keys to use to change the keyboard back to its original language.

1. At the System Console prompt, enter

   `[LOAD] KEYB`

2. From the list of keyboard types, find the keyboard type that matches the one you are using.

3. To change the keyboard type to match your keyboard, enter

   `[LOAD] KEYB keyboard_type`

   For example:

   `[LOAD] KEYB GERMANY`

For more information, see KEYB in *Utilities Reference*.

3 Optimizing the NetWare Server

Optimizing the NetWare® server requires staying up-to-date with Novell® Technical Support (http://support.novell.com) and performing one or more of the following tasks:

To	See
Learn how to obtain the most recent operating system updates and then patch your server before you optimize	“Applying Patches” on page 34
Isolate and resolve bottlenecks by making sure that your hardware components are well matched for power and potential performance	“Matching Performance Capabilities” on page 34
Learn how to improve the performance of your server by changing SET parameters	“Setting Server Parameter Values” on page 38
Identify where you can adjust the value of a server parameter and tune your server for its particular processing load	“Monitoring the NetWare Server” on page 82
Reduce network traffic by managing the protocols on your server	“Minimizing Replication Traffic” on page 45

Applying Patches

Novell makes every attempt to solve problems in the NetWare operating system software by periodically releasing updates that you can install on your server. The latest operating system update contains all previous updates, so be sure to install the most current file. It will keep your operating system current.

The latest operating system updates can be found at the following locations:

- In the patch lists on the Novell technical support Web site (http://www.support.novell.com/filefinder/).
- By File Transfer Protocol (FTP): Anonymous FTP to ftp.novell.com.
- By Gopher: gopher.novell.com.
- On the Novell Support Connection® CD (http://www.support.novell.com/additional/nsc-cd.html): Released monthly on CD-ROM and sent to subscribers.

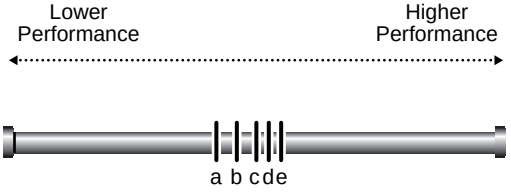
For information about installing NetWare patches, read the Readme file associated with the patch.

Matching Performance Capabilities

Each component's performance characteristics can have an effect on the system's performance as a whole. Bottlenecks can be created by a great number of subcomponents and component interactions. Protocols create bottlenecks. Specific software functionality creates bottlenecks. In fact, every part and process of a system is a potential bottleneck. However, it's important to keep in mind that only one bottleneck—the system's weakest point—can exist at one time.

Another point to remember is that all systems have a weak point somewhere. Your goal is to match the performance capabilities of your system's components in such a way that no single component hampers the performance of any other component. Figure 2 on page 35 shows a system with matched components.

Figure 2 A Well-Designed System

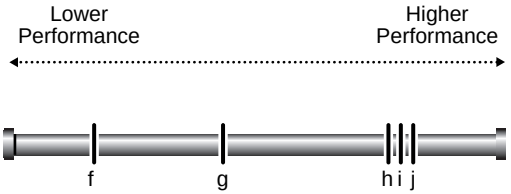


a,b,c,d,e represent the performance capabilities of each system component

Note that all components in a well-designed system are within the same range of performance. But in this case, a less than optimum component is cost effective. The components are so closely matched that upgrading the lower-end component *a* would not increase performance enough to make it worth the cost.

Figure 3 shows a poorly designed system with an inefficient mix of low- and high-performance components.

Figure 3 A Poorly Designed System



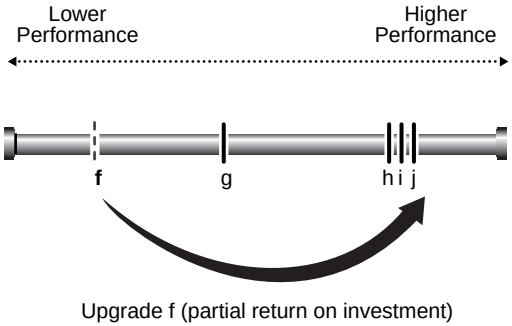
f,g,h,i,j represent the performance capabilities of each system component

In this system, components *f* and *g* have performance characteristics that are considerably inferior to components *h*, *i*, and *j*. With component *f* as the bottleneck, components *h*, *i*, *j*, and even *g* are constrained by *f* so that they run much more slowly than their designs would otherwise permit. In this system, the bottleneck is significantly hampering the system's performance.

This is a poorly designed system because the high-performance components aren't able to perform anywhere near their full potential. In fact, because of the high-performance characteristics of *h*, *i*, and *j*, this system might have cost more than the system in Figure 3. But it cannot perform as well because of the greater disparity between its low- and high-performance components.

The unbalanced system in Figure 4 would benefit noticeably if you were to upgrade component *f* to the performance level of *g*. But if you were to upgrade *f* to a performance level beyond *g*—as shown in the following figure—all additional performance characteristics in *f* would be lost because the bottleneck would move to component *g*.

Figure 4 Moving the Bottleneck



Thus you derive only a partial return on your investment in the upgrade. To accomplish more than moving the bottleneck, both components must be upgraded to the level of *h* before a full return on investment in *h*, *i*, and *j* can be reached.

It is useless to test any single component of a system to its fullest capacity without allowing for the possibility that another component is actually bottlenecking system performance. You can upgrade system components, but you won't see any significant improvement until you isolate the system bottleneck, assess its relationship to the performance characteristics of the entire system, and take appropriate action.

Bottleneck isolation is critical if you're building high-performance systems. You need to know how and where your system is bottlenecking. Moreover, you need to know how tightly that bottleneck is coupled with the performance characteristics of the rest of the system. If the poorly performing component is in a different performance category than the other components, you might obtain a greater return on investment by making the necessary upgrades to move the bottleneck to the highest possible performance level.

This discussion is taken from "Performance Analysis: Isolating the Real Bottleneck in a System," in the January 1996 *AppNotes*™ (http://developer.novell.com/research/appnotes/1996/january/04/index.htm).

Setting the Load Balancing Threshold

The load balancing threshold applies only to multiprocessor servers. Through extensive testing, Novell has determined the optimum threshold for load balancing across multiple processors—it addresses serious load imbalance while avoiding excessive thread migration. Without that play in the load balancing mechanism, threads would constantly move from one processor to another.

The optimum threshold has been preset by Novell and, in most cases, it provides the most efficient processor utilization. Although we strongly recommend that you do not change the threshold, this value is configurable.

WARNING: Adjusting this threshold should be done only with considerable research and consultation. Experimenting with different threshold levels can best be done in an isolated test system. Do not experiment in a production environment. Remember that you can always return to the optimum setting.

To set the load balancing threshold, complete the following:

1. In NetWare Remote Manager, click the Set Parameters link in the navigation frame and then click the Multiprocessor link.
2. Click the *value* link for the System Threshold parameter.

   The page displays the current setting and the range of valid values. The default value is 1536.
3. To change the threshold setting, type a new value in the field and click OK.

For more information about the value ranges and default setting, see SET Multiprocessor Parameters in *Utilities Reference* or the online help for the parameter in NetWare Remote Manager.

To view CPU utilization by an NLM™ program in NetWare Remote Manager, click the Profile/Debug link in the navigation frame, and then click the Profile CPU Execution by NLM link on the Profiling and Debug Information page.

Setting Server Parameter Values

Default values for NetWare server parameters provide maximum performance for most systems. You should seldom need to modify these values. But when you need to modify them, we recommend that you first read the topics listed here.

- "Understanding Server Defaults" on page 38
- "Finding Current Parameter Values" on page 40
- "Printing Current Parameter Values to a File" on page 41
- "Checking Current Parameter Values with DISPLAY ENVIRONMENT" on page 42
- "When to Modify Defaults" on page 42
- "When Not to Modify Defaults" on page 43
- "Restoring Default Values with RESET ENVIRONMENT" on page 43
- "Monitoring Dynamic Statistics" on page 43
- "Using Optional Commands in Startup Files" on page 44
- "Using SET Commands in Startup Files" on page 44

Understanding Server Defaults

NetWare has been tuned for the specific duties of a network server. It has been thoroughly tested with software tools designed to identify inefficiencies so they can be eliminated. NetWare gives outstanding off-the-shelf performance.

NetWare is also self-tuning. The following parameters are dynamically configured by the operating system:

Packet receive buffers
File cache buffers
Directory cache buffers
Memory for NLM programs
Service processes
Kernel processes
Kernel semaphores
Load balancing for multiple processors
File locks

Maximum number of open files

Turbo FAT index tables

TTS transactions

Router/server advertising

To tune the server for its particular processing load, three utilities are available to check or set server parameter values:

- NetWare Remote Manager (PORTAL.NLM) is a Web-based utility that you run from a workstation. You can use NetWare Remote Manager to navigate to a specific parameter quickly by clicking Set Parameters, then selecting the category and value you want to change, and then changing or resetting the values to the default. For more information, see the *NetWare Remote Manager Administration Guide*.
- MONITOR is a character-based utility that you must use at the server console or access through NetWare Remote Manager. MONITOR also allows you to configure SET parameters from its Server Parameters option. This means you can set server parameter values from within MONITOR without memorizing parameter names and their valid values. For more information, see MONITOR in *Utilities Reference*.
- SET is a command line utility executed at the System Console prompt. If you are familiar with the names of the server parameters, you might find that using SET is faster for routine tuning. For more information, see SET in *Utilities Reference*.

Most SET parameter values are persistent and are stored in a the NetWare Registry. A NetWare server retains any settings that have been modified from the default values—even when it is taken down and then rebooted, the server will come up again with all the settings you have made to tune the server.

To ensure that explicit SET parameter changes are perservered, you can add the command for each change to the STARTUP.NCF or AUTOEXEC.NCF file. For procedures on editing these files, see "Using NWCONFIG to Create and Edit Startup Batch Files" on page 57.

Finding Current Parameter Values

Locating the SET parameter values to check or set them is different is a little different in each utility (NetWare Remote Manager, MONITOR or SET).

In NetWare Remote Manager

1. Access NetWare Remote Manger.
2. Click the Set Parameters link in the navigation frame.
3. Click a parameter category.

   A list of parameters in that category that can be changed is displayed.

   If you want to view a description of a parameter, click the Information icon next to the value.

   If you are not sure what category a SET parameter is in, you can view and search the Configuration report in using NetWare Remote Manager. The Configuration report lists all the SET parameters by category with their current settings.
4. Click the value for the parameter you want to change.

   The current setting for the parameter and its range of valid values is displayed.
5. Type the new value in the current value field and click OK.

In MONITOR

1. At the System Console prompt, enter

   MONITOR
2. From the Available Options menu, select Server Parameters.
3. Press F1 for descriptions of the server parameter categories.
4. Press Esc to return to the menu of parameter categories.
5. Select a parameter category.

   The parameters are displayed in the upper window. As you highlight the field for each parameter, a pop-up window displays a description of the parameter, its current setting, and its range of valid values.
6. When you have finished, press Esc until you return to the Available Options menu.

In SET

1. At the System Console prompt, enter

   SET

   A numbered list of server parameter categories is displayed.

2. Enter the number associated with the category you want to view.

   A list of parameter names is displayed. The name of each parameter appears highlighted in white with the current setting highlighted in yellow. The information also includes the limits (or range of valid values), the .NCF file the parameter can be set in, and a brief description.

   If necessary, press any key to display additional parameters in the same category. Press Esc to exit the category.

3. To select another category, repeat the previous steps.

Printing Current Parameter Values to a File

Most settings for NetWare server parameters are now persistent, whether you set them using NetWare Remote Manager, MONITOR, or SET. Nevertheless, you should record your optimum server configuration as part of documenting your network.

To write current values of settable parameters to a file and print it, complete the following:

1. Access NetWare Remote Manger.
2. Click the Set Parameters link in the navigation frame.
3. In the Save Settings to a File on Volume SYS: field, accept the default filename (SETTINGS.TXT) or enter a different filename.
4. Click the Save button to the right of the Save Settings to a File on Volume SYS: field.
5. Browse to the file on the server and print it.

Checking Current Parameter Values with DISPLAY ENVIRONMENT

You can also check parameter values by using two other console commands: DISPLAY ENVIRONMENT and DISPLAY MODIFIED ENVIRONMENT.

- The DISPLAY ENVIRONMENT command displays the current search paths and the current values of the settable server parameters. (Hidden parameters are not displayed.)

  At the System Console prompt, enter

  DISPLAY ENVIRONMENT

  The name of each parameter appears highlighted in white. The current value appears in yellow. The limits (or range of valid values) and the default setting (if applicable) also appear.

- In comparison, the DISPLAY MODIFIED ENVIRONMENT displays *only* the server parameters that have values modified from the defaults.

  At the System Console prompt, enter

  DISPLAY MODIFIED ENVIRONMENT

  The display is similar to that of DISPLAY ENVIRONMENT. The difference is that only modified parameters values are shown.

For more information, see DISPLAY ENVIRONMENT and DISPLAY MODIFIED ENVIRONMENT in *Utilities Reference*.

When to Modify Defaults

NetWare defaults were chosen after thorough testing to provide both excellent performance and system balance.

Before modifying defaults, you should track and log performance statistics. You can do this using NetWare Remote Manager or MONITOR. You will also find the server log files useful in assessing the server's performance. See "Checking Server Error Logs" on page 97.

You can modify default values to

- Compensate temporarily for a poorly performing subsystem, allowing the server to remain in service.
- Resolve inefficiencies.
- Optimize performance and tune the server for its processing load.

For example, if your server has a slow hard disk or insufficient RAM, you can compensate temporarily by modifying defaults. The long-term solution is to replace the disk or to add RAM. See “Matching Performance Capabilities” on page 34.

When Not to Modify Defaults

If you were to modify some defaults, you could sacrifice the system’s balance and performance.

After thorough testing, we recommend, for example, that you do not modify the default settings of the Load Balancing Threshold or the Transaction Tracking parameters.

Restoring Default Values with RESET ENVIRONMENT

If you want to restore the default values of the settable server parameters, you can use the RESET ENVIRONMENT command.

When you run RESET ENVIRONMENT, you are prompted at each changed server parameter value.

At the System Console prompt, enter

```
RESET ENVIRONMENT
```

When the first parameter with modified values appears, you can choose to reset *all* values to their defaults or just reset the value of the parameter that is displayed. Or you can also skip to the next modified parameter.

For more information, see RESET ENVIRONMENT in *Utilities Reference*.

Monitoring Dynamic Statistics

MONITOR reports many useful statistics and updates most of them every second with the return values from direct calls to the operating system. However, not all statistics are of equal value to the network administrator. The key dynamic statistics are displayed in MONITOR’s General Information screen, which appears as soon as MONITOR is accessed. For a description of these statistics, see “What to Monitor and Why” on page 83.

NetWare Remote Manager and ConsoleOne™ are other utilities that allow you to monitor server performance.

Using Optional Commands in Startup Files

During initialization, NetWare executes two server boot files that are created by the installation process:

- **STARTUP.NCF**. Executes first and loads the server's disk drivers, name spaces, and some SET parameters. This file resides in the startup directory, C:\NWSERVER.
- **AUTOEXEC.NCF**. Stores the server name and IPX™ internal network number (if IPX is installed), loads the LAN drivers and settings for the network boards, binds the protocol to the installed drivers, and loads other NLM programs. This file resides in SYS:\SYSTEM.

  IMPORTANT: Even if you use IP, the internal network number stored in this file serves as a unique server ID. IP uses this number to provide passive IPX support called Compatibility Mode.

An .NCF file executes all the commands within it. However, you can make a command optional by placing a question mark (?) in front of it. For the procedure, see "Making a Command Optional in a Server Batch (.NCF) File" on page 58.

Using SET Commands in Startup Files

Remember that some SET commands can be executed only from the STARTUP.NCF file. To find out whether a SET command must be executed in STARTUP.NCF, see the detailed information for the parameter in NetWare Remote Manager.

If a SET command is nonpersistent and you want its setting to remain when the server is restarted, then add the SET command for any nonpersistent parameters to the STARTUP.NCF file.

When you install the server operating system, the installation process adds SET commands to the AUTOEXEC.NCF file—commands that control time zone and daylight savings time information, bindery context, and time server type.

You can add more SET commands to the AUTOEXEC.NCF file, if desired. To modify server batch files, you can use NWCONFIG or Editor at the server console or edit and upload the file using NetWare Remote Manger. When the server is rebooted, any parameter values set by commands in the AUTOEXEC.NCF file override previous values for those parameters.

Minimizing Replication Traffic

Careful choice and placement of tree replicas can minimize replication traffic on the network.

- Make sure that the replica containing the User object is on the server nearest the user.
- Do not create more partition replicas than you need. The more replicas, the more traffic required to synchronize them all.

For more information about optimizing eDirectory™, see Designing the eDirectory Tree or Managing Partitions and Replicas in the *Novell eDirectory 8.6 Administration Guide*.

4 Managing the NetWare Server

Managing the NetWare® server operating system involves such tasks as the following:

- Starting and Stopping the Server (page 48)
- Viewing and Accessing Server Console Screens (page 50)
- Starting and Stopping Processors (page 52)
- Using Server Batch Files (page 55)
- Using Server Utilities and Console Commands (page 60)
- Using Java on the Server (page 63)
- Securing the Server Console (page 67)
- Using NCP Packet Signature (page 70)
- Using the Transaction Tracking System (page 77)
- Using an Uninterruptible Power Supply (UPS) (page 81)
- Securing the Server Console (page 67)
- Preventing Virus Infection (page 82)
- Monitoring the NetWare Server (page 82)
- Displaying Server Alerts (page 87)
- Managing Workstation Connections (page 89)
- Performing Common Maintenance Tasks (page 96)
- Performing Preventive Maintenance Tasks (page 101)

Starting and Stopping the Server

This section contains information and procedures on starting the server, bringing it down using an orderly shutdown, and restarting the server without exiting to DOS.

Starting the Server

To start the server, change to the startup directory (usually C:\NWSERVER) and enter the following at the server's DOS prompt:

```
SERVER
```

HINT: You can also place the command to execute SERVER.EXE in the DOS AUTOEXEC.BAT file. Then, whenever the server computer is powered up, the server starts automatically.

When you execute SERVER.EXE, the Novell® logo is displayed. To prevent the Novell logo (server splash screen) from displaying, you can load SERVER with the `-nl` (no logo) command option.

If the splash screen is active and you want to see a list of modules as they load, you can still display the System Console screen by using the following procedure to toggle between server console screens.

1. Press Alt+Esc, tapping Esc until the System Console screen is displayed.

   A list of modules scrolls up the screen. If you have a color monitor, the color in which each module name is displayed indicates how the module is loaded.

   - Cyan (light blue) indicates a module is loaded by SERVER.EXE
   - Red indicates the module is loaded from the startup directory
   - White indicates a module loaded from the AUTOEXEC.NCF file
   - Purple indicates a module is loaded by other modules

2. After the server is running, you can display a list of all loaded modules by entering the following command at the System Console prompt:

   ```
   MODULES
   ```

   The module names are displayed in colors that represent the functional group they belong to, as described above.

For more information, see SERVER and MODULES in *Utilities Reference*.

Bringing Down the Server

To ensure data integrity, use the DOWN command at the server console before turning off power to the server. DOWN writes all cache buffers to disk, closes all files, updates the appropriate Directory Entry Tables and File Allocation Tables, and exits the network.

If you want to bring the server down and then restart the server immediately, without exiting to DOS, use the RESTART SERVER command instead of DOWN.

If you want to bring down the server and then warm boot the computer, use the **RESET** command. To make the server load automatically after a **RESET** command, enter a line to run SERVER.EXE in the DOS AUTOEXEC.BAT file on the server computer.

NOTE: Bringing down or restarting a server during a remote console session terminates the session.

You can also bring down, restart, or reset the server from a workstation using the options on the Down/Restart page in NetWare Remote Manager.

Before you bring the server down, you should inform all users to close files and log out of the server. You can do this using the Broadcast Message to Everyone field on the Connections page in NetWare Remote Manager or by using the Connections, Compose a Message (F4) option in MONITOR.

To send a message and shut down the server from the server console, do the following:

1. Send a message to all logged in users from Monitor.
   - **1a** From the Available Options menu, select Connections.
   - **1b** Highlight each connection you want to inform and press F5 to mark it.
   - **1c** Press F4 to display a Message Text window.
   - **1d** Type the message and press Enter to send the message to the designated connections.

     For example, you might send a message like this:

     Please close files and log out from *servername*
     Going down in 5 minutes.

2 Execute one of the following commands at the System Console prompt:

2a To bring down the server and exit to the local operating system, enter

```
DOWN
```

You can now shut off power to the system, if necessary.

2b To reboot the server without exiting to DOS, enter

```
RESTART SERVER
```

2c To bring down the server and then warm boot the machine, enter

```
RESET SERVER
```

Although most modules, including those in protected address spaces, unload automatically when you bring down or restart the server, some modules might require that you unload them individually first. You can unload them manually with the **UNLOAD** command. Or you can create a batch file called SHUTDOWN.NCF in the SYS:SYSTEM directory and place the unload commands in it. If you create SHUTDOWN.NCF, it is executed automatically whenever you bring down, restart, or reset the server.

For more information, see "Using EDIT to Create and Edit Text and Batch Files" on page 56 and UNLOAD, DOWN, and RESTART SERVER in *Utilities Reference*.

Viewing and Accessing Server Console Screens

After you start the server, the following screens are available at the server console by default.

- **System Console.** (Item 1 on Current Screen list) Lets you load or unload any NLM™ programs to the server, execute console commands, change SET parameter values, and view current messages sent to the server.
- **Logger Screen.** (Item 2 on the Current Screen list) Lets you view most of the information that used to be displayed on the System Console screen. This screen is scrollable and can be saved to a file. To access a list of commands for scrolling and saving to a file, press F1 while viewing the Logger screen.

- **X Server -- Graphical Console.** Lets you access and run the Java applications listed. To access the list, click Novell on the Graphical console.
  - The default screen that is shown when the server is started is the X Server -- Graphical screen unless you have disabled it.
  - To load this screen if you have disabled it, enter STARTX at the System Console prompt.
  - To close this screen from the GUI menu, click Exit.
  - To close this screen using the server keyboard, press Ctrl+Alt+Backspace.

Some NLM programs have console screens associated with them. If you load one of these NLM programs, then the console screens associated with it are automatically active at the server console.

To view which screens are active at the server console, press Ctrl+Esc on the server keyboard. A numbered list of active console screens is displayed. Enter the number for the screen you want to access.

To cycle through other console screens, press Alt+Esc on the server keyboard, and then continue to hold Alt down and tap Esc until the screen you want to access is displayed. Use the title bar at the top of the screen for navigation. When the X Server -- Graphical Console is displayed, you must release the keys and start over.

Another screen that is available at the server is the Emergency Console. This console can be useful when the server console seems to hang. On the Emergency console, you can shut down the server and exit to DOS, abort a volume mount, or open a new console screen to issue necessary commands such as unloading modules.

To access the Emergency Console, press Ctrl+Alt+Esc on the server keyboard. From this console you can do the following:

- Down the file server and Exit to DOS
- Cancel a volume mount
- Spawn a new command line process (brings up an additional console screen that you can enter console commands at).

  To exit the additional console screen, enter **BYE** at the console prompt.

Starting and Stopping Processors

This section explains how to start and stop individual processors in a multiprocessing server. Only secondary processors can be handled this way.

When the Platform Support Module (PSM) is loaded in the STARTUP.NCF file and the Auto Start Processors SET parameter value (Multiprocessor category) is set to On, NetWare can start the secondary processors automatically.

NOTE: Server console commands for processors affect only secondary processors. Processor 0 cannot be taken offline while the server is running.

You can start or stop secondary processors at any time while the server is running by using the console commands **START PROCESSORS** and **STOP PROCESSORS** or by clicking the Start Processor or Stop Process link on the Processor Information page in NetWare Remote Manager. (If you choose to start secondary processors manually, you can change the value for the Auto Start Processors SET parameter to Off.) When any secondary processor is stopped, the associated threads are automatically switched to another processor.

This section includes the following information:

- "Displaying Processor Information" on page 52
- "Starting Processors" on page 54
- "Stopping Processors" on page 53

Displaying Processor Information

Before starting or stopping a process, you should display the processor information to determine the status of the processor. Several utilities are available to display processor information.

Using NetWare Remote Manager

1. Click the Processors link in the navigation frame.
2. View the information on the Processor Information page.

   From this page you can view whether the processor is online or offline, start or stop a processor, and view the following information about each processor:

   - Speed, family, model, and stepping
   - Feature flags and CPUID

- L1 and L2 cache
- The amount of TLB Instruction and Data entries

Using Server Console Commands

To determine which processors are currently online from the System Console prompt, run the **DISPLAY PROCESSORS** command.

To determine processor speed and other generic information, enter the following at the System Console prompt:

CPUCHECK

For example, with a single processor, the output for CPUCHECK might be similar to the following:

```
Processor Speed 199 MHZ, CPUID 52C:1BF
Family 5, Model 2, Stepping C
```

For more information, see DISPLAY PROCESSORS and CPUCHECK in *Utilities Reference*.

Using Monitor

Per-processor statistics are also available from MONITOR. From the Available Options menu, select Kernel > Processors.

Stopping Processors

Processor 0 is the boot processor and cannot be taken offline.

When a secondary processor is taken offline, the threads running on that processor are switched to another processor automatically.

You can stop processors using NetWare Remote Manager or server console commands at the System Console prompt.

Using NetWare Remote Manager

To bring a secondary processor offline in NetWare Remote Manager, do the following:

1. Click the Processors link in the navigation frame.
2. Click the Stop Processor link for the applicable processor that you want to stop.

Using Server Console Commands

The following table specifies the commands to use at the System Console to take a processor offline.

To	Enter
Identify which processors are currently online and to obtain their ID numbers	**DISPLAY PROCESSORS**
Take a secondary processor offline	**STOP PROCESSORS** ***n*** *n*=processor number
Take two or more (but not all) secondary processors offline	**STOP PROCESSORS** ***n n*** *n*=processor number
Take all secondary processors offline	**STOP PROCESSORS**

For more information, see DISPLAY PROCESSORS and STOP PROCESSORS in *Utilities Reference*.

Starting Processors

The NetWare default is to start secondary processors automatically when the server boots. If a secondary processor is offline, you can bring in online by using NetWare Remote Manager or server console commands at the System Console prompt.

Using NetWare Remote Manager

To bring a processor online in NetWare Remote Manager, do the following:

1. Click the Processors link in the navigation frame.
2. Click the Start Processor link for the applicable processor that you want to start.

Using Server Console Commands

The following table specifies the commands to use at the System Console to bring a processor online.

To	Enter
Bring a specific secondary processor online	**START PROCESSORS** ***n*** *n*=processor number
Bring two or more (but not all) secondary processors online	**START PROCESSORS** ***n n*** *n*=processor number
Bring all secondary processors online	**START PROCESSORS**

For more information, see START PROCESSORS in *Utilities Reference*.

Using Server Batch Files

This section explains how to use .NCF batch files to load modules, execute System Console commands, and configure subsystems. For procedures, see the following:

- "Using EDIT to Create and Edit Text and Batch Files" on page 56
- "Using NWCONFIG to Create and Edit Startup Batch Files" on page 57
- "Making a Command Optional in a Server Batch (.NCF) File" on page 58
- "Changing Server Name and Internal Address in AUTOEXEC.NCF" on page 59

A server batch file is an executable file containing server console commands. You execute the file by entering its name at the System Console prompt. NetWare then executes all the commands in the file in order.

By default the NetWare installation process creates two batch files that are always executed whenever the server is booted:

- **STARTUP.NCF**—This file is executed first. It loads the server's disk drivers and name spaces, and can execute certain server parameters that cannot be executed anywhere else. This file resides in the server's startup directory, C:\NWSERVER.
- **AUTOEXEC.NCF**—This file is executed after STARTUP.NCF and after volume SYS: is mounted. It sets time synchronization parameters and the bindery context, stores the server name, loads the communication protocol, loads the LAN drivers and settings for the network boards,

binds the protocol to the installed drivers, loads other NLM programs, and executes server parameters. This file resides in the SYS:SYSTEM directory.

In addition, you can create a batch file called SHUTDOWN.NCF in SYS:SYSTEM to execute commands whenever you shut down the server. The DOWN command executes SHUTDOWN.NCF automatically whenever the server is shut down, therefore, you should never include the DOWN command in the SHUTDOWN.NCF file.

You can create any other batch files you need. Simply create a text file with a .NCF extension. Place NetWare console commands into the batch file in the order that you want them executed in.

Using EDIT to Create and Edit Text and Batch Files

NOTE: Each time you save the file, you can increase the file size by up to 4 KB.

1. At the System Console prompt, enter

   [LOAD] EDIT [*path*]

   If you specify a path, include both the directory and filename. The file must be located on a mounted volume or on a local drive of the server.

   If you do not specify a path, the system displays a prompt at which you can either enter the filename or display a browse window.

   - To enter the filename, type either the complete file path (volume, directory, and filename) or just the filename, and press Enter.

     If you enter only the filename, the system assumes a default location of SYS:SYSTEM.

     If the file does not exist, EDIT displays a prompt that asks whether the file should be created. Choose Yes to create the new file or No to redisplay the filename prompt. If you choose Yes, EDIT displays a blank screen so you can enter text into the file.

   - To display the browse window, press Insert.

     To see the contents of a volume or directory, highlight the volume or directory name and press Enter. Use the arrow keys to scroll up and down the list of files and directories. To display a file, highlight the filename and press Enter.

2. Create or edit the file as needed.

   To get a description of the keystroke to use while using Edit, press F1.

3. When finished, press Esc. Select Yes to save the file or No to exit the file without saving changes.

   The system redisplays the pathname prompt.

4. To edit or create another file, enter the file pathname. To redisplay the System Console prompt, press Esc.

For more information, see EDIT in *Utilities Reference*.

Using NWCONFIG to Create and Edit Startup Batch Files

The following procedure explains how to use NWCONFIG to create or edit the STARTUP.NCF and AUTOEXEC.NCF files.

1. At the System Console prompt, enter

   [LOAD] NWCONFIG

2. Choose NCF Files Options.

   The system displays a menu containing options to create or edit both the STARTUP.NCF and AUTOEXEC.NCF files and to upgrade a NetWare 3.1*x* AUTOEXEC.NCF file.

3. Highlight the desired option and press Enter.

   If you select the option to upgrade the NetWare 3.1*x* file, follow the screen prompts. NWCONFIG compares the file with the current NetWare configuration and makes changes to the file as necessary. You can edit the file before saving it.

   If you select an option to edit one of the files, the selected file appears in a window.

   If you select an option to create one of the files, the system displays the existing file, if there is one, in one window and a new file with default entries in another window, so you can compare the two.

   The default entries include only essential contents of the file and reflect the current system setup. For example, the default entries for AUTOEXEC.NCF might include time zone information and **LOAD** and **BIND** commands for currently installed LAN drivers, but would not include custom configuration settings you have in the original file.

   The cursor is active in the new file. Press Tab to toggle between the two files.

4. Edit the new or existing file as necessary.

Editing and navigation keystrokes are listed at the bottom of the screen. For additional help, press F1.

5. When finished, save the file by pressing F10 and selecting Yes when prompted. To exit without saving, press Alt+F10. Changes to the file take effect after you reboot the server.

   IMPORTANT: Each time you edit the AUTOEXEC.NCF file or the STARTUP.NCF file, NetWare saves the previous version as AUTONCF.OLD or STARTNCF.OLD.

For more information, see NWCONFIG in *Utilities Reference*.

Making a Command Optional in a Server Batch (.NCF) File

By default, an .NCF file executes all the commands within it. However, to make a command optional, you can place a question mark (?) in front of it.

The question mark causes the .NCF file to pause at the command and prompt you to execute it. You can respond either Yes or No. You can also specify a default response.

For example, the following line in the AUTOEXEC.NCF file causes the file to pause and ask whether to execute the LOAD MONITOR command:

```
? LOAD MONITOR
```

When the AUTOEXEC.NCF file is executed, it displays the following prompt:

```
LOAD MONITOR? Y
```

The default response is Yes. If you do not respond to the prompt, the default response is executed after 10 seconds.

Both the default response and the time period are configurable.

Setting the Default Response

There are two ways to configure the default response to the command prompt:

- Specify the default on the command line in the .NCF file. Place the default response (a Y or N) immediately following the question mark. For example,

  ```
  ?N LOAD MONITOR
  ```

  In this example, the default response is N. If the user does not respond to the prompt, MONITOR is not loaded.

- Set the Command Line Prompt Default Choice parameter (Miscellaneous category) to either On or Off. On means the default response is Y for Yes; Off means the default response is N for No.

  The parameter setting is overridden by a default specified on the command line.

Setting the Time Period

To configure the time period before the default response is executed, set the Command Line Prompt Time Out (Miscellaneous category) parameter to a time in seconds. The default value is 10 seconds.

Changing Server Name and Internal Address in AUTOEXEC.NCF

The server's name is stored in the AUTOEXEC.NCF file. You can change the server name by editing the file. However, changing the server name in the AUTOEXEC.NCF file does not affect Novell eDirectory Server objects. You must use ConsoleOne™ to rename eDirectory Server objects.

IMPORTANT: Be sure to use ConsoleOne to update any references to the former server name in the eDirectory tree and in the TIMESYNC.CFG file.

The server's internal network number is also stored in the AUTOEXEC.NCF file. Even if you use Novell's Native IP protocol, the internal network number is used as a server ID and will still be stored in the AUTOEXEC.NCF file. Do not delete the number.

To change either the server name or the internal network number in the AUTOEXEC.NCF file, use NWCONFIG or EDIT at the server console, and then reboot the server.

To use NWCONFIG to change the settings, see "Using NWCONFIG to Create and Edit Startup Batch Files" on page 57. To use EDIT, see "Using EDIT to Create and Edit Text and Batch Files" on page 56.

Using Server Utilities and Console Commands

This section explains how to access help for server utilities and console commands, discusses types of NLM programs, and provides instructions for loading and unloading an NLM at the System Console.

Server utilities are NetWare Loadable Modules (NLM) programs. Some NLM programs are loaded whenever you start the server, some are loaded by other NLM programs when they are needed, and some must be loaded manually.

Server console commands are executed by entering the command at the System Console prompt.

When you enter a command at the System Console prompt, the command is stored in the command queue. To repeat a command, press the Up-arrow key until the desired command is displayed. You can make changes to the command or press Enter to execute the command. Up to 16 commands can be saved in the queue.

You can also use the RECORD and REPLAY commands to enter commands that you enter frequently at the System Console.

For more information, see the following topics:

- "How to Access Help for Utilities and Console Commands" on page 60
- "Accessing MONITOR" on page 83
- "Using NetWare Loadable Modules" on page 61
- "Loading and Unloading NetWare Loadable Modules" on page 62
- RECORD and REPLAY in *Utilities Reference*

How to Access Help for Utilities and Console Commands

- For a complete list of all utilities and console commands, with descriptions, syntax, and examples, see *Utilities Reference*.
- To display a list of console commands on the server console, enter the following at the System Console prompt:

  HELP
- To see online help for a specific console command, enter:

  HELP *command_name*
- To see a description for all valid console commands, enter:

  HELP ALL

- To display a list of all the console commands in NetWare Remote Manager, click the Console Commands link in the navigation frame. For help on a specific command, click the Info icon next to the command.
- To see online help for an NLM that displays a menu, such as MONITOR, load the NLM and then press F1. You can also press F1 at subsequent menus, lists, and information windows.

Using NetWare Loadable Modules

When loaded, an NLM program is dynamically linked to the operating system and the NetWare server allocates a portion of memory to it.

The amount of memory an NLM program uses depends on the task. Some tasks make calls that cause the operating system to allocate more memory. The NLM uses the memory to perform a task and then returns control of the memory to the operating system when the NLM is unloaded. When an NLM is unloaded, all allocated resources are returned to the operating system.

NetWare has five types of NLM programs:

- **NWPA drivers** (.CDM and .HAM extensions) control communication between the operating system and host adapters.
- **LAN drivers** (.LAN extension) control communication between the operating system and the network boards.

  You can load and unload LAN drivers while the server is running and while users are logged in.
- **PSM modules** (.PSM extension) provide support for multiple processors in server class computers.
- **Management utilities and server applications modules** (.NLM and .EXE extensions) let you monitor and change configuration options.

  For example, you can run REBUILD or VREPAIR on a dismounted volume or use MONITOR to view server statistics.

  After you finish your tasks, you can unload the utility and free memory for other server functions.
- **Name space support** (.NAM extension) lets non-DOS naming conventions be stored in the directory and file naming system.

Some NLM programs, such as utilities, can be loaded, used, and then unloaded. Other NLM programs, such as LAN driver and disk driver NLM programs, must be loaded every time the server is started.

NCF files (STARTUP.NCF and AUTOEXEC.NCF) allow you to store commands that load NLM programs every time the NetWare server is started.

Most NLM programs included with NetWare are copied to SYS:SYSTEM during installation. As you acquire additional NLM programs, decide where you want to copy them. The operating system must be able to find the NLM programs when a LOAD command is issued.

NLM programs can be copied to any of the following areas:

- SYS:SYSTEM directory
- Any network directory on the NetWare server
- A local drive of the NetWare server

For more information about using NLM programs, see LOAD, UNLOAD, and SEARCH in *Utilities Reference*.

Loading and Unloading NetWare Loadable Modules

To load a NetWare Loadable Module (NLM), enter the following at the System Console prompt:

[LOAD] [*path*]*NLM_name*

- If the NLM is stored in the SYS:SYSTEM directory or if you have a server search path to the directory where the NLM resides, enter just the NLM name (instead of the complete path). For information about server search paths, see SEARCH in *Utilities Reference*.
- If you want the NLM to be loaded whenever the server boots, add the command to AUTOEXEC.NCF.
- If you want the NLM to be displayed in a language other than English, see "Changing NLM Message Files" on page 31.

NOTE: In most cases you can load an NLM by entering just the name of the NLM at the System Console prompt. The exception is if there is an .NCF file of the same name as the NLM. In this case, you must use the LOAD command. Using the LOAD command directs the server to load the NLM instead of executing the file of the same name. For information about the LOAD command, see LOAD in *Utilities Reference*.

To unload an NLM program, enter the following at the System Console prompt:

UNLOAD *NLM_name*

To unload an NLM program from a protected address space, enter the following at the System Console prompt:

```
UNLOAD ADDRESS SPACE = space_name module_name
```

For more information about loading and unloading modules, see LOAD and UNLOAD in *Utilities Reference*. For more information about unloading modules from protected address spaces, see Unloading Protected Address Spaces in the *Server Memory Administration Guide*.

You can also load and unload NLM programs from the server using NetWare Remote Manager. For more information, see Managing NLM Programs in the *NetWare Remote Manager Administration Guide*.

Using Java on the Server

This section explains how to set environment variables for Java, load and unload JAVA.NLM, and run Java-based applets and applications.

Most of the information you need about JVM for NetWare can be located in the Novell JVM for NetWare documentation (http://www.novell.com/documentation/lg/jvm/jvm/data/hkfpc6qr.html).

See the following sections for information about using and managing Java-based components on the NetWare server:

- "Environment Variables for Java" on page 63
- "Managing NetWare Server GUI" on page 65

Environment Variables for Java

The Novell JVM for NetWare is automatically installed when you install NetWare. The installation process sets default values for key environment variables. Setting environment variables for Java is necessary to run Java-based applications and applets.

The installation process places some of the variables into the SYS:\ETC\JAVA.CFG file. The JAVA.CFG file is read whenever you load Java. You can modify or add to the JAVA.CFG file.

The following table describes some key environment variables. Other key environment variables for Java are available in the Novell JVM 1.3 for NetWare in Novell Developer Kit (NDK) documentation (http://developer.novell.com/ndk/doc/jvm13/jvm13enu/data/hkfpc6qr.html).

Environment Variable	Description
JAVA HOME	Specifies the location of the JVM. The default value is SYS:\JAVA.
CLASSPATH	Specifies the location of the default classpath.
XLOCALDIR	Specifies the location of files needed to support other languages, including keyboard and font files.

To view current variable values and to set values, follow these steps:

1. To load JAVA.NLM, enter the following at the System Console prompt:

   JAVA

2. To view current environment variables and variable values, enter the following at the System Console prompt:

   ENVSET

   When the JAVA.NLM is loaded at the server, you can also view all the environmental settings using NetWare Remote Manager. Click the Java Application Information link in the navigation frame, and then click the Global Environment Settings link.

3. To set a value for the current session, enter the following at the System Console prompt:

   ENVSET VARIABLE=*VALUE;VALUE*

   Make sure there are no spaces on either side of the equal sign or between values. To set multiple values for variables such as CLASSPATH, separate the values with semicolons.

   The value of a variable set with ENVSET lasts until Java is unloaded.

   To append a value to the CLASSPATH variable, use $CLASSPATH to represent the existing values.

   For example:

   ENVSET CLASSPATH=$CLASSPATH;SYS:MYCLASSES

4. To make lasting changes to variable values, enter the ENVSET command line in the SYS:\ETC\JAVA.CFG file.

The JAVA.CFG file is read whenever Java is loaded.

To edit the file, use the Editor in the NetWare GUI, use EDIT at the System Console prompt, or use a word processing program at a workstation.

Managing NetWare Server GUI

Managing the NetWare GUI includes the following tasks:

- Starting the NetWare GUI (page 65)
- Shutting Down the NetWare GUI (page 65)
- Accessing the Desktop Menu and Other Console Screens (page 66)
- Activating the Desktop Menu (page 66)
- Configuring the Desktop Menu (page 66)
- Setting Taskbar Properties (page 67)

Starting the NetWare GUI

The NetWare GUI (X Server--Graphical Console) is loaded by default when the server is started. If you have closed the GUI and want to start it again, enter the following at the System Console prompt:

STARTX

This loads Novell JVM for NetWare if it is not already loaded, and then loads the NetWare GUI into memory.

Shutting Down the NetWare GUI

The following are three ways to shut down NetWare GUI. The first two close the NetWare GUI without shutting down the JVM.

- Activate the desktop menu (see Activating the Desktop Menu), and then click Close GUI > Yes.
- Press Ctrl+Alt+Backspace.
- To shut down the JVM as well as NetWare GUI, toggle to the System Console screen (see Accessing the Desktop Menu and Other Console Screens) and enter

  ```
  java -exit
  ```

Accessing the Desktop Menu and Other Console Screens

To toggle to the next screen, press Alt+Esc.

To display the NetWare screen selection list, press Ctrl+Esc.

Activating the Desktop Menu

To activate the desktop menu in NetWare GUI, click the Novell button in the lower left-hand corner of the screen.

Configuring the Desktop Menu

Installing Programs

Do the following to install a program into the desktop menu:

1. Copy all the necessary program files to the server.
2. Copy your program's menu files to the desktop menu directory SYS:/JAVA/LIB/TASKBAR.

   If this directory does not exist, you need to create it. For an example of the file format for a menu file, see SYS:/JAVA/LIB/TASKBAR.EXAMPLE.

   If your menu file uses a resource bundle for internationalization of the menu strings, copy the resource bundle to the desktop menu directory SYS:/JAVA/LIB/TASKBAR.

After you install your program, the next time you click the Novell button in the NetWare GUI, your menu items will appear. You can then start your program by selecting the appropriate menu item.

Modifying the Menu

You construct the desktop menu by merging any installed menu files and the custom menu file with the default desktop menu. You can modify the desktop menu by editing the custom menu file or any of the installed menu files.

To add items to the desktop menu, create a customized.MENU file and copy it to the SYS:\JAVA\LIB\TASKBAR directory. For an example menu file, see SYS:\JAVA\LIB\TASKBAR.EXAMPLE.

Removing Installed Menu Items from the Desktop Menu

You can remove either an entire menu file and all the contents, or you can remove only a single menu item.

To remove a whole menu file, either delete the file or rename it by changing the extension to something other than .MENU.

To remove a single menu item from the desktop menu, locate the item and delete it from the menu file.

Setting Taskbar Properties

Currently, the default taskbar property is the stay-on-top property. If you do not want the taskbar to stay on top, you can change this property by creating a NAWT.PROPERTIES configuration file and adding the following line to it:

```
taskbar.stayontop=false
```

For an example of a properties configuration file, see the SYS:\JAVA\LIB\NAWT.PROPERTIES.SAMPLE file.

Securing the Server Console

The first principle of securing your server console is physical security. If you don't provide physical security, nothing else you do matters very much.

The processing unit should be locked in a place where no one can remove it or reboot it. Some network administrators remove both the keyboard and the monitor and manage the server remotely by using NetWare Remote Manager or RCONSOLEJ. We suggest that you also consider using a power-on password whether you manage at the console or use RCONSOLEJ at a workstation.

Two features that provide additional security at the console are the following:

- The SECURE CONSOLE command. For more information:
  - "Why Should I Use SECURE CONSOLE?" on page 68
  - "Using the SECURE CONSOLE Command" on page 68
- The screen saver console-lock feature. For more information:
  - "Using SCRSAVER to Lock the Server Console" on page 69
  - "Unlocking the Server Console" on page 70

Why Should I Use SECURE CONSOLE?

After you have provided physical security for your server, you can use the SECURE CONSOLE command to provide the following security features, while still allowing you to use the console:

- Prevents NetWare Loadable Module programs from being loaded from any directory other than SYS:SYSTEM or C:\NWSERVER. This means that no one can load an invasive NLM from a server's diskette drive or boot partition unless it is already in a search path.
- Prevents keyboard entry into the operating system debugger. This restricts the ability to alter the operating system.
- Prevents anyone from changing the date and time. Some security and accounting features depend on date and time for their enforcement.
- When you issue the SECURE CONSOLE command, the server must be taken down and rebooted to unsecure the console. Now that server parameter settings are persistent in NetWare 6, you can shut down the server without losing the settings you made to optimize and tune your server.
- When you use SECURE CONSOLE with the NetWare Remote Manager or RCONSOLEJ, access is subject to the protections provided by SECURE CONSOLE.
- SECURE CONSOLE does not lock the server console. You can lock the console by using SCRSAVER. If the console is locked using the console-locking feature, an intruder can still access the console from a remote workstation; however, the intruder must still be authenticated to eDirectory through the SCRSAVER console lock.

  HINT: To protect the server console by encrypting the RCONSOLEJ password in the AUTOEXEC.NCF file, see Loading RConsoleJ Agent at Startup in the *Utilities Reference*.

Using the SECURE CONSOLE Command

To secure the server console, enter the following command at the System Console prompt:

```
SECURE CONSOLE
```

To secure the server console whenever the server is booted, add the SECURE CONSOLE command to the server's AUTOEXEC.NCF file. If the AUTOEXEC.NCF file loads modules from any directory other than

SYS:SYSTEM or C:\NWSERVER, then in the .NCF file the SECURE CONSOLE command must follow the LOAD commands for these modules.

IMPORTANT: To disable SECURE CONSOLE, you must first shut down the NetWare server and reboot it. If the SECURE CONSOLE command is in the AUTOEXEC.NCF file, use EDIT or any text editor to remove it before you shut down the server and reboot it.

For more information on using SECURE CONSOLE, see SECURE CONSOLE in *Utilities Reference*.

Using SCRSAVER to Lock the Server Console

The console-locking feature in the SCRSAVER.NLM allows you to require a password before gaining access to the server console prompt. If a key is pressed when the console lock is enabled, a dialog box appears. You must then supply an eDirectory username and password. In addition, the User object must have the Write right to the access control list (ACL) of the Server object to gain access to the server console prompt.

When the screen saver is activated, it displays a moving snake for each processor on the server. Each snake is a different color: the first one is red, the second is blue, etc. The speed of each snake and the length of its tail are directly proportional to the processor's utilization.

If the console is unlocked, press any key to activate the console. The snake screen will disappear.

1. To display command options for SCRSAVER, enter the following at the System Console prompt:

   SCRSAVER HELP

   Command options allow you to enable and disable locking, check the status of the lock options, and change the length of time the console is allowed to be inactive before the screen saver is activated. The default is 600 seconds (10 minutes).

2. For more information about a command option, enter the following at the System Console prompt:

   SCRSAVER HELP *command_option*

3. To load the SCRSAVER module, enter the following at the System Console prompt:

   SCRSAVER [option; option...]

When you load the screen saver, the default is to enable the console-locking feature and to require a password for access. The corresponding eDirectory user must have the Write right to the Access Control List (ACL) of the Server object.

For more information, see SCRSAVER in *Utilities Reference*.

Unlocking the Server Console

To unlock the server console after locking it using SCRSAVER.NLM, complete the following:

1. While the screen-saver snake is displayed, press any key on the server console keyboard.
2. At the Login dialog box, press Enter to select the Username field.

   The login box appears only if the console is locked.
3. Enter the username.

   The User object must have the Write right to the ACL for the Server object.

   If the username field is blank or if you want to change the username, enter an eDirectory username and context. Again the User object must have the required rights.
4. Press Enter again to select the password field.
5. Type the password for the username and press Enter twice.

   The screen saver snake disappears and the server console screen appears.

Using NCP Packet Signature

NetWare includes a feature called NCP Packet Signature that protects servers and clients using the NetWare Core Protocol™ (NCP™) services.

NCP Packet Signature prevents packet forgery by requiring the server and the client to sign each NCP packet. The packet signature changes with every packet.

Without NCP Packet Signature installed, a user could pose as a more privileged user and send a forged NCP request to a NetWare server. By forging the proper NCP request packet, an intruder could gain the Supervisor right to the Server object and access to all network resources.

NCP packets with incorrect signatures are discarded without breaking the client's connection with the server. However, an alert message about the invalid packet is sent to the error log, the affected client, and the server console. The alert message contains the login name and the station address of the affected client.

If NCP Packet Signature is installed on the server and all of its workstations, it is virtually impossible to forge a valid NCP packet.

For additional information about packet signature, see the following:

- "Why Should I Use Packet Signatures?" on page 71
- "NCP Packet Signature Options" on page 72
- "Effective Packet Signature" on page 72
- "Recommended Signature Levels" on page 73

To implement packet signature, see "Implementing NCP Packet Signature" on page 73.

Why Should I Use Packet Signatures?

We recommend using NCP Packet Signatures for security risks such as the following:

- You have an untrustworthy user at a workstation on the network
- Easy physical access to your network cabling system exists
- You have an unattended, publicly accessible workstation on the network

NCP Packet Signature is not necessary for every server installation. You might choose not to use NCP Packet Signature if you can tolerate security risks in situations such as the following:

- Only executable programs reside on the server
- You know and trust all network users
- Data on the NetWare server is not sensitive and loss or corruption of this data would not affect operations

NCP Packet Signature Options

Because the packet signature process consumes CPU resources and slows performance both for the client and the NetWare server, NCP Packet Signature is optional.

Several signature options are available, ranging from never signing NCP packets to always signing NCP packets. NetWare servers and Novell clients each have four settable signature levels.

The signature options for servers and clients combine to determine the level of NCP Packet Signature on the network.

You can choose the packet signature level that best meets both your system performance needs and network security requirements.

NOTE: Some combinations of server and client packet signature levels can slow performance. However, low-CPU-demand systems might not show any performance degradation.

Effective Packet Signature

The NCP Packet Signature levels for the server and the client interact to create the effective packet signature for the network. Some combinations of server and client levels do not allow logging in.

The following figure shows the interactive relationship between the server packet signature levels and the client signature levels.

If	Server = 0	Server = 1	Server = 2	Server = 3
Client = 0	○	○	○	⊘
Client = 1	○	○	●	●
Client = 2	○	●	●	●
Client = 3	⊘	●	●	●

● Packet signature
○ No packet signature
⊘ No logging in

Recommended Signature Levels

The default NCP Packet Signature level is 1 for clients and 1 for servers. In general, this setting provides the most flexibility while still offering protection from forged packets. Following are some examples of situations requiring different signature levels.

Situation	Example	Recommendation
All information on the server is sensitive.	If an intruder gains access to *any* information on the NetWare server, it could damage the company.	Set the server to level 3 and all clients to level 3 for maximum protection.
Sensitive and nonsensitive information reside on the same server.	The NetWare server has a directory for executable programs and a separate directory for corporate finances (such as Accounts Receivable).	Set the server to level 2 and the clients that need access to Accounts Receivable to level 3. All other clients remain at the default, level 1.
Users often change locations and workstations.	You are uncertain which employees will be using which workstations and the NetWare server contains some sensitive data.	Set the server to level 3. Clients remain at the default, level 1.
A workstation is publicly accessible.	An unattended workstation is set up for public access to nonsensitive information, but another server on the network contains sensitive information.	Set the sensitive server to level 3 and the unattended client to level 0.

For information on implementing NCP Packet Signature, see "Implementing NCP Packet Signature" on page 73.

Implementing NCP Packet Signature

To implement NCP Packet Signature, complete the following procedures:

- "Setting Server Signature Levels" on page 74
- "Setting Client Signature Levels" on page 75
- "Changing the Signature Level for an NLM" on page 76
- "Setting Packet Signature for Job Servers" on page 76

- To determine the server's current signature level, enter the following command at the System Console prompt or view the setting using NetWare Remote Manager:

  SET NCP Packet Signature Option

- To set a server's packet signature level, enter the following command at the System Console prompt or change the setting using NetWare Remote Manager:

  SET NCP Packet Signature Option = *number*

  Replace *number* with 0, 1, 2, or 3. The default is 1.

  For example:

  SET NCP Packet Signature Option = 2

Number	Explanation
0	Server does not sign packets (regardless of the client level).
1	Server signs packets *only* 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.

To ensure that the signature level is set each time the server is brought up, you can add this SET parameter command to your STARTUP.NCF file

You can also use the SET parameter command to change the signature level from a lower to a higher level or use NetWare Remote Manager.

You cannot change from a higher to a lower level unless you first reboot the server. For example, if the current signature level is 2, you can't set the signature level to 1 by using the SET command at the console. To change the signature level from 2 to 1, you must add the SET command to the STARTUP.NCF file and then restart the server:

Setting Client Signature Levels

Set client signature levels to 0, 1, 2, or 3. The default is 1. Increasing the value increases security, but decreases performance.

Number	Explanation
0	Disabled. Client does not sign packets.
1	Enabled, but not preferred. Client signs packets *only* if the server requests it (server level is 2 or higher).
2	Preferred. Client signs packets if the server is capable of signing (server level is 1 or higher).
3	Required. Client signs packets and requires the server to sign packets or logging in will fail.

To set DOS or MS Windows client signature levels, add the following parameter to the workstation's NET.CFG file:

```
signature level = number
```

To set the Windows 95 or Windows NT client signature level for an individual workstation, change the parameter setting with the Advanced Settings tab of Novell NetWare Client Properties, as follows:

1. From the system tray, right-click N.
2. Click Novell Client Properties > Advanced Settings.
3. Select Signature Level from the scrollable list.

You can set the signature level for multiple clients at once by adding the signature level to the configuration file when you install the clients. For information about configuring Windows clients, see the Novell Client online documentation (http://www.novell.com/documentation/).

Changing the Signature Level for an NLM

NLM programs that use the Novell Runtime Libraries are assigned a default NCP Packet Signature level that corresponds to the current signature level of the server.

To change the packet signature level for a single NLM, use the following command syntax when you load the NLM:

[LOAD] *NLM* [CLIB_OPT]/L *number*

Replace *number* with 0, 1, 2, or 3.

Setting Packet Signature for Job Servers

A job server is a server that performs a task and then returns the completed task. Most job servers are third-party products.

You should be aware that some job servers do not support NCP Packet Signature. A job server might produce unsigned sessions if one of the following occurs:

- It does not operate on top of DOS
- It does not use standard Novell clients
- It is not an NLM
- It uses its own implementation of the NCP engine (such as embedded print servers in printers)

Minimizing Risks

To minimize security risks associated with job servers, do the following:

- Install queues only on servers with signature level 3.
- Do not allow privileged users to put jobs in queues on servers with signature levels below 3.
- Make sure the job server's account is unprivileged.
- Disable the job server's ability to change to client rights.

Disabling Change to Client Rights

To prevent a job server from assuming the rights of a client, add the following SET command to the server's STARTUP.NCF file:

```
SET Allow Change to Client Rights = OFF
```

The default is On, because certain job servers and third-party applications cannot function without changing to client rights. To determine whether the job server can function without client rights, refer to the documentation that comes with the job server.

Using the Transaction Tracking System

NetWare includes a transaction-monitoring feature called the Transaction Tracking System™ (TTS™). If you flag a file as transactional, TTS can prevent corruption of records in the file by backing out of incomplete transactions and keeping a record of backed-out data.

NOTE: A file flagged as transactional cannot be deleted or renamed.

TTS can also back out file truncations or extensions and multiple changes to the same data area during a single transaction. TTS can even back out interrupted backouts if the NetWare server fails in the middle of backing out transactions.

But TTS cannot protect against these types of failures for any type of application that issues record-locking calls and stores information in records, including traditional databases, some electronic mail applications, and some workgroup appointment schedulers.

Files that aren't organized into discrete records (such as word processing files) aren't protected by TTS.

Transactions on a network can be saved improperly in any of the following situations:

- Power to a server or a workstation is interrupted during a transaction
- Server or workstation hardware fails during a transaction (for example, a parity error on a network board)
- A server or workstation hangs (a software failure) during a transaction
- A network transmission component (such as a hub, a repeater, or a cable) fails during a transaction

If the server fails and the file has been flagged transactional, TTS backs out the transaction when the server comes up again. If a workstation or network transmission component fails, TTS backs out the transaction immediately.

How TTS Works

The Transaction Tracking System (TTS) can prevent data corruption by backing out of incomplete transactions and keeping a record of backed-out data.

TTS guarantees that all changes to a database file are either wholly completed or not made at all. TTS follows these steps to track transactions:

1. When the application allocates a physical or logical record lock, TTS infers that the application is making a transaction. At this point, if you have flagged the file as transactional, TTS begins tracking the transaction so that the transaction can be backed out if a failure occurs.
2. TTS makes a copy of the original data so the data can be restored if the transaction fails. A copy of the data is placed in a file external to the database. This external file contains all transaction backout information; only the operating system uses it.
3. After the copy of the original data has been written to the backout file, TTS writes the changed data to the database file.
4. TTS repeats Steps 2 and 3 for additional changes (a single transaction can consist of a sequence of changes).
5. When all changed data has been written to disk, and the database application releases physical and logical record locks, TTS infers that the application has completed the transaction. TTS writes a record to the backout file, indicating that the transaction is complete, and stops tracking the transaction.

To learn how to enable and activate TTS, see "Enabling and Activating TTS" on page 78.

Enabling and Activating TTS

In NetWare 6, TTS has three possible states:

- Disabled
- Enabled but inactive
- Active

The disabled and inactive states are similar in that TTS operations have no effect. Only in the active state, do TTS operations have an effect.

Only one file system can have an active TTS. Therefore, if your server is using both the Novell Storage Service (NSS) file sytem and the Traditional File System, note the following:

- TTS might be enabled on both file systems but it will only be active for one of them.
- By default, the Traditional File System has TTS always enabled.
- NSS determines if the Traditional File System has TTS enabled and if this is the case, it automatically makes TTS inactive on the NSS file system. Therefore, if any traditional volumes are on your server, TTS on the NSS file system is automatically disabled or inactive.
- If TTS is disabled on the Traditional File System by using the DISABLE TTS console command, then TTS automatically becomes active on the NSS file system if it is enabled.

  Because the DISABLE TTS command is not persistent, the only way to persistently allow TTS to be active when it is enabled on NSS volumes is to put the DISABLE TTS console command in the AUTOEXEC.NCF file.
- By definition, if you have traditional and NSS volumes on the same server, then it is impossible for TTS to be available on all volumes.
- If you only have traditional volumes on your server, then TTS is available on all volumes.
- If you only have NSS volumes on your server, you can enable TTS on all volumes, but it will not, by default, be enabled on all volumes. To do so would result in a 4 MB tax on every volume.
- You can enabled TTS manually for any volume by entering the following command at the System Console prompt:

  `NSS /Transaction=VolName`

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

- Volume SYS: becomes full

  Volume SYS: is the TTS backout volume.
- The NetWare server has insufficient memory to operate TTS

If TTS has been disabled and you have solved the problems that led to its disabling, enter one of the following at the System Console prompt to enable it again:

- On a server with traditional volumes: **ENABLE TTS**
- On NSS volume: **NSS /Transaction=VolName**

To enable and manage transaction tracking for individual files on traditional volumes, use the commands and parameters in the following table.

To	Do the following
Enable transaction tracking for a file.	Use NetWare Remote Manager to flag the file as transactional. For more information, see Viewing Individual Files in *NetWare Remote Manager Administration Guide*. (Note that files flagged as transactional cannot be deleted or renamed.)
Enable TTS to backout transactions without displaying confirmation prompts.	Place the following command into the STARTUP.NCF file and restart the server: SET AUTO TTS BACKOUT FLAG = ON If this parameter is set to On (default), the backouts happen automatically. If this parameter is set to Off, you will be prompted to confirm file backouts. You can also set the parameter with NetWare Remote Manager > Set Parameters > Traditional File System.
Log backed out data to the SYS:TTS$LOG.ERR file.	Execute the following command at the System Console prompt: SET TTS ABORT DUMP FLAG = ON If this parameter is set to On, the transactions are stored in SYS:TTS$LOG.ERR. If this parameter is set to Off, the transactions are backed out, but the server does not provide you with a record of the backouts. You can also set the parameter with NetWare Remote Manager > Set Parameters > Traditional File System.

Using an Uninterruptible Power Supply (UPS)

An uninterruptible power supply (UPS) is a backup power unit that supplies uninterrupted power if a commercial power outage occurs. A UPS is an indispensable part of your network. Not only does it help prevent damage to your computers from power surges and brownouts, but it also prevents data loss during power outages.

Both online and offline UPS systems are available:

- **Online UPS** actively modifies the power as it moves through the unit. If a power outage occurs, the unit is already active and continues to provide power.

  An online UPS is usually more expensive than an offline UPS, but provides a nearly constant source of energy during power outages.

- **Offline UPS** monitors the power line. When power drops, the UPS is activated.

  The drawback to this method is the slight lag before the offline UPS becomes active. However, most offline UPS systems are fast enough to offset this lag.

Because UPS systems can be expensive, most companies attach them only to the most critical devices, such as NetWare servers, routers, and hard disk subsystems.

Attaching a UPS to a server enables the server to properly close files and rewrite the system directory to disk.

Unfortunately, most programs run on the workstation and data stored in RAM is not saved during a power outage unless each station has its own UPS.

If the UPS doesn't have its own form of surge protection, install a surge protector to protect the UPS.

Preventing Virus Infection

Keep viruses off the network by educating users about virus dangers and by enforcing procedures that reduce virus risks, such as the following:

- Back up data frequently.
- Maintain layers of archived backups so you can retrieve a backup from a preinfected file.
- Keep a write-protected, bootable diskette with the latest virus scan and removal software for all servers and workstations.
- Keep a backup of executable files and flag them Execute Only.
- Educate yourself about the infection techniques of the latest viruses.
- Educate network users about how to detect viruses.
- Warn users of the dangers of viruses. Discourage them from using diskettes and files that have been in computers away from work.
- Teach users to power down their workstations immediately upon encountering a virus.
- Restrict access to a server's diskette drives by locking the server in a secure room. Put tape over the drive openings to remind you not to use them unnecessarily.
- Avoid using the Admin account when possible. The fewer privileges your login account has, the less power a virus has to destroy data and to spread.

Monitoring the NetWare Server

Monitoring the server allows you to do the following:

- Isolate performance bottlenecks
- Optimize server performance
- Troubleshoot and resolve server problems

NetWare Remote Manager is a tool for debugging and monitoring the server from a Web browser at your workstation. You can also access a Java version of this tool from the server GUI. For more information, see Accessing NetWare Remote Manager, Managing Servers Remotely, and Troubleshooting Server Problems in the *NetWare Remote Manager Administration Guide*.

MONITOR is the key tool for performance monitoring at the server level from the server console. It runs in the NetWare kernel so that it can make calls directly to the operating system. Most statistics are updated every second.

Accessing MONITOR

- To load MONITOR at the System Console prompt, enter

  [LOAD] [path] MONITOR

  The LOAD command is necessary *only* if you have a batch file with the same name as the NLM. (Using the LOAD command indicates that MONITOR is a loadable module.)

  The path is specified only if you moved the utility from its default directory SYS:SYSTEM to a directory that does not have a search path.

- If MONITOR is running but is not the active screen at the console, there are two ways to toggle to the MONITOR screen:

  Press Alt+Esc. To cycle through other console screens, continue to hold Alt down and tap Esc until the current MONITOR screen reappears. Use the bar at the top of the screen for navigation.

  Press Ctrl+Esc. To see a numbered list of available console screens and then enter the number for the NetWare Console Monitor.

- To exit MONITOR, use either of the following procedures:

  Repeatedly press Esc until the Exit confirmation box appears. Then press Enter to return to the System Console prompt.

  To bring up the Exit confirmation box immediately, press Alt+F10. Then press Enter to return to the System Console prompt.

What to Monitor and Why

A monitoring utility can be overwhelming in the volume of information and statistics it provides. To simplify your access to key parameters, MONITOR's General Information includes most of them on one screen, including performance indicators that pertain to memory utilization and disk I/O.

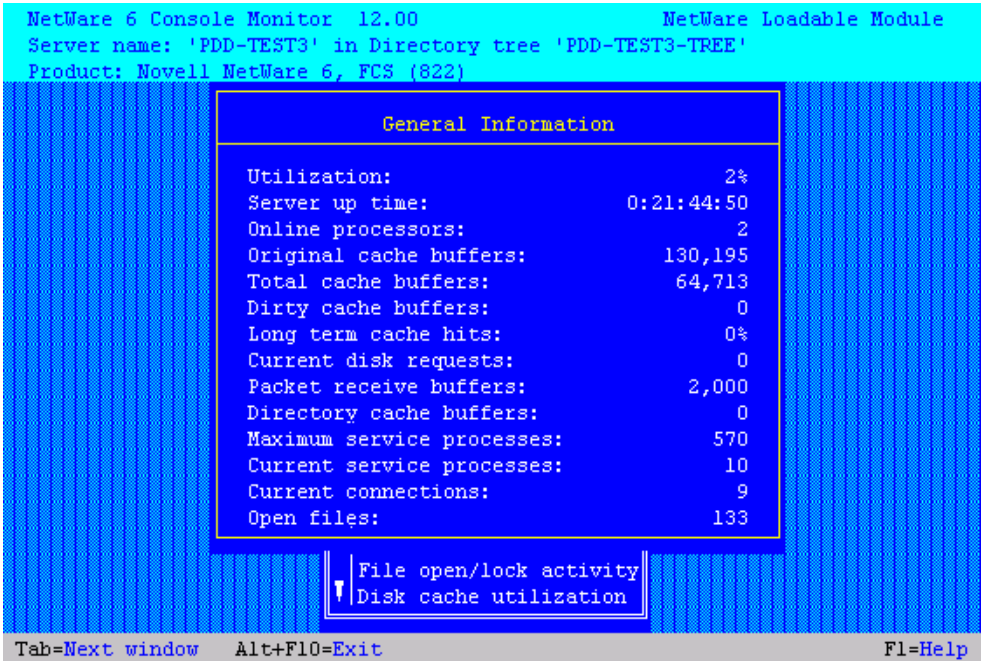
For an explanation of the interaction of three types of configurable parameters that control dynamically allocated services, see "Monitoring Allocated Services" on page 86. The guidelines allow you to be proactive in maintaining the level of service your users require.

The “Other Information and Statistics to Monitor” on page 87 section includes error logs, available free disk space, and user accounts. To be prepared for power supply interruptions, test your UPS (uninterruptable power system) periodically.

Becoming familiar with your server’s day-to-day performance and its characteristic response to its unique load will help you to better interpret the information and statistics that the monitoring utilities provide.

MONITOR’s General Information

Most of the important performance indicators that can be used to track, diagnose, and resolve server problems appear in the General Information screen in MONITOR. This window is displayed when you load MONITOR.



The following information describes the onscreen performance indicators.

- **Utilization.** Average of the server’s total processing capacity that was used during the last second, expressed as a percentage. The remainder of the time is spent in an idle loop. Monitor the patterns of utilization.

  Does utilization go to 100 percent? Does it reach a plateau or does it peak for a few seconds and then drop? What time and how frequently does it peak?

- **Server Up Time.** Amount of time that has elapsed since the server was most recently started. If your server has Auto Restart enabled, use this field to determine whether your server has abended and restarted. You can also use this information to detect power failures or intruders who bring down the server.
- **Online Processors.** Number of enabled and online processors. The Platform Support Module (PSM), loaded from STARTUP.NCF, enables NetWare to use secondary processors in a multiprocessing platform. The default is to autostart all processors.
- **Total Cache Buffers.** How many cache buffers are currently available for file caching. This number decreases as you load NLM programs.

  Because file caching has a dramatic impact on server performance, you want this number to be as high as possible.
- **Dirty Cache Buffers.** How many buffers contain data which has been changed but not yet written to disk.

  Monitor this number to see whether it is increasing. If it is, you might have a bottleneck in the Traditional file system.
- **Long Term Cache Hits.** The cumulative percentage of requests for disk blocks that were already in cache for the traditional file system. (When the requested data is already in memory, disk reads don't need to be made.)

  Use this percentage to assess overall disk cache utilization if you are using the traditional file system. If this value falls below 90%, the disk thrashes and server performance degrades. The solution is to install more physical memory (RAM).
- **Current Disk Requests.** How many read requests are pending.

  Monitor this number to see whether it is increasing. If it is, a slow hard disk might be your bottleneck.
- **Packet Receive Buffers.** How much memory is allocated for holding client requests while the server processes them. The server allocates more packet receive buffers as needed (within minimum and maximum values). Buffer size depends on the network adapter.

  This number is the result of the interaction of three configurable parameters. Monitor the current value to ensure that it does not reach the maximum value.

- **Maximum Service Processes.** How many task handlers the server can allocate to service client requests. As the number of client requests increases, the server creates more service processes. When no more service processes can be allocated, server performance is adversely affected.

  Monitor the current number of service processes to ensure that it does not reach this value.

- **Current Service Processes.** How many task handlers are currently being used to service client requests.

  Use this number to determine whether the server has enough free task handlers to service client requests. If the number of current service processes reaches the maximum, the value of the Maximum Service Processes (Communications category) parameter must be increased.

- **Current Connections.** Number of active connections, whether licensed or unlicensed, authenticated or Not-Logged-In.

- **Open Files.** Number of files currently being accessed by the server and by other clients. Certain files are always open, such as the hidden files that support eDirectory.

Monitoring Allocated Services

There are limits to resources in every computing environment. NetWare allocates resources according to need and availability. When a request is received, the operating system doesn't immediately allocate new resources. It waits a specified amount of time to see if existing resources become available to service the demand.

Dynamically allocated services are controlled by the interaction of three types of settable parameters. If you understand how they work together, you can interpret the statistics that you monitor and know how to configure the system's response to demand.

- **Maximum limits** control the amount of server resources the operating system can allocate for a particular service.

- **Minimum limits** allow the operating system to allocate a minimum amount 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.

- **Wait time limits** control how rapidly the operating system can allocate a new resource.

  If resources become available, no new resources are allocated. If they don't become available within the time limit, new resources are allocated. The time limit ensures that sudden, infrequent peaks of server activity don't permanently allocate unneeded resources.

Consider, for example, the allocation of directory cache buffers. If the minimum number of directory cache buffers is set to 20, the system allocates another buffer resource as soon as a request is made—until 20 cache buffers have been allocated.

When 20 directory cache buffers are allocated, the 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 system allocates 40 directory cache buffers before it starts slowing the growth by waiting 2.2 seconds after each request.

Other Information and Statistics to Monitor

Common maintenance tasks also include the following:

- Checking Server Error Logs (page 97)
- Checking Disk Drives (page 97)
- Reviewing Server Cache Statistics (page 97)
- Checking Free Space on Server Disks and Volumes (page 98)
- Reviewing User Accounts (page 98)
- Testing the Uninterruptible Power Supply (page 98)

Displaying Server Alerts

You can enable the server to display alert messages under various conditions, such as when NLM programs fail to relinquish control of a processor. Many alerts are controlled by server parameters that set a threshold when the alert will be generated. By default, whenever an alert is received, a bell also sounds.

To turn the bell sound off, set the following server parameter in the Miscellaneous category:

```
Sound Bell for Alerts = OFF
```

Available alert parameters are described in the following table.

Condition That Generates Alert	Relevant Parameters
Spurious interrupts are detected	Display Spurious Interrupt Alerts Spurious Interrupt Alert Threshold (See SET > Miscellaneous Parameters in *Utilities Reference*.)
Lost interrupts are detected	Display Lost Interrupt Alerts Lost Interrupt Alert Threshold (See SET > Miscellaneous Parameters in *Utilities Reference*.)
NLM programs fail to relinquish control of processor	Display Relinquish Control Alerts CPU Hog Timeout Amount (See SET > Miscellaneous Parameters in *Utilities Reference*.)
Incomplete IPX™ packets are received	Display Incomplete IPX Packet Alerts (See SET, Display Incomplete IPX Packet Alerts = value in *Utilities Reference*.)
Available file cache buffers are nearing minimum	Minimum File Cache Report Threshold (See SET > File Caching Parameters for the Traditional File System in *Utilities Reference*.)
A volume is becoming full	Volume Low Warn All Users Volume Low Warning Threshold Volume Low Warning Reset Threshold (See SET > File Parameters for the Traditional File System in *Utilities Reference*.)

Many other alerts can be generated by the system, but are not controlled by server parameters. For example, if the address of a server on the network is changed, an alert will be broadcast on other server consoles. You can control these alerts with the ALERT command. See ALERT in *Utilities Reference*.

Managing Workstation Connections

This section explains how to use utilities and commands for disabling logins, clearing connections, controlling resource allocation, sending messages, and working with watchdog packets. See the following:

- "Performing Connection Management Tasks" on page 89
- "Monitoring Workstation Connections to the Server" on page 89
- "Sending Console Messages to Workstations" on page 91
- "Clearing a Workstation Connection" on page 92
- "Disabling and Enabling Logins" on page 93
- "Controlling Resource Allocation with Locks" on page 94

Performing Connection Management Tasks

The tasks for which you can use NetWare Remote Manager or MONITOR include the following:

- Viewing a list of active workstation connections on the server
- Determining which users are logged in
- Viewing information about a connection
- Configuring a watchdog to monitor connections for activity
- Viewing a list of files that the connection has open
- Terminating one or more workstation connections

  You can also use **CLEAR STATION *n*** or **CLEAR STATION ALL** at the System Console prompt. For more information about these commands, see CLEAR STATION in *Utilities Reference*.
- Sending a message to one or more workstations

Monitoring Workstation Connections to the Server

The most effective tool for monitoring workstation connections to the server is NetWare Remote Manager. For information about monitoring workstation connections to the server using NetWare Remote Manager, see Monitoring Connections to the Server in the *NetWare Remote Manager Administration Guide*.

To monitor connections to the server from utilities at the server console, see the procedures in the following table.

To	Do the following
View a list of active server connections. Determine which users are logged in.	1. In MONITOR, from the Available Options menu, select Connections. The list of Active Connections appears. 2. (Optional) Press F3 to re-sort the connection list. List items without an asterisk (*) represent logged-in users. List items with an asterisk (*) are unlicensed connections (this means they do not count against a server's total licenses). These connections are authenticated to eDirectory but are not logged in.
View information about a connection: ◆ Connection number ◆ Connection name ◆ Elapsed connection time ◆ Network node address ◆ Read/write requests ◆ Authentication and license status ◆ Files in use ◆ Locks and semaphores in use ◆ Supervisory rights	1. In MONITOR, from the Available Options menu, select Connections to display the list of Active Connections. 2. Select a connection from the list. 3. Press Tab to activate the Connection Information screen in the upper window. 4. For an explanation of the information fields and statistics, press F1.
View a list of files that the connection has open. Use this procedure when you want to determine whether a crashed workstation has open files remaining on the server.	1. In MONITOR, from the Available Options menu, select Connections. 2. Select the connection from the list. 3. After determining whether files are open on the server, press Esc to return to the Active Connections list.

To	Do the following
Terminate one or more connections. Use this procedure to clear the connection when a workstation has crashed and left open files on the server. Note: Transaction monitoring (TTS) provides automatic backout for database records or files stored on the server if a workstation has crashed and left those files open on the server. Also a file is protected if the Transaction (T) file attribute is set for it.	See "Clearing a Workstation Connection" on page 92.
Send a message to one or more workstations. Use this procedure when you need to warn users to log out before you down the server.	See "Sending Console Messages to Workstations" on page 91.

Sending Console Messages to Workstations

To send a message from the server console to all workstations or to a single user using NetWare Remote Manager, see Sending Messages to Users in the *NetWare Remote Manager Administration Guide*.

To send a message from the server console to all workstations or to a single user using MONITOR, complete the following:

1. From the Available Options menu, select Connections.
2. Press F8 to display more options on the task bar.
3. On the list of Active Connections, select the connection for the user you want to send a message to. (Use F5 to mark additional recipients.)

   In the Active Connections list, items *without* an asterisk (*) represent logged-in users.
4. To display the message composition box, press F4.
5. Type your message in the message box and press Enter to send it.

   A confirmation box appears.
6. You can either choose to send the message immediately or you can press Esc to discard it.

For more information, see MONITOR in *Utilities Reference*. For information about receiving and clearing messages at the workstation, see the documentation for your NetWare client.

Clearing a Workstation Connection

To clear a client connection when the workstation has crashed and left open files on the server, use one of following procedures:

- Clearing Specific Connections in the *NetWare Remote Manager Administration Guide*
- "Using MONITOR to Clear a Connection" on page 92
- "Using CLEAR STATION to Clear a Connection" on page 92.

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

Using MONITOR to Clear a Connection

1. In MONITOR, from the Available Options menu, select Connections.

   A list of active connections appears.

2. (Optional) To view a workstation's open files, select the workstation's connection.

   After viewing files, press Esc to return to the Active Connections list.

3. Clear one or more connections.

   - To clear one connection, select the connection and press Delete. At the Clear Connection? prompt, select Yes.
   - To delete multiple connections, select each connection and press F5 to mark it. Then press Delete. At the Clear Connection? prompt, select Yes.
   - To clear all unused (not logged in) connections, press F6.

   Deleted connections are no longer listed on the Active Connections list.

For more information, see MONITOR in *Utilities Reference*.

Using CLEAR STATION to Clear a Connection

If you know the connection number, you can terminate a specific connection by entering the following at the System Console prompt:

```
CLEAR STATION n
```

Replace *n* with the connection number of the workstation.

To clear all connections, enter the following at the System Console prompt:

```
CLEAR STATION ALL
```

IMPORTANT: The CLEAR STATION ALL command clears all not-logged-in connections including connections by NLM programs. You should be carefull in clearing NLM-based connections because some backup NLM programs establish a connection during the server initialization process and maintain a not-logged-in connection to the server until it is time to log in and run the process. These type of NLM-based connections will not be able to re-establish a connection to the server unless the NLM is unloaded and reloaded at the server.

For more information, see CLEAR STATION in *Utilities Reference*.

Disabling and Enabling Logins

If you need to make repairs to the server, you can prevent users from logging in by entering the following command at the System Console prompt:

```
DISABLE LOGIN
```

This does not affect users who are already logged in to the network. However, a user who logs out cannot log in again until you execute ENABLE LOGIN.

To allow users to log in again, enter the following at the System Console prompt:

```
ENABLE LOGIN
```

You can also use ENABLE LOGIN to enable a SUPERVISOR account when it has been locked by the intruder detection function.

For more information, see DISABLE LOGIN and ENABLE LOGIN in *Utilities Reference*.

Clearing a Connection That Uses Auto Reconnect

Novell Client™ has automatic reconnection capabilities that make a complete restoration of the user environment after a network failure possible. Because auto-reconnect is enabled by default, you need to prevent workstations from reconnecting while you are trying to perform some function on the server.

Novell Client also supports file caching on the client side, which allows files to be cached as they are read from and written to the server. With the default settings for the Auto Reconnect Level and the File Cache Level parameters, Novell Client will restore all files to their actual state before the workstation connection was cleared (or the server went down).

The workstation monitor displays a message:

```
Client32: Please wait while Application retries
request to servername. To stop waiting, press Enter.
NetWare will then return an error and try to
reconnect in the background.
```

You can use a combination of the console commands to prevent clients from reconnecting long enough to complete your work on the server.

1. To warn users, see "Sending Console Messages to Workstations" on page 91.
2. To prevent auto-reconnect users from reattaching to the server while you are working on it, enter **DISABLE LOGIN** at the System Console prompt before you clear the connections. See "Disabling and Enabling Logins" on page 93.
3. Then use **CLEAR STATION** to terminate the connection as discussed in "Using CLEAR STATION to Clear a Connection" on page 92. With login disabled, a workstation with auto-reconnect enabled will still try to reestablish its connection automatically, but the necessary services on the login server won't be available. (After the connections are cleared, workstation attachments appear as *NOT-LOGGED-IN entries in MONITOR's Active Connections window.)
4. When you have completed your server tasks, enter ENABLE LOGIN to allow users to log in again.

   HINT: Note that if you don't clear a workstation's connection and a communication failure occurs (such as a broken or unplugged network cable), the workstation will be able to auto-reconnect when the problem is fixed.

Controlling Resource Allocation with Locks

A lock prevents a file or record from being updated by more than one user at a time. By controlling the number of file and record locks available to a workstation or a server, you control access to files and records.

You can increase the number of locks if clients cannot open files. Or you can limit the number of locks to prevent overuse of file resources.

Preventing Workstations from Overusing File Resources

If you are running out of file resources, use the following SET parameters (Traditional File System category) to limit the number of locks for the server and for each connection.

- Maximum Record Locks Per Connection = *value*
- Maximum File Locks Per Connection = *value*
- Maximum Record Locks = *value*
- Maximum File Locks = *value*

Before limiting file and record locks, make sure the workstations have an adequate number of locks to access the files and records they need. Limiting needed locks can cause applications to generate errors.

For the server, limit the total number of file and record locks allowed by decreasing the values of the following parameters:

Maximum Record Locks
Maximum File Locks

For each client, limit the total number of file and record locks allowed by decreasing the value of the following parameters:

Maximum Record Locks Per Connection
Maximum File Locks Per Connection

The changes to the parameter values take effect immediately and are persistent.

Increasing File Record Locks

To provide more file record locks if applications fail either because clients cannot open enough files or because not enough record locks are available, do the following:

1. Increase the values of the following (Traditional File System category) parameters to increase the number of file and record locks allowed for the server:

   Maximum Record Locks
   Maximum File Locks

   The changes to the parameter values take effect immediately and are persistent.

2 Increase the values of the following (Traditional File System category) parameters to increase the number of file and record locks allowed for each workstation:

```
Maximum Record Locks Per Connection
Maximum File Locks Per Connection
```

The changes to the parameter values take effect immediately and are persistent.

Performing Common Maintenance Tasks

This section includes information about the following tasks:

- Backing Up Server Data (page 96)
- Checking Server Error Logs (page 97)
- Checking Disk Drives (page 97)
- Reviewing Server Cache Statistics (page 97)
- Checking Free Space on Server Disks and Volumes (page 98)
- Reviewing User Accounts (page 98)
- Testing the Uninterruptible Power Supply (page 98)
- Documenting the Network (page 99)

Backing Up Server Data

Maintaining a daily backup of the data on your is crucial to the security of your data.

For information about the backup software included with NetWare, see *Storage Management Services Administration Guide*.

Checking Server Error Logs

Check server error logs at least once a week, even if you don't believe there have been errors. Problems caught early are easier to solve. View the error logs with EDIT (command line) or Editor (GUI) at the server console or with a text editor from a workstation.

When needed, NetWare creates the following error logs in SYS:SYSTEM:

- **BOOT$LOG.ERR** for errors generated during the process of starting the server.
- **SYS$LOG.ERR** for server errors, including system messages, alerts, and security violations.
- **VOL$LOG.ERR** for volume errors.
- **TTS$LOG.ERR** for data backed out by the Transaction Tracking System.
- **ABEND.LOG** for information generated by the abend process. This file is moved to SYS:SYSTEM as soon as the server is started after the abend.

Checking Disk Drives

Once a week check the Storage Devices statistics to make sure that the operating status of each disk is active. You can do this in MONITOR or in NetWare Remote Manager by clicking the View Statistics link in the navigation frame and then selecting the applicable drives you want to view.

If you rarely use the diskette drive on your server, you might want to test the drive about twice a year to make sure it's running properly.

Reviewing Server Cache Statistics

For more information about monitoring and optimizing server memory, see Optimizing Server Memory in the *Server Memory Administration Guide*.

For server's using Novell Storage Management, see Setting the Cache Buffers in the *Novell Storage Services Administration Guide*.

For servers using the traditional file system, do the following:

1. Review the traditional file server cache statistics weekly.

   These statistics are found on the System Memory Information page in NetWare Remote Manager or on the General Information screen of MONITOR.

2. Divide the value of Total Cache Buffers by the value of Original Cache Buffers to determine the percentage of available cache.

   Ideally, file server cache should be 70% or more of the total cache.

3. If the percentage falls below 50%, add more memory to the server.

Checking Free Space on Server Disks and Volumes

1. Check server disks and volumes weekly to make sure they have enough free space.

   To determine the amount of free space, load MONITOR and select Volumes. The Mounted Volumes screen lists all mounted volumes, their capacity, and the percentage of the volume that is full.

   Keep at least 15% to 20% free space on any disk.

   Keep at least 20% free space on volume SYS: and at least 10% free space on other volumes. If volume SYS: fills up, your server hangs.

2. If the free space is less than the recommended values, increase the size of the volume or remove unneeded files and directories.

You can use REBUILD on NSS logical volumes and VREPAIR on traditional volumes. See VREPAIR or REBUILD in *Utilities Reference*.

Reviewing User Accounts

1. Review all users and objects on the network once a month to make sure that there are no intruders, obsolete accounts, or unauthorized accounts.
2. Make sure accounts are closed for all users who have left the system.

Testing the Uninterruptible Power Supply

If your network has an Uninterruptible Power Supply (UPS), check it twice a year to make sure it's running properly. Choose a time when no users are logged in to the network.

1. Bring down the server and exit to DOS, but do not turn off the computer.
2. While the computer is still running, unplug it.

   If your UPS system is working properly, the computer should continue to run.

   If the server powers off, your UPS batteries are probably low or dead. Check and replace them.

Documenting the Network

It is important to document your network. Keeping records of network layout, hardware and software inventory, configuration, repairs, and backup schedules will save you time and work if you need to rebuild or replace parts of the network, justify new equipment, or restore the network after a disaster. You will also need much of this information if you ever need to call Novell Technical Support. You might want to keep documentation in a notebook or online in a database.

IMPORTANT: Whether you store your network documentation in a notebook or in a database, keep multiple copies and update them regularly. Always store one or more copies offsite—along with your taped backups. Documentation does no good if it's destroyed with the network itself in a major disaster.

Your network documentation should include the following:

- Inventory of all hardware and software

  Version numbers, serial numbers, warranty information, date purchased, license information, etc.

- Configuration information for workstations

  Copies of AUTOEXEC.BAT, NET.CFG (for DOS and Windows 3.1*x* clients) or the registry (for Windows 95/98 and Windows NT/2000).

  Any standard directory structures.

- Configuration information for server

  In NetWare Remote Manager, click Run Config Report in the navigation frame. Click the View Report button. Then print and save the report. This report contains the following:

  - Contents of all .NCF, .BAT, .CFG, .BAT, ABEND.LOGS
  - A file list of the C: directory
  - A file list of the SYS:SYSTEM directory
  - A list of all SET parameters and current settings
  - A list of all the modules currently running on the server
  - A list of LAN driver configurations
  - Storage device configuration information
  - Volume statistics for volume SYS: and _ADMIN

You should also gather the following information:

- Services provided by each server, such as file and print, databases, etc.
- General directory structure of each volume.

- Configuration information for printers

  Map of printer locations, the version of NLM programs, and the dates and versions of print drivers.

- eDirectory tree structure

  Print out the eDirectory structure from ConsoleOne or iMonitor. Document replicas and partitions.

- Procedures

  Login processes and backup procedures. Most important, procedures for restoring the system from backups.

- Backup information

  Rotation schedule of backup media, labeling system, names and phone numbers of backup operators, and locations of backup disks and tapes.

- User information

  Login scripts and special menus.

- Software and hardware repairs and service calls

  Repair records and receipts, service calls log, and solutions in case the same problem occurs again.

- Diagram of network and cable plant

  Locations of servers, workstations, printers, routers, hubs, etc.; name of each element; the kinds of cables and connections.

- Changes to the system.

  Any updates to the network or its components.

Performing Preventive Maintenance Tasks

To avoid common server problems, review the following:

- “Preventing Memory Problems” on page 101
- “Preventing Power Supply Errors” on page 101
- “Preventing Static Electricity Problems” on page 102
- “Monitoring the NetWare Server” on page 82
- “Matching Performance Capabilities” on page 34
- “Documenting the Network” on page 99
- Preventing Cabling Problems in the *Server Communications Administration Guide*

Preventing Memory Problems

- Make sure you have adequate memory installed on the system.
- Modify the NET.CFG file to load only necessary drivers.
- Modify the CONFIG.SYS file to load only necessary drivers.
- Check the AUTOEXEC.BAT and CONFIG.SYS files to make sure no memory managers, such as HIMEM.SYS or EMM386.EXE, are being loaded and that there is no DOS=HIGH statement in either file. Make sure no DOS device drivers are being loaded.

For information about freeing up memory on a server, see “Freeing Server Memory Temporarily” on page 139.

Preventing Power Supply Errors

An inconsistent power source is the most common cause of hardware problems. It also produces the most devastating results.

Power outages cause workstations, network servers, print servers, and backup devices to reboot. When this happens, all information stored in RAM is lost and sometimes hardware is damaged.

Power spikes and brownouts can also cause a variety of hardware errors.

You can have reliable network performance only if you plan for power outages and fluctuations and protect against them. The following tips can help you do this:

- Add a dedicated power feed and ground line from your breaker box to critical equipment. Make sure the ground line connects to earth ground.
- Install an uninterruptible power supply (UPS) or a standby power system (SPS) to provide power to critical equipment for 15 minutes after a power outage.

  The capacity of such power supplies is limited, so you might not want to plug nonvital hardware (such as monitors or printers) into the UPS or SPS line.
- Train users to save data and log out of the network when the power goes out. Then you can bring down the NetWare server in an orderly manner without forcing users off the system while the server is running on UPS or SPS power.
- Install a surge suppressor or power conditioner on all power lines that are used by computers. Many UPS and SPS devices already have this feature.
- Do not allow anyone to plug fans, printers, copy machines, vacuum cleaners, or other motor-driven appliances into the dedicated line or into any power line with computers.

  Insert "dummy plugs" into open outlets to prevent people from plugging such appliances into computer power sources.

Preventing Static Electricity Problems

An electrostatic discharge (ESD) must equal about 3000 volts before you can feel it, but sensitive electronic components such as microchips and circuit boards can be damaged by ESDs of as little as 20 or 30 volts. These small discharges do not cause a component to fail immediately, but can cause the component to degrade over time and fail at a later date.

We recommend that you take the following precautions to protect electronic components from electrostatic discharge:

- Ground yourself and your equipment with a proper wrist strap and mat before working on computers and computer boards. Test grounds daily to make sure they have not become loose or intermittent.

  WARNING: *Do not* use a wrist strap when working on monitors! They can carry a large voltage that can reach you through the strap.

- Never touch components or integrated chips by their electrical leads.
- Do not allow anyone to touch you when you are working on boards that contain integrated circuits. They might cause a static charge.
- Transport and store boards and integrated circuits in *static-shielding* bags, usually grey-silver in color. The bags must be in perfect condition because tiny pin holes will defeat their purpose. *Anti-static* bags (blue or pink) do not shield their contents from external static fields and should not be used.
- Keep nonconductors, such as polyester clothing and plastic, away from open computers and components. Nonconductors are a source of static charges.
- Never place components on any conductive surface, such as metal.
- Keep the humidity of any area where you have open computers at 70 to 90 percent. Static electricity problems are more likely to occur in low humidity.

5 Troubleshooting the NetWare Server

This chapter contains the following information for troubleshooting your NetWare® server:

- "Using a Troubleshooting Methodology" on page 105
- "Creating a Core Dump" on page 112
- "Troubleshooting Hardware and Network Problems" on page 114
- "Troubleshooting the NetWare Server" on page 115
- "Monitoring and Resolving Communication Problems" on page 147
- "Suspected Multiprocessing Problems" on page 149
- "Unable to Communicate with Server, -625 Errors" on page 150
- "Workstations Can't Communicate with Server" on page 153
- "Preventive Maintenance Tasks" on page 158

Using a Troubleshooting Methodology

Novell® Technical Support recommends that you follow the same basic steps in all troubleshooting efforts. Following a standard procedure helps you solve technical problems faster and in an orderly way.

The following tasks are those that any Novell Technical Support representative would ask you to perform if you called Technical Support. By following these steps on your own, you might be able to resolve problems without assistance. Then, if you still need to call Technical Support, you will already have the information prepared for the representatives to solve your technical problems more quickly.

- "Keeping Your Servers Patched" on page 106
- "Eliminating Obvious Causes" on page 107

- "Gathering Information" on page 107
- "Simplifying the System" on page 109
- "Using Troubleshooting Resources" on page 109
- "Developing Hypotheses and Performing Tests" on page 111
- "Looking for Additional Help" on page 111
- "Documenting the Solution" on page 112

You can find additional tips in TID 2938836, "Before Calling Support for OS Issues" at Novell's Support Web site (http://support.novell.com/cgi-bin/search/tidfinder.cgi?2938836).

Keeping Your Servers Patched

Many problems that might occur on your server will have already been solved by Novell and provided in the form of a patch file. It is essential that you load all server and client patches.

Novell provides regular Support Packs that contain patches for the complete operating system and associated products. To locate the latest patches for your network, see the Minimum Patch List page on the Novell Support Web site (http://support.novell.com/misc/patlst.htm).

To locate specific patches for SERVER.NLM and updates for other NLM™ programs, see the Patches and Files page on the Novell Support Web site (http://support.novell.com/filefinder/). Copy updated NLM programs to the server's startup directory where they will overwrite the previous versions.

In addition, be sure you use up-to-date drivers for the version of NetWare that you are using. Use drivers that ship with the product; drivers that are tested, certified, and made available on the Novell's Support Web site (http://support.novell.com/); or certified drivers released by hardware vendors. Check product certification bulletins on the DeveloperNet® Web site at Novell Solutions Search (http://developer.novell.com/solutions). In the Software category, select LAN adapters or WAN adapters to learn which versions are most recent.

ODI™ HSM Specification 3.31 supports NBI (NetWare Bus Interface), HIN (hardware instance number), instance unload, and industry-standard PCI Hot Plug technology. Do not mix uses of a driver written to the 3.3*x*/1.1*x* ODI Specification with 3.2 ODI Specification support modules. The LAN driver certification bulletin will list the specification a LAN driver is written to. In

some cases, you will need to contact the IHV (independent hardware vendor) that wrote the driver.

To verify the compatibility of the ODI modules with the LAN drivers on your server, download and run DRVSPC.EXE (http://support.novell.com/servlet/tidfinder/2911341).

NetWare 6 drivers for storage devices and host bus adapters are written to the NWPA (NetWare Peripheral Architecture™) specification.

Eliminating Obvious Causes

Be sure to eliminate any obvious causes for network problems—such as making sure that everything is plugged in and that the power is on. Consider the following:

- Check the Novell Knowledgebase (http://support.novell.com/search/kb_index.htm) for known problems with software and hardware.
- Inventory the hardware and cabling systems to make sure that everything is plugged in, connected, and terminated properly.
- Check for user errors.
- Make sure that all hardware is Novell certified. Check the Novell DeveloperNet Web site (http://developer.novell.com) for a list of hardware and software products certified to run with NetWare.
- Make sure that there are no rights problems. Insufficient rights prevent you or your users from accessing volumes, directories, and files and from performing file operations.

Gathering Information

Start gathering information about the context of the problem. Ask the following questions:

- When does the problem happen? For example, a problem that occurs regularly at midnight could be related to file compression. A problem occurring in the morning could be related to spikes in network usage as users log in.
- Can you duplicate the problem? Is it constant or intermittent? If intermittent, at what intervals does it happen?

- Can the problem be associated with other activities happening on the network at the same time or with specific hardware and software? For example, does the problem occur only when the network activity is highest? Does it occur only on certain workstation platforms?
- Did anything change shortly before the problem began to occur? For example, did you install new software?
- What components of the network are involved—the server, some or all of the workstations, printers, or other peripheral devices?
- What error or console messages are displayed? What NLM program is the source of the message? Check server error logs.
- What do configuration and log files reveal? If you need to call Novell Technical Support, gather information about your server and network, including log files such as ABEND.LOG, SYS$LOG.ERR, and VOL$LOG.ERR. Also have your hardware and software configuration and version numbers available.

  To get this information, you can run, view, and send a configuration report on your server using NetWare Remote Manager. For procedures, see Running and Viewing the Server Configuration Report in the *NetWare Remote Manager Administration Guide*.
- If you suspect problems with eDirectory, gather the following information:
  - Number of servers in the tree
  - Structure of the tree
  - Number of objects per partition
  - Error messages
  - Names of servers holding master replicas
  - Versions of eDirectory on pertinent servers
- Compare the affected computers to similar computers. Do some computers have the problem, while others do not? If so, what is different between the affected and unaffected computers?

Simplifying the System

If there is any danger of losing data, back up the system before you do any further troubleshooting.

Simplify the system and eliminate as many variables as possible to isolate the source of the problem.

- Try running the server without the AUTOEXEC.NCF or STARTUP.NCF file. You can comment out the commands in the .NCF files, or you can execute **SERVER** with the **-na** or **-ns** option. (To comment out a command, type **REM** and a space at the beginning of the command line.)

  For an explanation of these load options, see SERVER in the *Utilities Reference*.

- Unload all NLM programs. Remove all nonessential products, including virus scanners and server metering modules, until the server software is in a basic or default configuration.

- Remove or disconnect peripheral devices.

- Remove extra network boards or LAN adapters.

When you have simplified the server as much as possible, note whether the problem happens again. To determine whether the operating system is the source of the problem, restore each component of the system, one at a time, checking to see whether the addition of the component generates the problem.

Using Troubleshooting Resources

Novell and other vendors provide research tools you can use to resolve problems.

For example:

- The Novell Knowledgebase (http://support.novell.com/search/kb_index.htm).

  This site contains Technical Information Documents (TIDs), Solutions, and patches. You can browse by product or search using partial filenames and wildcards. You might look for the Top 20 Downloads or the most recently released files.

- Novell Support Forms (http://support.novell.com/forums/).

  Here you can post technical questions and receive a response from a Novell Certified System Operator (SysOp). You can also browse responses that have already been posted.

- The Novell DeveloperNet Web site (http://developer.novell.com).

  This site contains information about third-party products certified to run with NetWare. You can use a search facility that is form-based to locate tested and approved bulletins by category.

- Novell user groups, located in most cities and countries. Novell Users International (NUI) offers NetWare support forums on the World Wide Web (http://www.nuinet.com/).

- Novell Support Forums (http://support.novell.com/pforum/).

  Here you can post technical questions and receive a response from a Novell Certified System Operator (SysOp). You can also browse responses that have already been posted.

- Vendor Web sites that provide information and updated software to download.

- NetWare utilities, such as NetWare Remote Manager or MONITOR.

  NetWare Remote Manager can be used from a workstation through a Web browser. From this utility, you can track down high users of server memory, server CPU, server processes, server disk space, etc. For more information about using this utility, see the *NetWare Remote Manager Administration Guide*.

  The MONITOR utility can provide important clues to the source of server or network performance problems. For more information about using this utility, see MONITOR in the *Utilities Reference*.

Developing Hypotheses and Performing Tests

After you have gathered information, eliminated obvious causes, or simplified your system, you can determine what you think is the most likely cause of the problem. You might develop several hypotheses. If so, decide which is the most likely, the next mostly likely, etc. Base your hypotheses on the data you have gathered and on your own experience with the system.

After you have developed your hypotheses, test them, keeping these tips in mind:

- Decide which hypothesis seems the most likely and test this one first. Test the least likely hypothesis last. The only exception might be a hypothesis that is very quick and easy to test, in which case you might want to eliminate it first.
- Break down hypotheses into the smallest possible components and test each one separately. For example, if you suspect the problem is with the physical network, try to isolate which cable segments, boards, or connectors might be the source of the problem and then test each one individually. Test only one component at a time.
- Try replacing components. If you suspect a faulty component is causing the problem, replace it with a component that you know is good. Make sure that you replace only one component at a time.
- Simplify the system. If you have not already done so, try removing components from the system. If the problem still occurs, you have a smaller set of components left that can be the source of the problem. If the problem goes away, start reloading components one at a time. After each addition, note whether the problem occurs.

Looking for Additional Help

Be prepared, when asked, to tell the Novell Technical Support representative what troubleshooting steps you have already taken.

Using Novell Authorized Reseller Representatives

Find Service Partners by locality or area. For a list of resellers and distributors worldwide, check the Novell Support Web site > Partner Services (https://support.novell.com/partner_services.html).

Using Novell Support Tools

Novell has additional support tools available. For a list of these tools, see the Novell Support Web site > Support tools (http://support.novell.com/tools.html).

Opening a Support Incident

You can open a support incident online. To access the form, see the Novell Support Web site > Electronic Incident (https://support.novell.com/elecinc/eiLogin.jsp).

Documenting the Solution

After you resolve a server or network problem, document the solution thoroughly. The information will be helpful if similar problems occur in the future. Be sure to document changes to the server or network configuration, software and hardware updates or additions, new version numbers, workarounds, etc.

Creating a Core Dump

Novell might request a core dump when a server experiences a lockup or abend and other troubleshooting has failed to resolve the problem. A core dump is a copy of a NetWare server's memory at the time the server abended. Core dumps can be analyzed by Novell engineers and are often the key to finding software bugs. However, now that servers typically use large amounts of RAM, creating a core dump is less likely to be a routine troubleshooting procedure. Your ABEND.LOG file could be equally valuable for diagnosis.

IMPORTANT: You will be expected to install all necessary patches before Novell requests a core dump. To send a core dump file to Novell, you must first open a support incident, which will be billable. You will not be charged until the incident is resolved or closed. If the problem is a Novell bug and no patches were previously available, then there will be no charge.

The procedure for creating a core dump file follows, but your support representative can explain it when you call.

You can perform the following types of core dumps:

- **Full core dump** copies all server memory to a local drive or device.
- **Full core dump minus cache** copies all server memory except file cache (disk cache) to a local drive or device. The cacheless core dump is smaller, but it provides as much useful information as a full core dump.

A core dump can be started two ways:

- By responding to the core dump choices displayed by NetWare after an abend has occurred.

  The Type? prompt allows you to specify a full core dump or a cacheless core dump, as explained above.

  The Device? prompt allows you to specify a local drive or a DOS-writeable device.

  NOTE: Other types of core dumps might become possible in the future. Your Novell Technical Support representative will inform you if that is the case.

- By forcing a core dump by entering **.C** while in the NetWare debugger.

  If the server is not completely frozen, you can enter the debugger by pressing: Shift+Shift+Alt+Esc.

  HINT: Press the left Shift key with the left hand, and press both the right Shift key and Alt with the right hand. Then press Esc with the most convenient finger of the left hand.

  Then enter **.C** and the server then displays core dump choices.

  When the core dump is finished, enter **G** to exit the debugger and to redisplay the System Console prompt. Or enter **Q** to exit to DOS.

Performing a Core Dump to a Local Drive

After you start the core dump, you are asked to specify the DOS drive letter and file path that the memory image file will be written to. The size of the full image file will be approximately equal to the total RAM installed in the server. For a cacheless core dump, the size of the image file will be approximately equal to total RAM minus the amount of file cache (disk cache memory).

The drive can be any writable DOS device that contains enough storage space. But remember that it must be set up not only before the server abends, but before the server is booted.

When the image is written to a local hard disk on the server, the default name of the image file is C:COREDUMP.IMG. After the file is on the hard disk, it can be compressed, copied to diskettes, backed up to tape, or sent by FTP to ftp.novell.com (if you have opened a support incident).

The image file can also be written to a network drive later, after the server is up and running. This can be done using IMGCOPY.NLM or any other third-party NLM that provides this functionality. To locate IMGCOPY.NLM, use the search on the Patches and Files page on the Novell Web site (http://support.novell.com/filefinder/).

Sending the Core Dump to Novell

Before sending the memory image to Novell, contact a support representative to open a support incident. You will be assigned to a Technical Support Engineer who will help you analyze the memory image file. The Technical Support Engineer will make arrangements to receive the image either in the regular mail or through the Internet and will advise you on the best media format to use.

Troubleshooting Hardware and Network Problems

The following sections provide troubleshooting information for resolving hardware but not really NetWare-related errors.

- "Identifying Problems after Installation" on page 114
- "Resolving Hard Disk Access Problems" on page 114
- "Making Computer Memory Available for Network Drivers" on page 115

Identifying Problems after Installation

If the problem occurred after installation, it might indicate that the network was installed incorrectly.

- Check all network boards for conflicting address and I/O settings.

  Each component should be able to work as a standalone system.

- Make sure that all cables are fastened securely to all network boards and network connectors, and that terminating resistors are installed correctly.

Resolving Hard Disk Access Problems

To diagnose hard disk access problems, determine whether any of the following conditions exist:

- 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 disk coprocessor board, and the hard disk is not functioning.
- The hard disk controller board is not terminated or addressed correctly.

To resolve hard disk access problems, perform the following actions:

- Make sure that the disk driver is loaded. In NetWare Remote Manager, click the Disk / LAN Adapters link in the navigation frame, and then click the Info icon for each network board in your server.
- Check the cables between the hard disks and the controller boards. Make sure that Pin 1 of each cable is attached to Pin 1 of each connector.
- Check the power cables and make sure that they are seated correctly in the power sockets on the hard disks.
- Check the disk partition and volume information on the hard disk using ConsoleOne™ or NetWare Remote Manager.

Making Computer Memory Available for Network Drivers

To increase the amount of workstation memory available for network drivers, do any or all of the following:

- Add more memory.
- Unload unneeded terminate-and-stay-resident (TSR) programs (DOS clients only).
- Modify the NET.CFG file to load only necessary drivers.
- Modify the CONFIG.SYS file to load only necessary drivers.

Troubleshooting the NetWare Server

This section provides troubleshooting suggestions for typical NetWare server problems such as the following:

- Abends
- Insufficient Packet Receive Buffer, No ECB Available Count Errors
- Slow Response
- Console Hangs
- High Utilization Statistics
- General Server Disk I/O Errors
- Disk Space Problems
- Memory Problems

- Locked Device Errors
- Event Control Block Allocation Errors
- Console Command Problems
- Keyboard Locking Problems when Copying Files from CD-ROM

Resolving Abends

The NetWare operating system is very resilient, but errors can occur. Serious problems are usually accompanied by abend (abnormal end) messages. When an abend message appears, either NetWare or the CPU has detected a critical error condition and started the NetWare fault handler. NetWare uses abends to ensure the integrity of operating system data.

When a server abends, users might not be able to log in to the server, workstations might not be to read from or write to the server, and an abend message usually appears on the System Console or Logger screen of the server console. If the NetWare auto-recovery mechanism is enabled (default), NetWare might restart the server automatically or suspend the offending process, depending on the nature of the abend.

If there is no abend message on the console, no ABEND.LOG file in SYS:SYSTEM, and no number in brackets within the System Console prompt, but users still can't access the server, see "Monitoring and Resolving Communication Problems" on page 147. If there is no abend message but the console is frozen so that you cannot enter commands, see "Server Console Hangs" on page 124.

Understanding What Happens When You Get an Abend

When the server abends, it displays an abend message similar to the following:

```
Abend: SERVER-5.xx-message_number message_string
ADDITIONAL INFORMATION: message
```

The Additional Information section states the probable cause of the abend. It indicates where the problem occurred and gives the name of any NLM associated with the abend. This information helps you determine how to resolve the abend.

The abend message, along with additional information, is saved in the ABEND.LOG file on drive C:. As soon as the server is restarted, the ABEND.LOG file is moved to SYS:SYSTEM.

You can respond to the abend manually or have the server respond automatically.

When you respond manually, the server determines the nature of the abend and displays the appropriate response option on the screen, along with additional options for bringing down the server or executing a core dump. You must execute an option to respond to the abend.

When the server responds automatically, it executes the appropriate response without intervention.

IMPORTANT: Sometimes an abend (or a faulty NLM program) can cause the server console to stop functioning. In this case, the abend message is not displayed and you cannot enter commands at the console prompt.

After a server failure, we recommend turning the power off of the computer and restarting it rather than just exiting to the DOS prompt, C:\NWSERVER, and typing SERVER again.

Responding to the Abend Manually

The default method of responding to an abend is automatic. (See "Responding to the Abend Automatically" on page 120.)

To respond manually to abends, change the following SET parameter (Error Handling category) to the value shown:

```
AUTO RESTART AFTER ABEND = 0
```

This SET parameter controls what the server does after an abend. See the online help for a description of each value.

When an abend occurs, the server displays a short list of options appropriate to the nature of the abend. To respond to the abend, you must execute one of the options by typing the first letter of the option.

The following options could be displayed. Note that several of the options have the same first letter (such as R, S, or X). In a given abend situation, the option list will include only one option for any given first letter.

- `S=Suspend the running process, update ABEND.LOG, and attempt to down the server`

  This option appears if the abend was software-detected— that is, detected by the network operating system. It is important to save files, shut down the server, and try to solve the problem that caused the abend. Review the ABEND.LOG file to help determine the source of the problem.

When you execute this option, the server sends a message to users that the server is going down and advising them to save their files and log out. The server then stops the running process, updates the ABEND.LOG file, and attempts to shut down and restart the computer.

The amount of time before the server shuts down and restarts is determined by the SET parameter AUTO RESTART AFTER ABEND DELAY TIME. You can set this value from 2 to 60 minutes. The default is 2 minutes.

You can submit the ABEND.LOG file the the abend log database (http://abend.provo.novell.com/index.html) at Novell to help you troubleshoot the abend.

- `R=Resume the running process, update ABEND.LOG, and attempt to down the server`

  This option appears if the abend has detected a hardware problem. Shut down the server, fix the hardware, run diagnostics, and contact the harware manufacturer for additional assistance.

  When you execute this option, the server sends a message to the users that the server is going down and advising them to save their files and log out. The server then resumes the running process, updates the ABEND.LOG file, and attempts to shut down and restart the computer.

  The amount of time before the server shuts down and restarts is determined by the SET parameter AUTO RESTART AFTER ABEND DELAY TIME. You can set this value from 2 to 60 minutes.

- `S=Suspend the running process and update ABEND.LOG`

  This option appears if the abend was hardware-detected—that is, detected by the processor. All hardware-detected abends have the words *processor exception* in the abend message.

  These abends include page faults, protection faults, and invalid op codes stack overflows, double faults, etc. When this option is available, the server has determined that it cannot return the process to a safe state, but it does not need to shut down the server immediately to resolve the problem. You might still need to shut down the operating system and restart it at a later time.

  When you execute this option, the server suspends the currently running process and updates the ABEND.LOG file, but does not shut down the

computer. Server performance might be poor, because a loaded NLM is probably malfunctioning.

Read the Additional Information part of the abend message to learn which NLM *might* be causing the problem. At a convenient time, shut down the server and restart it. Examine the ABEND.LOG file for more information about the source of the problem.

You can submit the ABEND.LOG file the the abend log database (http://abend.provo.novell.com/index.html) at Novell to help you troubleshoot the abend.

- `S=Return the running process to a safe state and update the ABEND.LOG file`

  Like the previous option, this option appears if the abend was hardware-detected—that is, detected by the processor. All hardware-detected abends have the words *processor exception* in the abend message.

  These abends include page faults, protection faults, and invalid op codes, stack overflows, double faults, etc. When this option is listed, the server has determined that it can return the process to a safe state.

  When you execute this option, the server returns the running process to a safe state and updates the ABEND.LOG file, but it does not shut down the server. In most cases, the server completely recovers and no further action is necessary.

- `Y=Copy diagnostic image to disk`

  Execute this option to perform a core dump that can be examined to determine the cause of an abend. For information on core dumps, see "Creating a Core Dump" on page 112.

- `X=Restart`

  This option appears only if DOS has been removed. Execute this option if you want to restart the server.

  If DOS has been removed, the server will not create or update an ABEND.LOG file.

- `X=Update ABEND.LOG and then exit`

  Execute this option if you want to shut down the server and exit to DOS. If you power off the server without first executing one of the S or R options to resolve the abend, the server will not update the ABEND.LOG file.

- Otherwise, power off and back on to restart

  If the console has been secured, you must power it off and then back on to restart the server. If you power off the server without first executing one of the S or R options to resolve the abend, the server will not update the ABEND.LOG file.

When the server restarts, it moves the ABEND.LOG file from the DOS partition to the SYS:SYSTEM directory.

Responding to the Abend Automatically

You can require the server to respond automatically to abends. Two automatic responses are possible.

- When both of the following SET parameters (Error Handling category) are set to the values shown, the server responds to the abend automatically by evaluating the source of the abend and executing the appropriate S or R option described in the previous section.

  AUTO RESTART AFTER ABEND = 1
  DEVELOPER OPTION = OFF

  Because these are the default values of the parameters, the default mode is to respond to abends automatically.

- When both of the following SET parameters are set to the value shown, the server responds to the abend by shutting down the server and attempting to restart it.

  AUTO RESTART AFTER ABEND = 2
  DEVELOPER OPTION = OFF

Use the following SET parameter to specify how long the server waits after an abend before attempting to shut down and restart the computer:

AUTO RESTART AFTER ABEND DELAY TIME = *minutes*

To set the parameter values, use the SET command or MONITOR at the server console or NetWare Remote Manager from a workstation.

The Developer Option parameter is in the Miscellaneous category.

The Auto Restart After Abend and Auto Restart After Abend Delay Time parameters are in the Error Handling category.

All parameters can be set in the STARTUP.NCF file.

Because the server responds to the abend automatically, you might not know when an abend has occurred. Therefore, you should periodically check the ABEND.LOG file or the Profiling and Debug Information screen in NetWare Remote Manager (look for Suspended by Abend Recovery status).

Insufficient Packet Receive Buffers, No ECB Available Count Errors

The ECB (event control block) counter is incremented when a device sends a packet to your NetWare server but no packet receive buffer is available. This mean a packet has been dropped by the server.

The server allocates more packet receive buffers after each incident until it reaches its maximum limit (Maximum Packet Receiver Buffer setting).

If you are using an EISA busmaster board (such as the NE3200™ board), you will probably need to increase both the minimum and maximum number of packet receive buffers.

For procedures on setting the Minimum Packet Receive Buffers and Maximum Packet Receive Buffers parameters, see SET > Communications Parameters in *Utilities Reference*.

No ECB Available Count messages can also indicate that the driver is not configured correctly or that the Topology Specific Module (TSM) and the Hardware Specific Module (HSM) are incompatible. This value is maintained by the TSM.NLM program.

If the ECB count is increasing and all the packet receive buffers are in use, take a coredump (see "Creating a Core Dump" on page 112) and contact Novell technical support.

Resolving Slow Server Response

To diagnose slow server response problems, identify whether the following conditions exist:

- The workstation network board is slow or faulty.
- Network cabling is faulty.
- The server network board is slow or faulty.
- Too many users are using the network.
- The server hard disk is slow or faulty.

- The server is low on memory.
- The volume has too many deleted files that have not been purged.
- Network traffic is extremely high.
- The cabling system is experiencing too much interference.
- Insufficient directory buffers, cache buffers, or packet receive buffers have been allocated.
- An EISA controller board needs to be configured to use interrupts.

To resolve slow server response problems, perform the following actions:

- If a workstation or the 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 then replace the cable attaching the workstation or server to the network.
- Check the status of packet receive buffers and service processes. Compare their values to the maximum allowable values.

  To check the health of these values, use NetWare Remote Manager. Click the Health Monitor link in the navigation frame. Click the links for the Allocated Server Processes, Available Server Processes, and Packet Receive Buffers on the Server Health Monitoring page.

  Packet receive buffers are used to transmit and receive packets. If the number of Pack Receive Buffers is increasing, the server operating system will be sluggish. If the number of Packet Receive Buffers reaches the maximum and no ECBs are available, the system will become very sluggish and might not recover.

  If the current server process are approaching the maximum, you should consider increasing the Maximum Server Processes SET parameter value. If you have only a few available server processes, your server is probably very busy. You might consider increasing the Minimum and Maximum Server Process SET Parameter.

  To change the values for these parameters, access NetWare Remote Manager. Click the Set Parameter link in the navigation frame. On the Set Parameter Categories page, click the following:

  - Communications link > Current Value link for Minimum Packet Receive Buffers
  - Communications link > Current Value link for Maximum Packet Receive Buffers

- Miscellaneous link > Current Value link for Minimum Service Processes
- Miscellaneous link > Current Value link for Maximum Service Processes

You can also use MONITOR or the SET commands at the server console.

- Check the Hot Fix™ status of all hard disks that use the Traditional file system. To view these status,
  - Access Monitor.
  - From the Available Options menu, click Storage Devices.
- Verify that all mirrored disks are still mirrored by entering the following command at the System Console prompt:

  MIRROR STATUS
- Purge deleted files.
  - Access NetWare Remote Manager.
  - Click the Volumes link in the navigation frame.
  - Click the Volume Information icon next the volume you want to delete files on.
  - Click the Purge Deleted Files button.

  You can also set the Purge attribute on files you want to be purged.
- Check the LAN driver statistics.
  - Access NetWare Remote Manager.
  - Click the Disk / LAN Adapters link in the navigation frame.
  - Click the Network Adapter Info link for each network board on the Hardware Adapters page.

  If you are using more than one network board in the server, compare the boards' Total Packets Transmitted statistics. If one board is receiving most of the traffic, recable the network so that the boards have equal loads.
- Check the CPU usage.
  - Access NetWare Remote Manager.
  - Click the Profile/Debug link in the navigation frame.
  - Click the Profile CPU Execution by NLM link and look for unusually high CPU usage.

- 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.
- Take a sniffer or LAN trace of the problem and analyize it.
- As a last resort, perform a core dump (see “Creating a Core Dump” on page 112) and contact a Novell Support technician.

Server Console Hangs

If the server console locks up so that you cannot enter commands, but there is no abend message on the System Console or Logger screen, follow these steps to troubleshoot the problem. If there is an abend message on the screen, see “Resolving Abends” on page 116.

1. Verify whether you can toggle among console screens.

   If yes, the problem might be caused by high server utilization. See “High Utilization Statistics” on page 125. If no, continue with the following steps.

2. Verify whether the server console hangs when you unload a specific NLM.

   If yes, the NLM is probably the source of the problem. Contact the NLM vendor.

3. Make sure you are using the latest disk and LAN drivers, BIOS, and firmware.

   If not, update disk and LAN drivers. For information on NetWare drivers, see “Keeping Your Servers Patched” on page 106.

4. Verify whether the server console hangs after you mounted the last volume.

   If yes, the network board might not be seated correctly or might not be configured correctly. Check the board and its configuration and correct any problems.

5. Verify whether you can you break into the debugger by pressing Shift+Shift+Alt+Esc on the system console keyboard.

6. If the console is locked, you can’t toggle among screens and you can’t enter the debugger, contact Novell Technical Support or your computer vendor to learn how to generate a nonmaskable interrupt to shut down the server.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105; search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp); and contact a Novell Support Provider.

High Utilization Statistics

Network performance is a key concern for network administrators and for Novell as well. Unfortunately, sometimes there is confusion about performance indicators and what their statistics mean.

For example, the idea that processor utilization is the key performance indicator for NetWare is much too simple. Some network administrators are concerned when the CPU Utilization health status in NetWare Remote Manager or the Utilization value in MONITOR's General Information screen approaches 100%, on the assumption that the higher the percentage, the worse NetWare's performance is. This is entirely *false*.

What Is Normal?

Consider first what the Utilization value represents: the average of the server's total processing capacity that was used during the last second (update interval). The remainder of the capacity was spent in the idle loop process. In other words, it is an indication of how much of that time the processor had something to do. A high utilization value means that NetWare is using that percentage of the processor's capacity and wastes less time doing nothing.

Some processes make efficient use of the processor and as a result might cause 100% utilization. This type of utilization is entirely appropriate. Most of the time, when utilization moves up to 100%, it means that the thread is using the processor efficiently. It might stay at 100% for a couple of minutes; this is normal.

It is *not* normal, however, when the utilization is at 100% for 15 to 20 minutes or more, when connections are dropped, or when server performance deteriorates noticeably. High utilization with these conditions indicates a problem. If you're not seeing these conditions, your utilization might be normal, even when it's at 100%.

How do you know what is normal for your server? You will recognize problems if you "baseline" your server. Know what is normal and know the difference between a cosmetic problem and a true performance problem. (You can test for a cosmetic problem by loading or unloading any NLM; this will cause the processor information to be recalculated.)

What Are the Most Common Solutions?

Before troubleshooting high utilization problems, make sure that you have followed the steps in "Using a Troubleshooting Methodology" on page 105. Check the Novell Support Connection Web site (http://support.novell.com) for NetWare patches or updated NLM programs. Available patches will contain fixes for reported high utilization problems related to the actual code of the operating system and eDirectory.

However, a number of high utilization conditions can still result from problems with configuration, levels of NLM programs, and tuning issues.

One of the first things you might want to do is discover the NLM program and threads that are using the CPU. To do this, complete the following steps:

1. Access NetWare Remote Manager.
2. Click the Profile/Debug link in the navigation frame.
3. Click the Profile CPU Execution by NLM link.
4. Note the parent NLM program and threads that are taking the longest execution time.
5. If possible, unload the offending NLM program to see if the problem disappears.

You can also use the following list of issues to help you resolve problems.

The items in the list are categorized, but are otherwise in no particular order. The list represents the collective experience of Novell Support representatives. We recommend that you review each item, using each to carefully analyze your system. Except for problems new to NetWare 6, you will be able to resolve the problem on your own in almost every case.

- Operating System Issues
- Storage Device Issues
- Memory Issues
- Novell eDirectory Issues
- Client Issues

Operating System Issues

- **Server resources.** Server resources can be divided into LAN, disk, and processor resources. LAN and disk resources are the number of buffers available. Processor resources are the number of service processes available. When a network packet arrives or when a disk read or write is performed, a buffer should be available to hold the data until a service process is available to service it. Running low on either buffers or service processes for even a brief period can cause high utilization on the server and delay for the users.

  To understand how server parameters work together to control the allocation of server resources, see "Monitoring Allocated Services" on page 86.

  For the procedure to configure the allocation of packet receive buffers (communication buffers), see Increasing Maximum and Minimum Packet Receive Buffers in the *Server Communications Administration Guide* and SET > Communications Parameters in *Utilities Reference* for parameter descriptions.

  For information on controlling the allocation of directory cache, see Tuning Directory Cache for the Traditional File System in the *Server Memory Administration Guide* and SET > Directory Caching Parameters for the Traditional File System in *Utilities Reference*.

  For setting up and tunning cache buffers in the NSS file system, see Setting the Cache Buffers in the *Novell Storage Services Administration Guide*.

  For parameter descriptions, see also the service processes parameters in SET > Miscellaneous Parameters in *Utilities Reference*.

  We suggest that the server parameters in the following table be set as indicated to avoid running low on server resources. This is especially important if you have 100 or more users. To change the following parameters, you can use NetWare Remote Manager at the workstation or SET or MONITOR at the server console.

  In NetWare Remote Manager, click the Set Parameters link in the navigation frame > *Category* > *current value for parameter*. Enter the new value and then click OK.

  In MONITOR, from the Available Options menu, select server Parameters > *Category* > *current_value_for_parameter* and then press Enter. Enter the new value, and then do applicable action.

Category	SET Parameter Name and Value
Communications	**Minimum Packet Receive Buffers=*value*** Recommended value is 2 to 3 per connection.
Communications	**Maximum Packet Receive Buffers=4000**
Traditional File System	**Minimum Directory Cache Buffers=*value*** Recommended value is 2 to 3 per connection.
Traditional File System	**Maximum Directory Cache Buffers=4000**
Miscellaneous	**Maximum Service Processes=1000**
Miscellaneous	**New Service Process Wait Time=0.3**

- **Processor hog.** Determine whether one thread is hogging the processor. In NetWare Remote Manager, click Profile / Debug link in the navigation frame. View the data in the Execution Profile Data by Thread table.

  In MONITOR, from the Available Options menu, select Kernel Options > Threads, and then press Enter.

  You can set the CPU Hog Timeout Amount to a value lower than the default. Specify the amount of time in seconds to wait before terminating a thread that has not relinquished control of the processor. See SET > Miscellaneous Parameters in *Utilities Reference*.

  IMPORTANT: Use caution when changing this value. You must understand the impact of what you are changing.

Storage Devices and Adapter Issues

- **Drivers.** See "Keeping Your Servers Patched" on page 106. For a brief explanation of NetWare Peripheral Architecture (NWPA), see Drivers for Host Adapters and Storage Devices in *NetWare Server Disks and Storage Devices Administration Guide*.

- **Free blocks.** When using the traditional file system, adequate free blocks are essential. A free block is a disk block that has no salvageable files stored there. A file that has been both deleted and purged becomes free space. Maintain a minimum of 1000 free blocks on each NetWare volume that has suballocation enabled.

  Suballocation, normally a low priority process, uses free blocks to perform its function. When free blocks are low, suballocation can go into an "aggressive" mode. Maintaining over 1000 free blocks will usually avoid this problem.

  To check how many free blocks you have on a volume, do either of the following:

  - In NetWare Remote Manager, click Volumes in the navigation frame, then click the Volume Information icon.
  - In MONITOR, from the Available Options menu, select Volumes > *the specific volume*. Press Tab to view the free blocks information on the Volume Information screen.

  If there are not at least 1000 free blocks on the volume, access NetWare Remote Manager, click Volumes in the navigation frame, click the Volume Information icon for the applicable volume, and then click the Purge Deleted Files button.

  This removes all deleted files from the directories and subdirectories and increases your free disk space.

  If you have applications that create large numbers of temporary, files you might want to set the P (Purge) flag on the directories where these files are stored. Every temporary file that is created will be put on the deleted file list. These files are kept on the disk until PURGE is run. You could also run SET Immediate Purge of Deleted Files=On at the System Console prompt.

- **Suballocation.** The traditional file system uses a disk block size of 64 KB. It is very important to monitor the disk space. Novell Technical Support recommends keeping 10% to 20% of the volume space free to

avoid suballocation problems. Suballocation does not have any server parameters to adjust.

To view disk space usage with NetWare Remote Manager, click the Health Monitor link in the navigation frame and then the Available Disk Space link on the Server Health Monitoring page. Print the Volume Information page for your records.

- **Compression.** When using compression in the NSS file system, see the following procedures, Other NSS Commands in the *Novell Storage Services Administration Guide*.

  When using compression with the Traditional file system, it is essential to have the server patched. Because it takes processor cycles to compress and decompress files, compression needs to be monitored carefully to avoid utilization problems. The default SET File Parameters for the Traditional File System for compression takes this into consideration.

  For example, file compression is set by default to occur during off-hours or periods of low server usage. Make sure that change have not been made that are causing high utilization problems.

  File decompression occurs on the fly. However, a very large file, such as 100 MB, can take a noticeable amount of time even with a Pentium* processor.

  SET Deleted Files Compression Option=2 causes the immediate compression of files that have been deleted. This can cause high utilization because the processor immediately compresses files upon their deletion.

  Directories that are flagged IC (Immediate Compression) can cause excessive decompression during work hours. Users with disk space restrictions might flag their home directories to IC in an attempt to save disk space. This can affect server performance.

  To ensure that frequently used files are not compressed, you can specify an appropriate value for the SET Days Untouched Before Compression parameter.

  To proactively eliminate compression as a possible problem, use SET Enable File Compression=Off parameter (Common File System category). This will cause files to be queued for compression but the files will not be compressed. However, accessing compressed files causes them to be decompressed.

Memory Issues

- **Insufficient RAM.** Memory resources are critical in a server environment.

  To view buffer cache statistics for the NSS file system, enter the following command at the System Console prompt:

  ```
  NSS CACHESTATS
  ```

  The best indicator for assessing server RAM in a traditional file system is displayed in the following ways:

  - In NetWare Remote Manager, click the View Memory Config link in the navigation frame and then Traditional File System Cache Statistics link, and view the LRU Sitting Time.
  - In MONITOR, from the Available Options menu, select Disk Cache Utilization and view the LRU Sitting Time.

  The value of this field should be a minimum of 15 to 20 minutes. A number lower than this indicates that the server's memory resources might be low. Another good indicator, Long Term Cache Hits, is displayed on the same page or screen in either utility.

- Also see "Resolving Server Memory Problems" on page 136.

Novell eDirectory Issues

- **eDirectory partitions.** We recommend having no more than three replicas of each partition in the tree. Efficient tree design is essential to avoid utilization problems. Because Novell® eDirectory™ needs to maintain synchronization among all servers in the replica ring, the more replicas there are of any partition, the more traffic will be on the wire. Three replicas are enough to provide fault tolerance and to allow for eDirectory if a database were to become corrupt.
- **eDirectory synchronization.** To test the possibility that eDirectory synchronization is the problem, turn off inbound and outbound synchronization for an hour by setting dstrace=!D60.

  After turning synchronization off, wait 5 to 15 minutes to allow the server to catch up with queued work. Cancel the test by setting dstrace=!E.

- **eDirectory errors.** To test for other errors, run SET dstrace=On.

Client Issues

- **Hung connections.** Check for them and clear them. See “Clearing a Workstation Connection” on page 92.
- **Client software.** You can identify client problems by changing SET NCP SET parameter. For more information, see NCP Parameters in *Utilities Reference*.

  By setting these server parameters to On, the server displays a warning each time a bad packet is received at the server. The warning message also includes the MAC (Media Access Control) addresses of devices where the packets originated.

  These parameters are in the NCP category:

  ```
  Display NCP Bad Component Warnings=On
  Reject NCP Packets With Bad Components=On
  Display NCP Bad Length Warnings=On
  Reject NCP Packets With Bad Length=On
  ```

  Update client software.
- **Cabling.** If you have installed high-speed 100 MB network boards, you might need to upgrade your cabling, too.

If the problem still occurs, follow the troubleshooting steps in “Using a Troubleshooting Methodology” on page 105; review tips in TID 10011512 “Troubleshooting High Utilization” (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10011512.htm); search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp) for High Utilization; and contact a Novell Support Provider.

Disk Errors

To resolve disk I/O, disk space, and mirroring problems, see the following sections:

- “Resolving General Server Disk I/O Errors” on page 133
- “Resolving Server Disk Space Problems” on page 133
- “Mirrored Partitions Do Not Remirror Automatically” on page 134
- “Mirroring Takes a Long Time” on page 134
- “Mirroring Stops Just Before It Is Finished” on page 135

Resolving General Server Disk I/O Errors

To resolve a general disk I/O error on the server, try one or more of the following remedies:

- Check the disk subsystems to make sure that the power is on and the cables are correctly connected between the controller and the subsystems.
- Make sure that the subsystem cables are terminated correctly.
- Make sure that the hardware and disks are installed correctly.
- Make sure that the current disk drivers loaded are certified for NetWare 6. Many drivers can be found on the *NetWare 6 Operating System* CD or on the master diskettes. Updated drivers might also be available from third-party disk driver manufacturers.
- Make sure that the interrupt parameters, I/O port settings, slot settings, etc., for the driver match those for the hardware. Also, make sure that the custom parameters have been set correctly for your hardware.
- Make sure all devices are recognized.
- Make sure that the device is visible and has a valid Hot Fix partition.

If you have tried all the preceding suggestions without success, contact your Novell Support Provider or the drive manufacturer.

Resolving Server Disk Space Problems

To resolve an insufficient disk space error, do one or more of the following:

- Delete unnecessary files and directories from the volume.
- Change the Minimum File Delete Wait Time SET parameter in your server's AUTOEXEC.NCF file equal to 0 so that files can be removed immediately rather than being retained in a salvageable state on the volume.
- Purge deleted files if they cannot be purged automatically. (The deleted files are using up directory table space.)
- Increase the volume size and/or add more disks to the volume.
- Increase the percentage of disk space that can be used by a directory.
- If the disk or volume does have space available, check the disk drives and disk channel to see if a failure has occurred.
- Delete NLM programs that you no longer use.

- Check and adjust or remove any volume restrictions placed upon users.
- Check the size of error or log files and delete any that are unnecessary.

Mirrored Partitions Do Not Remirror Automatically

When mirrored partitions become unsynchronized, they should resynchronize automatically. If partitions do not resynchronize, complete the following steps:

1. In ConsoleOne, browse and select the tree you want to manage, and then click the Partition Disk Management icon.
2. Enter the eDirectory tree and context and server information.
3. Click Properties > Media > Mirror > Resync.
4. If the partitions still do not resynchronize, you must re-create the mirrored set.

   4a. Determine which disk partition has the data you want to save and mirror.

   4b. Delete the other disk partitions.

   4c. Recreate new partitions in place of the ones you deleted.

   4d. Mirror the partition containing data to the new partitions.

   For information about mirroring, see Creating a Partition in the *Novell Storage Services Administration Guide*.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Mirroring Takes a Long Time

If partitions are very large, mirroring can sometimes take several hours to complete; this is normal. The following might help to speed the mirroring process:

- Make sure you are using the latest disk drivers.
- Make sure there are no problems related with the hard disks or drivers you are using.

  For known problems with specific hard disks or drivers, contact the drive vendor to ask if there are ways to speed drive mirroring. For example,

some drivers can be loaded with parameters that speed the mirroring process.

- Make sure the Enable Disk Read After Write Verify (Disk category) SET parameter is set to Off.

  Most disk drives provide their own form of read-after-write verification; therefore, NetWare's read-after-write-verify feature is not needed and can increase the time required to mirror partitions.

- If the Maximum Concurrent Disk Cache Writes (Traditional File System category) parameter is set at the default value or lower, try increasing the setting.

  IMPORTANT: Increasing the value too much can cause some disk controllers or drivers to fail. You must experiment to see if a larger value speeds the mirroring process.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Mirroring Stops Just Before It Is Finished

Sometimes, the mirroring process proceeds without error but stops at 99% completion. To troubleshoot the problem, do the following:

- Check whether any faulty disk blocks exist.

  If there are faulty disk blocks, troubleshoot and replace the disk if necessary.

- Make sure you are using the latest disk drivers.

- Make sure there are no problems related with the hard disks or drivers you are using.

  For known problems with specific hard disks or drivers, contact the drive vendor.

- If the Maximum Concurrent Disk Cache Writes (Traditional File System category) parameter is set at its highest value, try reducing the setting.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Resolving Disk Error Problems When a Traditional Volume Is Mounting

To diagnose problems when disk errors occur while a Traditional volume is mounting, identify whether the following conditions exist:

- The 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 server is turned off without the DOWN command.

To resolve problems when disk errors while a volume is mounting, do the following:

- Load MONITOR and check the status of the available cache buffers. If the cache buffers are fewer than 20%, add more memory to your server.
- Minor errors usually 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 might be corrected automatically by TTS™ (Transaction Tracking System™) software.

Resolving Server Memory Problems

To troubleshoot different kinds of server memory problems, to resolve memory leaks, and to resolve memory problems by freeing memory, see the following sections:

- "NetWare Doesn't Recognize All the Memory in the Server" on page 137
- "Server Displays Memory Error Messages" on page 141
- "Resolving Server Memory Leaks" on page 137
- "Freeing Server Memory Temporarily" on page 139
- "Resolving Memory Errors When a Traditional Volume Is Mounting" on page 140

NetWare Doesn't Recognize All the Memory in the Server

Use the following steps to find the source of the problem.

1. Verify whether you are using the NetWare memory manager or an external memory manager. Does CONFIG.SYS or AUTOEXEC.BAT include a DOS=HIGH statement or commands to load memory managers or DOS device drivers? For example, is there a command to load HIMEM.SYS or EMM386.EXE? Both are memory managers.

   Comment out these statements from CONFIG.SYS or delete CONFIG.SYS altogether. Comment out these statements from AUTOEXEC.BAT. (To comment out a command, type **REM** and a space at the beginning of the command line.)

   If there is a memory manager in the server, NetWare relies upon the memory manager to determine the amount of available memory instead of registering the memory itself. Some memory managers in older computers cannot recognize more than 64 MB of memory. DOS device drivers take memory away from NetWare's memory pool.

   Make sure Windows 95 is not being used to boot the server. Windows 95 autoloads memory managers.

2. Make sure the server BIOS is current.

   An out-of-date BIOS might be reporting the wrong amount of memory. If a newer version is available, update the BIOS.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Resolving Server Memory Leaks

A memory leak means that an NLM or set of NLM programs has requested memory from the server, but has not returned the memory when finished with it. Over time, the amount of available memory decreases until eventually the server generates memory error messages. The memory leak might be slow or fast depending on the amount of memory requested each time.

If you reboot the server, the memory is returned to the memory pool, and the low memory error messages stop temporarily, until the memory leak ties up enough memory to generate the error messages again.

To see if the server has a memory leak, restart the server and then monitor memory statistics (Total Cache Buffers) over time. When traffic hasn't increased and no new applications are installed on the server and the statistics change, use the following steps to find the source of the problem.

1. Load all the latest patches on the server.

   Server patches are available from Novell's Support Web Site (http://support.novell.com/misc/patlst.htm) and other locations. See "Applying Patches" on page 34 for a list of sources.

2. Restart the server to free memory and establish a baseline for memory use.

3. View the memory statistics for the module:

   3a. Access NetWare Remote Manager.

   3b. Click the List Modules in the navigation frame.

   3c. Sort the list for memory usage by clicking the Alloc Memory button.

   3d. Click the *value* link for allocated memory for each module name you suspect might be the source of the leak.

   Under normal conditions, modules such as SERVER.NLM, NSS.NLM and DS.NLM are usually at the top of the list.

   3e. Print this page and use it as a the baseline as you monitor the module's memory use over time.

4. Repeat Step 3 for each NLM you suspect might be the source of a memory leak.

5. (Conditional) If the memory error messages occur again, repeat Step 3 to view the memory statistics for each suspected NLM. Note whether memory use increased substantially for any of the modules.

   If there is a memory leak, one or more modules will show a large increase in the Bytes in Use value.

6. When you discover the source of the memory leak, contact the module vendor to tell them about the problem. If possible, update the module or remove the module from the server.

Freeing Server Memory Temporarily

To free server memory temporarily (until you can add more memory to the server), do one or more of the following:

- On traditional volumes, delete unused files and directories and purge them.
- Shorten the time period before deleted files are purged.
  - Lower the value of the Minimum File Delete Wait Time SET parameter (Common File System category).
  - Change the setting to On for the Immediate Purge of Deleted Files SET parameter (Common File System category).
- Unload any NLM, such as NWCONFIG, MONITOR, backup software, virus scanners, that is not currently needed.
- Dismount traditional volumes that are not being used and reduce the size or number of volumes that the server supports.
- Streamline the directory structure. Every subdirectory in the Traditional file system takes at least one directory block (by default, a 4 KB 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 then purge the deleted subdirectories and files, you will free up memory.
- Try converting volumes from the Traditional file system to the NSS file system. It requires less memory to mount NSS volumes. For procedures, see Converting Traditional Volumes to Logical Volumes in the *Novell Storage Services Administration Guide*.
- If you are using the Traditional file system, remove name space support.

  WARNING: This is a destructive step that destroys all the extended file information. Before taking this step, try to free up 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.

  To remove the name space, load VREPAIR, select Set VRepair Options and then select two options: Write All Directory and FAT Entries Out to Disk and Remove Name Space Support from the Volume. Then run VREPAIR > Repair a Volume on the volume that would not mount.

- As a last resort, back up all files in the volume, bring down the server, and reinitialize the volume. Specify a block size of 64 KB and turn the Block Suballocation option to Off.

  (This setting uses a lot of disk space but increases the amount of memory available.)

- Check the AUTOEXEC.BAT and CONFIG.SYS files to make sure no memory managers, such as HIMEM.SYS or EMM386.EXE, are being loaded and that there is no DOS=HIGH statement in either file. Make sure no DOS device drivers are being loaded.

- On NSS volumes, monitor and adjust the cache statistics. For more information, see Setting the Cache Buffers in the *Novell Storage Services Administration Guide*.

Resolving Memory Errors When a Traditional Volume Is Mounting

To diagnose problems when memory errors while a volume is mounting, identify whether the following conditions exist:

- Traditional 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).

- Traditional volumes and directory entries grow dynamically. Therefore, if your server is using most of the RAM (file cache buffers are close to 20% of the memory) and you dismount a volume, you might not be able to remount the volume unless additional memory is available.

- Each additional name space support that you add to a Traditional volume increases the size of the FATs and DETs. Adding name space support can cause the tables to grow so large that the server does not have enough RAM to mount the volume.

To resolve problems when memory errors while a volume is mounting, perform the following actions or ensure that the following conditions exist:

- Check the status of the available cache buffers. If the cache buffers are fewer than 20%, add more RAM to your server.

- Free up memory by unloading resources.

- Streamline the directory structure on Traditional volumes. Every subdirectory takes at least one directory block (by default, a 4 KB block of memory). Thus, 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 then purge the deleted subdirectories and files, you will free up memory.

- Calculate how much memory you need and add memory to the server.
- Note the Cache Buffers settings in the Server Memory Statistics.

  If the percentage is below 20%, add more memory.

- Remove the recently added name space support.

  WARNING: This is a destructive step that destroys all the extended file information. Before taking this step, try to free up 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 server's disk drivers. Dismount any mounted volumes.

  To remove the name space, load VREPAIR, select Set VRepair Options and select two options: Write All Directory and FAT Entries Out to Disk and Remove Name Space Support from the Volume. Then on the volume that would not mount, run VREPAIR, select Repair a Volume.

Server Displays Memory Error Messages

Typical memory error messages include the following:

- Cache memory allocator out of available memory
- Cache memory allocator out of available memory, size requested was *x* bites by *NLM_name*.
- Short term memory allocator is out of memory
- Cache memory allocator exceeded the minimum cache buffer limit

If any of these conditions exist, use the following steps to find the source of the problem:

1. Make sure the server is not loading a memory manager or a DOS device drivers.

   Check the AUTOEXE.BAT and CONFIG.SYS files to make sure no memory managers, such as HIMEM.SYS or EMM386.EXE, are being loaded, and that there is no DOS=HIGH statement in either file. Make sure no DOS device drivers are being loaded.

   Comment out these statements from CONFIG.SYS or delete CONFIG.SYS altogether. Comment out these statements from

AUTOEXEC.BAT. (To comment out a command, type **REM** and a space at the beginning of the command line.)

If there is a memory manager in the server, NetWare relies upon the memory manager to determine the amount of available memory instead of registering the memory itself. Some memory managers cannot recognize more than 64 MB of memory. DOS device drivers take memory away from NetWare's memory pool.

Make sure Windows 95 is not being used to boot the server. Windows 95 autoloads memory managers.

2. Make sure the server BIOS is current.

   An out-of-date BIOS might be reporting the wrong amount of memory. Update the BIOS if a newer version is available.

3. Verify that the setting for the Reserved Buffers Below 16 MB SET parameter (Memory category) is set at 300 or higher.

   For older drivers, increase the value to 300 or higher, especially if there is a CD-ROM or tape device that needs memory below 16 MB.

4. Make sure memory is being registered automatically.

   Manually registering memory can cause memory fragmentation. Some old system boards might require you to register memory manually, but the better solution is to upgrade to a newer board so that NetWare will register the memory automatically.

   If memory has been registered manually, reboot the server to free memory and do not manually register memory again. Upgrade the system board if necessary.

5. Verify whether memory errors occur when a traditional volume is mounting.

   If yes, the server might be low on memory.

   To free memory temporarily, see "Freeing Server Memory Temporarily" on page 139. To solve the problem, add more RAM.

6. Verify whether the "LRU sitting time" (in NetWare Remote Manager or MONITOR), average is more than 15 minutes during peak work hours.

   If no, the server might be low on memory.

   To free memory temporarily, see "Freeing Server Memory Temporarily" on page 139. To use the LRU Sitting Time to tune memory, see Tuning

File Cache in the *Server Memory Administration Guide*. To solve the problem, add more RAM.

7 Check for memory leaks.

Do the LRU Sitting Time and Long Term Cache Hits gradually decline over time, even when network traffic has not increased and no new applications have been installed on the server?

If yes, the server might have a memory leak. See "Resolving Server Memory Leaks" on page 137.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Resolving Locked Device Errors

To resolve a locked device error, try one or more of the following:

- Wait for a while (sometimes a few hours); the task in process might complete and free the device.
- Retry the action that resulted in the error.
- Delete all user connections and disable logins.
- For a disk device error, unload NLM programs (other than the device driver) that might be using the disk. Dismount all volumes on the disk.

If you have tried all of the above without success, contact a Novell Support Provider or the drive manufacturer.

Resolving Event Control Block Allocation Errors

Event control block allocation system messages can occur when you first start the server or after the server has been running for some time.

These messages indicate that the server was unable to acquire sufficient packet receive buffers, usually called event control blocks (ECBs). Running out of ECBs is not a fatal condition. However, it can indicate either a LAN or server problem.

Servers that run for several days where high loads occur in peaks might exceed the set maximum number of ECBs, causing the system to generate ECB system messages.

If these situations are caused by occasional peaks in the memory demand, you should probably maintain your current maximum ECB allocation and allow the message to be generated at those times.

Otherwise, if your server memory load is very high and you receive frequent ECB allocation errors, try setting your maximum ECB allocation higher. Use the following SET command in the STARTUP.NCF file:

SET MAXIMUM PACKET RECEIVE BUFFERS=*number*

Memory allocated for ECBs cannot be used for other purposes.

The minimum number of buffers available for the server can also be set in the STARTUP.NCF file with the following command:

SET MINIMUM PACKET RECEIVE BUFFERS=*number*

Resolving Server Console Command Problems

To diagnose server console command problems, identify whether the following conditions exist:

- Some SET parameters can only be set in the STARTUP.NCF file.
- You are not at the System Console screen prompt. Press Alt+Esc to toggle through the screens.
- The server has been shut down.
- The server has failed (hung).
- The SERVER.EXE file is corrupted.
- The network operating system has been configured incorrectly.

To resolve server console command problems, do the following:

- Enter the SET parameter in the STARTUP.NCF file and then shut down and restart the server.
- Make sure that all cables are fastened securely to all network boards and network connectors. Make sure that terminating resistors are installed correctly.
- From a backup, or from the *NetWare 6 Operating System* CD, copy a new version of SERVER.EXE to the server boot directory. Have all users close their files and log out.

  Shut down the server, if possible. If not, wait a few minutes after all users have logged out, and then reboot the server.

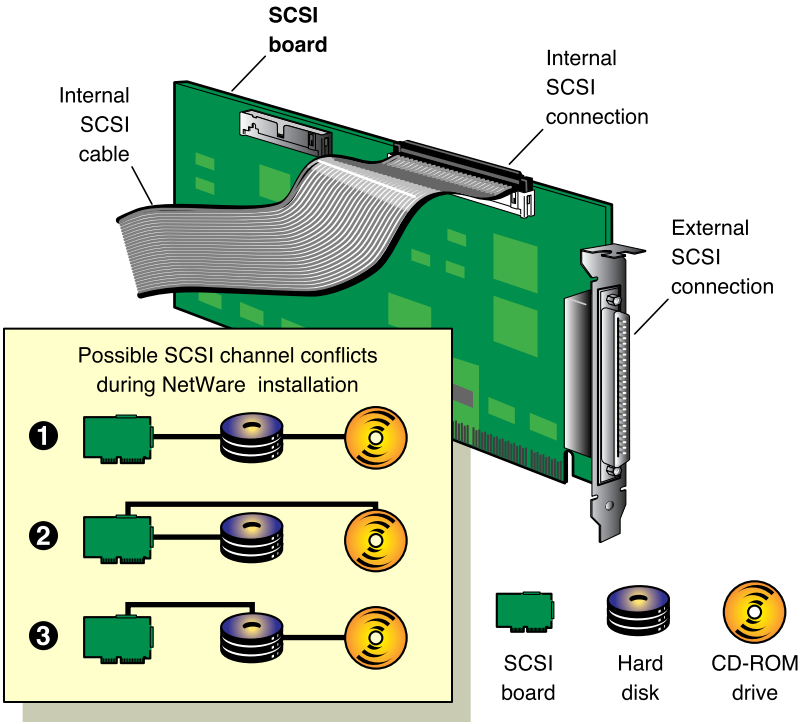
- Check the hardware configuration on each network board in the server to make sure that the configuration is correct.
- If you recorded network board configurations and they do not agree with the actual hardware configurations, reload the LAN driver with the correct parameters or change the hardware settings to match the LAN driver parameters.
- Check all network board settings for possible interrupt and I/O port conflicts. The server can boot up initially even if the interrupt on a network board is set incorrectly.

  The most common conflict occurs when a network board is set to interrupt 4 and a printer is connected to the server's serial port, which also uses interrupt 4.
- Run a virus scan on the DOS partition.

Resolving Keyboard Locking Problems When Copying Files from CD-ROM

To diagnose keyboard locking problems when copying files from CD-ROM, identify whether the following conditions exist.

If you have a CD-ROM device that shares a SCSI bus with a disk subsystem containing volumes that network operating system installation files are copied to (typically volume SYS:), your keyboard might lock while loading drivers or copying files to the volume. The following figure shows possible configuration conflicts.



Remove the CD-ROM device drivers that you used to set up the CD-ROM drive as a DOS device from your CONFIG.SYS file. This will avoid possible conflicts when the *Operating System* CD is mounted as a NetWare volume.

To resolve keyboard locking problems when copying files from the CD, use the following procedure:

1. Press Alt+Esc until you are at the console prompt.
2. Enter **DOWN**.
3. Using a text editor, remove the CD-ROM device drivers from your CONFIG.SYS file.
4. Save the updated CONFIG.SYS file.
5. Using a text editor, remove any references to the CD-ROM drivers from your AUTOEXEC.BAT file.
6. Save the updated AUTOEXEC.BAT file.
7. Reboot the server by pressing Ctrl+Alt+Del.

8. (Conditional) If the server doesn't boot automatically from the AUTOEXEC.BAT file, change to the subdirectory where the SERVER.EXE file and other boot files are located (the default is C:\NWSERVER), and enter the following at the DOS prompt:

   SERVER

9. (Conditional) If you are using ASPI device drivers (for example, for an Adaptec* controller), you need to enter one of the following commands:

   AHA*xxxx*

   where *xxxx* specifies the Adaptec board number

   or

   ASPICD

   or

   CDNASPI

10. At the console prompt, enter **NWPA**.

11. (Optional) At the console prompt, enter **CD DEVICE LIST**.

    A list appears with numbers associated with all the devices on your network. Determine which number is the volume number.

12. At the console prompt, enter

    CD9660.NSS
    CD MOUNT *volume_name|number*

13. At the console prompt, enter **NWCONFIG**.

Monitoring and Resolving Communication Problems

Problems that occur with networking can originate for any of several reasons: corrupted hardware or software, bad links, not enough memory, etc.

The following are tips for solving network communication problems.

- Check all hubs and repeaters to make sure that they are on.
- Check concentrators and look for flashing yellow lights that indicate collisions.
- Make sure that all routers are functioning properly and have enough memory. A router with insufficient memory becomes the weak link in the chain and can slow down an entire LAN.

- Check the cables for proper termination. Make sure that cables are not running close to sources of interference.
- Make sure that the server network board is seated properly and is initializing.
- Make sure that a protocol is bound to each board and check the configuration of the network boards. Then shut down the server, turn off the power, and check the actual network board settings:
  - Make sure that 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 that the node address on the board is a legal address. (Addresses 0 and FFFFFFFFFFFF are reserved; do not use them.)
  - Make sure that the memory range for the I/O ports and memory addresses do not overlap. If there are conflicts, reconfigure the equipment so that no conflicts exist.
- Make sure that network boards do not conflict with other boards, the monitor board, or ports in the server. Make sure that no two pieces of hardware are using the same I/O port, interrupt, or memory address. Avoid interrupts 2, 9, and 15.
- Make sure that the network board works correctly; replace it if it doesn't. Check the lists of certified products at Novell Solutions Search (http://developer.novell.com/solutions). In the Hardware Category, select LAN adapters or WAN adapters to make sure that the adapter works with NetWare. Make sure that drivers are the latest versions.
- Run VOLUMES at the server console. If volume SYS: is not mounted, mount it. The server does not broadcast to the network until volume SYS: is mounted.
- Check workstation addresses and server node numbers.

  Each node address on the network should be unique. Sometimes you can find the problem by turning off all workstations and then turning them back on one at a time.
- Make sure that workstations are using the correct frame type.
- Have a user log in to the network from a workstation. In NetWare Remote Manager, click the Connections link in the navigation frame.

  If the Connections list shows the user's login name, the server is receiving and responding to the workstation's request.

If the workstation receives a “Server cannot be found” error, make sure that the server and workstation are using the same frame type.

If using 10baseT, try using a cross-cable to connect the server directly to the workstation. If this solves the communication problem between the server and workstation, then something on the network is causing the problem.

Suspected Multiprocessing Problems

If you suspect a multiprocessing problem, complete the following steps. You will be able to eliminate most probable causes.

1. Make sure the secondary processors are functioning properly.

   If the server is already up, stop all processors except Processor 0. In NetWare Remote Manager, click the Processor link in the navigation frame. Click the Stop Processor link for each processor online except processor 0. (Processor 0 cannot not be taken offline.)

   If the server is down, bring up the server and then stop all processors.

   If the problem still occurs, go to Step 2. If not, go to Step 4.

2. To verify that this is *not* an interrupt issue, remove the PSM. Then reboot the server; only processor 0 will start.

   The MPS14.PSM, CPQMPK.PSM or *.PSM in the STARTUP.NCF file is the interrupt abstraction layer and communicates with the APIC (Advanced Programmable Interrupt Controller) rather than the PIC for interrupt handing in the machine.

   If the problem still occurs, it *not* a multiprocessing issue. If it no longer occurs, go to Step 3.

3. Make sure you have the latest machine updates (current ROM BIOS, etc.).

   If you confirm that your hardware is current and the problem still occurs, it’s possible that you are using a new version that wasn’t available at the time NetWare 6 was released. Whatever is different about the hardware requires a newer PSM to work with the machine.

   HINT: Problems that occur only in a multiprocessing environments are not necessarily MP problems. More likely, it is an issue with a piece that has been loaded in an MP environment and that does not function properly.

4. Gather information as explained in "Using a Troubleshooting Methodology" on page 105. View the STARTUP.NCF and AUTOEXEC.NCF to determine what software pieces are running. Check with the software vendors and developers and tell them what steps you have taken and give them enough information to duplicate the problem.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Unable to Communicate with Server, -625 Errors

Communication problems among servers can generate messages such as Unable to Communicate with Server or messages that a directory partition operation can't be completed. If DSTRACE is set to on, -625 errors appear in the DSTRACE output because the directory cannot be synchronized among the servers.

Use the following steps to troubleshoot server-to-server communication problems.

1. Make sure the server is up and can been seen on the network.

   If the server is down, restart it.

   If the server has abended, troubleshoot the abend. See "Resolving Abends" on page 116.

2. Make sure the server's time is synchronized to the network.

   To see if server time is synchronized to the network, enter **TIME** at the System Console prompt.

   If time is not synchronized, troubleshoot the time synchronization problem. For general information about time synchronization, see *Network Time Management Administration Guide*.

3. Make sure the IPX™ internal network number of the server unique and the IP addresses unique. Make sure all replicas have the correct address for each server.

   If all the servers in a replica ring cannot communicate with one of the servers in the ring, there is probably an address problem.

   Make sure all addresses are unique. Make sure all replicas have the correct address for each server. Load DSREPAIR, select Advanced

Options > Replica and Partition Operations > *replica* > Display Replica Information.

4. Make sure all replicas have the correct server name.

   Incorrect or duplicate server names in directory replicas make it impossible to communicate with the server. Make sure all replicas have the correct name for each server. Load DSREPAIR, select Advanced Options > Replica and Partition Operations > *replica* > Display Replica Information.

   If names are not correct, contact a Novell Support Provider for assistance in renaming servers.

5. If the servers share the same cabling system, make sure addresses are unique for each cable segment.

   If addresses are not unique, change addresses as necessary.

6. Make sure all LAN drivers are loaded and protocols are bound. Make sure all LAN adapters and drivers are the latest versions.

   Load and bind LAN drivers, if necessary. If drivers are not the latest versions, update the drivers. In addition, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp) for known problems with specific adapters. Replace adapters if necessary.

7. Make sure the LAN is functioning.

   Ping the servers to see if the connection is active. View LAN statistics using NetWare Remote Manager or MONITOR to make sure packets are being sent and received. Review statistics such as packets received and sent, collisions, and retries.

   If the LAN connection is malfunctioning, troubleshoot the physical link between the servers. See “Tips for Resolving General Communication Problems” on page 156.

8. Make sure the routers have enough memory to handle the increase in packets.

   If your servers have just been upgraded from NetWare 3, some routers might not have enough memory to buffer the increase in packets from NetWare 3 to NetWare 4, 5, or 6 servers. Make sure the routers have enough memory.

9. Remove routing filters.

   If the servers are using IPX and the routers are filtering SAP types 004, 26b, and 278 packets, remove the filters.

10 If you are using IPX, reset the server's internal IPX router.

Use the RESET ROUTER command at the System Console prompt to reset the server's internal IPX router. Troubleshoot other routers.

11 Make sure data can transfer over WAN links.

- Are servers separated by 56 KB WAN links?
- If yes, this could be the source of the problem. Consider the following:
- Is there a guaranteed transfer rate or does the rate decline when network traffic is heavy? If the rate declines, the link might not provide the performance you need to maintain consistent communication.

Are you trying to transfer large files or an entire replica across the link? You might be able to synchronize replicas across a 56 KB link, but not transfer an entire replica.

Do the servers have to traverse more than one 56 KB link?

To solve the problem, you might need to provide faster links.

12 Make sure server utilization is not high.

Do the affected servers have utilization at or close to 100%?

If yes, take steps to reduce server utilization. See "High Utilization Statistics" on page 125.

13 Make sure the eDirectory database is not locked.

If DSREPAIR is running, the eDirectory database will be locked. Other applications might also lock the database while writing to it.

If the database is locked, wait for DSREPAIR or other modules to finish using the database or shut down the utility or module.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Workstations Can't Communicate with Server

To troubleshoot different kinds of workstation to server problems, see the following sections:

- "Errors Reading from and Writing to Network, Server Cannot Be Found Errors" on page 153.
- "Connections Dropped Periodically" on page 156.
- "Tips for Resolving General Communication Problems" on page 156.

Errors Reading from and Writing to Network, Server Cannot Be Found Errors

When workstations can't communicate with the server, users lose their connections to the server or cannot log in at all. Users might see Server Cannot Be Found messages or errors about reading from or writing to the network.

Follow these steps to troubleshoot the problem.

1. Make sure other clients can connect to the server.

   If other clients can connect to the server, then the problem is with this client, not with the server or network. Consider the following:

   - If the user cannot log in, did the user power off without logging out?

     If the user powers off without logging out, the client connection remains open and the user cannot to log in again until the connection is cleared. The server's watchdog process retries the connection a designated number of times, and then the connection times out and the server clears the connection. After the connection is cleared, the user can log in again.

     Watchdog processes are controlled by Watchdog (Communications category) SET parameters.

   - Has the user's password expired?

     Sometimes users don't understand that they *must* change their passwords before they use up their grace logins.

   - Are there other restrictions on the user account, such as time periods when the user is not allowed to log in? Check the user's properties.
   - Has intruder lockout been activated?
   - Is the workstation LAN cable functioning?

2 Check whether the server has had an abend.

If the server has had an abend, it displays an abend message on the System Console screen. If the abend auto recovery process restarted the server, the message might have scrolled off the screen. Check the ABEND.LOG log file in SYS:SYSTEM to read the message.

To troubleshoot a server abend, see "Resolving Abends" on page 116. For general information about types of server abends, see "Understanding What Happens When You Get an Abend" on page 116. To manage the abend auto recovery process, see "Responding to the Abend Automatically" on page 120.

3 Verify whether the server console has hung.

If you cannot enter commands at the System Console prompt, then the console is hung. In some cases, you won't be able to toggle among server screens.

Try pressing Ctrl+Alt+Esc. This should display a prompt to shut down the file server and exit to DOS. If the prompt is not displayed, try entering the debugger by pressing Shift+Shift+Alt+Esc. If you can enter the debugger, type **q** and press Enter to exit to DOS. Then reboot the server. See "Server Console Hangs" on page 124 to troubleshoot the problem.

If neither of the commands just described works, the only way to exit the server is to force a nonmaskable interrupt (NMI) error. Contact a Novell Support Provider or your computer hardware vendor for assistance.

If you do not have time to obtain the assistance to generate an NMI, you can power off the server, but this can corrupt operating system files. Try this measure at your own risk.

4 Verify that volume SYS: is mounted.

Enter **VOLUMES** at the System Console prompt to display a list of mounted volumes. If volume SYS: is not mounted, mount it. The server does not broadcast to the network until volume SYS: is mounted.

5 Make sure no LAN problems exist.

In NetWare Remote Manager, click the Health Monitor link in the navigation frame, and then click the LAN Traffic link in the Description column of the Server Health Monitoring page.

View LAN driver statistics to see if packets are being lost or if there are excessive collisions or retries. To do this in NetWare Remote Manager,

click the Disk / LAN Adapters link in the navigation frame, and then click the name link for each of the network boards in your server.

For tips on troubleshooting communications problems, see "Tips for Resolving General Communication Problems" on page 156

If necessary, use LANalyzer® or a similar product to monitor network traffic and isolate the problem.

6 Make sure server utilization is normal.

Check utilization statistics. For help in responding to high utilization, see "High Utilization Statistics" on page 125.

If you suspect heavy LAN traffic is causing the problem, try unplugging the LAN cable. If heavy LAN traffic was the problem, utilization should drop.

7 Make sure the server has sufficient resources.

Is the server receiving No ECB Available Count messages or messages about insufficient packet receive buffers?

These messages could indicate that the server is running out of resources. For help in resolving these errors, see "Insufficient Packet Receive Buffers, No ECB Available Count Errors" on page 121.

8 Make sure the eDirectory database is functioning.

Is the eDirectory database closed or locked by another utility, such as DSREPAIR?

If the eDirectory database is not functioning, the workstation clients will not display the login screen.

9 Check for -625 or other communication errors at the server.

Are servers receiving -625 or other communication errors?

If so, see "Unable to Communicate with Server, -625 Errors" on page 150 or see the online documentation Novell Error Codes (http://www.novell.com/documentation/lg/nwec/docui/index.html) > NDS or eDirectory Error Codes.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Connections Dropped Periodically

Follow these steps to troubleshoot the problem:

1. Make sure server utilization is normal.

   Check utilization statistics. For help in responding to high utilization, see "High Utilization Statistics" on page 125.

2. If users are using old Novell clients, upgrade them to the newest version of the applicable Novell client.

3. Make sure the node number for each workstation is unique.

4. Make sure all network boards in the server and user's workstations are working properly and are using the latest boards and drivers.

   Check Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp) for any known problems with your drivers and boards, update drivers, and replace boards if necessary.

5. Check all cables to make sure they are firmly connected, terminated correctly, and not running near any equipment that might cause interference.

If the problem still occurs, follow the troubleshooting steps in "Using a Troubleshooting Methodology" on page 105, search the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp), and contact a Novell Support Provider.

Tips for Resolving General Communication Problems

To resolve general network communication problems, do the following:

- Check all hubs and repeaters to make sure they are on. Check concentrators and look for flashing yellow lights that indicate collisions.
- Make sure all routers are functioning properly and have enough memory. A router with insufficient memory becomes the weak link in the chain and can slow down an entire LAN.
- Check the cables for proper termination. Make sure cables are not running close to sources of interference.

- Make sure the server network adapter is seated properly and is initializing. Then bring down the 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 address on the board is a legal address. (Addresses 0 and FFFFFFFFFFFF are reserved; do not use them.)
  - Make sure that the memory range for the I/O ports and memory addresses do not overlap. If there are conflicts, reconfigure the equipment so that no conflicts exist.
- Make sure that adapters do not conflict with other boards, the monitor board, or ports in the server. Make sure no two pieces of hardware are using the same I/O port, interrupt, or memory address. Avoid interrupts 2, 9, and 15.
- Make sure the network adapter works correctly; replace it if it doesn't. Make sure drivers are the latest versions. Check the lists of certified products at Novell Solutions Search (http://developer.novell.com/solutions). In the Hardware Category, select LAN adapters or WAN adapters to make sure that the adapter works with NetWare. Make sure that drivers are the latest versions.
- Run VOLUMES at the server console. If volume SYS: is not mounted, mount it. The server does not broadcast to the network until volume SYS: is mounted.
- Check workstation addresses and server node numbers.

  Each node address on the network should be unique. Sometimes you can find the problem by turning off all workstations and then turning them back on one at a time.
- Make sure workstations are using the correct frame type.
- Have a user log in to the network from a workstation. In NetWare Remote Manager, click the Connections link in the navigation frame.

  If the Connections list shows the user's login name, the server is receiving and responding to the workstation's request.

  If the workstation receives a Server Cannot Be Found error, make sure the server and workstation are using the same frame type.

If using 10baseT, try using a cross-cable to connect the server directly to the workstation. If this solves the communication problem between the server and workstation, then something on the network is causing the problem.

Admin Account Has Been Deleted or Admin Password Is Unknown

There is only one solution when the Admin account has been deleted or the Admin password has been lost: contact a Novell Support Provider for assistance.

To avoid losing the Admin account, we recommend that you create one or more additional user accounts with the same privileges as the Admin account.

IMPORTANT: Do not assign privileges to the additional accounts by setting up security equivalence with Admin. The accounts will lose security equivalence if Admin is deleted.

Preventive Maintenance Tasks

The following sections provide tips for preventing server problems:

- "Monitoring the NetWare Server" on page 82
- "Matching Performance Capabilities" on page 34
- "Preventing Memory Problems" on page 101
- "Preventing Power Supply Errors" on page 101
- "Preventing Static Electricity Problems" on page 102
- Preventing Cabling Problems in the *Server Communications Administration Guide*
- "Documenting the Network" on page 99