Novell NetWare® 6

www.novell.com

SERVER MEMORY
ADMINISTRATION GUIDE

Novell®

Legal Notices

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

www.novell.com

Server Memory Administration Guide
October 2001
103-000147-001

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

Novell Trademarks

eDirectory is a trademark of Novell, Inc.

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

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

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

Novell Storage Services is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

Server Memory Administration Guide

Welcome to the *Server Memory Administration Guide*. This documentation contains the following information:

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 Understanding Server Memory

The NetWare® server operating system provides increased memory efficiency with three important features: logical memory addressing, virtual memory, and protected memory. The following information is a general introduction to these and other aspects of NetWare's memory architecture.

Introduction to NetWare Memory

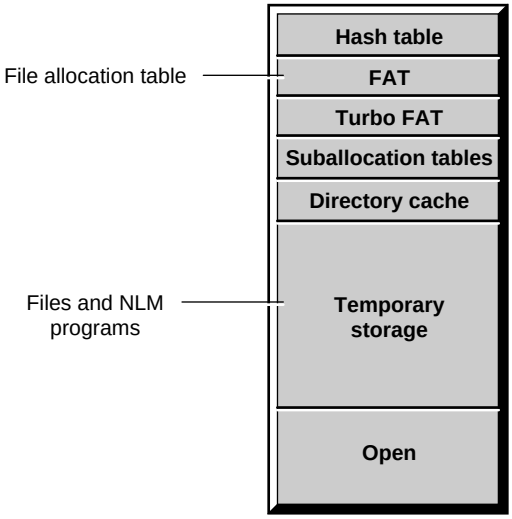
NetWare 6 requires a minimum of 256 MB of RAM and can access up to 64 GB of RAM. After the SERVER.EXE file is loaded, all remaining memory is assigned to cache memory and Virtual memory, which is available for NetWare Loadable Module™ (NLM™) programs and other processes to use. The memory allocator will only allocate up to 4 GB of memory to cache memory and the remaining will be using by the virtual memory system. When data is stored in cache, it is stored in 4 KB blocks called cache buffers.

Recently used data is kept in cache buffers in case it is needed again. Caching data speeds processing because data can be written to or read from cache hundreds of times faster than it can be read from or written to disk.

Cache memory is used for all the server's processing needs, such as the following:

- Storing volumes' File Allocation Tables (FAT) and suballocation tables
- Storing volumes' directory entry tables

- Storing data files for users
- Storing NLM programs, such as LAN drivers, disk drivers, and management utilities
- Building hash tables for directory names
- Creating protected address spaces
- Allocated memory used by NLM programs



Memory from cache is allocated to an NLM program when requested. When an NLM program is finished using the memory, it releases the memory and returns it to cache. NetWare also provides a garbage collection process to recover unused memory. The garbage collector runs in the background, but you can manually initiate the process if needed. See "Optimizing Garbage Collection" on page 31.

Directory Cache Buffers and File Cache Buffers

There are two kinds of cache: directory cache and file cache.

Directory cache is used only with the traditional NetWare file system, not with the Novell® Storage Services™ (NSS) file system. Directory cache stores disk directory entries. When the server is first installed, NetWare allocates 20 directory cache buffers of 4 KB each. If more buffers are needed, NetWare tunes the server by increasing the number of directory cache buffers. You can

also tune the number of directory cache buffers yourself, using two server parameters that establish the minimum and maximum number of directory cache buffers the server can allocate. For information about tuning directory cache, see “Tuning Directory Cache for the Traditional File System” on page 24.

File cache is used with both the traditional file system and the NSS file system. File cache is a pool of 4 KB memory pages. File cache stores recently used file data and also parts of the Novell eDirectory™ database.

In an ideal environment, there is enough memory so that all frequently used data can be retrieved from file cache rather than from disk.

Monitoring the disk cache utilization statistic can help you estimate whether your server has sufficient memory to service requests from cache. For information about optimizing file cache, see “Tuning File Cache” on page 20.

Logical Memory Addressing

The physical memory of the server is divided into 4 KB blocks, called pages. When a NLM program wants to store information in memory, it requests memory pages that are contiguous, so that all the information can be stored in a sequential group of pages.

As contiguous blocks of memory pages are allocated and then made free, small segments of memory are often left over. After a while, there are many such isolated pieces of memory too small to be used. This situation is called memory fragmentation. When memory is fragmented, the server often cannot satisfy memory requests even when a lot of memory is available.

NetWare's logical memory addressing scheme helps to prevent memory fragmentation. The memory management subsystem provides a logical space manager that lists logical memory addresses from 0 to 4 GB. The logical space manager lists addresses up to 4 GB even if the server contains only the minimum 256 MB of RAM.

When an NLM program needs a contiguous block of memory, the operating system finds a set of logical, contiguous addresses in the logical space. Because table has so many logical addresses (4 GB), the operating system can almost always find the contiguous logical memory addresses the NLM program needs. Then the operating system allocates physical memory which might or might not be contiguous. The operating system then binds the logical addresses to the physical addresses.

Protected Address Spaces

Portions of the logical address space are set aside for protected address spaces (sometimes called user address spaces or ring 3). This protected address space is a portion of the logical address space that has carefully controlled interaction with the server operating system. All protected address spaces use virtual memory. For general information about virtual memory, see “Virtual Memory” on page 14.

A key benefit is that you can use protected address spaces to take advantage of virtual memory or to run untried or troublesome applications. Because any modules loaded into a protected address space can't corrupt the operating system or cause server abends, the protected address space provides a safe place to run applications.

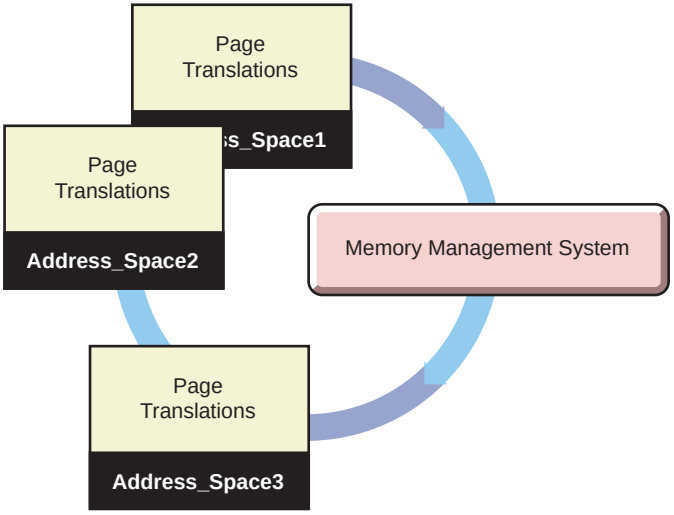
The operating system address space (ring 0) is sometimes called the OS address space or the kernel address space. The memory protection marshalling layer, in conjunction with the memory protection subsystem, prevents modules in a protected address space from having direct access to anything outside the address space. In particular, the memory protection marshalling layer serves as the interface between the protected address spaces and the server operating system. These layers prevent NLM programs in protected spaces from making calls or passing parameters to the operating system that would corrupt or fault the core operating system.

You can load modules into a protected address space, unload modules from a space, delete a space, or kill a space. See “Using Protected Address Spaces” on page 34 and “Loading Protected Address Spaces” on page 35.

Protected Address Spaces and Logical Memory Addressing

Each protected address space has its own set of page translations to provide logical memory addressing. The memory management subsystem ensures that the page translations of each protected address space refers to a different set of physical memory addresses.

Only one set of translations is visible in the memory management subsystem at a time. When there is more than one protected address space, the memory management subsystem loads one set of page translations for a specified time and then replaces it with another.



Replacing visible page translations is part of a context switch. Context switches take place when the NetWare kernel changes from running one thread to running another thread.

Modules Not Allowed in Protected Address Spaces

The following NLM programs and executables cannot be loaded into a protected space:

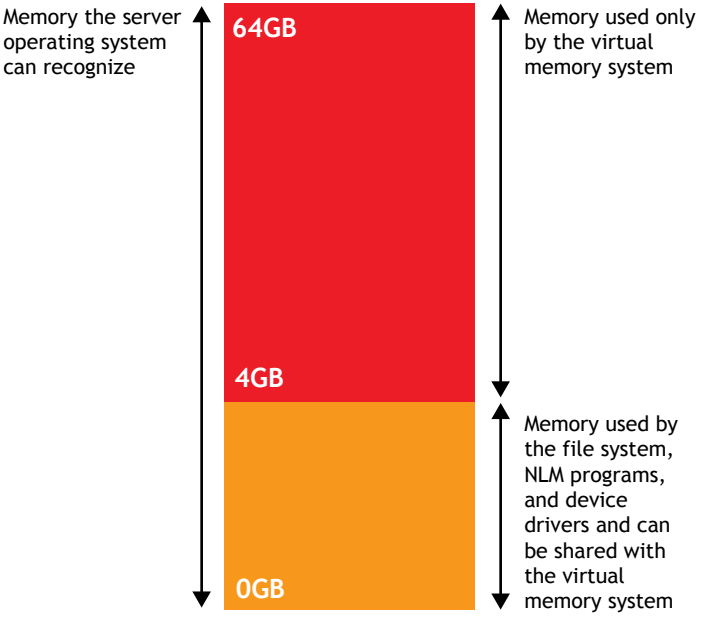
- SERVER.EXE
- LAN and disk drivers

  Hardware and LAN drivers make calls to the operating system and the processor that are not allowed from the protected address spaces.
- MONITOR

  MONITOR makes calls to the operating system that are not allowed from protected address spaces.
- Modules that use interrupt time processing
- Modules that use direct operating system interfaces
- Modules that import operating system data items
- Other modules or applications that aren't designed to run in protected address spaces

Virtual Memory

NetWare also provides a virtual memory system that swaps little-used data to disk, thereby freeing memory for more frequently used data. Applications that run in protected address spaces use virtual memory, as does Java*. The following illustration shows the amount memory the server can recognize and what portions the virtual memory system uses.



Virtual memory provides more efficient use of memory and lessens the likelihood that low memory conditions will cause problems with the server. Server operating system modules do not use virtual memory, because their execution cannot be interrupted except at certain locations in these modules.

A periodic aging process assesses available memory to see which data has been used less recently than the rest. Data that has not been used for some time can be moved from memory to disk, thereby freeing memory for other uses.

When the data on disk is needed again, it is moved back into available memory. Because data is swapped in and out of the disk, the available memory can be used for a larger amount of data than its actual physical capacity would allow.

The memory management subsystem assesses the memory needs of all server and NLM processes and determines where the freed memory should be used.

The Java Virtual Machine and any modules that are loaded into protected address spaces use virtual memory. Both the modules and the data they access are subject to being swapped to disk.

When data is moved from memory to disk, it is stored in a swap file. You can create one swap file for each NetWare volume. A swap file is created for volume SYS: by default.

To create a swap file, delete a swap file, change swap file parameters, or view information about the swap file, you can use NetWare Remote Manager, MONITOR, or the SWAP command at the System Console prompt. See "Using Virtual Memory" on page 26.

Swapping the data between memory and disk requires additional system resources, but it increases the memory available for use. The availability of the additional memory can improve overall server performance.

2 Optimizing Server Memory

This chapter includes information for completing the following tasks:

Assessing Server RAM

Insufficient physical memory (RAM) in the server is a common cause of a slow network. To determine whether your server has sufficient physical memory installed, check the amount of server memory currently available for disk cache.

In NetWare Remote Manager

1. Click the Health Monitor link in the navigation frame and view the Available Memory status and values.
2. If the status is Suspect or Bad, view the System Memory Information page to determine the source of the problem. View the System Memory Information by clicking the Available Memory link on the Server Health Monitoring page or clicking the View Memory Config link in the navigation frame.

In MONITOR

1. View the General Information window and note the percentage for the Long Term Cache Hits.
2. If the percentage of Long Term Cache Hits falls below 90 percent, add more RAM to the server.

   HINT: If you are unable to add more RAM now, a short-term fix can help. We suggest unloading unneeded NLM™ programs or removing DOS from memory. Remember that these actions treat symptoms only and are not long-term solutions.

Ensuring That Devices Can Access Memory

Some older network boards, such as many ISA and MCA devices, cannot access memory above 16 MB. To make sure these devices have enough memory below 16 MB, make sure that the following SET command is in the STARTUP.NCF file:

```
SET RESERVED BUFFERS BELOW 16 MEG = 300
```

The default number of buffers is 300. If necessary, you can increase the value, but remember that too many reserved buffers can prevent large volumes from mounting. As soon as possible, upgrade the system to a newer board that can access higher memory. For a discussion of network bottlenecks, see Matching Performance Capabilities in the *Server Operating System Administration Guide*.

NetWare® automatically registers memory above 16 MB so the memory can be recognized by EISA and PCI machines. If memory above 16 MB isn't being recognized, you can register memory manually using the REGISTER MEMORY command. For more information, see REGISTER MEMORY in *Utilities Reference*.

IMPORTANT: Use the REGISTER MEMORY command only if absolutely necessary. Manually registering memory can cause memory fragmentation problems. Ideally, you should upgrade the system board so that the NetWare® automatic memory registration will work.

Determining Which Processes Use Too Much Memory

To determine which NLM programs are using excessive amounts of memory, do the following.

In NetWare Remote Monitor

1. Click the List Modules link in the navigation frame.
2. Sort the list by allocated memory usage by clicking the Alloc Memory button in the table.

   NOTE: SERVER.NLM and NSS.NLM will always be high memory users.
3. View the Allocation Summary page for each NLM that is listed at the top of the list by clicking the Alloc Memory value link for each NLM.

   If the corruption count is anything larger than 0 in the Memory Allocation Summary L!=P list, the NLM might have a memory leak.

In MONITOR

1. From the Available Options menu, select Loaded Modules.
2. Select a module from the list to display its information and statistics in the upper window.
3. Press Tab to expand and activate the Module Information window.
4. Check the module's Allocated Memory.

   The information includes bytes of memory required to load, allocated memory bytes in use, percent of memory in use, allocated memory bytes free, percent of memory free, and the module's load flags. Press F1 for a description of these statistics.
5. Press Tab to return to the list of loaded modules.
6. Check the memory statistics for other modules.
7. (Optional) Press F4 to free memory allocated for a selected module.

   Remember that the memory recovery operation also uses memory.

Tuning Server Memory

NetWare is a self-tuning operating system; however, there are some things you can do to adjust the server's memory subsystem (as well as other aspects of server operation) to fine tune its performance.

Before attempting to tune a new server's memory, let the server operate at full capacity for a week or two to allow NetWare to self-tune. After the server settles in to a predictable pattern of daily use, you can begin to fine-tune the server's memory as described in the following sections.

- "Tuning File Cache" on page 20
- "Tuning Directory Cache for the Traditional File System" on page 24

Tuning File Cache

File cache not only speeds access to file data, it is used to cache portions of the Novell eDirectory™ database. If you want to tune your NetWare server in general, or eDirectory in particular, tune the file cache.

Novell Storage Services File System

In NetWare 6, the Novell Storage Services™ (NSS) is loaded on the server by default, but cache memory is not allocated to it unless it is actually running. NSS uses memory differently that the traditional file system and you must use specific parameters for tuning your server when using NSS.

To view statistics for cache buffers used by NSS, enter the following command at the System Console prompt:

```
nss /cachestats
```

For heavy access on an NSS logical volume, the server might incur some performance issues. NSS has its own caching and parameters to be set during the loading of the NSS modules. The following are several SET parameters that you can use to tune the performance of NSS:

- **Cachebalance** controls how much memory is available for NSS to use for cache. The cachebalance percentage determines how many cache blocks NSS will take from the traditional file system for its own cache. A high cache balance percentage will impede the performance of the traditional file system. A low cache balance will impede the preformance of NSS. We recommend that you set the cache balance parmeter to equal the percentage of the total disk space you allocate for NSS. The default is

60 percent. If you are using mostly NSS volumes, you can run at a much higher percentage, such as 85 to 90 percent.

- **Closefilecachesize** dictates how many closed files are kept in cache. The recommended minimum is 50,000.
- **Fileflushtimer and Bufferflushtimer** Increasing these parameters from their defaults helps the caching up to a certain point, but too much increase causes a *throttling* problem with writing out the metadata. This is somewhat dependent on processor speed and disk speed, so you could try adjusting them for your system. If NSS performance is very poor, 75 might be too high and you could try 50. If performance is just below normal, you could try increasing the values a little.

To activate these parameters, you can issue the following command at the startup of NSS, or place it in the AUTOEXEC.NCF file:

```
nss /cachebalance=80 /fileflushtimer=75 /bufferflushtimer=75
/closedfilecachesize=50000
```

For more information on setting Cache Buffers for NSS, see Setting the Cache Buffers in the *Novell Storage Services Administration Guide*.

Traditional File System

Because it is much faster to get data from memory than to get it from disk, caching frequently requested data increases server performance. The more RAM installed in the server, the more cache memory is available. Cache hits occur when a client requests data and the server supplies the data from cache memory instead of from disk. The least recently used algorithm determines whether data is kept in cache memory or written to disk.

File cache buffers are organized into a linked list. Most recently used (MRU) buffers are at the head of the list and least recently used (LRU) buffers are at the tail of the list. The length of time the oldest buffer has been in the list is shown as the LRU Sitting Time statistic.

In tuning file cache for the traditional file system, the goal is to determine how much memory the server needs so that recently accessed data can always be retrieved from cache. Monitoring the LRU Sitting Time statistic is key to tuning file cache.

Understanding LRU Sitting Time

The LRU Sitting Time status is updated and displayed once per second. The statistic is calculated by taking the difference between the current time and the

time stamp of the last block in the cache list. (The time stamp is the time at which the last block entered the list.) The result is displayed in HH:MM:SS.0 format. The LRU Sitting Time measures the length of time it takes for a cache buffer at the head of the list to make its way down to the tail, where it becomes the least recently used (LRU) buffer. Every cache buffer in the list is being reused within that period of time.

In configurations with excessive cache, the LRU Sitting Time can be very high, even many hours. In configurations with too little cache, the LRU Sitting Time can be measured in seconds. The time can vary widely, depending on circumstances.

On inactive servers, such as those sitting unused overnight or those in lab environments with long periods of idle time, the LRU Sitting Time statistic is incremented by one second every second. This is because the LRU Sitting Time indicates the age of the LRU cache buffer. The LRU Sitting Time statistic is useless under these circumstances, except to confirm the obvious: that new data is not being written to the server's cache. This statistic is most useful during peak workloads when the server's cache is servicing the greatest number of users and the broadest possible data set.

You can view the LRU Sitting Time statistic using NetWare Remote Manager or MONITOR.

In NetWare Remote Manager, do the following:

1. Click the View Memory Config link in the navigation frame.
2. Click the Traditional File System Cache Statistics link on the System Memory Information page.

In MONITOR, from the Available Options menu, select Disk Cache Utilization.

Calculating Cache Memory Needs

To determine how much file cache your server needs, do the following:

1. Track server resource utilization statistics. Chart the results for daily, weekly, monthly, period-end, and year-end cycles. Identify recurring periods of peak workloads.
2. Observe the LRU Sitting Time statistic during peak workload periods of the day. Keep a record of the *lowest* LRU Sitting Time during the peak periods for at least one week, longer if necessary, to see a consistent pattern.

3. Based on the observations you made of the server's resource utilization and LRU Sitting Time, determine an average low LRU Sitting Time.
4. Tune the cache. Size the cache in such a way that the server can sustain an average low LRU Sitting Time of at least 12 minutes during peak workloads.

   For example, if your server's original average low LRU was 7 minutes, you will need to add enough memory to increase the LRU Sitting Time to an average low of 12 minutes during peak workloads. This added memory increases the likelihood that repeatedly used data will still be cached when the next user request is received.

   On the other hand, if the server's original lowest LRU sitting time was 18 minutes, the server has more than adequate cache. You can leave the excess memory in the server for future growth or remove it and use it somewhere else.

Setting a File Cache Buffer Alert

You can control when the server alerts you to serious decreases in the number of available file cache buffers. Use the following SET parameters (Traditional File System category).

- **Minimum File Cache Buffers** establishes the minimum number of buffers that will always be reserved for file cache and not made available for other processes. When this minimum is reached, the server displays the message `Cache memory allocator exceeded minimum`.
- **Minimum File Cache Report Threshold** instructs the server to send an alert *before* the minimum number of file cache buffers is reached. Set this parameter to the number of buffers above the minimum at which you want the server to send an alert. For example, if the Minimum File Cache Buffers value is 20 and the Minimum File Cache Report Threshold value is 30, the server sends an alert when 50 file cache buffers are left.

eDirectory

If you suspect that your server is slow in accessing eDirectory™, see Improving eDirectory Performance in the *Novell eDirectory 8.6 Administration Guide*.

Tuning Directory Cache for the Traditional File System

The information for tuning directory cache applies only to NetWare servers using the traditional NetWare file system. Directory cache is not used by the Novell Storage Services™ (NSS) file system.

As directory entries are read and operated upon by a user, NetWare caches the entries to make repeated use of an entry more efficient. In a default configuration, NetWare allocates 20 cache buffers of 4 KB each. Each block read into a cache buffer contains 32 entries.

The default number of buffers is appropriate for only a small number of users. The tuning strategies in this section can help you tune the directory cache to meet your network's requirements.

Three Directory Cache Tuning Strategies

Sizing the directory cache depends largely on the characteristics of the workload the server supports. The key is the frequency and breadth of directory searches, file opens, closes, and creations.

- A low-use scenario involves any number of users in which a small number of directories are shared or in which each user's activity is limited to a small region of the directory, such as a home directory.
- A high-use scenario involves any number of users, but user activity spans a very large number of directories and files. An extreme case might be a document-based system in which document searches routinely traverse large portions of a very large directory.

Strategy 1: Tuning for Low Use

To handle low memory use, you probably won't need to allocate any more cache than the NetWare default. By default, NetWare allocates 20 buffers immediately upon request, followed by a maximum allocation of up to 500 buffers (about 2 MB). This is sufficient for the majority of low-use scenarios.

Strategy 2: Tuning for High Use

To tune for very high use, change the following SET parameters to the values shown using NetWare Remote Manager, MONITOR, or SET commands at the System Console prompt.

```
MINIMUM DIRECTORY CACHE BUFFERS = 2000
MAXIMUM DIRECTORY CACHE BUFFERS = 4000
```

In NetWare Remote Manager, click the Set Parameters link in the navigation frame, click the Traditional File System category link, click the parameter value link that you want to change, enter the new value, and click OK.

In MONITOR, from the Available Options menu, select Server Parameters > Traditional File System, select the parameter you want to change, type the new value, and press Enter.

Strategy 3: Tuning for Name Spaces

When a name space is installed on a traditional NetWare volume, the volume's Directory Entry Table (DET) must include an additional directory entry for each file. So, for example, if a volume supports DOS, NFS, and LONG name spaces, there are three directory entries in the DET for each file instead of just one.

In such a case, a directory cache buffer with 32 directory entries no longer represents 32 files, it represents only 10 files, because each file now requires three directory entries.

This means the efficiency of your directory cache is decreased by a factor equal to the number of name spaces loaded. Therefore, you might need to add more memory if you load multiple name spaces. By carefully tuning the directory cache, you can maintain high performance even under these conditions.

Before adding name spaces, allow your server to operate in its production environment for several weeks. This lets NetWare allocate the appropriate number of directory cache buffers for the native DOS environment.

After this settling-in period, check the Directory Cache Buffer value in the MONITOR General Information window. This is the highest number of directory cache buffers allocated since the server was last started.

Use the following formulas to determine the optimum minimum and maximum number of directory cache buffers.

```
(# of names spaces, including DOS) x highest number of
  Directory Cache buffers since server was last started =
  minimum cache buffers
(minimum cache buffers) + 100 = maximum cache buffers
```

For example, if your server's highest number of Directory Cache buffers since server was last started is 250, and you want to load one additional name space, you would calculate the minimum and maximum values of directory cache buffers as follows:

```
2 x 250 = 500
500 + 100 = 600
```

Before loading the additional name space, change the following SET parameter values using NetWare Remote Manager, MONITOR, or SET commands at the System Console prompt:

```
MINIMUM DIRECTORY CACHE BUFFERS
MAXIMUM DIRECTORY CACHE BUFFERS
```

These settings increase the likelihood that repeatedly used directory cache buffers will remain in cache and that those buffers will remain in cache longer, providing the best possible read response times.

Monitoring the New Settings

After you tune the directory cache, let the server operate for a few weeks to settle in. Then check to see whether the server allocates the additional directory cache buffers that the new settings allow. If the allocated buffers do not increase to near the level allowed, then you know that your users' directory access patterns don't require the additional cache. On the other hand, if your server uses all the cache you made available, your user community's directory access patterns might be more intensive than you anticipated.

Using Virtual Memory

NetWare provides a virtual memory system that moves data out of memory and into a swap file on disk if the data isn't used frequently. Thus, the virtual memory system ensures that RAM is used more efficiently. It lessens the likelihood that low memory conditions will cause a problem with the server. For general information about virtual memory, see “Virtual Memory” on page 14.

NetWare Remote Manager has several pages that can assist you in monitoring and managing the use of Virtual Memory system in your server.

To	Do the following in NetWare Remote Manager
View the overall perfomance of the Virtual Memory system	1. Click the Monitor Health link in the navigation frame. 2. Click the Virtual Memory Performance link on the Server Health Monitoring page. 3. Click the Info icon for each item listed on the Health Info table on the Virtual Memory Health Information page
View specific perfomance of the Virtual Memory system	1. Click the View Memory Config link in the navigation frame. 2. Click the Virtual Memory Page link on the System Memory Information page. 3. Click the Virtual Memory Cache Pool link to view the statistics for each cache pool type. For information on each type of statistic listed, see the online help. 4. Click the Virtual Memory Statistics link to view the following statistics: Current Available Memory, Free Desired Pages, Free Lots Pages, Free Minimum Pages, Memory Available State, Need Free Clean Pages, Need Free Pages, and Upper Page I/O Threshold. For information on each type of statistic listed, see the online help.
Change SET parameters associated with the Virtual Memory System	1. Click the Set Parameter link in the navigation frame. 2. Click the Memory link in the Category Name table on the Set Parameter Categories page. 3. Click the value link for each specific Virtual Memory parameter you want to change. 4. Enter the new value in the Current Value field and click OK.

You can manage the swapping of data by controlling the swap files where the data is stored on disk. To create, delete, and manage swap files, access NetWare Remote Manager and complete the tasks in the following table:

To	Do the following in NetWare Remote Manager
Learn about the SWAP command	Click the Console Commands link in the navigation frame and then the SWAP Info icon on the Console Commands page.
Display the Swap File Usage Information page	Click the View Memory Config link in the navigation frame and then the Swap File Size icon on the System Memory Information page.
Create a swap file on a designated volume	1. Click the View Memory Config link in the navigation frame and then the Swap File Size link on the System Memory Information page. 2. Click the No value link in the Swapping Enabled column for the volume you want to enable. 3. (Optional) On the Enable Swapping page, enter the values you want in the Minimum Size (2), Maximum Size (5), and Minimum Volume Free Size fields (free volume space). If you leave these fields blank, the default values in the parenthesis are used. These parameters specify minimum and maximum size of the swap file and the minimum free space that must be left on the volume. 4. On the Enable Swapping page, click the Enable button. 5. If the file is not on volume SYS: add the commands to create swap files to the AUTOEXEC.NCF file so the files are created each time the server is started. The command syntax is SWAP ADD *volume_name* [parameter=*value*...] Optional parameters are MIN, MAX, and MIN FREE. For example: SWAP ADD VOL1 MIN=3, MAX=6, MIN FREE=2000

To	Do the following in NetWare Remote Manager
Delete a swap file from a designated volume	1. Click the View Memory Config link in the navigation frame and then the Swap File Size link on the System Memory Information page. 2. Click the Yes value link in the Swapping Enabled column for the volume you want to delete the Swap file from. 3. On the Enable Swapping page, click the Disable button. If you are using protected address spaces, the Java Virtual Machine, or any other application that uses virtual memory, be sure to keep at least one swap file. If the swap file is being used when it is deleted, then the swapped data is moved to another swap file. If there is no other swap file and there is not enough physical memory to move all the swapped data, an error message is displayed and the file is not deleted. By default, a swap file is created on the volume SYS:. If you do not want a swap file on volume SYS:, place the SWAP DEL SYS command in the STARTUP.NCF file.
Change the parameter values for a swap file on a designated volume	1. Click the View Memory Config link in the navigation frame and then the Swap File Size link on the System Memory Information page. 2. Click the link for the value you want to change. 3. On the Enable Swapping page, enter the new values you want. 4. On the Enable Swapping page, click the Change button.

Using Swap Files

You can create one swap file per volume. The swap file for volume SYS: is created by default; you can delete it if necessary.

Data moved to disk by virtual memory is stored in any available swap file; it does not matter which volume the swap file is on. Generally, you should place swap files on the fastest volume, the one with the most available space, or the one that is used the least.

When you dismount a volume, the swap file is deleted. To keep a swap file on that volume, you must create the swap file again when the volume is mounted. The exception is the swap file for volume SYS:, which is created by default. For convenience, add the commands to create swap files to the AUTOEXEC.NCF file, so the files are created each time the server is started.

Swap files are dynamic; they expand and contract as data is swapped in and out of memory.

Responding to Disk Thrashing

The real value of virtual memory is in using a sufficient supply of memory more efficiently, thereby improving server performance.

If the overall supply of memory is running low, then swapping will occur more often when virtual memory is in use. If memory is extremely low, the system might spend a significant amount of its time swapping memory in and out of disk and have little time to accomplish useful work. This is called *disk thrashing*.

In extremely low memory conditions, NetWare moves all the memory from a protected address space into the swap file, temporarily stopping the modules within the space. After a period of time, NetWare moves the memory back into the protected address space and shuts down another space, moving its memory to the swap file. Without virtual memory, these extremely low memory conditions would cause processes to fail. With virtual memory, the server keeps running, although very slowly.

If the Average Clean Free Available State or the Average Page I/O state is Suspect or Bad on the Virtual Memory Health Information page in NetWare Remote Manager, your server is experiencing disk thrashing.

If your server is experiencing disk thrashing, you can use the following two hidden SET parameters (Memory category) to manage the balance between the virtural memory cache pool and the file system cache pool. Use caution when changing these parameters, because until you have more than 4 GB of memory in the server, increasing these parameters will remove memory from the file system cache pool and cause low memory conditions there.

- VM Cache Pool Free Desired Pages, range 0 to 2147483647, default 256

  Specifies the number of pages that the viritual memory system cache needs to operate properly.

- VM Cache Pool Free Lots of Pages, range 0 to 2147483647, default 512

  Specifies the number of pages that the virtual memory system cache considers to be excessive. Having an available page count higher than this number might result in the pages being be given to another cache pool.

You can specify the point at which the server sends an alert to the console because of excessive memory swapping by using the Average Page In Alert Threshold Set parameter (Memory category).

The value is the average number of pages swapped from disk to memory per second, calculated over the last five seconds. The default is 2000.

To change the values for this parameter using NetWare Remote Manager, do the following:

1. Click the Set Parameters link in the navigation frame and then the Memory Category link on the Set Parameter Categories page.
2. Click the value link for the Average Page In Alert Threshold setting.
3. Enter the new value in the Current Value field and click OK.

When disk thrashing occurs, the complete solution is to add more RAM. Virtual memory cannot compensate for an overall lack of server memory, although it can prevent processes from failing and allow a server to continue to function.

Optimizing Garbage Collection

The NetWare server provides a garbage collection or memory recovery process that periodically collects alloc memory freed by NLM programs and returns it to cache.

Garbage collection responds to pressure from the virtual memory system. (For an explanation of virtual memory, see "Virtual Memory" on page 14.) The virtual memory system is checked every 10 seconds.

If pressure on virtual memory is high, then garbage collection is accelerated.

If pressure on virtual memory is low, then garbage collection happens at the regularly scheduled garbage collection interval. This interval is controlled by the Garbage Collection Interval server parameter.

To view or change this interval in the NetWare Remote Manager, in the navigation frame click the Set Parameters link > Memory > Garbage Collection Interval *value* link.

Normally, garbage collection happens in the background. The only indicator that garbage collection has taken place is an increase in the amount of free memory displayed in MONITOR after garbage collection has freed memory.

However, you can initiate garbage collection manually for individual modules using the following steps.

1. In MONITOR, from the Available Options menu, select Loaded Modules.
2. Select the module that you want to garbage collect memory from.
3. Press F4 to garbage collect memory for that module.

   HINT: You can also garbage collect memory from protected address spaces. In MONITOR, from the Available Options menu, select Virtual Memory > Address Spaces. Then select the desired address space and press F4.

3 Managing Server Memory

This chapter contains information about the following:

Server Memory Management Tools

NetWare® provides several tools to help you manage and tune the memory system:

- NetWare Remote Manager (PORTAL.NLM) provides the ability to monitor the memory used in each of the following categories:
  - Original Cache Memory
  - Current Cache Memory
  - File System Memory
  - Reserved Swap Memory
  - Swap File Size
  - NLM Memory
  - Virtual Memory system

  You can also use NetWare Remote Manager to load and unload modules in to protected address spaces and change SET parameter values and

access the server console to run MONITOR and execute any console commands.

In most cases, NetWare Remote Manager is more useful than MONITOR when diagnosing server memory problems. For more information, see the *NetWare Remote Manager Administration Guide*.

- The MONITOR utility provides statistics that indicate how efficiently memory is being used by the server and individual modules. For more information, see MONITOR in *Utilities Reference*.
- Settable parameters and console commands let you tune the memory system to achieve optimal performance. For more information, see SET > Memory Parameters in *Utilities Reference*.

Using Protected Address Spaces

You can use a portion of server memory called a protected address space to protect the server operating system from untried or troublesome applications and to use virtual memory. When applications are loaded into a protected address space, they can't corrupt the operating system, cause server abends, or corrupt other applications that are running in other protected address spaces.

All protected address spaces use virtual memory, so running modules in a protected address space also uses RAM more efficiently.

For general information about protected address spaces and the applications that can be loaded into them, see "Protected Address Spaces" on page 12. For general information about virtual memory, see "Virtual Memory" on page 14.

- Because modules loaded into a protected address space have controlled interaction with the operating system, all modules that must communicate with each other by directly importing another module's data or functions (such as those of an e-mail application or a database) should be loaded into the same protected address space.
- If you load a NetWare Loadable Module™ (NLM™) that depends upon another module, such as CLIB, the other module will be loaded automatically into the same address space.
- If the same module is loaded into more than one address space, the module's code will be shared among the address spaces. Therefore, loading the module into multiple address spaces does not require additional memory for the module itself. Only data for the required module is unique for each address space.

- Even if an NLM is designed to be loaded only once, you can load multiple copies of the NLM on your server if you load them into different address spaces.
- When you load modules into a protected address space, NetWare assigns whatever amount of memory the loaded modules need, up to a maximum size of 512 MB. The maximum size of a protected address space is fixed; but within that maximum limit, the memory size of the space grows and shrinks as needed by the modules in the address space.
- If you want the server to clean up address spaces that abend, make sure the Memory Protection Fault Cleanup parameter (Memory category) is set to the default setting of On. If an address space abends, the server removes the address space and its modules and returns the resources to the system.

  If the Memory Protection Fault Cleanup parameter is set to Off, the situation is left to the abend recovery mechanism.

Loading Protected Address Spaces

You can create a protected address space when you load one or more modules.

To load protected address spaces, use the commands in the following table at the System Console prompt or in NetWare Remote Manager on the Address Space Information page (access by clicking Protected Memory link in the navigation frame).

To	Enter this command at the System Console prompt	Do this on the Address Space Information Page of NetWare Remote Manager	Example
Load one module into the next available protected address space	**[LOAD] PROTECTED *module_name***	1. Type ***module_name*** in the Load Module Protected field. 2. (Optional) If you want to view the System Console screen when the module loads, check the Display System Console for Module Load check box. 3. Click the Load Module Protected button.	**[LOAD] PROTECTED DATABASE.NLM** Creates a new address space called ADDRESS_SPACE*n*, where *n* is a numerical number, and loads DATABASE.NLM into it.

To	Enter this command at the System Console prompt	Do this on the Address Space Information Page of NetWare Remote Manager	Example
Load one module into the next available protected address space with restart functionality ◆ Restart functionality means that if the protected space abends, the system closes the space, cleans up its resources, restarts the space, and reloads the module into it. ◆ To prevent the server from restarting a memory space that continues to fault, use the Memory Protection No Restart Interval Set parameter (Memory category).	**[LOAD] RESTART *module_name***	1. Type **RESTART *module_name*** in the Load Module Protected field. 2. (Optional) If you want to view the System Console screen when the module loads, check the Display System Console for Module Load check box. 3. Click the Load Module Protected button. 4. (Optional) If you want to change the restart state to No, click the Yes button in the Restartable column of the Address Space Information table.	**RESTART DATABASE.NLM** Creates a new address space called ADDRESS_SPACE*n*, where *n* is a numerical number, and loads DATABASE.NLM into it. If the address space abends, the system will shut down the space, restart the space automatically, and reload DATABASE.NLM into it.

To	Enter this command at the System Console prompt	Do this on the Address Space Information Page of NetWare Remote Manager	Example
Load one module into a protected space with a user-defined name ◆ Use this command when you want to create your own name for the space. ◆ Also use this command when you want to load more than one module into the same protected space. ◆ Repeat the command for each module you want to load into the space. ◆ You can also include the restart option on the same command line.	**[LOAD] ADDRESS SPACE = *space_name module_name***	1. Type **ADDRESS SPACE = *space_name module_name*** in the Load Module Protected field. 2. (Optional) If you want to view the System Console screen when the module loads, check the Display System Console for Module Load check box. 3. Click the Load Module Protected button. 4. (Optional) If you want to load more than one module in the same space, repeat Steps 1 through 3 for each module you want to load.	**[LOAD] ADDRESS SPACE = DB_SPACE DATABASE.NLM** Creates a new address space called DB_SPACE and loads DATABASE.NLM into it. [LOAD] ADDRESS_SPACE = DB_SPACE RESTART TEST.NLM Loads TEST.NLM into the DB_SPACE address space and also adds restart functionality to the address space. [LOAD] ADDRESS SPACE = DB_SPACE TEST.NLM Loads the TEST.NLM in to the same DB_SPACE address space that the DATABASE.NLM was loaded into.

To	Enter this command at the System Console prompt	Do this on the Address Space Information Page of NetWare Remote Manager	Example
Load multiple modules at once using an .NCF file The command creates a protected space with the same name as the .NCF file and executes the .NCF file to load all the modules into the space.	**PROTECT *filename***	1. Type ***NCF_filename*** in the Load NCF File Protected field. 2. (Optional) If you want to view the System Console screen when the module loads, check the Display System Console for NCF Execution check box. 3. Click the Load NCF File Protected button.	**PROTECT LOAD_DB** Creates an address space called LOAD_DB and executes LOAD_DB.NCF to load modules into the protected space.

Unloading Protected Address Spaces

To unload a module from a protected space or to unload the space itself, use the commands in the following table at the System Console prompt or in NetWare Remote Manager on the Address Space Information page (access by clicking Protected Memory link in the navigation frame).

To	Enter this command at the System Console prompt	Do this on the Address Space Information Page of NetWare Remote Manager	Example
Unload a specified module from the specified address space If the module is loaded into more than one address space, this command removes the module only from the designated address space.	**UNLOAD ADDRESS SPACE = *space_name module_name***	1. Click the link for the address space name. 2. Click the link for name of the NLM on the NetWare Loadable Modules Information page. 3. Click the Unload button on the Information page for that module.	**UNLOAD ADDRESS SPACE = ADDRESS_SPACE1 DATABASE.NLM** Unloads DATABASE.NLM from ADDRESS_SPACE1, but does not remove the address space unless it is the last module loaded.
Unload all modules from the designated address space and removes the space	**UNLOAD ADDRESS SPACE = *space_name***	Click the Unload button in the Unload column of the Address Space Information table for the address you want to unload the modules from.	**UNLOAD ADDRESS SPACE = ADDRESS_SPACE1** Unloads all the modules from ADDRESS_SPACE1, closes ADDRESS_SPACE1, and returns its resources to the system.
Remove an address space without unloading the modules first Use this command only if you know the space can't be unloaded with the UNLOAD ADDRESS SPACE command.	**UNLOAD KILL ADDRESS SPACE = *space_name***	Click the Remove button in the Remove column of the Address Space Information table for the address space you want to remove.	**UNLOAD KILL ADDRESS SPACE=ADDRESS_SPACE1** Removes ADDRESS_SPACE1 without unloading modules and returns its resources to the system.

If a module hangs while it is being unloaded with the UNLOAD ADDRESS SPACE command, the system waits a specified time and then displays the following error message:

Module_name in *address_space* did not unload yet. Killing the address space is the only way to remove the NLM. Should the address space be killed? Yes/No.

If you answer Yes, the system shuts down the address space without unloading modules from it. If you answer No, the system waits a specified time and displays the message again.

You can designate the amount of time before the message appears by setting the HUNG UNLOAD WAIT DELAY (Error Handling category) parameter. The default is 30 seconds.

In some circumstances, the server might not completely clean-up an address space that has faulted. This failure is caused by NLM programs that are not written to allow external cancellation.

When NetWare cannot clean up an address space after it faults, it sends an alert message to the server console. If you execute the PROTECTION command, the address space will be listed as in the clean-up failure state.

Because you cannot unload an address space that is in the clean-up failure state, you must shut down and restart the server to recover the remaining resources from the address space.

Viewing Information about Address Spaces

You can see which modules are loaded in which address spaces.

In NetWare Remote Manager

1. Click the Protected Memory link in the navigation frame.
2. View the Address Space Information on the Address Space Information page.
3. To view the modules that are loaded in a specific address space, click the Address Space *name* link for the specific address.

At the System Console Prompt

1. To display a list of loaded modules with their address space names, enter :

   MODULES

   Each NLM name displayed is followed by the name of the address space where the NLM resides, the full utility name, version number, date, and other information. The module names are displayed in the order in which they were loaded.

2. To display a list of all address spaces, enter

   PROTECTION

   Each address space name that is displayed is followed by a list of all modules loaded into that space, with a short description of each module.

In MONITOR

To view additional statistics for address spaces, do the following:

1. From the Available Options menu, select Virtual Memory and then Address Spaces.
2. Use the arrow keys to select an address space.
   - The information window displays data about the selected address space.
   - To activate and expand the information window, press Tab.
   - To see a description of each field, press F1.
   - To exit the window, press Esc twice.
3. Select a specific address space and press Enter to see a list of all modules loaded into the address space.
   - Use the arrow keys to select a module in the list.
   - The information window displays data about the selected module.
   - To activate and expand the information window, press Tab.
   - To see a description of each field, press F1.
   - To exit the window, press Esc twice.