IBM TotalStorage™ Network Attached Storage 300
Model 325

Release Notes
9/14/01

IBM TotalStorage™ Network Attached Storage 300
Model 325

Release Notes
9/14/01

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED ON AN ″AS IS″ BASIS. In no event will IBM be liable for damages arising directly or indirectly from any use of the information contained in this document.

First Edition (September 14, 2001)

This edition applies to the IBM 5195 TotalStorage Network Attached Storage 300 (Model 325) (product number 5195-325).

Order publications through your IBM representative or the IBM branch office servicing your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for reader's comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Design & Information Development
Department CGF
PO Box 12195
Research Triangle Park, NC 27709–9990
U.S.A.

You can also submit comments on the Web at www.ibm.com/networking/support/feedback.nsf/docsoverall.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2001. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Release notes

This document contains the release notes for the Network Attached Storage 300 Model 325 Version 1.50 software refresh.

Refer to www.storage.ibm.com/support/nas for possible updates to these release notes and for copies of the base documents.

Fixes and enhancements

Your Model 325 comes with a preloaded set of software (described in detail in the *User's Reference*). As the preloaded software is updated with newer software components (containing problem fixes, functional enhancements, or both), the changes are applied in product manufacturing before the product is shipped to you. For this reason, the exact release of preloaded software on your Model 325 may vary, depending on when you received your Model 325.

To identify the exact release of preloaded software, from the Model 325 desktop (via Terminal Services or direct-attached keyboard and monitor), click **IBM NAS Admin**, then on the left pane select **Software Version**. The first line of text that appears on the right pane provides the software release (version and build number).

The original level of Model 325 software is Version 1.00, Build 66. The following sections describe fixes and enhancements to newer levels of software, in reverse chronological order. If you have an older version of Model 325 software and require fixes or enhancements that are provided in newer versions, go to www.storage.ibm.com/support/nas for information on obtaining those fixes and enhancements. They may be provided in code packages which you must download and install, in technical tips informing you of software configuration changes (applied by IBM to later versions of Model 325 software preloads) that you must apply, or as CDs which you must contact IBM technical support to obtain and install.

Fixes and enhancements in Version 1.50

Microsoft Server Appliance Kit Version 2.01

Version 1.50 of the Model 325 software includes Microsoft Server Appliance Kit (SAK) Version 2.01 (upgraded from Version 1.7). The SAK supports the Windows 2000 for Network Attached Storage (NAS) Web-based user interface for administering the Model 325. SAK 2.01 contains an improved look and feel over its predecessor, including better organization of the task groups, and some problem fixes.

Columbia Data Products Persistent Storage Manager Version 2.2

Version 1.50 of the Model 325 software includes Persistent Storage Manager (PSM) Version 2.2 (upgraded from Version 2.0). In addition to having more reliability than PSM 2.0, PSM 2.2 adds the capability for restoring multiple-volume persistent images, and has an improved user interface (via SAK 2.01 described earlier) and more user-friendly disaster recovery. For more information on PSM 2.2, see "Updated information on Persistent Storage Manager" on page 6.

© Copyright IBM Corp. 2001

Tivoli Storage Manager Client Version 4.20

Version 1.50 of the Model 325 software includes Tivoli Storage Manager (TSM) Client Version 4.20 (upgraded from Version 3.7), which supports archival data backup and restore in conjunction with a TSM Server (running on another server on the LAN).

IBM Universal Manageability Services / IBM Director Support Program Version 2.22

Version 1.50 of the Model 325 software includes Version 2.22 of Universal Manageability Services (upgraded from Version 2.12), which contains the IBM Director Support Program that enables management of the Model 325 from an IBM (or Tivoli IT) Director console.

Microsoft Services for UNIX Version 2.2

Version 1.50 of the Model 325 software includes the official release of Services for UNIX Version 2.2 (upgraded from a Version 2.2 prerelease version shipped in previous Model 325 software releases). Services for UNIX 2.2 contains fixes for a number of problems, particularly in User Name Mapping support. For more information on Services for UNIX, see “Microsoft Services for UNIX and NFS Support in the Model 325” on page 5.

Telnet Server support

Version 1.50 of the Model 325 software includes Telnet server capability. The Telnet server provides limited administrative capability for the Model 325. This may be useful in cases where you need to remotely administer the Model 325, but do not have access to a Windows-based workstation (from which you could remotely administer the appliance via a supported Web browser or Terminal Services Client).

You can access the Model 325 from any Telnet client by specifying the IP address or hostname of the Model 325, then logging in using an ID and password (defined on the Model 325) with administrative authority. Once you have logged in, you will be presented with a command-line interface similar to that of a DOS command prompt in Windows (in fact, it will start at the C:\ prompt). From this interface, you can issue DOS-like commands (such as dir and cd), and some UNIX-like commands (such as grep and vi). You can launch some applications, but only character-mode applications are supported.

By default, the Telnet server is disabled. To enable the Telnet server, from the Windows 2000 for NAS user interface, go to the Network task group, then select **Telnet**. On the Telnet Administration Configuration page that appears, turn on the “Enable Telnet access to this appliance” check box. Later, if you wish to disable Telnet access, you can turn this check box back off. If you do not require Telnet access to the Model 325, then it is recommended that you leave the Telnet server disabled.

SNMP support

In Version 1.50 of the Model 325 software, support for the Simple Network Management Protocol (SNMP) is enabled. In order to manage the Model 325 from your SNMP-capable management application, you will need to install the Management Information Base (MIB) files for various components of the Model 325 on the management application workstation, so that the application can recognize those SNMP elements (values, alerts, etc.) supported by the components. Go to www.storage.ibm.com/nas for information on MIB files that are supported by the Model 325.

Fixes and enhancements in Version 1.00, Build 70

Windows Powered Service Pack 2

Version 1.00, Build 70 of the Model 325 software contains Service Pack 2 for Microsoft Windows Powered, the operating system on which the Model 325 is based. Earlier versions of the Model 325 software contained Service Pack 1. Service Pack 2 fixes the following known Model 325 problem:

- When using Terminal Services to administer a Model 325 node, you cannot shut down the node using the Shut Down Windows dialog box (accessed by selecting **Shut Down...** from the Start menu on the Model 325 [Windows Powered-based] desktop displayed via Terminal Services).

"Code Red" worm exposure

Your Model 325 runs the Microsoft Internet Information Services (IIS) Server to provide Web-based management. Because of this, the Model 325 is vulnerable to attack by the "Code Red" worm. Version 1.00, Build 70 of the Model 325 software contains a fix for IIS Server that eliminates this exposure.

Fixes and enhancements in Version 1.00, Build 67

Director Support Program problem

If you are using the IBM Director (or Tivoli IT Director) Management Console on your network to manage the Model 325 appliance, the appliance names (one name for each of the two nodes of the appliance) may not appear in the list of systems and devices. (The appliance name for each node should appear in the list as IBM5195-*xxxxxxx*, where *xxxxxxx* is the serial number of the node, located in the lower right corner of the bezel on the front of the node.) A fix for this problem is included in Version 1.00, Build 67 of the Model 325 software, as a patch to the IBM Director Support Program that is part of the software.

If your Model 325 is running Version 1.00, Build 67, and you later use the Recovery CD (provided with that level of software) to restore the preloaded software image on your Model 325, the Model 325 will be reverted to Version 1.00, Build 66, which does not include the fix for this problem. You will need to download and install a patch for the IBM Director Support Program.

Go to www.storage.ibm.com/support/nas, and then go to the Downloads section under 5195 TotalStorage NAS 300 (Model 325) to find the patch package titled IBM Director Support Program patch. Download and install the patch on your appliance as instructed by the documentation accompanying the package.

Startup problem caused by addition of SCSI adapter

If you purchase the optional PCI Fast/Wide Ultra SCSI adapter and install it in one of the nodes of your Model 325, you may experience a problem where the node will not boot to the Microsoft Windows Powered operating system because it cannot recognize its internal hard drives. You will need to update the SCSI adapter firmware to Version 2.20 to correct this problem. This firmware can be downloaded from the Web.

Go to www.storage.ibm.com/support/nas, then go to the Downloads section under 5195 TotalStorage NAS 300 (Model 325) to find the package titled PCI Fast/Wide Ultra SCSI Adapter Flash Diskette Version 2.20. Download and install the firmware on your appliance node's SCSI adapter as instructed by the documentation accompanying the package.

Functional notes

The following sections contain information on Model 325 function.

Ethernet adapter teaming

The Ethernet adapters (Gb Ethernet SX and 10/100 Ethernet) that you install in the PCI slots of the Model 325 nodes support adapter teaming. With adapter teaming, two or more PCI Ethernet adapters can be physically connected to the same IP subnetwork and then logically combined into an adapter team. Such a team can support one of the following functional modes:

Fault tolerance

In fault tolerance mode, only one adapter in the team is fully active on the Ethernet network (for example, sending and receiving data) at any point in time, while the other adapters are in standby mode (receiving data only). If that adapter detects a link failure or fails completely, another adapter in the team automatically and rapidly takes over as the active adapter, and all Ethernet traffic being handled by the failing adapter is seamlessly switched to the new active adapter, with no interruption to network sessions (for example, file transfers) in progress at the time of the failover.

Load balancing

In load balancing mode, all adapters in the team are active, increasing the total transmission throughput over the common IP subnetwork. If any adapter in the team fails (link failure or complete failure), the other adapters in the team continue to share the network transmission load, although total throughput is decreased. Load balancing is only supported for adapter teams consisting of only one type of adapter; different types of adapters cannot be combined in a load balancing team.

You configure adapter teaming with Intel PROSet II, which is preloaded on the Model 325, as follows (you must do this on both nodes).

Note: It is strongly recommended that you configure adapter teaming before you set up Microsoft Cluster Server (MSCS) clustering, as described in Chapter 5 of the *User's Reference*. Additionally, for each team you configure on one Model 325 node, you must configure an identical team (same type of team, same set of adapters, and so on) on the other node.

1. Physically connect the adapters that you wish to team to the same IP subnetwork.
2. Access the Model 325 desktop by directly attaching a keyboard, mouse, and monitor, or over the network by starting Terminal Services on another workstation. (For instructions on how to invoke Terminal Services, see *Terminal Services and the IBM NAS Administration Consol*e in Chapter 2 of the *User's Reference*.
3. From the Model 325 desktop, go to the Start menu, then select **Settings**, then select **Control Panel**.
4. Double-click the Intel PROSet II icon in the Control Panel to start Intel PROSet II.
5. You will see a list of all adapters for each slot and type supported under Network Components.
6. Under Network Components, you will see a list of resident and non-resident adapters for each slot and type supported. Drivers are preset for all supported adapter configurations but will be loaded only for resident adapters.

7. Identify which adapters you are going to team. You do this by left-clicking the adapter under Network Components, and selecting one of the adapters that will be part of the teaming.
8. Right click the adapter, then select **Add to Team**, then select **Create New Team...**.
9. Select the type of team you wish to create.
10. Select the adapters for the team you are creating by selecting the check box for the appropriate adapters in the list, and then select **Next**.
11. Verify that these settings are correct, and then select **Finish**.

This procedure creates a device named Intel Advanced Network Services Virtual Adapter. It also binds all network protocols that were bound to the physical adapters that were added to the team to this virtual adapter, and unbinds those protocols from the physical adapters. If you delete the team, the settings will return to the state prior to creating the team.

For complete help on adapter teaming, from Intel PROSet II click **Network Components**, and then select **Help** from the Help menu.

Note: The onboard (planar) Ethernet controller on each Model 325 node is dedicated to the clustering interconnection between the two nodes and does not support adapter teaming.

Microsoft Services for UNIX and NFS Support in the Model 325

Support for the Network File System (NFS) is provided in the Model 325 by a preloaded and preconfigured software component, Microsoft Services for UNIX. The levels of NFS supported by Services for UNIX, and in turn the Model 325, are NFS Versions 2 and 3. Any client workstation that is using an NFS software stack supporting NFS Version 2 or NFS Version 3, regardless of the client workstation's operating system, should be able to connect to the Model 325 and access its storage as defined by the Model 325 administrator.

You administer NFS file shares and other attributes with standard Windows administration tools, including those provided as part of the IBM NAS desktop, and the Microsoft Windows 2000 for NAS user interface. Additional configuration of the User Name Mapping component of Services for UNIX, which maps the UNIX user name space to the Windows user name space, is required to support NFS security.

Note: As documented in the *User's Reference*, a Windows Primary Domain Controller (PDC) is required to support initial setup and configuration of the Model 325. For NFS security in the Model 325, it is strongly recommended that you set up the same PDC as a Services for UNIX User Name Mapping server. The design of Services for UNIX with respect to clustering and failover forces both Model 325 nodes to be configured to use the same User Name Mapping server, whether that server is on one of the nodes or is on another server or workstation in the network. If one of the nodes is configured as the User Name Mapping server, and that node should fail, NFS users will not be able to attach to the Model 325 storage until the node comes back up. Centralizing the user name mapping on a PDC ensures that if either node fails, NFS users can continue to be authenticated and given access to the Model 325 storage.

To set up the PDC as a User Name Mapping server, you must install Services for UNIX Version 2.0 or higher on the PDC, selecting the

components **Server for NFS** and **Server for NFS Authentication**, and then you must configure the **User Name Mapping** component on the PDC. Additionally, you must configure the **User Name Mapping** component on the Model 325 to use the PDC as the User Name Mapping server.

Consult the online documentation for Services for UNIX for more information on configuring User Name Mapping. To view the online documentation for Services for UNIX on the Model 325 (either node can be used):

1. From the Model 325 desktop, click the **IBM NAS Admin** icon.
2. On the left pane of the IBM NAS Admin console, expand **File Systems**.
3. Expand **Services for UNIX**.
4. Select any of the items that appear under **Services for UNIX**.
5. Click anywhere on the right pane of the IBM NAS Admin console, then press the **F1** key to bring up the online documentation for Services for UNIX in a separate window.

Updated information on Persistent Storage Manager

The information in the section “Persistent Images” in Chapter 6 of the *User’s Reference* applies to Version 1.00 of the Model 325 software (containing Persistent Storage Manager [PSM] Version 2.0). For Version 1.50 (containing PSM Version 2.2), the information in this section replaces the information in Chapter 6 of the User’s Reference.

Persistent Images

A persistent image is a copy you make of one or more file system volumes at a specific time. The Persistent Images function allows the recovery of a file or volume to the state it was in at the time you created the persistent image. Persistent images are maintained in a way that minimizes the storage required to keep a second (or third or fourth, and so on) copy of the volume. This is done by using a copy-on-write technique that uses, for each volume, an area of pre-allocated storage (the PSM cache file) that keeps only those data blocks which have been written since the time you made a persistent image of the volume.

Persistent Storage Manager (PSM) allows you to create and preserve images of the Model 325 drives. You can take a persistent image immediately or schedule persistent images as one-time events or regularly repeated events. You can access the PSM tasks in the Disks / Persistent Storage Manager task group within the Windows 2000 for Network Attached Storage user interface, in one of two ways:

- By going to the IBM NAS Admin console on the appliance desktop (via Terminal Services or directly-attached keyboard, monitor, and mouse) and selecting Persistent Storage Manager (this automatically launches the Windows 2000 for Network Attached Storage user interface and brings up the Disks/Persistent Storage Manager page containing the PSM tasks).
- By starting the Windows 2000 for Network Attached Storage user interface directly

Once you create a persistent image, it appears as a directory on the original drive. Access rights and permissions from the original drive are inherited by the persistent image. Persistent images are used in the same way as conventional drives. However, unlike conventional drives, persistent images are records of the content of the original drive at the time you created the persistent image. Persistent images are retained following shutdown and reboot.

There are six PSM tasks in the Disks/Persistent Storage Manager group:

- Global Settings
- Volume Settings
- Persistent Images
- Schedules
- Restore Persistent Images
- Disaster Recovery

Each of these tasks are described in the following sections. More detailed descriptions and instructions for each of the control panels and topics are contained in the online help.

Global Settings: On this panel you can configure the following attributes of the persistent image system:

Attribute:	**Default value:**
Maximum number of persistent images	250
Inactive period	5 seconds
Inactive period wait timeout	15 minutes

Volume Settings: This panel displays statistics for each volume, such as total volume capacity, free space, and cache file size and usage. You can also select any volume and configure volume-specific PSM attributes for that volume, such as:

Attribute:	**Default value:**
Cache-full warning threshold	80 percent full
Cache-full persistent image deletion threshold	90 percent full
Cache size	15 percent (of the total volume capacity)

Note: You cannot change the cache size for a volume while there are persistent images on that volume (the Cache size combo box will be disabled). You must delete all persistent images on the volume before changing the cache size for that volume.

Persistent Images: This panel lists all of the persistent images that exist on all volumes. On this panel you can:

- Create a new persistent image immediately (without scheduling it via the Schedules panel). When you create the persistent image, you can specify properties for the persistent image, including:

  Volume(s) — The persistent image can contain a single volume or multiple volumes. To select multiple volumes, hold down the **Ctrl** key while clicking on the volumes you wish to select. For multi-volume persistent images, a virtual directory containing data for a volume will appear under the persistent image directory in the top level of each volume in the persistent image (the name of the persistent image directory is configured in the Global Settings panel).

Name — You can name the persistent image. This will be the name of the virtual directory containing the persistent image, underneath the persistent image directory in the top level of the volume (the name of the persistent image directory is configured in the Global Settings panel).

Read-only or read-write — A persistent image is read-only by default, so no modifications can be made to it. However, you can set the persistent image to read-write, which permits you to modify it. When a persistent image is written, the modifications made are also persistent (they survive a reboot of the system). Changing a persistent image from read-write to read-only resets the persistent image to its state at the time you took the persistent image, as does selecting **Undo Writes** for a read-write persistent image from the Persistent Images panel.

Retention value — A persistent image can be given a relative retention value or weight. This is important when PSM needs to delete some persistent images for a volume because the cache file for the volume for which the persistent image was taken capacity has reached a certain threshold, as described later in this section. If the volume cache file completely fills, then all persistent images for that volume are deleted regardless of the retention values. By default, a new persistent image is assigned a “Normal” retention value (there are other higher and lower values which can be selected).

- Delete an existing persistent image.
- Modify properties of an existing persistent image, including read-only or read-write, and retention value.

Schedules: Use this panel to schedule persistent images to be taken at specific times (this is independent of the scheduled backup function via NAS Backup Assistant described earlier). Each PSM schedule entry defines a set of persistent images to be taken starting at a specified time and at a specified interval, with each image having the set of properties defined in the entry. This allows you to customize scheduled persistent images on a per-volume basis.

For instance, you could set a persistent image for one volume to occur every hour, and for another volume to occur only once a day. The set of properties you can define are the same properties described in the Persistent Images panel description above; when you define these properties, all persistent images created according to this schedule entry will be given those properties. Once a scheduled persistent image is created, certain properties of that persistent image can be modified via the Persistent Images panel, independently of other persistent images created according to the schedule.

Once a schedule entry is created, it appears in the list of scheduled persistent images. Subsequently you can modify the properties of an existing entry, such as start time, repetition rate, the volume(s), and so on. For a schedule you can name the persistent images based on a pattern you configure; format specifiers (defined

on the New Persistent Image Schedule panel under the Persistent image name(s) entry field) allow you to customize variable portions of the name.

Restore Persistent Images: On this panel, you can select an existing persistent image and quickly restore the volume contained in the image back to the state it was in at the time the selected persistent image was taken. This is useful if you need to recover an entire volume, as opposed to just a few files. This volume restore function is available for the data volumes, but not the system volume.

Disaster Recovery: PSM provides a disaster recovery solution for the system drive. This extends the volume restore function of PSM to provide disaster recovery in the event that the system drive is corrupted to the point where the file system is corrupt, or the operating system is unbootable. Note that while disaster recovery is also supported via the Recovery CD-ROM and backup and restore capability, that is a two-step process. In contrast, the method supported by PSM allows you to restore the system drive from a single image, without having to go through the entire recovery procedure and then additionally having to restore a system drive backup.

Use the Disaster Recovery panel to schedule and create backup images of the system drive, and to create a bootable diskette which will allow you to restore the system drive from a backup image (located on the maintenance partition, or network drive). The remainder of this section provides additional information on how to perform backup and recovery operations for the Model 325.

Note: Restoration of a PSM backup image over the network is not supported for the Gigabit Ethernet Adapter. If you have only Gigabit Ethernet adapters installed, it is recommended that you perform PSM backup of each node to its maintenance partition (D: drive), which would allow you to recover if the system volume is corrupt and/or unbootable. Should the hard disk drive fail completely, you would need to use the Recovery CD as described in “Using the Recovery Enablement Diskette and Recovery CD” on page 20 to restore the node to its original (factory) configuration.

Backing up the system drive: On the Disaster Recovery panel you will find status information for backup operations, both scheduled and immediate, as well as buttons for starting and stopping a backup operation, for configuring backup, and for creating a recovery diskette.

Click the **Modify Settings** button to open the Disaster Recovery Settings page. Modify the settings for backup as you desire. Note that you must not include spaces in the *Backup name* field. When you have modified the settings, click the **OK** button to save the changes.

On the Disaster Recovery page, click the **Start Backup** button to begin the backup. The backup process will first create a persistent image of the system drive (C:), named *System Backup*. Then it will create the backup images from that persistent image, and then delete that persistent image once the backup operation is complete.

Creating a recovery diskette: You will now create a bootable recovery diskette which, when used to boot up the node, will use the backup location settings you configured on the Disaster Recovery Settings page to locate the backup image and restore it to the system drive of the node.

1. Insert a blank, formatted diskette in the diskette drive of the node.
2. On the Disaster Recovery page, click **Create Disk**.

3. Click **OK** on the Create Recovery Disk page to create the diskette. The diskette drive LED will turn off when the creation is complete. The diskette creation should take no more than two minutes.
4. One of the files that is copied onto the diskette is a utility to make it DOS bootable, called fixboot.exe. From a command prompt, either via the desktop of the node itself (with the diskette still in the diskette drive of the node), or on another system with the diskette in its diskette drive, type **a:\fixboot.exe** and answer the prompts.

   Note: Once you have run fixboot.exe for the diskette, the diskette remains bootable unless you format it again (without specifying an option to make it bootable), so if you later erase files on the diskette you do not need to run fixboot.exe again.
5. Remove the diskette from the diskette drive (of the node itself, or other system if you used that system to run the fixboot utility). You should label the diskette appropriately and keep it in a safe place.

You may create additional copies of the diskette using the above procedure for each new copy. Please note that if you change the backup location or logon settings using the Disaster Recovery Settings page, you will need to rebuild the recovery diskette(s) for that node to reflect the new backup location and/or logon settings for that node.

Static IP addressing: If you do not have a DHCP server on your network, and you must access a backup image that is only accessible via the network (for example, no backup image is located on the maintenance partition [D: drive] of the node to be recovered), then you must configure the recovery diskette so that it will use a static IP address and subnet mask when accessing the network.

On the recovery diskette, edit the file a:\net_sets.bat. Near the top of this file are two lines that begin with *rem* (comment lines) that, when you uncomment them, set the IPAddress and SubnetMask environment variables. Change these lines as follows:

1. Uncomment both lines by removing *rem* from the beginning of both lines.
2. For each line, what follows the equals sign (=) is an IP address expressed as a set of four space-separated numbers (an IP address without the dots [.]). Change the SubnetMask value to match the subnet mask your network uses. Change the IPAddress value to match the IP address you want to assign to the node, during the recovery operation. Do not insert dots between the numbers (octets) in either value.

As an example, here is how the lines would look for a node using IP address 192.168.1.200, and subnet mask 255.255.255.0:

```
set SubnetMask=255 255 255 0
set IPAddress=192 168 1 200
```

If you later want to reconfigure the recovery diskette to use DHCP to obtain an IP address instead of static IP addressing, you must reinsert *rem* in front of the SubnetMask and IPAddress lines to disable static IP addressing, as follows (based on the previous example):

```
REM set SubnetMask=255 255 255 0
REM set IPAddress=192 168 1 200
```

If you have multiple 10/100 Ethernet adapters: If your Model 325 has more than one 10/100 Ethernet adapter (per node), then you must configure the recovery

diskette to select the 10/100 Ethernet adapter to be used for disaster recovery over the network (the network over which the network drive(s) containing backup image(s) can be accessed). On the recovery diskette, edit the file a:\net_sets.bat, and add the following line:

set SLOT=*slotvalue*

where *slotvalue* is one of the following, depending on the PCI slot (on the rear of the node) in which the desired 10/100 Ethernet adapter is installed:

- 0x0009 for PCI slot 1
- 0x000a for PCI slot 2
- 0x0025 for PCI slot 3
- 0x0026 for PCI slot 4

Restoring the system drive: If you need to restore the system drive from a backup image created via the PSM Disaster Recovery panel as described above, you must use a recovery diskette created via the Disaster Recovery panel. If you did not create a recovery diskette then you must use the Recovery CD as described in "Using the Recovery Enablement Diskette and Recovery CD" on page 20 to restore the system drive to its original (factory) configuration.

To restore the system drive:

1. Set the write-protect tab of the recovery diskette to the write-protect position. This is a protection feature to prevent accidental initiation of the recovery process (by booting the node with the recovery diskette in the diskette drive).
2. Insert the recovery diskette in the diskette drive of the node, and restart the node.
3. The recovery process begins. The recovery diskette software will locate the first backup image it can find, based on the backup locations specified on the Disaster Recovery Settings panel in Microsoft Windows 2000 for NAS when the diskette was created. Once it has located a backup image it will begin restoring the system drive from the image. During the restore operation the hard disk drive LED (on the front right of the node's hard disk drive) will flash green or stay nearly solid green; this indicates write activity to the system volume.

   Note: If the hard-disk drive LED stays off for at least 10 minutes since you restarted the node, then there is a problem with the recovery procedure and it will not be able to restore the system volume from a backup image. Should this occur, you will need to use the Recovery CD as described in "Using the Recovery Enablement Diskette and Recovery CD" on page 20.
4. When the restore operation completes, the hard disk drive LED will turn off, and a short song will play periodically (every 15 seconds). Remove the diskette, set the write-enable tab back to the write-enabled position, and reinsert the diskette. The log file RESULTS.HTM will be written to the diskette; this log file can be viewed with any Web browser to examine the results of the restore operation.
5. Once the log file is written, another song will play (continuously). Remove the diskette and restart the node. If the restore was successful, the node will come back up in the state it was in at the time you created the backup image used for the recovery operation.

   Note: The persistent image that was created on the system drive (named *System Backup*) by the backup process is restored by the restore process as it is preserved in the backup image. It is recommended that you now delete that persistent image as it is no longer needed. On the

Persistent Images panel, select the persistent image named **System Backup** on drive C: from the list of persistent images, then click **Delete**, then click **OK** on the Delete Persistent Image panel that appears.

If the restore was unsuccessful, then you must use the Recovery CD as described in “Using the Recovery Enablement Diskette and Recovery CD” on page 20.

Rebuilding the maintenance partition: If this is a new hard drive or if the Maintenance (D:) partition is unusable, you will need to rebuild the Maintenance partition. You do this with the following steps:

Start Disk Management on the node. You can do this in one of two ways:

- Start a Terminal Services session to the node, then click the **IBM NAS Admin** icon, and then from the IBM NAS Administration console that appears, select **Computer Management**, then **Disk Management**.
- Start a Windows 2000 for NAS user interface session to the node, then select **Disks and Volumes**, then select **Disks**, and then provide your Administrator user name and password when prompted.

Once Disk Management has started, do the following:

1. In the Disk Management window, right-click on the unallocated area of Disk 0, and then click **Create Partition**.
2. In the Create Partition wizard, click **Next** and select **Primary Partition**.
3. Click **Next** and select **D:** as the drive letter.
4. Click **Next** and select **FAT32** as the file system and change the drive label to *Maintenance*.
5. Click **Finish** to close the wizard.

The partition will then be formatted. Once formatting is complete, the status of the partition should appear as *Healthy*, and the other properties should appear as: name *Maintenance*, drive letter *D:*, file system *FAT32*, size (approximately) *5.9 GB*.

Granting user access to persistent image files: You can give end-users access to files in the persistent images. For example, this would be helpful to a user who has accidentally corrupted a file and needs to get an uncorrupted copy of that file.

To enable end-user access to persistent image files, go into Terminal Services. Once you are in Terminal Services, click the **My Computer** icon. Next, click the volume on which you want to enable persistent image access. Then, go into the persistent images directory and right-click the mouse on your desired persistent image mount point, select **Sharing**, then specify sharing as desired. If you want to enable the same access to all persistent images on the volume, you can right-click on the persistent images directory (from the top level of the volume), select **Sharing**, and then specify sharing as desired.

Note: The share settings are maintained in a persistent image. Therefore, granting access to all end-users only permits those users to access files and directories within the persistent image that they would have been able to access originally on the actual drive.

PSM notes:

1. As mentioned, you can take and keep a maximum of 250 persistent images. These can be taken on local drives, or drives on the external storage that are logically local.

Note that on various panels, such as the New Persistent Image Schedule panel, you will see a field, *Keep the last:* (number of persistent images). The total number of persistent images that you enter in these fields will not override the maximum number of persistent images that you set in the Global Settings panel. For example, if your maximum number of persistent images is 10, and you enter in numbers in other fields that add up to greater than 10, only 10 persistent images will be taken.

2. You cannot take a persistent image of the maintenance drive (D:). Hence, you will not see it as a choice in either the New Persistent Image Schedule panel or the Create Persistent Image panel. Also, it is highly recommended that you do not take a persistent image of the clustering Quorum disk.
3. PSM stores the cache file for each drive on the drive itself. The first persistent image created on a particular drive will take a significant amount of time because the PSM cache file must be created (pre-allocated) for that drive.

   The time required for creation depends on the configured size of the cache file (15 percent of the total drive size by default). Creation takes roughly three to four minutes per gigabyte. For example, a 10-GB cache file would take 30 to 40 minutes to create. You should create a persistent image for a drive before scheduling any persistent images for that drive, to build the cache file. You may then delete the persistent image that you just created if you do not need to keep it.

   After the creation of the first persistent image on a volume, future persistent images on that volume will complete faster.
4. As mentioned, the default size of the cache file per drive is 15 percent of the total drive capacity. In most cases, that should be sufficient.

   However, it is possible that it will not be enough to maintain the number of persistent images you wish to keep concurrently on the drive, given the amount of file-write activity to the drive. PSM will automatically take action to prevent the cache file from overflowing, because if that occurred, PSM would be forced to automatically delete all persistent images on the drive (once it cannot keep track of changes made to the drive, it cannot maintain a valid persistent image).

   PSM takes the following actions as the cache file usage approaches a full condition:

   - Once the cache file usage exceeds the warning threshold (configured in the PSM Volumes panel for the drive; the default value is 80 percent), PSM generates a warning message to the system event log (viewable via the Windows 2000 Event Viewer in the IBM NAS Admin console), and to the alert log in the Microsoft Windows 2000 for Network Attached Storage user interface. The name of the source for the message will be *psman5*. Additionally, while the cache file usage is above the warning threshold, PSM prohibits any attempt to create a new persistent image, and logs an error message (to the system log and alert log). The text of the error message that is logged in the system event log (from *psman5*) is “A persistent image could not be created due to error 0xe000102b”.
   - Once the cache file usage exceeds the automatic deletion threshold (also configured in the PSM Volumes panel for the drive; the default value is 90 percent), PSM automatically selects a persistent image on the volume and deletes it to reduce the cache file usage. It selects the persistent image with the lowest retention value (as described above in the Persistent Images panel section). If more than one persistent image has the same (lowest) retention value, then the oldest image will be selected for deletion. If this deletion does not reduce the cache file usage below the automatic deletion threshold, then it will continue to select and delete persistent images until the cache file usage is reduced below the automatic deletion threshold. For each deletion,

PSM generates an error message to the system event log and to the Windows 2000 for Network Attached Storage alert log indicating that a persistent image was deleted.

You should periodically check the system event log or Windows 2000 for Network Attached Storage alert log to ensure that the cache file usage is not consistently high, forcing existing persistent images to be deleted and preventing new persistent images from being created. If you find that this is the case, you can increase the size of the cache file using the PSM Volumes page, but you will need to delete all persistent images currently on that volume as dynamic cache file resizing is not supported in this release.

5. When a shared volume is failed over from one engine in the Model 325 to the other engine, the persistent images for that volume move over with the volume. The Persistent Images panel on a particular engine will display only those persistent images which are on volumes that the engine owns at a point in time. If persistent images are scheduled for a volume, on a particular engine, a scheduled persistent image is created only as long as that engine owns the volume at the time the scheduled persistent image is to occur.

   To ensure that a scheduled persistent image will take place regardless of which engine owns the volume, you must do the following:

   a. Use the Schedules panel to create the schedule on the engine that currently owns the volume.
   b. Use the Cluster Administrator to move the disk group that contains the volume to the other engine.
   c. Use the Schedules panel on the other engine to create the same schedule that you created on the original engine, with all of the same parameters (start time, frequency, number to keep, etc.). In the previous step you had to move the volume to the other engine. The reason is that you can only create or edit a schedule for a volume on the engine that currently owns the volume. If an engine does not own the volume, you cannot select the volume when creating a new schedule via the New Persistent Image Schedule panel (under Schedules).
   d. Use the Cluster Administrator to move the disk group that contains the volume back to the original engine.

6. Volume restore of the system volume (C: drive) is not supported. If you attempt to restore a persistent image containing the system volume, the restore operation will not take place.
7. Volume restore of a data volume may require a reboot of the node. You will be notified by the Restore Persistent Images panel whether a reboot is required after a restore operation is initiated.

Attention: The recovery process invalidates persistent images and leaves them in an inconsistent state. So, if you plan to use the Recovery CD, it is recommended that you first delete all persistent images to ensure a clean reload of the system software. For more information on using the Recovery CD, see “Using the Recovery Enablement Diskette and Recovery CD” on page 20.

Recovering from a corrupted Quorum disk

The IBM TotalStorage Network Attached Storage 5195 Model 325 appliance is based on the Microsoft Windows Powered operating system and support Microsoft clustering. Clustering relies on data stored on a Quorum disk to maintain resource synchronization between the two nodes in the cluster. In the event of a power loss

to both nodes or a hardware failure that corrupts the Quorum data, the cluster service may not start, leading to the following eventlog error:

```
Event ID: 1147
Source: ClusSvc
Description: The Microsoft Clustering Service encountered a fatal error.
```

The Quorum drive data must be available so the cluster service can confirm that the cluster configuration on the local node is up to date. If it cannot read the log, the cluster service does not start to prevent the loading of old configuration data.

To restore the Quorum disk, a Microsoft Windows Backup utility backup of the System State of the boot drive (C:) of one node must be available. Backing up the entire boot drive also saves the System State. Backing up the System State automatically saves the Quorum log and other cluster files.

A Microsoft tool is needed as part of the Quorum restore procedure. This tool is called Clusrest.exe and can be downloaded from the Microsoft Web site at the following URL:
http://download.microsoft.com/download/win2000platform/clusrest/1.0/NT5/EN-US/clusrest.exe

The Quorum restore procedure involves restoring the system state and cluster state to the node followed by execution of the Clusrest.exe tool. Upon completion of the restore, the node should rejoin the cluster and return to normal operation.

1. Restore the entire boot drive of the node if needed. Otherwise, restore the System State to the node.
2. Ensure that the cluster service is stopped on the other node.
3. Restore the Quorum/cluster information to that node by selecting to restore at least the system state. This creates a temporary folder under the Winnt\Cluster folder called Cluster_backup.
4. Run the Clusrest.exe tool to rebuild the Quorum drive. The tool moves the cluster information from the node's boot drive to the Quorum drive.
5. After you complete the process and the cluster service has started successfully on the newly restored node, restart the cluster service on the other node.

Notes:

1. If you do not follow this process, and another node with a more current database takes ownership of the Quorum before you update the database from the restored node, the restore does not work.
2. Restoring a Quorum rolls the cluster back in time to the backup date. There are impacts to performing this operation that include loss of data. This operation should only be undertaken when it is absolutely necessary.

Replacing hot-swap drives

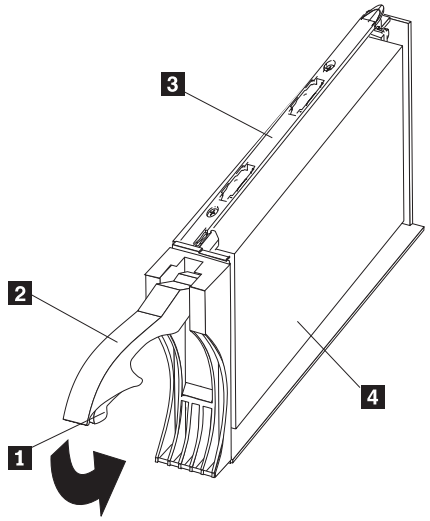
Drive problems include any malfunctions that delay, interrupt, or prevent successful I/O activity between the hosts and the hard disk drives. This section explains how to replace a failed drive.

Attention: Failure to replace the drives in their correct bays might result in loss of data. If you are replacing a drive that is part of a RAID level 1 or RAID level 5 logical drive, ensure that you install the replacement drive in the correct bay.

Use the following procedure to replace host-swap drives:

1. Check the hardware and software documentation that is provided with the system to see if there are restrictions regarding hard-disk-drive configurations. Some system Fibre Channel configurations might not allow mixing different drive capacities or types within an array.
2. Check the storage-management software for recovery procedures for a drive that has failed. Follow the steps in the software procedure before continuing with this procedure.
3. Determine the location of the drive that you want to remove.

   Attention: Never hot-swap a drive CRU when its green Activity LED is flashing. Hot-swap a drive CRU only when its amber Drive fault LED is on and not flashing, or when the drive is inactive with the green Activity LED on and not flashing.
4. Remove the drive CRU.
   a. Press on the inside of the bottom of the tray handle to release the blue latch **1** .
   b. Pull the handle **2** on the tray **3** out into the open position.
   c. Lift the drive CRU partially out of the bay.
   d. To avoid possible damage to the drive **4** , wait at least 20 seconds before fully removing the drive CRU from the RAID controller to allow for the drive to spin down.



   e. Verify that there is proper identification (such as a label) on the drive CRU, and then slide it completely out of the 5191 RAID Storage Controller.
   f. If you are replacing the drive, ensure that the filler piece remains in place for use with the new drive.
5. Install the new drive CRU.
   a. Gently push the drive CRU into the empty bay until the tray handle **2** touches the storage-server bezel.
   b. Push the tray handle **2** down into the closed (latched) position.
6. Check the drive LEDs.
   a. When a drive is ready for use, the green Activity LED is on, and the amber Drive fault LED is off.
   b. If the amber Drive fault LED is on and not flashing, remove the drive from the unit and wait 10 seconds; then, reinstall the drive.
7. Return to normal operation.

Administration notes

The following sections contain information on administering the Model 325.

Using a keyboard, monitor, and mouse for initial setup and configuration

It is highly recommended that you directly attach a keyboard, monitor, and mouse to the Model 325 when:

- Initially setting up and configuring the device
- Changing or adding to RAID arrays (for example, adding a new array with Storage Manager 7, adding a new RAID controller, or adding a storage expansion unit)
- Troubleshooting the device

Summary of configuration and administration tools for the Model 325

There are several ways to setup and administer the Model 325. Table 1 on page 18 suggests which tool you can use for specific functions, but does not list all options or combinations. The administrator training-level or administrator preferences may determine an alternate approach from that suggested in the table.

Table 1. Summary of configuration and administration tools for the Model 325

Administration Tool	Main functions
Windows Domain Controller (not NAS appliance)	On a clustered node, users and user groups must be defined and authenticated by the Windows Domain Controller.
IBM Advanced Appliance Configuration Utility	Access a headless Model 325 node, particularly for the initial setup of the network connectivity. (Alternatively, you can attach a keyboard, mouse, display to each node of the Model 325.) • Set time and date • Configure initial network connectivity parameters • Access to Windows 2000 for NAS GUI, Terminal Services (NAS Desktop), and Universal Manageability Services
Windows 2000 for NAS GUI	Provides ease-of-use administration, but not all the capability of Terminal Services and IBM NAS Administration • Configure networking connectivity, private (for clustering) and public LAN connections (must do on each node) • Create and format logical drives • Join domains • Setup access permissions and disk quotas for CIFS, NFS, HTTP, FTP, and NetWare shares (must configure on node where volume is active) • Use Persistent Storage Manager
IBM NAS desktop and IBM NAS Admin program, via a Terminal Services session or a directly-connected keyboard and display	Provides in-depth administration of all aspects of Model 325. Provides all of the Windows 2000 for NAS GUI functions above, plus: • Use NAS Backup Assistant, or NT Backup and Restore wizard • Learn detailed inventory information about hardware, OS, and so on, using Universal Manageability Services • RAID configuration via Storage Manager 7 – Create RAID arrays and LUNs – Add additional RAID or storage enclosure after initial purchase – Rename storage subsystems • Cluster Administration – Setup cluster – Define failover for each volume – Evict a node (force failover of a node) – Cluster resource balancing by assigning preferred node • Diagnose system problems – Check 10/100 or GB Ethernet using PROSet II – Check Fibre Channel card using FastTCheck – Check RAID subsystem using Storage Manager 7
Disaster Recovery	Restores a previously saved PSM image of the system partition to a failed machine. This will restore all configuration information on the failed node. You create the recovery boot diskette from the PSM tools in the Windows for 2000 NAS GUI.
Recovery CD	Reinstalls the software to the original state as shipped on the machine; however, does not restore configuration information (so configuration changes you applied to the original shipped configuration are lost). You must first boot with the Recovery Enablement Diskette, and then reboot with the Recovery CD. To create the Recovery Enablement Diskette run \DiskImages\Recovdsk.bat on the Supplemental CD-ROM.
Planar ASM Adapter configuration program	Configures the onboard planar Advanced Systems Management Adapter. To create this diskette, run C:\IBM\ASMP\UPDATES\32P0083.EXE on the Model 325 operating system volume.
ASM PCI Adapter configuration program	Configures the optional Advanced Systems Management PCI Adapter. To create this diskette, run C:\IBM\ASMP\UPDATES\24P1874.EXE on the Model 325 operating system volume.

Determining who is using the network-attached storage

Occasionally, the administrator may want to know who is using the network-attached storage. The administrator can determine this information as follows:

1. Start a Windows Terminal Services session from the administrator's console to the Model 325.
2. Click on the **IBM NAS Admin** icon on the desktop.
3. In the left plane, click on **File Systems**, then **Shared Folders**, then **Sessions**.
4. The users currently using the storage are displayed. If necessary, you can close those sessions with a right-click. Before you close a session, you can notify the user that you are going to close the session by clicking on **Start**, **Programs**, **Accessories**, **Command Prompt**, and then issuing the **net send** *hostname messagetext* command.

AntiVirus protection

You can perform AntiVirus scanning of Model 325 storage from clients having the appropriate access permissions. Also, you can install Norton AntiVirus Version 7.5 or later on the Model 325 engine using normal Windows 2000 software installation procedures.

Depending on configuration options, AntiVirus scanning may use substantial CPU or disk resources. Therefore, you should carefully select scanning options and scan schedule.

Norton AntiVirus is not included with the Model 325; you must purchase it separately.

Memory notes

The following sections contain information on adding memory.

Adding more engine memory to increase performance

You can enhance the performance of the Model 325 in an NFS environment by adding more RAM to its processor. To do this:

1. Purchase one or two 512M memory SIMMs (part number 33L3127) from Options by IBM at www.pc.ibm.com/us/options/.
2. Follow the instructions in Chapter 3, section "Replacing memory modules," of the *Installation Guide*.
3. Before rebooting the box, attach a keyboard and display directly to the rear connectors of the product. During the first IPL, you will have to read and answer questions about the additional memory you have installed.

Using the Recovery CD-ROM if you have added more processor memory

If you have installed more processor memory, and later use the Recovery CD-ROM (see "Updated information on using the Recovery and Supplementary CDs"), you will have to attach a keyboard and display and answer questions about the additional memory you have installed.

Updated information on using the Recovery and Supplementary CDs

The information in Chapter 8 of the *User's Reference* applies to Version 1.00 of the Model 325 software. For Version 1.50, the information in this section replaces the

information in Chapter 8. Note that the Recovery CD for Version 1.50 is now a set of 2 CDs, referred to collectively as the Recovery CD Set, consisting of Recovery CD 1 and Recovery CD 2.

Attention: Changing the preloaded software configuration of this product, including applying or installing unauthorized service packs or updates to preinstalled software, or installing additional software products that are not included in either the preloaded image or on the Supplementary CD, may not be supported and could cause unpredictable results. For updated compatibility information, please see http://www.storage.ibm.com/support/nas

To correct problems with a preloaded software component, back up your user and system data. Then use the Recovery CD Set to restore the preloaded software image.

This chapter describes the applications included on the Supplementary and Recovery CDs, and how and when you should use them.

As an alternative to using the Recovery CD Set, you can use the restore portion of the disaster recovery solution provided by Persistent Storage Manager (PSM) to recover the node, if you have met the requirements (including creating a PSM backup image and PSM recovery diskette). The restore function allows you to restore the node to the state it was in at the time of the PSM backup, in one step, without having to revert back to the original (factory) configuration which would require you to subsequently reconfigure clustering and other components. See “Restoring the system drive” on page 11 to determine whether you have met the requirements. If so, you can use the PSM recovery method. If you have not met the requirements for using the PSM recovery method, or if the PSM recovery fails, then you must use the Recovery CD Set as described in this chapter.

Using the Recovery Enablement Diskette and Recovery CD

The Recovery CD Set (set of 2 CDs, labeled as Recovery CD 1 and Recovery CD 2) contains the preload image for your Model 325 and is used to recover the preloaded image on either node of your appliance. You must start the (failed) appliance node using the Recovery Enablement Diskette before you can boot Recovery CD 1.

Attention: The Model 325 does not have a monitor, keyboard, or mouse attached to it under normal operating conditions. Because of this, you can not interact with the preload-image restore process using a monitor. Starting Recovery CD 1 will, without visually prompting the user, automatically destroy all data on the system drive. Use the Recovery Enablement Diskette and Recovery CD Set only when it is absolutely necessary to restore the preloaded system image.

To recover the preloaded image on a (failed) node, do the following steps. Note that the recovery process invalidates persistent images and leaves them in a state that is inconsistent with their pre-recovery state. So, if you plan to use the Recovery CD Set, it is recommended that you first delete all persistent images to ensure a clean reload of the system software.

1. On the other (working) node of the Model 325, select Cluster Administration, located in the Cluster Tools folder in the IBM NAS Admin. If prompted for a cluster name, enter the name of the cluster, and then click **Open**.
2. The cluster name appears in the left panel. Underneath it, locate the name of the failed node, right-click on the failed node machine name, and select **Evict Node**. The name of the failed node will be removed from the left pane, and the cluster will now contain only the working node of the Model 325.

3. Attach a keyboard and display to the failed node.
4. Insert the Recovery Enablement Diskette into the diskette drive of the failed node and restart the node. When the Recovery Enablement Diskette has completed loading and modifying your node startup sequence, the node will begin a continuous beep. Do not continue with this procedure until the node begins the beep.

> **Important**
>
> The Recovery Enablement Diskette enables the Model 325 to start from the CD-ROM drive. You will not be able to restore the preload image from the Recovery CD Set without first restarting the appliance using the Recovery Enablement Diskette.

5. Remove the Recovery Enablement Diskette from the diskette drive of the failed node.
6. Place Recovery CD 1 in the CD-ROM drive of the failed node and restart the node.
7. If you have installed more processor memory on the failed node, the BIOS configuration program will now appear. Click **Continue** on the first screen, then click **Continue** again, then click **Exit Setup**, and finally, click **Yes, save and exit Setup**.
8. The recovery process will begin automatically and the original manufacturing preload will be restored. During the restoration of the preload, you will be prompted (by the image restoration software) to insert the CD containing the file NASIMG.002. At this point, remove Recovery CD 1 from the CD-ROM drive and insert Recovery CD 2 in the drive, and then press Enter to complete the restoration. Once the preload image is restored, the node restarts automatically.
9. If you have installed more processor memory, the BIOS configuration program will now appear a second time. Click **Continue** on the first screen, then click **Continue** again, then click **Exit Setup**, and finally, click **Yes, save and exit Setup**. You may now detach the keyboard and display from the failed node and allow the recovery process to complete automatically.

> **Important**
>
> - After the node restarts, a series of configuration and system preparation programs that finish configuring the node run automatically. These programs must finish running before you use any included applications (such as the IBM Advanced Appliance Configuration Utility or the Terminal Services Client) to connect to or configure your Model 325. Do not connect to or configure the node for at least 15 minutes after system restart. This notice applies only to the first time the Model 325 node is started after using the Recovery CD Set.
> - Logical Disk 0 will be configured to have a 3-GB NTFS boot partition. Any other previously configured logical disk drives, as well as the remainder of Logical Disk 0 (which, on the original hard disk drive of the node, contains the Maintenance partition, but for a replacement hard disk drive would not contain any other partitions), will be left unchanged.

10. Reinstall all software updates you had installed on the failed node since you installed the Model 325 out of the box. Or, if the Recovery CD Set you used in

this procedure is a newer version than the one you received with the Model 325, reinstall only those software updates that are newer than those on the Recovery CD Set.

11. If you are using the recovery procedure to restore the failed node after replacing the internal hard disk drive, continue with this step. Otherwise, go to Step 12. You must now rebuild the Maintenance (D:) partition on the new hard disk drive, as the recovery process only rebuilds the System (C:) partition.

    Start Disk Management on the failed node. You can do this in one of two ways:
    - Start a Terminal Services session to the node, then click the **IBM NAS Admin** icon, and then from the IBM NAS Administration console that appears, select **Computer Management**, then **Disk Management**.
    - Start a Windows 2000 for NAS user interface session to the node, then select **Disks and Volumes**, then select **Disks and Volumes** again, and then provide your administrator user name and password when prompted.

    Once Disk Management has started, do the following:
    a. In the Disk Management window, right-click on the unallocated area of Disk 0, and then click **Create Partition**.
    b. In the Create Partition wizard, click **Next** and select **Primary Partition**.
    c. Click **Next** and select **D:** as the drive letter.
    d. Click **Next** and select **FAT32** as the file system and change the volume label to *Maintenance*.
    e. Click **Finish** to close the wizard. The partition will then be formatted. Once formatting is complete, the status of the partition should appear as *Healthy*, and the other properties should appear as: name *Maintenance*, drive letter *D:*, file system *FAT32*, size (approximately) 5.9 GB.

12. On the failed (now recovered) node, follow the procedures outlined in Step 3, Chapter 1, of the *User's Reference* (and described in detail in other chapters, for which the outline provides a roadmap) for configuring a joining node. The recovered node will rejoin the cluster which already contains the other (working) node. You will also need to reconfigure any cluster resource balancing you had set up prior to recovery, such that the recovered node will once again be the preferred owner of any resources for which it had been the preferred owner prior to the recovery. See "Cluster resource balancing" in Chapter 5 of the *User's Reference* for more details on configuring resource balancing.

Using the Supplementary CD

The Supplementary CD contains documentation and copies of key software applications that are preinstalled on your Model 325. Table 2 on page 23 includes the names of the directories found on the Supplementary CD and a description of the contents of the directory.

Table 2. Supplementary CD directories

Directory Name	Contents
IBM Advanced Appliance Configuration	IBM Advanced Appliance Configuration console and agent installation files. The IBM Advanced Appliance Configuration agent is preinstalled as a Windows Powered service on the Model 325. To install the Advanced Appliance Configuration console (on another network-attached workstation running Windows 98, Windows NT, or Windows 2000), run lpsetup.exe (if you have Supplementary CD Version 1.5) or setup.bat (if you have Supplementary CD Version 1.0) from the *x*:\IBM Advanced Appliance Configuration directory, where *x* is the drive letter assigned to your workstation's CD-ROM drive. **Note:** When the installation completes, it will leave behind a temporary directory named iaacu on the workstation, under the directory specified by the TEMP environment variable (usually c:\temp; you can determine the value of the TEMP variable by typing `set temp` from a DOS command prompt). You should remove this directory (using Windows Explorer) after the installation has completed.
DiskImages	Contains diskette image for the Recovery Enablement Diskette. To create the Recovery Enablement Diskette, run RecovDsk.bat and insert a HD 1.44 floppy diskette into drive A: when prompted. Be sure to read the readme!.txt file located in this directory for last minute and model specific updates.
I386	Windows Powered installation files. If you add device drivers, OS features, and so on, you may be prompted to insert your Windows Powered CD-ROM. If so, insert the Supplementary CD, and specify path x:\i386, where x is the drive letter assigned to your CD-ROM drive.
W2KSP2	Windows Powered Service Pack 2, which is preloaded on your Model 325 (if you are at Version 1.00, Build 70 or later). If you add any device drivers, OS features, and so on, you should reapply Service Pack 2. Run the executable w2ksp2.exe, and follow the instructions provided.
Services for UNIX	SFU 2.2 installation files, zipped into a self-extracting executable, sfu22.exe. If you add features that are not preloaded, you will be prompted for these installation files. You will need to extract the installation files onto the hard drive of your Model 325. It is recommended that you use the maintenance drive (D: drive) as the destination, but you can use the system drive (C: drive). On whatever drive you choose, make sure that you have at least 250 MB of free space available, create a temporary directory on the drive, and then issue the following command from the Services for UNIX directory on the Supplementary CD: sfu22 *path*, where *path* is the drive letter and path of the temporary directory you created. Then when you are prompted by the Services for UNIX installation to provide the path of the installation files, specify the same path you specified in extracting the files from the CD.
Terminal Services Client	The stand-alone Win32 Terminal Services Client application. The Model 325 appliance supports Web-based terminal services, so this is an optional installation. To install the Terminal Services Client, run setup.exe from the Disk1 subdirectory.
readme.txt	This is a text file that describes the contents of the Supplementary CD.

Alternate method for managing FAStT200 storage

Storage Manager 7 provides two methods for managing storage subsystems: the host-agent managed method and the directly managed method. One or both methods can be used. The Model 325 comes preconfigured with the host-agent

management method. The directly managed method is used when an alternate management path is desired in the case of failure of the host-agent management path.

Directly managed method

With this method, you use the SM7 client software to manage the storage subsystem directly over the network through each controller's Ethernet connection. The following is required for directly managing a controller:

- A Windows 2000 client computer connected to the local Ethernet network
- SM7 client software. The SM7 version 7.02 client software package can be downloaded from the NAS 5195 Model 325 download Web page using the following URL:
  http://ssddom02.storage.ibm.com/techsup/nas/nasdown.nsf/fToolProdView/KUGPJE9903P?Openform
- DHCP server connected to the local Ethernet network
- 1 Ethernet cable for each storage subsystem controller in the FAStT200 to connect to the local Ethernet network. (1 dual storage subsystem controller FAStT200 = 2 Ethernet cables, 2 dual storage subsystem controller FAStT200s = 4 Ethernet cables)
- Ethernet hub or switch

The directly managed installation and configuration steps are:

1. Install the SM7 client software on the Windows 2000 client computer (not Node A or Node B)
2. Connect each storage subsystem controller in the FAStT200 to an existing Ethernet network using ethernet cables. A separate stand-alone diagnostic network can be created by connecting the SM7 client computer, DHCP computer and all storage subsystem controllers to an Ethernet hub.
3. Start SM7. The Enterprise Management window will appear and a pop up window will say that it is not configured to monitor any devices. Select **Yes** to have it search for subsystems.

If the subsystems do not appear, then the IP address assigned to each storage subsystem controller in the FAStT200 must be identified so it can be input into SM7. To identify the IP addresses:

1. Write down the ethernet MAC addresses of each storage subsystem controller in the FAStT200. The MAC address is located on a label directly under the RJ-45 Ethernet port on the rear of each storage subsystem controller of the FAStT200; for example, 10-11-12-13-14-15.
2. Find the IP addresses on the DHCP server that were assigned to the MAC addresses of the storage subsystem controllers. There will be either two or four IP addresses.
3. From the SM7 Enterprise Management window, select **Edit ->Add Device** and add the IP addresses that were assigned to the storage subsystem controllers.

The storage can now be managed using the external Ethernet connection regardless of the state of the Node A and Node B engines.

Part Number: 38P8454

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

(1P) P/N: 38P8454