TotalStorage™ Network Attached Storage 300G
Models G01 and G26

User's Reference

Release 2

> **Note**
>
> Before using this information and the product it supports, be sure to read the general information in "Appendix A. Notices" on page 101.

First Edition (November 2001)

This edition applies to Release 2 of the IBM 5196 TotalStorage Network Attached Storage 300G, (Models G01 and G26, product number 5196-G26) and to all subsequent releases and modifications until otherwise indicated in new editions.

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.

Contents

Figures

Tables

About this book

This book provides information necessary to configure and administer the IBM 5196 TotalStorage Network Attached Storage 300G (Models G01 and G26).

Hereafter, the Models G01 and G26 are generically referred to as the "NAS 300G" unless otherwise noted.

Who should read this book

This book is for NAS 300G administrators.

Note that although this product is relatively easy to install, configure, and administer, the NAS 300G administrator should have experience in at least the following skills, or have access to personnel with experience in the skills:
- Microsoft® Windows®
- Networking and network management
- Disk management
- SAN Management
- General technologies of the product (such as clustering, storage, RAID, and so on)
- Critical business issues (such as backup, disaster recovery, security)

Frequently used terms

This document contains certain notices that relate to a specific topic. The caution and danger notices also appear in the multilingual Safety Information on the Documentation CD that came with the appliance. Each notice is numbered for easy reference to the corresponding notices in the Safety Information.

The following terms, used within this document or within the Safety Information, have these specific meanings:

Term	Definition in this document
Attention	These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
Caution	These notices indicate situations that can be potentially hazardous to you. A caution notice is placed just before descriptions of potentially hazardous procedure steps or situations.
Danger	These notices indicate situations that can be potentially lethal or extremely hazardous to you. A danger notice is placed just before descriptions of potentially lethal or extremely hazardous procedure steps or situations.
Notes	These notices provide important tips, guidance, or advice.

Publications

The latest versions of the following product publications are available in softcopy at:

`http://www.ibm.com/storage/support/nas`

Descriptions of the NAS 300G publications

The NAS 300G library consists of the following publications:

- *Hardware Installation Guide*

  This book describes hardware physical specifications, electrical specifications, cabling, environmental specifications, and networking specifications for installing the NAS 300G.

- *User's Reference* GA27-4271

  This book describes such operational and administrative activities as:
  - Using the configuration utilities
  - Administering the NAS 300G
  - Troubleshooting
  - Using the Recovery and Supplementary CDs

Hardcopy publications shipped with the NAS 300G

The following publications are shipped in hardcopy and are also provided in softcopy (PDF) form at:

`http://www.ibm.com/storage/support/nas`

- *IBM 5196 TotalStorage Network Attached Storage 300G Installation Guide*, GA27-4270-01
- *Release Notes*

  This document provides any changes that were not available at the time this book was produced.

Note that the *User's Reference* is provided in softcopy only.

Related publications

The following publications contain additional information about the NAS 300G:
- *IBM 5196 TotalStorage Network Attached Storage 300G Installation Guide* GA27–4270–01
- *IBM 5196 TotalStorage Network Attached Storage 300G (NAS 300G) Service Guide* GA27–4274–01
- *UM Services User's Guide* (on the Documentation CD that came with the appliance)

Web sites

The following Web site has additional and up-to-date information about the NAS 300G:

- **http://www.ibm.com/storage/nas/**

In addition, for the latest troubleshooting guidance and symptom-fix tip information, go to the IBM support Web site at:

- **http://www.ibm.com/storage/support/nas**

This site contains additional information, gathered from field experience, not available when this document was developed.

Chapter 1. Introduction

The NAS 300G connects clients and servers on an IP network to Fibre Channel storage, efficiently bridging the gap between LAN storage needs and SAN storage capacities.

This appliance offers a storage solution for both Windows, UNIX, and UNIX-like environments, including mixed Windows/UNIX environments that enable Windows and UNIX clients and servers to share the same Fibre Channel storage. The NAS 300G delivers excellent value, state-of-the-art systems management capabilities, and task-optimized operating system technology.

Models G01 and G26 replace Models G00 and G25. Enhancements provided by the new models include more:

- Options in configuring Ethernet connections
- Options in configuring Fibre Channel connections
- Options for tape backup

To provide an easier installation, both NAS 300G models have preloaded, preconfigured, pretuned, and pretested operating systems, and supporting system management software.

The single-node Model G01 features one engine (IBM 5187 Network Attached Storage Model 6RZ) with:

- Dual 1.133 GHz processors
- 1 GB memory
- Two redundant 270 watt power supplies
- 1-port Fibre Channel adapter for storage area network (SAN) connection
- Four high-performance PCI adapter slots for optional adapters:
  - Additional Single-Port or Dual-Port Fibre Channel adapter
  - Single-Port 10/100 Ethernet adapter
  - Quad-Port 10/100 Ethernet adapter
  - Gigabit Ethernet adapter
  - ServeRAID-4Lx adapter
  - Remote Supervisor Adapter

The dual-node Model G26 features:

- Two engines (IBM 5187 Network Attached Storage Model 6RZ), each with:
  - Dual 1.133 GHz processors
  - 1 GB memory
  - Two redundant 270 watt power supplies
  - 1-port Fibre Channel adapter for storage area network (SAN) connection
  - Four high-performance PCI adapter slots for plugging in optional adapters. (Communication between the two engines takes place through an integrated 10/100 Mbps Ethernet port on each engine's planar board.)
- Optional adapters:
  - Additional Single-Port or Dual-Port Fibre Channel adapter
  - Single-Port 10/100 Ethernet adapter
  - Quad-Port 10/100 Ethernet adapter
  - Gigabit Ethernet adapter
  - ServeRAID-4Lx adapter
  - Remote Supervisor Adapter

In addition, the Model G26 provides clustering and failover protection. This high-availability design helps protect against appliance failure and increases uptime to provide continuous access to data.

Note: Information about the Model G26 engine applies to both its engines.

The preloaded software stack is based on the Windows Powered OS operating system, which is very similar to Microsoft® Windows® 2000 Advanced Server. Preloaded software includes:

Microsoft Windows 2000 for Network Attached Storage
>   Enables remote administration of the appliance using a web-based graphical user interface (GUI)

Microsoft Windows Terminal Services
>   Enables remote administration of the appliance using its Windows desktop

Microsoft Cluster Services
>   Provides clustering support and failover protection

Microsoft Services for UNIX
>   Provides file access to UNIX and UNIX-based clients and servers via Network File System (NFS) protocol

IBM Director Agent and Universal Manageability Server Extensions
>   Provides system management support based on industry standards (in conjunction with the IBM Director console application as well as other management software)

IBM Advanced Appliance Configuration Utility agent
>   Supports management via the IBM Advanced Appliance Configuration Utility console application (supports aggregate web-based management of all of your IBM appliances)

ServeRAID Manager RAID Configuration and Monitoring
>   Provides configuration tools and RAID management of the ServeRAID-4x adapter

IBM FAStT Management Suite Java (MSJ)
>   Provides diagnostics for the fibre channel adapters

Intel PROSet II
>   Provides diagnostics for the Intel Ethernet adapters

Alacritech SLICuser
>   Provides diagnostics for the quad-port Ethernet adapter

Columbia Data Products® Persistent Storage Manager (PSM)
>   Provides 250 persistent images of customer data and enables full online backup of system with Microsoft&'s backup applications

Tivoli® Storage Manager Client
>   Provides data backup/archive support (in conjunction with Tivoli Storage Manager Server)

Tivoli SANergy
>   Provides shared data access to the SAN storage at fibre channel speed

Roadmap for setting up and configuring the NAS 300G

The following roadmap presents the requirements and instructions required to set up and configure the NAS 300G. Following these directions and referring to the appropriate sections of this book will help you in this task.

Prerequisites

Note that these prerequisites apply only to the Model G26.

- A Domain Controller must exist on the network and a login ID must be defined for each node to log on. Each node must join the same domain.
- All Windows shared disks must be defined as basic. Windows 2000 dynamic disks are not supported.
- All shared disks between the two cluster nodes must have the same drive letter.
- All shared storage must be defined as NTFS and be primary partitions
- Compression cannot be enabled on any disk partition
- Each node must have one private and one public adapter

Cluster setup requirements (Model G26)

See "Cluster setup requirements" on page 5.

Configuration and administration tools ("Chapter 2. Configuration and administration tools" on page 9)

The NAS 300G is a network-attached storage appliance that has several different methods of configuration depending on your environment.

Determine how you will manage the device. You can manage the NAS 300G in "headless" mode or with a keyboard, display, and mouse directly attached to each node. For "headless" management of the NAS 300G, you can use one of the following tools:

- Terminal Services, for remote configuration and management from another device on the network
- Universal Manageability Services (UMS) for management through a web browser
- Windows 2000 for NAS, a Web-based GUI for those not familiar with the Windows desktop
- IBM Advanced Appliance Configuration Utility (IAACU) for setup and configuring multiple devices or other appliances on a single network

Having determined how you will manage the NAS 300G, you can begin setup and configuration of the device.

Step 1 - Initial Network Setup ("Chapter 3. Getting started" on page 25)

- Configure both nodes to enable access over the network. First, use DHCP or static addressing to set up one public network connection in each node. If you are running with a keyboard, display, and mouse, set up a public network connection to access the device.
- If you are running in a headless environment, you can use one of the following methods:
  - If DHCP is installed and the IP address requested can be determined, you can use this method for initial setup, but you should change this address to static later in the configuration.

– If you have multiple appliances or cannot determine the DHCP address, you can install the IAACU utility to identify appliances and define IP addresses. The tool will also allow you to set static addresses.

• Complete the steps in "Maintenance (Date and Time)" on page 27 and "Network Setup" on page 27.

Step 2 - Define storage and set up partitions ("Chapter 4. Setting up storage" on page 29)

The NAS 300G attaches to your SAN-attached storage device, via fibre-channel, and provides your Ethernet LAN-attached clients access to that storage. You must define storage arrays and logical drives on the SAN-attached storage device and set up Windows partitions on the logical drives as defined in "Chapter 4. Setting up storage" on page 29.

Step 3 (Model G26) - Complete network setup and cluster installation ("Chapter 6. Completing networking, clustering, and storage access setup for the Model G26" on page 39)

1. Power on either node. As a reference point, this is the first node.
2. First node setup steps:
   a. Networking setup

      See "Networking setup" on page 39. Note the cautionary statement at the beginning of that section.
   b. Domain setup

      See "To join a node to a domain" on page 41.
3. Power down the first node.
4. Power on the other node. As a reference point, this is the joining node.
5. Joining node setup steps:
   a. Networking setup

      See "Networking setup" on page 39.
   b. Shared storage setup

      For the joining node, the only part of this step that you will need to complete is assigning drive letters on the shared storage, making sure that the drive letters are the same as those on the first node.

      Also, if you are having trouble with the Fibre Channel connection, you can use the steps in "Testing the fibre-channel host adapter with FAStT MSJ" on page 91 to diagnose the problem.
   c. Domain setup

      See "To join a node to a domain" on page 41.
   d. Power down the joining node.
6. Power on the first node and complete "Cluster setup" on page 42.
7. Power on the joining node and complete "Cluster setup" on page 42.

Step 3 (G01) - Complete storage access setup ("Chapter 5. Completing storage access setup for the Model G01" on page 31)

At this point you can add users and file shares to the Model G01, to allow the storage to be accessed by clients and servers on the network.

Step 4 (Model G26) - Cluster administration ("Cluster administration" on page 43)

At this point you can add users, file shares, and complete other configuration tasks to improve operations of the NAS 300G in a cluster environment.

Step 5 - Additional functions ("Chapter 7. Additional administrative functions" on page 51)

Additional functions are available for backup, persistent images, and adding more storage areas. It is recommended that once you complete the setup and configuration procedures, you use the Persistent Storage Manager Disaster Recovery option ("Disaster Recovery" on page 56) or other method to back up the system configuration in the event of a failure.

Also, for the Model G26, **it is imperative to use the system shutdown procedure** described in "Appendix F. Powering off and powering on the NAS 300G" on page 135 to ensure system integrity.

Cluster setup requirements

Before you configure the NAS 300G nodes for clustering function, ensure that the following requirements are met:

Network Requirements

- A unique NetBIOS cluster name
- At least three unique, static IP Addresses for the public network: one for each node (for client access through the PCI NIC adapter) and one for the cluster itself (the administration IP Address)

  Table 1 on page 7 shows a summary of the networking information you will need for the public connection.
- Two static IP addresses for the cluster interconnect on a private network or crossover, through the onboard Ethernet adapter. The default IP addresses for the private network adapters are 10.1.1.1 for the first node in the cluster, and 10.1.1.2 for the node that joins the cluster. (The top node in the NAS 300G is considered the first node, and the bottom node is considered the joining node.)

Notes:

1. If you are not the system administrator, contact that person for the applicable IP addresses.
2. One additional static IP address will be required for creating each clustered group.
3. Each node in a cluster must join the same domain and be able to access a Primary Domain Controller (PDC) and DNS server, but it is not required that the nodes log into the domain.
4. Each node in the cluster must have at least two network adapters: at least one for the public network and the other for the private interconnect.

Shared Disk Requirements

- All shared disk arrays and devices, including the Quorum Disk, must be physically attached to a shared storage bus
- All shared disks must be configured as **basic** (not dynamic) disks
- All shared disks **must have the same drive letter** on each node
- All partitions on these disks must be formatted with NTFS
- All partitions on these disks must also be Primary Partitions

• Compression must not be enabled

Powering off and powering on the NAS 300G

The clustering function requires special considerations when you need to power off and power on the NAS 300G. See "Appendix F. Powering off and powering on the NAS 300G" on page 135 for details.

Table 1. Networking information worksheet for the public connection

Cluster component	Information needed
Cluster	**Cluster name:** **IP address:** **Subnet:**
First node	**Computer name (example: IBM5196–23H1234):** **IP address:** **Subnet:** **Gateway:** **Preferred DNS:** **WINS server (optional):**
Joining node	**Computer name:** **IP address:** **Subnet:** **Gateway:** **Preferred DNS:** **WINS server (optional):**
Domain to join	**Domain name:**

Chapter 2. Configuration and administration tools

> **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/nas/index.html`
>
> To correct problems with a preloaded software component, back up your user and system data. Then use the Recovery CD to restore the preloaded software image.

The NAS 300G appliance comes with the following configuration programs that you can use to configure and administer the appliance:

- Terminal Services Client
- IBM Advanced Appliance Configuration Utility (IAACU)
- Universal Manageability Services
- Windows 2000 for Network Attached Storage

This chapter describes these tools in general and then in detail.

There are several ways to setup and administer the NAS 300G. Table 2 on page 10 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.

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

It is highly recommended that you directly attach a keyboard, monitor, and mouse to the NAS 300G when:

- Setting up and configuring the device
- Changing or adding to RAID arrays defined on the fibre-attached storage
- Troubleshooting the device

Table 2. Summary of configuration and administration tools for the NAS 300G

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 NAS 300G node, particularly for the initial setup of the network connectivity. (Alternatively, you can attach a keyboard, mouse, display to each node of the NAS 300G.) • Set time, date, and 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, Novell® NetWare®, and Apple Macintosh 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 NAS 300G. 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
	• 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 FastT MSJ
	  – Check Alacritech® Quad-Port Ethernet Adapter using SLICuser

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 Set	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 Supplementary CD-ROM.
Integrated System Management Processor (ISMP) configuration program	Configures the ISMP that is integrated on the engine's planar board. To create this diskette, run C:\IBM\ASMP\UPDATES\32P0303.EXE on the NAS 300G operating system volume.
Remote Supervisor Adapter (RSA) configuration program	Configures the optional RSA. To create this diskette, run C:\IBM\ASMP\UPDATES\33P2474.EXE on the NAS 300G operating system volume.

Terminal Services Client

The Terminal Services Client, when installed on a workstation that is attached to the same network as the NAS 300G, enables you to remotely administer the appliance using the NAS 300G desktop. If you are familiar with administrative tasks using a Windows desktop, you can use Terminal Services.

See "Terminal Services and the IBM NAS Administration Console" on page 12 for more information.

IBM Advanced Appliance Configuration Utility (IAACU)

The IBM Advanced Appliance Configuration Utility (IAACU) aids in setting up and reconfiguring the network configuration on your appliances. The IAACU agent works with the IAACU Console to automatically detect the presence of appliances on the network.

Once the appliance is detected by the IAACU Console, you can use the IAACU to:

- Set up and manage the appliance's network configuration, including assigning the IP address, default gateway, network mask, and DNS server to be used by the appliance. (See the note in "Network Setup" on page 27, regarding the Ethernet adapter that is integrated on the planar board.)
- Start Universal Manageability Services on the appliance, enabling you to do more advanced systems-management tasks

See "IBM Advanced Appliance Configuration Utility" on page 13 for more information.

Universal Manageability Services

Universal Manageability Services (UM Services) provides point-to-point remote management of client systems through a Web browser window. You can use UM Services to:

- Learn detailed inventory information about your computers, including operating system, memory, network cards and hardware
- Track your computers with features such as power management, event log, and system monitor capabilities
- Upwardly integrate with Tivoli Enterprise, Tivoli NetView®, Computer Associates Unicenter, Microsoft SMS, and Intel® LANDesk Management Suite

In addition, you can link to Windows 2000 for Network Attached Storage and Terminal Services from UM Services.

See "Universal Manageability Services" on page 20 for more information.

Windows 2000 for Network Attached Storage

For administrators who are not familiar with the Windows operating systems, the NAS 300G provides a Web-based GUI, Microsoft Windows 2000 for Network Attached Storage (Windows 2000 for NAS). Using Windows 2000 for NAS, you navigate through various administrative task categories by clicking on the appropriate links or buttons, and then selecting a task from that category.

See "Windows 2000 for Network Attached Storage" on page 22 for more information.

Terminal Services and the IBM NAS Administration Console

If you are familiar with Windows operating systems, you can use Terminal Services. In some cases, you must use Terminal Services to complete administrative tasks.

You can access Terminal Services in two ways:

1. Through the UM Services browser, as described in step 3 on page 21.
2. By using the Terminal Services Client software.

To use Terminal Services Client, complete the following steps to install it on the remote workstation and connect to the NAS 300G appliance:

1. Insert the Supplementary CD into the workstation CD-ROM drive.
2. Click **Start** → **Run**.
3. In the **Open** field, type (with quotes)

   `"x:\Terminal Services Client\Disk 1\setup.exe"`

   where *x* is the drive letter assigned to the CD-ROM drive. Then click **OK** to begin the Terminal Services Client Setup program.
4. Accept the defaults in each window that opens or refer to the Microsoft Windows documentation for more instructions. When the Terminal Services Client Setup program is completed, proceed to the next step.
5. Check the workstation network TCP/IP protocol configuration settings.

Connecting to the desktop through Terminal Services

To connect to Terminal Services from your workstation, do the following:

1. Click **Start** → **Programs** → **Terminal Services** → **Terminal Services Client**.
2. In the Server field, select the computer name of the desired NAS 300G. If the desired NAS 300G is not listed, enter the IP address or the computer name of the NAS 300G. The computer name is predefined as IBM5196-xxxxxxx, where *xxxxxxx* is the serial number located in the lower right corner of the bezel on the front of the appliance. If you have changed the computer name from the predefined value, use that name instead.

   For Size, select a size other than full screen in which the NAS 300G desktop will appear, then click **Connect** to start the Terminal Services Client session. A user log in window displays.

   Log in. Type *Administrator* in the Username field, type *password* in the password field, and then click OK to log in. Once you have logged in, you can begin using Terminal Services Client to configure and manage the NAS 300G.

Once you have logged into Terminal Services, you can perform administrative tasks on the NAS 300G, as if a keyboard, mouse, and monitor were directly attached to it. The NAS 300G desktop contains a shortcut, titled **IBM NAS Admin**, to a special console, the IBM NAS Administration console.

IBM NAS Administration console

The IBM NAS Administration console contains all of the standard functions that are contained in the standard Computer Management console available on any Windows 2000 desktop, plus the following functions specific to the NAS 300G:

- Cluster Administration, as described in "Cluster administration" on page 43
- As described in "Chapter 7. Additional administrative functions" on page 51:
    - FAStT MSJ
    - NAS Backup Assistant
    - Persistent Storage Manager
    - Tivoli SANergy

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 NAS 300G.
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.

IBM Advanced Appliance Configuration Utility

The IBM Advanced Appliance Configuration Utility (IAACU) helps you to set up and reconfigure the network configuration on the NAS 300G appliance, as well as other IBM appliances. The IAACU agent, preinstalled on the NAS 300G appliance, works with the IAACU Console, a Java™-based application that is installed on a network-attached system. You can use this system as a systems-management console to automatically detect the presence of NAS 300G appliances on the network. Once the NAS 300G appliance is detected by the IAACU Console, use the IAACU to set up and manage the appliance's network configuration, including assigning the IP address, default gateway, network mask, and DNS server to be used by the appliance. You can also use the IAACU to start Universal Manageability Services (UM Services) on the appliance, enabling you to perform more advanced systems-management tasks.

For networks that are not currently running DHCP servers, the IAACU is useful for automatically configuring network settings for newly added appliances, such as the NAS 300G.

However, networks with DHCP servers will also benefit from using the IAACU because it enables you to reserve and assign the appliance IP address in an orderly, automated fashion. Even when you use DHCP and do not reserve an IP address for the appliance, you can still use the IAACU to discover appliances and to start UM Services Web-based systems-management.

Notes:

1. The IAACU configures and reports the TCP/IP settings of the first adapter (excluding the integrated Ethernet controller which is used for the

interconnection of the two engines) on each appliance. The "first" adapter is defined by its position: if there is an adapter in slot 2, it is the first adapter; if there is an adapter in slot 3, it is the first adapter.

Be sure to connect the first adapter, according to the previous definition, to the same physical network as your systems-management console. You can do this in one of two ways:

- By manually configuring the network adapter to be on the same subnetwork as the systems-management console.
- By creating a Family that assigns the network adapter to the same subnetwork as the systems-management console. See "Creating a Family" on page 17 for more details. Note that the values for Min IP address, Max IP address, Subnet Mask, and Default Gateway need to be in the same range that the IAACU is configured.

2. The IAACU must be running to configure newly installed appliances automatically.

3. The system running the IAACU Console automatically maintains a copy of its database (ServerConfiguration.dat) in the Advanced Appliance Configuration Station installation directory. To remove previous configuration data, close the IAACU, delete this file, and then restart the utility. This deletes all previously configured Families. However, the IAACU will automatically discover connected appliances and their network settings.

IAACU Agent

Once you connect the NAS 300G to your network, the IAACU agent automatically reports the appliance's serial number and type, the MAC address of its onboard Ethernet controller, and whether DHCP is in use by the appliance. Furthermore, it will report the hostname, primary IP address, subnet mask, primary DNS server address, and primary gateway address if these are configured on the system.

The IAACU agent is preinstalled on the NAS 300G appliance.

Note: The IAACU agent periodically broadcasts the appliance IP settings. To prevent the service from broadcasting this data periodically, stop the iaaconfig service.

IAACU Console

The IAACU Console is a Java application that you install on one system in your network for use as a systems-management console. For information on how to install the IAACU Console, see Table 14 on page 99.

Note: The IAACU creates a private database that is specific to the IP subnetwork to which it is attached. Therefore, do not install it on more than one systems-management console residing on the same IP subnetwork.

The IAACU Console enables you to:
- Automatically discover NAS 300G appliances, as well as other IBM appliances, that run the IAACU agent and are attached to the same physical subnet as the IAACU Console.

  When you start the IAACU Console, it automatically detects all appliances on your physical subnet that are running the IAACU agent.
- Use a GUI-based application to configure the appliance network settings.

  Use the IAACU to assign network parameters such as IP addresses, DNS and gateway server addresses, subnet masks, and hostnames.

- Group discovered appliances into function-specific Families. Appliances are added to a Family based on the appliance type. Appliances that perform the same function appear in the same Family.
- Start UM Services Web-based systems-management console.

  Launch UM Services on your appliances and perform advanced systems-management tasks on a selected appliance with a single mouse click.

The IAACU Console is divided into two panes:

- **The Tree View Pane**

  The Tree View Pane, located on the left side of the IAACU Console window, presents a list of all discovered NAS 300G appliances and includes any Families you have previously defined. The Tree View Pane also includes groups for appliances that do not fit any of the defined Families, that were not configured using the IAACU, or that have IP addresses that conflict with other devices on your network. When you click on any item in the Tree View, information about that item (and any items that are nested below that item in the tree view) displays in the Information Pane.

- **The Information Pane**

  The Information Pane, located at the right side of the IAACU Console, displays information about the item that is currently selected in the Tree View Pane. The information that displays in the Information Pane varies depending on the item that is selected. For example, if you select the All Appliances item from the Tree View Pane, the Information Pane displays configuration information (IP settings, hostname, serial number, and so on) about each of the NAS 300G appliances that have been discovered by the IAACU Console. However, if you select a Family, the Information Pane displays information about the Family settings for the selected Family.

The IAACU Console also features the following menus:

- **File**: Use the File menu to import or export the IAACU Console configuration data, to scan the network, or to exit the program.
- **Family**: Use the Family menu to add or delete Families, or to move Families up or down in the tree view.
- **Appliance**: Use the Appliance menu to remove a previously discovered appliance from a Family or group, and to add an appliance to the first matching Family in the tree view.
- **Help**: Use the Help menu to display product information.

Discovering NAS 300G Appliances

Any NAS 300G appliance, or other IBM appliance, that is running and is connected to the same subnet as the system running the IAACU Console is automatically discovered when you start the IAACU Console. Discovered appliances appear in the IAACU Console tree view (in the left pane of the IAACU Console window). Each appliance will appear in two locations in the tree view:

1. Every discovered appliance is listed in the tree view under All Appliances.
2. Each discovered appliance will also appear in one of the following portions of the tree view:
   - In a *Family*

     If the discovered appliance fits the requirements of a Family, it will automatically appear as part of a Family.

Notes:

    a. If a discovered appliance fits the requirements of more than one Family, it is automatically added to the first appropriate Family that is listed in the tree view, starting from the top of the tree. For information on how to move appliances between families, see "Using Families and Groups in the Tree View".

    b. If the NAS 300G cannot be discovered by the IAACU console, check the IP and subnet addresses of the NAS 300G and the computer that is running the IAACU console.

- In the *Orphaned Appliances* group

  If the discovered appliance does not fit a previously configured Family, it is placed in the *Orphaned Appliances* group.

- In the *Orphaned Externally Configured Appliances* group

  Appliances that are running the IAACU agent, but that have a network configuration that was not set by the IAACU agent or console, will appear in the *Orphaned Externally Configured Appliances* group. If an appliance is contained in the Orphaned Externally Configured Appliances group, you can use the Adopt By First Matching Family function to add it to a previously defined Family. For more information, see "Using the Adopt by First Matching Family Function" on page 19.

Using Families and Groups in the Tree View

Families are important elements of the IAACU. They specify the parameters that the IAACU uses to automatically categorize discovered appliances and to configure them with the appropriate network settings. Family rules are defined solely by appliance type or purpose. Each Family can contain only one type of appliance. The only way to automatically apply predetermined network settings to newly installed and discovered appliances is to create and use Families.

Appliances that match the rules criteria for a Family group can be automatically configured to use predefined network settings. A Family can be configured to allow appliances to use DHCP to configure their IP settings, or can be defined to automatically assign IP settings (such as primary gateway and DNS server addresses, assigning an IP address from a specified IP address range, and specifying a subnet mask). Host names for discovered appliances can also be defined so that they are allocated using either a prefix or appliance serial number.

The IAACU is not the only way to configure network settings. For example, network settings can be configured using Terminal Services for Windows or by attaching a keyboard and mouse to the appliance and using Windows Control Panel. If the appliance network settings have been configured by a method other than using the IAACU, the appliance will be discovered by the IAACU and it will be added to an appropriate Family, if one exists. Appliances that have been configured using a method other than the IAACU for which no appropriate family exists will appear in the Orphaned Externally Configured Appliances group.

The Tree View Panel contains the following items:

- **All Appliances**

  Every discovered appliance is listed in the tree view under All Appliances.

- **Families**

  The Families group in the Tree View Pane shows all Families that have been defined, with appliances that have already been assigned to each Family nested beneath the Family name in the tree view. Families are defined by appliance purpose, so all appliances that appear in a given family are of the same type. If

you select a Family from the Tree View Pane, a description of the Family and the rules that are used to define the selected Family display in the Information Pane. If you select an appliance from a Family in the Tree View Pane, the selected appliance network settings display in the Information Pane.

If you are not using DHCP, the IAACU automatically assigns one IP address per appliance, using available addresses within the range defined in the Family rules. When a Family's IP address range has been exhausted, the IAACU automatically searches for other Families that have rules matching the appliance being configured. If a matching Family with an available address is found, the appliance will automatically be assigned to the Family that has available IP addresses. This enables you to define multiple Families, each of which uses a set of non-contiguous IP address ranges.

When an appliance is discovered on the network, the IAACU automatically searches all previously defined Families, starting with the first Family listed in the Families tree view and moving downward. Appliances are automatically added to the first defined Family that matches the appliance purpose. Therefore, the order in which Families appear is important. To adjust this search order, right-click on a Family and then select **Move Up** or **Move Down** to adjust its position within the Families list.

- **Orphaned Appliances**

  Any discovered appliances that have been configured using the IAACU but that do not meet the rules for any existing Family are automatically added to the Orphaned Appliances group.

- **Orphaned Externally Configured Appliances**

  Any discovered appliance that has been configured without using the IAACU tool and that does not meet the rules for any existing Family is automatically added to the Orphaned Externally Configured Appliances group. Appliances configured without the IAACU that meet the rules for any existing Family are automatically added to the matching Family. To add an Orphaned Externally configured Appliance to an appropriate Family that was created after the orphaned appliance was discovered, right-click on the orphaned appliance and select **Adopt by First Matching Family**. For more information, see "Using the Adopt by First Matching Family Function" on page 19.

  Note: The IAACU will not change manually configured network settings of discovered appliances. If the manually configured IP and Subnet addresses fit an existing Family, the IAACU will place that appliance into that Family, but will not change any other settings (such as Host Name, DNS, or gateway addresses).

- **Conflicting Network Addresses**

  Any discovered appliance that has the same IP address as a previously discovered appliance will be listed in the Conflicting Network Addresses group.

Creating a Family: To create a Family:

1. Select **Create Family** from the Family menu.

   The IAACU Family Setup window displays.

2. Select the Appliance Family Rules.

   The Appliance Family Rules determine what purpose an appliance must serve to be included in the Family. You can select one of the following values:

   - IBM TotalStorage NAS Appliances
   - IBM xSeries 130 and 135

3. Specify a Family name.

In the Family Name field type the name that will be used for this Family.

4. Specify network resources to be used by members of the Family.

   You can use the IAACU to assign network resources for members of this Family, or you can use a DHCP server to assign network resources.

   - To use the IAACU to assign network resources, uncheck the **Use DHCP** checkbox and fill in the following fields:

     Min IP Address
     > The lowest IP address in a range of IP addresses that can be assigned to an appliance that is a member of this Family

     Max IP Address
     > The highest IP address in a range of IP addresses that can be assigned to an appliance that is a member of this Family

     Subnet Mask
     > The subnet mask value that will be used by appliances that are members of this Family

     Default Gateway
     > The IP address of the default gateway that will be used by appliances that are members of this Family (optional)

     DNS The IP address of the DNS server that will be used by appliances that are members of this Family (optional)

   - To use a DHCP server to assign network resources, check the **Use DHCP** checkbox. This will allow a DHCP server on your network to assign an IP address and subnet mask and to specify the default gateway address and address of the DNS server that will be used by appliances that are members of this Family.

5. Select a Host Name Allocation Type.

   The Host Name Allocation Type enables you to automatically specify a Host Name that members of this Family will use. You can select one of the following Host Name Allocation Types:

   No Allocation
   > No preconfigured host name format will be assigned to appliances that are members of this family.

   Use Serial Number
   > The Serial Number of the discovered appliance will be used as a host name for the appliance.

   Use Prefix Name
   > A user-specified prefix, along with an incremental number for each appliance, will be used for the host name of each appliance that is a member of this Family. Type the desired prefix in the **Host Name Prefix** field.

6. Click **OK** to save this Family.

Removing Appliances from Families: Use the Remove Appliance function to delete an appliance from the IAACU Console database and view panel. Removing an appliance that is no longer in use allows the IP address that was assigned to the appliance to be allocated to another appliance. You can also remove an appliance from a family and then rescan the network to add it to an appropriate Family that appears higher in the Tree View pane.

To remove an appliance, right-click on the appliance, and then select **Remove Appliance** from the pop-up menu.

- If the IAACU is unable to communicate with the selected appliance (because, for example, it has been removed from the network or has failed), the appliance is removed immediately.
- If the IAACU is able to communicate with the selected appliance, you will be asked to confirm removal of the appliance before the appliance removal task is completed. This helps prevent accidental removal of an active and functional appliance.

Using the Adopt by First Matching Family Function: Use this function to:

- Add an *Orphaned Externally Configured Appliance* to an appropriate Family.

  Appliances that have been configured without using the IAACU tool and that do not meet the rules for any existing Family are automatically added to the Orphaned Externally Configured Appliances group. If, after the orphaned appliance is discovered, you create a Family that is appropriate for the orphaned appliance, right-click on the orphaned appliance and select **Adopt by First Matching Family** to move the appliance from the Orphaned Externally Configured Appliances group to the newly created Family.

- Move an appliance from one Family to another appropriate Family that occurs higher in the list of previously defined Families. If there is more than one appropriate Family for a newly discovered appliance, it automatically appears in the first appropriate Family in the list of Families. If you want to move a discovered appliance from one appropriate Family to another appropriate Family:

  1. Right-click on the Family that you want the appliance moved to.

  2. Select **Move Up in List** to move the selected Family up in the list of families. Repeat steps 1 and 2 until the Family that you want to add the appliance to displays above the Family that currently contains the appliance.

  3. Right-click on the appliance that you want to move to another Family and then select **Adopt by First Matching Family**.

Universal Manageability Services

The Universal Manageability Services (UM Services) GUI enhances the local or remote administration, monitoring, and maintenance of IBM systems. UM Services is a lightweight client that resides on each managed computer system. With UM Services, you can use a Web browser and UM Services Web console support to inventory, monitor, and troubleshoot IBM systems on which UM Services is installed.

This "point-to-point" systems-management approach, in which you use a Web browser to connect directly to a remote client system, enhances support and enables you to effectively maintain IBM systems without requiring the installation of additional systems-management software on your administrator console.

In addition to point-to-point systems-management support, UM Services also includes support for UM Services Upward Integration Modules. These modules enable systems-management professionals who use any supported systems-management platform (including Tivoli Enterprise, CA Unicenter TNG Framework, and Microsoft Systems Management Server [SMS]) to integrate portions of UM Services into their systems-management console. Because it was designed to use industry-standard information-gathering technologies and messaging protocols, including Common Information Model (CIM), Desktop Management Interface (DMI), and Simple Network Management Protocol (SNMP), UM Services adds value to any of these supported workgroup or enterprise systems-management platforms.

Complete documentation on how to use UM Services is included on the Documentation CD that came with the appliance.

System requirements

The UM Services client is preinstalled on the NAS 300G appliance. However, you must have a Web browser installed on your systems-management console. It is recommended that you set Microsoft Internet Explorer 5.x (or later) as the default browser.

Notes:

1. You must install the optional Java Virtual Machine (VM) support to access a client system running UM Services.

2. If you reinstall Internet Explorer after installing UM Services, you must reapply the Microsoft VM update. The UM Services client requires Microsoft VM Build 3165 or later. Download the latest Microsoft VM from:

   `http://www.microsoft.com/java`

3. If you install UM Services before you install MMC 1.1 (or a later version), you will not have an icon for Microsoft Management Console in the IBM Universal Manageability Services section of the Start menu.

Starting UM Services

You can use IAACU or Terminal Services Client to configure the network setting remotely, or you can attach a keyboard and mouse to your appliance and configure the Network settings using the Windows Control Panel. Once you have configured the network settings for your appliance, you are ready to use UM Services.

To start UM Services:

1. Start a Web browser and then, in the **Address** or **Location** field of the browser, enter:

   `http://`*`ip_address`*`:1411`

   where *ip_address* is the IP address of the NAS 300G, and then press **Enter**.

   Or, type:

   `http://`*`computer_name`*`:1411`

   where *computer_name* is the computer name of the NAS 300G. The computer name is predefined as: IBM5196-xxxxxxx, where *xxxxxxx* is the serial number located in the lower right corner of the bezel on the front of the appliance.

   If you have changed the computer name from the predefined value, use that name instead. After you have entered the computer name, press **Enter**.

2. A user log in window displays. Type *Administrator* in the Username field, and type *password* in the Password field. You can leave the Domain field blank. Make sure the "Save this password in your password list " checkbox is not checked, and then click **OK**.

   Note: To ensure system security, change the Administrator password from "password" to something else. Once you do, or if you create another user in the Administrator group in the future, use your new username/password combination instead of the default username/password combination.

   The first time you connect you may be prompted to install XML and Swing components. Follow the on-screen instructions to install these components and then close and restart Internet Explorer before you proceed.

3. You are now connected to the NAS 300G through UM Services. In addition to the standard UM Services functionality, the appliance includes functionality for administering the appliance, available from the Appliances tab in the left pane of the UM Services browser. The default view (in the right pane of the UM Services browser) when you connect to the appliance is Windows 2000 for NAS. The other selectable view in the Appliances tab is Windows 2000 Terminal Services, which displays a Terminal Services Web Connection page.

   To start Windows 2000 for NAS, click **Administer this server appliance** in the right pane of the UM Services browser. To connect to the NAS 300G and manage it as though you were running Terminal Services Client from the desktop, select **Terminal Services** in the Appliances tab of the UM Services browser, and then follow the instructions for connecting to the NAS 300G using Terminal Services described in "Terminal Services and the IBM NAS Administration Console" on page 12.

Launching UM Services from the configuration utility

You can use the IAACU to launch UM Services on the NAS 300G appliances.

Note: The selected appliance must be running Universal Manageability (UM) Services as a UM Services client. Also, the systems-management console (the system that is running the IAACU Console) must use a Web browser that is supported for use with UM Services. If you have not used UM Services from this system, you will need to install several plug-ins before proceeding. If you are using an unsupported browser, or if the browser does

not have the necessary plug-ins, you will be notified when you attempt to launch UM Services on the appliance. For more information on UM Services, go to:

`http://www.ibm.com/pc/ww/software/applications/ums/library.html`

To use the IAACU Console to start UM Services on an appliance:

1. Click on the appliance in the IAACU Console Tree View Pane.

   When you select the appliance from the tree view, information about the selected appliance displays in the Information Pane. A **Start Web-Based Management** button displays as well.

2. Click **Start Web-Based Management**.

   Your default Web browser starts, loading the UM Services browser automatically.

3. Log in to the UM Services browser. Refer to step 2 on page 21 for log in instructions.

For more information on using UM Services to manage your appliances, see the *Universal Manageability Services User's Guide*, included on the Documentation CD that came with the appliance.

Windows 2000 for Network Attached Storage

You can perform the appliance administration tasks with the Windows 2000 for Network Attached Storage GUI. You navigate through various administrative task categories by clicking on the appropriate links on pages or buttons at the top of the page, and then selecting the task from that category.

Online help is available for Windows 2000 for NAS. This online help can be accessed in two ways:

1. By clicking the **Help** button at the top of any Web page. This will display a table of contents which you can navigate to find help for any Windows 2000 for NAS task.

2. By clicking the question mark (**?**) button at the top of any Web page. This will display context-sensitive help for the task you are currently performing.

While you can perform most administrative tasks using Windows 2000 for NAS, there are some advanced tasks for which you must use Terminal Services Client. See "Terminal Services and the IBM NAS Administration Console" on page 12 for more information.

You can start Windows 2000 for NAS in one of three ways:

1. Through UM Services, as described in step 3 on page 21.

2. From a Web browser, by entering **http://***ip_address***:8099** or **http://***computer_name***:8099** and then logging on to the NAS 300G.

3. From the NAS 300G desktop while using Terminal Services Client and starting a browser.

Telnet Server support

CAUTION:
When you Telnet to another machine, your user name and password are sent over the network in plain, unencrypted, text.

The NAS 300G includes Telnet server capability. The Telnet server provides limited administrative capability. This may be useful in cases where you need to remotely administer the NAS 300G, 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 NAS 300G from any Telnet client by specifying the IP address or hostname of the NAS 300G, then logging in using an ID and password (defined on the NAS 300G) 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, put a check in the *Enable Telnet access to this appliance check box.* Later, if you wish to disable Telnet access, you can remove the check. If you do not require Telnet access to the NAS 300G, then it is recommended that you leave the Telnet server disabled.

SNMP support

Support for the Simple Network Management Protocol (SNMP) is enabled. To manage the NAS 300G from an SNMP-capable management application, you will need to install the Management Information Base (MIB) files for various components of the NAS 300G on the management application workstation, so that the application can recognize those SNMP elements (values, alerts, and so on) supported by the components. For information on MIB files that are supported by the NAS 300G, go to

```
http://www.storage.ibm.com/nas
```

.

Chapter 3. Getting started

This chapter gives details to set up the initial communication to the NAS 300G to enable setup and configuration. You can choose from several options to accomplish this task. These instructions refer specifically to a base configuration as shipped and do not cover the setup of additional storage units, which can be purchased separately.

Note: For the Model G26, you will need to follow these procedures for both nodes.

Methods for setting up the NAS 300G

The following sections detail how to set up the NAS 300G. You first need to ensure that the network recognizes the new appliance. The appropriateness of the method you use to do this depends on several conditions:

- If you are operating in "headless" mode (that is, without a keyboard, monitor, and mouse directly attached to the unit), you can use one of the following methods:
  - Windows Terminal Services

    If DHCP is installed and the IP address requested can be determined, you can use this method for initial setup, but you should change the address to static later in the configuration. This condition is most appropriate for use of Windows Terminal Services for operation of the NAS 300G.

    If you are using this method, proceed with "Initial setup and configuration" on page 26.
  - IBM Advanced Appliance Configuration Utility

    If you have multiple appliances or cannot determine the DHCP address, you can install the IAACU to identify appliances and define IP addresses. The tool will also allow you to set static addresses.

    If you are using this method, proceed with "The IBM Advanced Appliance Configuration Utility".
- The use of a keyboard, display, and mouse is most appropriate when there is a single or few appliances in the network and you use static setup and definition.

  If you are using this method, proceed with "Initial setup and configuration" on page 26.

The IBM Advanced Appliance Configuration Utility

These instructions assume that you have installed and powered on the appliance according to the installation guide procedures. You are now ready to install the IAACU Console application from the Supplementary CD.

Note: The IAACU creates a private database that is specific to the IP subnetwork to which it is attached. Therefore, do not install it on more than one systems management console residing on the same IP subnetwork.

Install the Advanced Appliance Configuration console application from the Supplementary CD onto a Windows NT 4.0 or Windows 2000 workstation that is attached to the same IP subnetwork to which the appliance is attached.

For information on how to install the IAACU Console, see Table 14 on page 99.

After you have installed the Advanced Appliance Configuration console application, the following steps will take you to the point where you can administer the appliance.

1. Start the Advanced Appliance Configuration console application by clicking its icon.

2. On the left pane of the Advanced Appliance Configuration console, select the appliance you want to administer. Initially, the appliance will be named **IBM5196**-*serial number*, which is located in the lower right corner of the bezel on the front of the appliance.

3. Click the **Start Web Management** button at the bottom of the right pane of the Advanced Appliance Configuration console to start the Universal Manageability (UM) Services browser. This will open a separate Web browser.

To read more information on the IAACU, see "IAACU Console" on page 14.

Accessing Universal Manageability Services

1. You will be prompted to authenticate with the administrative user name ("Administrator") and password (initially "password," but you can change it later; note that the password is case-sensitive, but the user name is not).

   If this is the first time you have accessed the UM Services browser (on any appliance) from this workstation, you will also be prompted to install the Swing and XML Java libraries in your Web browser. You can download these libraries from the NAS 300G via the network link.

2. The UM Services browser will start. In the left pane, Microsoft Windows 2000 for Network Attached Storage will be automatically selected, on the Appliance tab. In the right pane, Windows 2000 for Network Attached Storage will start.

3. Again, you will be prompted to authenticate with administrative user name and password.

4. Click **Administer this server appliance** to bring up the Microsoft Windows 2000 for Network Attached Storage GUI.

You are now ready to begin administering the appliance. Details for this task are described in "Initial setup and configuration".

Initial setup and configuration

This section provides details on the initial setup and configuration of the NAS 300G.

Note that if you are administering the NAS 300G without a keyboard, monitor, and mouse ("headless" mode), there are one of two methods that you can use:

- Terminal Services, which provides full administrative function. (See "Terminal Services and the IBM NAS Administration Console" on page 12.)
- Windows 2000 for Network Attached Storage, which provides a subset of the full administrative function in Terminal Services. (See "Windows 2000 for Network Attached Storage" on page 22.)

In general, you administer the appliance by adjusting information contained in the following task groups:

Note: In this example, you access the task groups through the Windows 2000 for Network Attached Storage Web-based GUI.

- "Maintenance (Date and Time)" on page 27
- "Network Setup" on page 27

Although you can modify multiple appliance and network attributes in each task group, the information given here is the minimum you need to know to administer the appliance and network.

You can find more information on administration elsewhere in this book and in the online help.

Note that the icons for the task groups on the Windows 2000 for NAS GUI are not in the same order as presented here.

You can access these task groups in one of three ways:
1. Click the **Home** tab and then select the task group link.
2. Click the top tab associated with that task group.
3. Click the **Back** button on the browser until you arrive Home and then select the task group link.

Maintenance (Date and Time)

In the Maintenance task group, you will need to change the date and time. To do so, click on **Date and Time** or the green arrow. (Remember that you can also access all of these task groups by clicking on the titled tabs at the top of the page.) The Set Date and Time page displays, allowing you to adjust information as necessary.

Network Setup

Note: All appliances have an initial default user name of "administrator" and password of "password."

In the Network Setup task group, you can change the administrator password. Optionally, you can configure the properties of each network interface that resides on the appliance.

To change the administrator password, click on **Change Administrator Password** or the green arrow. The Change Administrator Password page displays, allowing you to change the password. Note the warning on the page that any information you enter can be viewed by others on the network. To prevent others from seeing your information, set up a secure administration Web site as described in the online help.

To optionally change interface properties such as IP addresses, click on **Interfaces** or the green arrow. The Network Adapters on Server Appliance page displays. You would use this page primarily to change IP addresses from dynamic (DHCP, which is the system default) to static.

Note: During the initial setup, you should configure the non-planar Ethernet adapter only. The NAS 300G engine uses the Ethernet adapter that is integrated on the planar board as the interconnect private network for clustering.

If you want to use an Ethernet adapter other than the default Ethernet adapter (in slot 2) as the network interface to be attached to the subnet, then you can change the order of precedence later with the Windows Networking Properties option. The order of precedence for the initial configuration is: PCI slot 2, then PCI slot 3.

Note that you may need to enable some of the NAS 300G NIC connections, because the NICs in slots 1, 3, and 4 are set to disabled. During initial setup, the IAACU first looks for a 10/100 adapter in slot 2 (if you ordered it), which is enabled by default. If there is no adapter in slot 2, the IAACU looks for a Gigabit adapter card in slot 3 (if you ordered it) and it should be enabled. If the Gigabit adapter card is not enabled, right-click the adapter icon to enable it. After the initial setup, you can then enable all other NIC interfaces installed.

You must modify the adapter by completing the **IP** task (to modify IP configurations) and then choosing one or more of the following tasks, as appropriate:

- **DNS** (to modify DNS configurations)
- **WINS** (to modify WINS configurations)
- **HOSTS** (to modify host configurations)

Chapter 4. Setting up storage

This chapter gives the details for setting up and configuring the fibre-attached storage for the NAS 300G.

For the Model G26, note that you need to configure the storage on one node only. For the other node (the joining node), the only part of shared storage setup that you will need to complete is assigning drive letters on the shared storage, making sure that the drive letters are the same as those on the first node.

Configuring arrays and logical drives on the fibre-attached storage

You will need to configure the RAID arrays and logical drives (LUNs) on the fibre-attached storage, or contact your disk administrator to do the configuration. The specific procedures for configuring arrays and LUNs are defined by the fibre-attached storage, so its documentation must be consulted for those procedures.

You will need to get the World Wide Name (WWN) of the Fibre Channel host adapter to set up an association between the NAS 300G node and each LUN you create on the fibre-attached storage. To get the WWN:

1. Click on the **IBM NAS Admin** icon.
2. Select **NAS Management**.
3. Select **Storage**.
4. Select **NAS Utilities**.
5. Select **WWN Fibre Utility**.

   The WWN Fibre Utility panel will display information for each fibre channel adapter installed in your NAS 300G, including PCI slot number and World Wide Name. If you have only one fibre channel adapter, the information for that adapter will appear immediately in the fields on the right side of the panel.

   If you have multiple fibre channel adapters, select the radio button next to each adapter listing until you find the one whose displayed PCI slot number matches the PCI slot number of the actual adapter. Make a note of the World Wide Name that is displayed so that you can provide this when configuring your fibre-attached storage to be accessed via the NAS 300G.

For the Model G26, there is an additional requirement imposed on the configuration of the fibre-attached storage: one LUN must be defined for the Quorum drive. The Quorum drive is used by Microsoft Cluster Service to manage clustered resources, including the fibre-attached storage. The requirements for the Quorum drive LUN are the following::

- The array in which you create the Quorum drive LUN should be RAID 5. This is recommended for performance and redundancy.
- The Quorum drive LUN should be at least 500 MB in size, but no larger than 1 GB.
- The Quorum drive LUN should be completely dedicated for use by Microsoft Cluster Service; no other data should be stored on this LUN. However, it is acceptable for the array in which this LUN is created to have other LUNs.
- See "Recovering from a corrupted Quorum drive" on page 135 in the event of a power loss to both nodes or a hardware failure that corrupts Quorum data.

You can configure other arrays and LUNs for user data as required. However, do not create any arrays that are RAID 0, as this is not supported. It is recommended that all arrays be RAID 5 arrays.

Formatting the logical drives

Note the following restrictions when formatting logical drives:

1. Disk 0 (the internal hard disk drive) is an 18-GB drive, preformatted into two partitions: a 6-GB partition (label System, drive letter C:) and a 12-GB partition (label MAINTENANCE, drive letter D:). Do not reformat or repartition these partitions. Doing so could wipe out important data and seriously impair the functioning of your system.

2. For the Model G26, do **NOT** upgrade any disks to dynamic. Only basic disks are supported for clustering. In addition, all partitions used for clustering must be primary partitions.

3. For the Model G26, do not use Drive letter F: for volume drive letters. This is reserved for Persistent Storage Manager-based backup using NAS Backup Assistant.

Follow this procedure to format logical drives.

1. Open IBM NAS Admin and select **Disk Management (Local)**, in the Storage folder.

2. You will see a Write Signature and Upgrade Disk Wizard pop up on the screen. Click **Cancel**.

3. Right-click on the bottom right, where it says **Disk 1**, and select **Write Signature**.

4. Write Signature to all disks that will be accessed by the NOS (all disks in view).

5. On each disk:

    a. Right-click and select **Create Partition** and click **Next**.

    b. Select **Primary Partition** and click **Next**.

    c. Select the entire disk size and click **Next**.

    d. Specify *NTFS* as the file system. For the Model G01, specify as the Volume Label whatever name you want to assign to the partition. For the Model G26, if this is the Quorum disk, specify *Quorum disk* as the Volume Label; otherwise, specify whatever name you want to assign to the partition.

    e. Click **Finish**. Do not enable disk compression, and select Finish.

6. Format all other drives, but do not enable compression. Use all space available for each drive for each logical drive assigned by the operating system. For the Model G01, assign a drive letter of *F* for the first drive (the first user volume), *G* for the second drive (the second user volume), and so on. For the Model G26, assign a drive letter of *G* for the first drive (the Quorum drive), *H* for the second drive (the first user volume), and so on.

At this point, you have set up shared storage. You can now continue with "Chapter 6. Completing networking, clustering, and storage access setup for the Model G26" on page 39. for more information.

Chapter 5. Completing storage access setup for the Model G01

This chapter gives the details for setting up the Model G01 so clients and servers on your network can access the storage.

- If Windows clients and servers will access your storage, follow the steps in "Defining Windows users and groups".
- If UNIX and UNIX-based clients and servers will access your storage, follow the steps in "Defining UNIX users and groups" on page 32.
- If both Windows and UNIX clients and servers will access your storage, you will need to follow the steps in "Defining Windows users and groups" and then follow the steps in "Defining UNIX users and groups" on page 32.

Defining Windows users and groups

This section describes how to set up Windows users and groups who will access the Model G01 storage.

You may define Windows users and groups locally on the Model G01. Alternatively, you can add the Model G01 to an existing Windows domain that is controlled by a Primary Domain Controller (PDC), and define new users and groups on the PDC who can access the Model G01 storage and/or allow existing users and groups to access the Model G01 storage.

If you are defining local Windows users and groups, follow the steps in "Defining local Windows users and groups". If you are giving access to the Model G01 storage to users and groups in an existing Windows domain, follow the steps in "Giving storage access to Windows domain users and groups" on page 32.

Defining local Windows users and groups

If you are defining local Windows users and groups, you may use the Windows 2000 for Network Attached Storage user interface. In the Users task group, you create and manage local users and groups on the Model G01. Clicking on **Users** takes you to the Users page. From this page you can create, edit, and delete local users and groups on the Model G01 by clicking either **Local Users** or **Local Groups**.

To create new local users, do the following:

1. Click **Local Users**.
2. Click **New...**
3. Fill in user name, password, and description (optional).
4. Click **OK**. The new user name should appear in the list of user names.
5. Repeat Steps 1 through 4 for each new local user you wish to add.
6. When you are finished adding new users, click **Back** to return to the Users and Groups page.

To create new local groups, do the following:

1. Click **Local Groups**.
2. Click **New....**
3. Fill in group name and description (optional).

4. Click **Members**.

5. For each user you wish to add to the group, select the user name from the list of users, and then click **Add**.

6. Click **OK**. The new group name should appear in the list of group names.

7. Repeat Steps 1 on page 31 through 6 for each new local group you wish to add.

If your storage is also going to be accessed by UNIX or UNIX-based clients and servers, continue with "Defining UNIX users and groups". Otherwise, continue with "Creating shares" on page 36.

Giving storage access to Windows domain users and groups

You must first join the Model G01 to the Windows domain. You may use the Windows 2000 for Network Attached Storage user interface to do this. Start the Windows 2000 for Network Attached Storage user interface, then do the following:

- Click **Network**.

- Click **Identification**.

- Select the radio button labeled **Domain**, and specify the name of the domain being joined.

- Specify a user name and password that can be used to log on to the domain.

- Click **OK**.

- Shut down and restart the Model G01.

Users and groups already defined in the domain can now be given access to any file shares that you create on the Model G01. If you need to add new users and groups to the domain, consult the online documentation on the PDC for information on performing this procedure, or if you are not the administrator of the domain (PDC), contact the domain administrator to have the users and groups defined.

If your storage is also going to be accessed by UNIX or UNIX-based clients and servers, continue with "Defining UNIX users and groups". Otherwise, continue with "Creating shares" on page 36.

Defining UNIX users and groups

This section describes how to set up UNIX users and groups who will access the Model G01 storage via the Network File System (NFS) protocol.

Support for NFS is provided in the Model G01 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 G01, are NFS Versions 2 and 3. Any client or server that is using an NFS software stack supporting NFS Version 2 or NFS Version 3, regardless of the operating system, should be able to connect to the Model G01 and access its storage via NFS.

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.

You can define a local UNIX name space on the Model G01 by configuring the Server for PCNFS component of Services for UNIX. Alternately, you can point Services for UNIX to an existing Network Information Service (NIS) domain which

defines the UNIX name space. In both cases, you will need to configure the User Name Mapping component to map the UNIX name space you select to the Windows name space, since file shares and individual file/directory permissions on the Model G01 are defined in the context of the Windows name space.

If you are going to define a local UNIX name space, continue with "Using a local UNIX name space". If you are going to use a UNIX name space defined on a NIS domain, continue with "Using the UNIX name space on an NIS domain" on page 35.

Using a local UNIX name space

This procedure should only have to be performed once. You may have to add more groups and users in the **Server for PCNFS** page if you add more users and groups to your UNIX environment and Model G01 or Windows domain at a later time.

1. Open the IBM NAS Administration console by double-clicking the **IBM NAS Admin** icon on the NAS desktop.
2. In the left pane, click the plus sign (**+**) next to File Systems, then click the plus sign next to Services for UNIX.
3. In the left pane, click **Server for NFS**.
4. In the right pane, in the Computer name: field, enter *localhost*.
5. In the left pane, click **Server for PCNFS**.
6. In the right pane, click **Groups**.
7. On the Groups page, you will need to add the groups from your UNIX host to which all of your UNIX users belong. You will need to know both the group name and the group ID (GID) number. This information can be found in the /etc/group file on most UNIX systems.

   As an example, on an AIX system, in the following line from an /etc/group file, the fields are separated by a colon (:). The first field (″staff″) is the group name; the third column (″1″) is the GID:

   ```
   staff:!:1:pemodem,ipsec,netinst,protcs
   ```

   You add a group by entering the group name and GID number in the Group name and Group number (GID) fields, respectively, and then clicking **New**.
8. When you have finished adding groups, click **Apply**.
9. Click **Users**.
10. On the Users page, you will need to add all of the UNIX users who will be accessing and storing files on the Model G01 through an NFS share. For each user you will need to know the Windows user name, the UNIX user name, the primary group, and the user ID (UID) number. This information can be found in the /etc/passwd and /etc/group files on most UNIX systems.

    As an example, on an AIX system, in the following line from an /etc/passwd file, the fields are separated by a colon (:). The first field (″user1″) is the user name; the third field (″3135″) is the UID, and the fourth field (″1″) is the GID of the user's primary group. This will correspond to a line in the /etc/group file, where you can find the primary group name corresponding to the GID.

    ```
    user1:!:3135:1:User 1:/home/user1:/bin/ksh
    ```

    You add a user by clicking **New**, entering the required information, and then clicking **OK**.
11. When you have finished adding users, click **Apply**.
12. In the left pane, click **User Name Mapping**.

13. In the right pane, click the radio button next to Personal Computer Network File System (PCNFS).

14. In the Password file path and name field, enter *c:\winnt\system32\drivers\etc\passwd*.

15. In the Group file path and name field, enter *c:\winnt\system32\drivers\etc\group*, then click **Apply**.

16. Click **Maps**.

17. On the Maps page, you can configure simple maps or advanced maps. Configure simple maps if the Windows user name and UNIX user name is the same for each UNIX user to be mapped, and the Windows group name and UNIX group name is the same for each UNIX group to be mapped. Otherwise, you should configure advanced maps.

    To configure simple maps, check the Simple maps checkbox and continue with Step 18. To configure advanced maps, uncheck the Simple maps checkbox and continue with Step 19.

18. Under the Simple maps checkbox, select the Windows domain name from the drop-down list, then continue with Step 20 on page 35. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)

19. Under Advanced maps, do the following:
    a. Define user mappings as follows:
       1) Click **Show user maps**.
       2) Select the Windows domain name from the drop-down list. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)
       3) Click **Show Windows Users** to display all of the Windows user names in the Windows domain you selected.
       4) Click **Show UNIX Users** to display all of the UNIX user names in the NIS domain you selected.
       5) Enter a Windows user name, or select one from the list of Windows user names.
       6) Enter a UNIX user name to be mapped to the Windows user name you specified, or select one from the list of UNIX user names.
       7) Click **Add** to add the mapping between the UNIX user name and Windows user name to the list of maps.
       8) If multiple Windows user names are mapped to one UNIX user name, you must select one Windows user name to be the primary user name. Select the mapping corresponding to the primary user name from the list of maps, and then click **Set Primary**.
    b. Define group mappings as follows:
       1) Click **Show group maps**.
       2) Select the Windows domain name from the drop-down list. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)
       3) Click **Show Windows Groups** to display all of the Windows group names in the Windows domain you selected.
       4) Click **Show UNIX Groups** to display all of the UNIX group names in the NIS domain you selected.

5) Enter a Windows group name, or select one from the list of Windows group names.

6) Enter a UNIX group name to be mapped to the Windows group name you specified, or select one from the list of UNIX group names.

7) Click **Add** to add the mapping between the UNIX group name and Windows group name to the list of maps.

8) If multiple Windows group names are mapped to one UNIX group name, you must select one Windows group name to be the primary group name. Select the mapping corresponding to the primary group name from the list of maps, and then click **Set Primary**.

20. Click **Apply**.

You may now continue with "Creating shares" on page 36.

Using the UNIX name space on an NIS domain

The following procedure applies whether your NIS server is UNIX-based or Windows-based (implemented as a Windows domain controller running Microsoft's Server for NIS).

1. Open the IBM NAS Administration console by double-clicking the **IBM NAS Admin** icon on the NAS desktop.

2. In the left pane, click the plus sign (**+**) next to File Systems, then click the plus sign next to Services for UNIX.

3. In the left pane, click **Server for NFS**.

4. In the right pane, in the Computer name: field, enter *localhost*.

5. In the left pane, click **User Name Mapping**.

6. In the right pane, click the radio button next to Network Information Services (NIS), then click **Maps**.

7. On the Maps page, you can configure simple maps or advanced maps. Configure simple maps if the Windows user name and UNIX user name is the same for each UNIX user to be mapped, and the Windows group name and UNIX group name is the same for each UNIX group to be mapped. Otherwise, you should configure advanced maps. To configure simple maps, check the Simple maps checkbox and continue with Step 8. To configure advanced maps, uncheck the Simple maps checkbox and continue with Step 9.

8. Under the Simple maps checkbox, do the following:
   a. Select the Windows domain name from the drop-down list. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)
   b. In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.
   c. Continue with Step 10 on page 36.

9. Under Advanced maps, do the following:
   a. Define user mappings as follows:
      1) Click **Show user maps**.
      2) Select the Windows domain name from the drop-down list. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)
      3) In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.

4) Click **Show Windows Users** to display all of the Windows user names in the Windows domain you selected.
5) Click **Show UNIX Users** to display all of the UNIX user names in the NIS domain you selected.
6) Enter a Windows user name, or select one from the list of Windows user names.
7) Enter a UNIX user name to be mapped to the Windows user name you specified, or select one from the list of UNIX user names.
8) Click **Add** to add the mapping between the UNIX user name and Windows user name to the list of maps.
9) If multiple Windows user names are mapped to one UNIX user name, you must select one Windows user name to be the primary user name. Select the mapping corresponding to the primary user name from the list of maps, and then click **Set Primary**.

b. Define group mappings as follows:
1) Click **Show group maps**.
2) Select the Windows domain name from the drop-down list. (If your Windows users are defined locally on the Model G01, select the entry containing the computer name of the Model G01, preceded by two backslash characters ("\\"). Otherwise, select the name of the Windows domain where the users are defined from the list.)
3) In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.
4) Click **Show Windows Groups** to display all of the Windows group names in the Windows domain you selected.
5) Click **Show UNIX Groups** to display all of the UNIX group names in the NIS domain you selected.
6) Enter a Windows group name, or select one from the list of Windows group names.
7) Enter a UNIX group name to be mapped to the Windows group name you specified, or select one from the list of UNIX group names.
8) Click **Add** to add the mapping between the UNIX group name and Windows group name to the list of maps.
9) If multiple Windows group names are mapped to one UNIX group name, you must select one Windows group name to be the primary group name. Select the mapping corresponding to the primary group name from the list of maps, and then click **Set Primary**.

10. Click **Apply**.

You may now continue with "Creating shares".

Creating shares

To create new file shares on the Model G01, do the following:
1. Start the Windows 2000 for Network Attached Storage user interface.
2. Click the **Shares** tab.
3. Click the **Shares** task.
4. Click **New....**
5. Specify the share name (the name which clients and servers will use to access the share).
6. Specify the share path, and check the *Create folder if it does not already exist* checkbox.
7. By default, the Microsoft Windows (CIFS) and UNIX (NFS) checkboxes are checked (enabled). If this share is not to be accessed by Windows clients and

servers, uncheck (disable) the Microsoft Windows (CIFS) checkbox. If this share is not to be accessed by UNIX clients and servers, uncheck the UNIX (NFS) checkbox.

8. If this share is to be accessed by
   - Windows clients and servers, then click **CIFS Sharing** and specify access permissions as desired. (Note that by default, every user has full access to all files and directories under the shared folder.)
   - UNIX clients and servers, then click **NFS Sharing** and specify access permissions as desired. (Note that by default, every user has full access to all files and directories under the shared folder.)

9. Click **OK**. The new share should appear in the list of shares.

10. Repeat Steps 4 on page 36 through 9 for each additional share you wish to create.

You may now continue with "Chapter 7. Additional administrative functions" on page 51.

Chapter 6. Completing networking, clustering, and storage access setup for the Model G26

The Model G26 uses Microsoft's Cluster Server (MSCS) software to provide clustering technology for your storage. Clustering ensures availability of the storage, regardless of individual component failure.

After installing the clustering function, you can use Cluster Administration to set up the failover function. Then, if a node or a node's component were to fail, the Model G26 detects the failure and begins a failover process in less than 10 seconds, and completes the process within 60 seconds. Failover/Failback includes Active/Active support for the CIFS and NFS protocols.

Active/Active support is available for HTTP and FTP. See the online cluster administration guide for this procedure.

Novell NetWare and Apple Macintosh shares are available on both nodes, but not through clustering services. If either node fails, the shares become unavailable until the node is brought back up.

This chapter gives the details for installing and initially configuring MSCS on the NAS 300G. Administrative concepts and procedures are provided in the online help and at the following Web sites:

`http://www.microsoft.com/windows2000/library/technologies/cluster/default.asp`

`http://www.microsoft.com/ntserver/support/faqs/clustering_faq.asp`

`http://support.microsoft.com/support/kb/articles/Q248/0/25.ASP`

Networking setup

CAUTION:
Before you begin installing cluster services on the first node, make sure that the joining node is powered off. This is required to prevent corruption of data on the shared storage devices. Corruption can occur if both nodes were to try to simultaneously write to the same shared disk that is not yet protected by the clustering software.

Configuring the interconnect (private) network adapter

Do the following steps on both nodes to configure the interconnect (Private) network adapter. The **Private** connection is the heartbeat interconnect for the cluster.

1. Right-click **My Network Places** and then select **Properties**.
2. Select the network connection that uses the IBM 10/100 Adapter.
3. Right-click the adapter icon and click **Properties**.
4. Click **Configure**, select the **Advanced** tab, and verify that the following characteristics are set:

   Link speed and Duplex   100 Mbps / Full Duplex
5. Click **OK**.
6. If prompted to restart the node, select **NO**.
7. In the Properties panel for the IBM 10/100 Adapter connection, select **Internet Protocol (TCP/IP)** from the components section, and click **Properties**.

8. The default IP address should be 10.1.1.1 for the first node, and 10.1.1.2 for the joining node. If not, it is recommended that you set them to those values.

9. Ensure a Subnet Mask of 255.255.255.0.

10. Click on **Advanced**, and select the **WINS** tab.

11. Select the **Disable NetBIOS over TCP/IP** radio button.

12. Click **OK.**

13. Select **YES** when you are asked if you want to continue using an empty Primary WINS address.

14. Click **OK** on the Internet Protocol (TCP/IP) Properties panel.

15. Click **OK** on the Local Area Connection Properties (Private) panel.

16. Rename the connection to **Private**.

Configuring the public local area connection

Note: While the public network adapter's IP address can be automatically obtained if a DHCP server is available, this is not recommended for cluster nodes. It is strongly recommended that you set static IP addresses for all network adapters in the cluster. If IP addresses are obtained through DHCP, access to cluster nodes could become unavailable if the DHCP server goes down.

Do the following steps on each node to configure each public local area connection.

1. Right-click **My Network Places**, then click **Properties**.

2. Select the desired **Local Area Connection**.

   When you do this step, the connection that uses the IBM 10/100 Adapter is the private connection. The other active connection is the public connection. Use that other active connection for this step and the next step.

3. If desired, click **Rename**, and then type (for example) **Public 1**, and press **Enter** Ensure that local area connection names are unique.

   When you do these renaming steps for the joining node, ensure that the local area connection name for each physically connected network is identical on each server. See Table 3 on page 41 for a further example.

4. Use the networking information in Table 1 on page 7 to enter the networking addresses:
   • Right-click **My Network Places**
   • Click **Properties**
   • Right-click the **Public** icon, then click **Properties**.
   • Select **Internet Protocol (TCP/IP)**
   • Click **Properties**, select **Use the following IP address:**, and enter the addresses for the IP, subnet mask, default gateway, and preferred DNS server.

5. If needed, configure the DNS, WINS, HOSTS, or whichever method you will be using for names resolution. You can view this information by clicking the **Advanced** button on the **Properties** window.

6. Click **OK** on each panel to back up to the Properties window.

Do not place paired adapters on the same IP network, unless you are going to use adapter teaming or adapter load balancing.

Verify network connectivity and names resolution

Verify network connectivity and names resolution after you have installed clustering on the joining node.

To verify that the private and public networks are communicating properly, open an MS-DOS command prompt and type **ping** *ipaddress* where *ipaddress* is the IP address for the corresponding network adapter in the other node, and press **Enter**.

For example, assume that the IP addresses are set as follows:

Table 3. Example of local area connection names and network adapter IP addresses

Node	Local area connection name	Network adapter IP address
1	Private	10.1.1.1
1	Public 1	192.168.1.12
1	Public 2	192.168.2.12
2	Private	10.1.1.2
2	Public 1	192.168.1.13
2	Public 2	192.168.2.13

In this example, you would type **ping 192.168.1.12** and **ping 192.168.2.12** for the first node, and you would type **ping 192.168.1.13** and **ping 192.168.2.13** for the joining node. You can do this from any machine that is physically connected to each node's networks.

In case you need to view the addresses, retrieve them using the **ipconfig** command on each node:
- Click **Start**, click **Run**, type **cmd** in the text box, and click **OK** to bring up an MS-DOS prompt.
- Type **ipconfig /all** and press **Enter**. IP information should display for all network adapters in the machine.

To check or change the Network Binding order

The clustering function requires the following binding order:
- Private
- Public 1
- Public 2
- :
  :

The top-most connection is first in the binding order. Typically, this will be the most used network adapter.

To check the binding order and change it:
1. Right-click **My Network Places** and then select **Properties**.
2. Select **Advanced**, **Advanced Settings**.
3. Reorder the position of the adapters by selecting them, then pressing the **up** or **down** arrow keys, then clicking **OK**.

If you change the binding order, a reboot is not necessary until after you have joined the node to the domain. If prompted to restart, click **No**.

To join a node to a domain

All nodes in the cluster must be members of the same domain and be able to access a Primary Domain Controller (PDC) and a DNS Server.

Also, note that the Administrator in the following procedure must have a valid account on the PDC.

1. Right-click **My Computer**, and click **Properties**.
2. Click **Network Identification**. The System Properties dialog box displays the full computer name and workgroup or domain.
3. Click **Properties** and do these steps to join a domain:
   a. Select the **Domain** radio button
   b. Type in the name of your domain and click **OK**.
   c. When prompted, enter the Administrator user id and password and press **OK**.
4. Close the **System Properties**
5. Once completed, restart the node, and proceed with "Cluster setup".

   After the computer restarts, it is recommended that you do not login to the domain. If you do, you will see the Windows 2000 Configure Your Server window. Click the **I will configure this server later** radio button, then click the **Next** button. The next window has a checkbox, *Show this screen at startup*. Uncheck the checkbox and click **Finish**.

Cluster setup

At this step, you have completed the cluster installation steps on each node and are ready to set up the cluster. Do the following steps.

Note that the nodes are equivalent in hardware and software. In the following sequence, "first node" and "joining node" refer merely to the sequence in which you set up the nodes, and not to an order of importance.

1. To begin setting up the cluster on the node, open **IBM NAS Admin**, then the **Cluster Tools** folder, and click the **Cluster Setup** icon.
2. You will be asked to verify that you have completed the steps that precede this cluster setup step. If you have, click the **Continue** button.
3. If this is the first node, click the **First Node** button. If this is the joining node, go to Step 12 on page 43 and continue from there.
4. The Cluster Information panel appears. Enter the data for the following fields (some of this data comes from Table 1 on page 7):
   - Administrator's ID and password

     Note: The ID and password are any valid user ID and password with administrator privileges on the domain.
   - Domain name
   - Cluster name
   - Cluster IP address
   - Subnet mask
   - Quorum drive (select from the pulldown)
5. After you have entered the data, click **Continue**.
6. You will be asked to verify the information. If it is correct, click **Yes** to start the configuration. You will see a message that configuration takes a few minutes.
7. If you are asked by the Cluster Service Configuration Wizard to select a user account, enter the user name and password for the domain account you want the cluster service to use. If you are not asked, cluster configuration completes.
8. If you are asked to select a disk on which to store cluster checkpoint and log files, do the following:

a. Select the disk on which the Quorum is located (for instance, *G*, if this is what you specified earlier) and click **Next**.

b. The Cluster Information panel displays. Click **Finish**.

If you are not asked, cluster configuration completes.

9. Cluster configuration completes for the first node.

10. **Power on the joining node.** (You will join the this node to the cluster.)

11. Go to "Networking setup" on page 39.

12. Click the **Joining Node** button.

13. The First Node Information panel appears. Enter the name of the <u>first</u> node.

14. You may asked to confirm the Administrator name and password. Enter that information and click **Finish**.

15. You will see a message that configuration takes a few minutes. When configuration completes, the Cluster Administration function starts.

You have now completed cluster setup.

Cluster administration

This section contains procedures to assist you in configuring basic cluster functions. It is assumed that the cluster installation has completed without errors, and both cluster nodes are running.

It is recommended that you review the *Cluster Administration Guide*, located in the IBM NAS Admin in the Cluster Tools folder before continuing with the following steps.

Recommended settings

The following steps are needed to reset the size of the logfile and set the priority and purpose of the private network.

1. Select **Cluster Administration**, located in IBM NAS Admin, in the Cluster Tools folder.

   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 are the Groups (there is one disk group for each disk that you created on the shared storage), Resources, Cluster Configuration folders, and the two nodes in the cluster. Under the nodes are the respective active groups, active resources, and network interfaces. These folders allow you to select cluster resources on either node to view or change their properties.

3. Click on the cluster name to see the status of the cluster nodes in the right hand pane. The state of both nodes should be "Up".

4. Right click on the cluster name and select **Properties**. The Properties window has four tabs:
   • **General**
   • **Quorum Disk**
   • **Network Priority**
   • **Security**

5. Select **Quorum Disk**, and change the *Reset quorum log at:* field from 64 KB to 4096 KB.

6. Select **Network Priority** to view all networks acknowledged by the cluster server, then select the private network connection and move it to the top for cluster communication priority by clicking the **Move Up** button.

   Doing this provides internal communication to the private network before attempts are made to communicate over any public networks that are installed. Do not make any changes to the communication options for the public network adapters as they should support both network and cluster traffic.

7. Open the properties for the private network and select **Internal cluster communication only (private network)** to ensure that no client traffic will be placed on the private network.

8. Click **Apply**, **OK**, and then **OK**.

Cluster resource balancing

When you configure cluster resources, you should manually balance them on the disk groups to distribute the cluster resource functions between the two nodes. This allows for a more efficient response time for the clients and users accessing these resources.

To set up cluster resource balancing:

1. Select a disk group and bring up its Properties panel by right-clicking it.
2. Click on the **General** tab.
3. Click the **Modify** button to the right of the *Preferred owners:* field.
4. In the Available nodes pane, select a node and click the **arrow** button to move the node to the Preferred Owners pane.

This is accomplished by selecting each disk group, right clicking and selecting Properties. The first tab, General will allow you to set this.

Each disk group has a preferred owner so that, when both nodes are running, all resources contained within each disk group will have a node defined as the owner of those resources. Even though a disk group has a preferred owner, its resources can run on the other node in the cluster following a failover. If you restart a cluster node, those resources that are preferentially owned by the restarted node failback to that node once the cluster service detects that the node is operational, and provided that the defined failover policy allows this to occur. If you have not defined the node as the preferred owner for the resources, then they do not failback to the node.

Failover setup

The failover of resources under a disk group on a node allows users to continue accessing the resources if the node goes down. Individual resources contained in a group cannot be moved to the other node; rather, the group it is contained in is moved. If a disk group contains a large number of resources and any one of those resources fail, then the whole group will failover according to the group's failover policy.

The setup of the failover policies is critical to data availability.

To set up the failover function:

1. Open the Properties panel for the disk group.
2. Select the **Failover** tab to set the Threshold for Disk Group Failure.

For example, if a network name fails, clustering services attempts to failover the group 10 times within 6 hours, but if the resource fails an eleventh time, the resource will remain in a failed state and Administrator action is required to correct the failure.

3. Select the **Failback** tab to allow, or prevent, failback of the disk group to the preferred owner, if defined.

In allowing failback of groups, is a slight delay in the resources moving from one node to the other. The group can also be instructed to allow failback when the preferred node becomes available or to failback during specific off-peak usage hours.

Each resource under each disk group has individual resource properties. The properties range from restart properties, polling intervals to check if resource is operational, to a timeout to return to an online state. The default settings for these properties are selected from average conditions and moderate daily usage.

User creation

The creation of users is performed through normal procedures. Users do not need to be created exclusively for use on the cluster resources. You will need to define properties of the resources for users to access the resources within the domain policies. All user-accessible cluster resources have the same properties as standard Microsoft Windows resources, and should be set up following the same policies.

Clustered file share creation (CIFS and NFS)

Note: For HTTP and FTP clustering setup and file sharing, refer to the information at the following URL:

```
http://support.microsoft.com/support/kb/articles/Q248/0/25.ASP
```

The creation of file shares involves dependencies on a physical disk, a static IP address, and a network name. The various dependencies allow resources that are defined to the same disk group to move as a group. The dependencies also assure necessary access for the given resource.

Physical disk

Is the base resource in which to store user data. It is not dependent on any other resources except for the physical disk that it defines. The disk resource must also have the same drive letters on both nodes so that the definitions of resources that depend on it will not change if the resource is moved to the other node.

Static IP address

Is a virtual address that will bind onto an existing IP address on one of the cluster's public networks. This IP address provides access for clients, and is not dependent on a particular node, rather a subnet that both nodes can access. Because this address is not the physical adapter's permanent address, it can bind and unbind to its paired adapter on the same network on the other node in the cluster. You can create multiple IP addresses through the Cluster Administrator on the same physical network.

Note: Note that the cluster IP Address is not to be used for file shares. That address is reserved to connect to and manage the cluster through the network that it is defined on.

Network name

> Provides an alternate computer name for an existing named computer. It is physically dependent on an IP address on one of the public networks. When a disk group contains an IP address resource and a network name, it is a virtual server and provides identity to the group, which is not associated to a specific node and can be failed over to another node in the cluster. Users access the groups using this virtual server.

In the creation of a basic file share that is publicized to the network under a single name, you will need to set it up to be dependent on the physical disk and network name in the same disk group you are creating the file share in. The network name is dependent on the IP address, so do not add that to the dependency list. You can set the share permissions and advanced share resources also. Users will access the cluster resources using \\<*network_name*>\<*fileshare_name*>.

Clustered file share creation example

An example of how to create a clustered file share follows. For this example, assume that you are creating a file share in Disk Group 2.

1. Creating the IP address resource
   a. Right-click Disk Group 2, and select **New → Resource**.
   b. Enter an IP address name, for example *ipaddr2*, and change the resource type to IP Address.
   c. Select **Run this resource in a separate Resource Monitor** and click **Next**.
   d. A list of possible owners displays, and both nodes should remain as assigned. Click **Next**.
   e. There are no resource dependencies on this panel, so click **Next**.
   f. Enter your TCP/IP Parameters. This will be the first virtual IP Address. The value in the Network field identifies to the system which network the address is located on. Click **Finish** to create the resource.
   g. Right-click the resource and bring it online.
2. Creating the network name resource
   a. Right-click Disk Group 2, and select **New → Resource**.
   b. Enter the virtual server name you want to use, for example, *NN2*, select **Network Name** as the resource type, and click **Next**.
   c. Both nodes will be possible owners. Click **Next**.
   d. Add the IP address you created as a resource dependency in Step 1 and click **Next**.
   e. Enter the virtual server name, NN2 into the Network Name Parameters field and click **Finish**.
   f. It takes a few moments to register the virtual server name with your Name Server. After this has completed, bring the resource online.
3. Creating the CIFS or NFS file share resource
   a. Right-click Disk Group 2, and select **New → Resource**.
   b. Enter a file share name, for example, *FS2*, and select either **File Share** or **NFS Share**.
   c. Both nodes are possible owners. Click **Next**.
   d. Add the resource dependencies for the Physical Disk and Network Name that the file share will use and click **Next**.
   e. Enter the share name of FS2 and the path to the disk in this group, either drive or sub-directory. You can then set:
      • For CIFS shares Properties:

- User Limit
- Permissions
- Advanced File Share
- For NFS shares Properties
  - Permissions
  - Share

   f. Click **Finish** and bring the resource online.

Note: If your storage is going to be accessed by UNIX or UNIX-based clients and servers, continue with "Defining UNIX users and groups". Otherwise, you have completed networking and clustering setup because the Model G26 is on a Windows domain, and it inherits those Windows users, eliminating the need to define local Windows users and groups. Also, shares are created in the clustering setup.

Defining UNIX users and groups

This section describes how to set up UNIX users and groups who will access the Model G26 storage via the Network File System (NFS) protocol.

Support for NFS is provided in the Model G26 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 G26, are NFS Versions 2 and 3. Any client or server that is using an NFS software stack supporting NFS Version 2 or NFS Version 3, regardless of the operating system, should be able to connect to the Model G26 and access its storage via NFS.

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.

You can define a local UNIX name space on the Model G26 by configuring the Server for PCNFS component of Services for UNIX. Alternately, you can point Services for UNIX to an existing Network Information Service (NIS) domain which defines the UNIX name space. In both cases, you will need to configure the User Name Mapping component to map the UNIX name space you select to the Windows name space, since file shares and individual file/directory permissions on the Model G26 are defined in the context of the Windows name space.

If you are going to define a local UNIX name space, continue with "Using a local UNIX name space". If you are going to use a UNIX name space defined on a NIS domain, continue with "Using the UNIX name space on an NIS domain" on page 49.

Using a local UNIX name space: This procedure should only have to be performed once. You may have to add more groups and users in the **Server for PCNFS** page if you add more users and groups to your UNIX environment and Model G26 or Windows domain at a later time.

1. Open the IBM NAS Administration console by double-clicking the **IBM NAS Admin** icon on the NAS desktop.
2. In the left pane, click the plus sign (**+**) next to File Systems, then click the plus sign next to Services for UNIX.
3. In the left pane, click **Server for NFS**.
4. In the right pane, in the Computer name: field, enter *localhost*.
5. In the left pane, click **Server for PCNFS**.

6. In the right pane, click **Groups**.

7. On the Groups page, you will need to add the groups from your UNIX host to which all of your UNIX users belong. You will need to know both the group name and the group ID (GID) number. This information can be found in the /etc/group file on most UNIX systems.

   As an example, on an AIX system, in the following line from an /etc/group file, the fields are separated by a colon (:). The first field (″staff″) is the group name; the third column (″1″) is the GID:

   ```
   staff:!:1:pemodem,ipsec,netinst,protcs
   ```

   You add a group by entering the group name and GID number in the Group name and Group number (GID) fields, respectively, and then clicking **New**.

8. When you have finished adding groups, click **Apply**.

9. Click **Users**.

10. On the Users page, you will need to add all of the UNIX users who will be accessing and storing files on the Model G26 through an NFS share. For each user you will need to know the Windows user name, the UNIX user name, the primary group, and the user ID (UID) number. This information can be found in the /etc/passwd and /etc/group files on most UNIX systems.

    As an example, on an AIX system, in the following line from an /etc/passwd file, the fields are separated by a colon (:). The first field (″user1″) is the user name; the third field (″3135″) is the UID, and the fourth field (″1″) is the GID of the user's primary group. This will correspond to a line in the /etc/group file, where you can find the primary group name corresponding to the GID.

    ```
    user1:!:3135:1:User 1:/home/user1:/bin/ksh
    ```

    You add a user by clicking **New**, entering the required information, and then clicking **OK**.

11. When you have finished adding users, click **Apply**.

12. In the left pane, click **User Name Mapping**.

13. In the right pane, click the radio button next to Personal Computer Network File System (PCNFS).

14. In the Password file path and name field, enter *c:\winnt\system32\drivers\etc\passwd*.

15. In the Group file path and name field, enter *c:\winnt\system32\drivers\etc\group*, then click **Apply**.

16. Click **Maps**.

17. On the Maps page, you can configure simple maps or advanced maps. Configure simple maps if the Windows user name and UNIX user name is the same for each UNIX user to be mapped, and the Windows group name and UNIX group name is the same for each UNIX group to be mapped. Otherwise, you should configure advanced maps.

    To configure simple maps, check the Simple maps checkbox and continue with Step 18. To configure advanced maps, uncheck the Simple maps checkbox and continue with Step 19.

18. Under the Simple maps checkbox, select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list, then continue with Step 20 on page 49.

19. Under Advanced maps, do the following:
    a. Define user mappings as follows:
       1) Click **Show user maps**.

2) Select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list.

3) Click **Show Windows Users** to display all of the Windows user names in the Windows domain you selected.

4) Click **Show UNIX Users** to display all of the UNIX user names in the NIS domain you selected.

5) Enter a Windows user name, or select one from the list of Windows user names.

6) Enter a UNIX user name to be mapped to the Windows user name you specified, or select one from the list of UNIX user names.

7) Click **Add** to add the mapping between the UNIX user name and Windows user name to the list of maps.

8) If multiple Windows user names are mapped to one UNIX user name, you must select one Windows user name to be the primary user name. Select the mapping corresponding to the primary user name from the list of maps, and then click **Set Primary**.

b. Define group mappings as follows:

1) Click **Show group maps**.

2) Select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list.

3) Click **Show Windows Groups** to display all of the Windows group names in the Windows domain you selected.

4) Click **Show UNIX Groups** to display all of the UNIX group names in the NIS domain you selected.

5) Enter a Windows group name, or select one from the list of Windows group names.

6) Enter a UNIX group name to be mapped to the Windows group name you specified, or select one from the list of UNIX group names.

7) Click **Add** to add the mapping between the UNIX group name and Windows group name to the list of maps.

8) If multiple Windows group names are mapped to one UNIX group name, you must select one Windows group name to be the primary group name. Select the mapping corresponding to the primary group name from the list of maps, and then click **Set Primary**.

20. Click **Apply**.

Note: You have now completed networking and clustering setup.

Using the UNIX name space on an NIS domain: The following procedure applies whether your NIS server is UNIX-based or Windows-based (implemented as a Windows domain controller running Microsoft's Server for NIS).

1. Open the IBM NAS Administration console by double-clicking the **IBM NAS Admin** icon on the NAS desktop.

2. In the left pane, click the plus sign (**+**) next to File Systems, then click the plus sign next to Services for UNIX.

3. In the left pane, click **Server for NFS**.

4. In the right pane, in the Computer name: field, enter *localhost*.

5. In the left pane, click **User Name Mapping**.

6. In the right pane, click the radio button next to Network Information Services (NIS), then click **Maps**.

7. On the Maps page, you can configure simple maps or advanced maps. Configure simple maps if the Windows user name and UNIX user name is the same for each UNIX user to be mapped, and the Windows group name and UNIX group name is the same for each UNIX group to be mapped. Otherwise,

you should configure advanced maps. To configure simple maps, check the Simple maps checkbox and continue with Step 8. To configure advanced maps, uncheck the Simple maps checkbox and continue with Step 9.

8. Under the Simple maps checkbox, do the following:
   a. Select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list.
   b. In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.
   c. Continue with Step 10.

9. Under Advanced maps, do the following:
   a. Define user mappings as follows:
      1) Click **Show user maps**.
      2) Select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list.
      3) In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.
      4) Click **Show Windows Users** to display all of the Windows user names in the Windows domain you selected.
      5) Click **Show UNIX Users** to display all of the UNIX user names in the NIS domain you selected.
      6) Enter a Windows user name, or select one from the list of Windows user names.
      7) Enter a UNIX user name to be mapped to the Windows user name you specified, or select one from the list of UNIX user names.
      8) Click **Add** to add the mapping between the UNIX user name and Windows user name to the list of maps.
      9) If multiple Windows user names are mapped to one UNIX user name, you must select one Windows user name to be the primary user name. Select the mapping corresponding to the primary user name from the list of maps, and then click **Set Primary**.
   b. Define group mappings as follows:
      1) Click **Show group maps**.
      2) Select the Windows domain name (the domain to which you joined the Model G26 earlier in this chapter) from the drop-down list.
      3) In the NIS domain field, enter the NIS domain name. You may also enter the name of a specific NIS server in the NIS server field.
      4) Click **Show Windows Groups** to display all of the Windows group names in the Windows domain you selected.
      5) Click **Show UNIX Groups** to display all of the UNIX group names in the NIS domain you selected.
      6) Enter a Windows group name, or select one from the list of Windows group names.
      7) Enter a UNIX group name to be mapped to the Windows group name you specified, or select one from the list of UNIX group names.
      8) Click **Add** to add the mapping between the UNIX group name and Windows group name to the list of maps.
      9) If multiple Windows group names are mapped to one UNIX group name, you must select one Windows group name to be the primary group name. Select the mapping corresponding to the primary group name from the list of maps, and then click **Set Primary**.

10. Click **Apply**.

Note: You have now completed networking and clustering setup.

Chapter 7. Additional administrative functions

This chapter describes the additional administrative functions that you can do on the NAS 300G.

The following functions are available:
- "NAS Backup Assistant", accessed through IBM NAS Admin icon
- "Persistent Images" on page 53, accessed through the Windows 2000 for Network Attached Storage user interface
- "Tivoli SANergy" on page 62
- "FAStT MSJ" on page 63, accessed through the IBM NAS Admin icon
- "System management adapters" on page 64
- "Ethernet adapter teaming" on page 67

NAS Backup Assistant

The NAS Backup Assistant is a preloaded utility that helps you create and schedule backup batch files, and maintain log files. It can be used for backing up either the NAS 300G operating system or user data.

You invoke the NAS Backup Assistant by clicking on the **IBM NAS Admin** desktop icon to open the IBM NAS Administration console. Select **Backup and Restore** to expand that tree, then select **IBM NAS Backup Assistant**. Once you have selected this option, a logon prompt appears. You will need to log on as a user who has backup operator privileges (that is, as an Administrator or backup Administrator).

If you want to back up selected folders, you can use NT Backup without the NAS Backup Assistant (which backs up an entire volume). However, if you use NT Backup, it is recommended that you select and back up the copy of the files in a previous persistent image, rather than the original data itself. When selecting the files for the NT Backup operation, you must select the specific folders in the persistent image. If you select the entire group of persistent images, the files in those images will not be selected for backup. For more information about persistent images see "Persistent Images" on page 53.

Because NAS Backup Assistant only creates and launches scripts, and is not a comprehensive backup application, it does not support interactive error messages. To check status of jobs, you must either view the Backup Logs or view the Windows Event Viewer. If a logon prompt does not appear, right-click on the **IBM NAS Backup Assistant** link, and select refresh. Once you log on, the main panel appears.

There are four tabs on the main panel:

Backup Operations

> This tab is the main window where you create and schedule backup batch jobs.

> There are two backup methods you can select in the Backup Operations window. You can choose a standard NT Backup operation, but this backs up only those files on the drive that are not in use. Therefore, to guarantee a complete backup image using this method, you would need to ensure that no users are accessing files on the drive. Hence, this method is useful only for offline backup.

To do a complete online backup that includes files that are in use, you should choose the Persistent Storage Manager (PSM) Persistent Image backup method. This method creates a persistent image (mapped as an unused drive letter on the system), backs up a copy of that persistent image, and then deletes the original persistent image (drive letter). For more information about persistent images see "Persistent Images" on page 53.

Scheduled Jobs
This tab displays a list of backup batch jobs that you scheduled.

Backup Logs
This tab displays a list of log files for each backup that has run.

Displayed Logs
This tab displays the text contained in the log files that you can select from the **Backup Logs** tab.

All of the options on each tab are described in detail in the online help. To access the online help, click on the **IBM NAS Admin** icon, then expand the Backup and Restore directory, then select **IBM NAS Backup Assistant Help** and log in.

Restoring using the NT Backup panel

To restore backups, use the following procedure:

1. Note the following conditions:
   - If you are restoring a backup that you created using the standard backup method, go to step 2.
   - If you are restoring a backup that you created using Persistent Images in the NAS Backup Assistant, the NT Backup file (*.BKF) was created for the persistent image virtual drive letter instead of the original drive letter. For example, if you selected drive C for backup, a persistent image was created on the next available drive letter in the system, and that drive was backed up instead of drive C. If you do not remember the original drive letter, you can view the backup log files in NAS Backup Assistant. The top section of the log file gives you the original drive letter, and the bottom section gives you the persistent image drive letter. When you have the original drive letter, go to step 2.

2. Click on the **Restore using NT Backup** link in the Backup and Restore section of the IBM NAS Admin console to open the backup GUI.

3. Click **Restore Wizard**, then click **Next**.

4. You are asked what you want to restore. Select the appropriate media that you are restoring from.

5. If you are restoring from tape, expand the backup media pool name, and then double-click on the media (this will normally be named *media created on {date - time})*. This action will read the set list from the tape.

   If you are restoring a file, select **Tools** → **Catalog a backup file**, then click **Browse** and find the backup file (.BKF) created for this backup. If you do not know the .BKF file name, refer to the backup log in NAS Backup Assistant. Click **OK**. You will now have a *Media created on {date - time}* listed under file. Click on the plus sign (**+**) to the left of this media to see the set list. You may be prompted to enter the path to the file you want to catalog; if so, select the same file that you just imported. This will build a set list.

6. Select the files and directories you want to restore by placing a check in the corresponding check box.

7. In the bottom left corner of the window, there is an option called **Restore files to:**. Using the pull-down, select **Alternate Location**. In the alternate location window, select the root directory of the original backup drive letter you determined in step 1 on page 52.

8. If desired, select **Tools** from the menu bar at the top of the window, then select **Options** to change restore options. Refer to NT Backup online help (see **Restore files from a file or a tape**) for use of these options.

9. Once you have selected the files or directories for restore, the alternate location, and options, click the **Start Restore** button in the lower right corner.

10. You will now be prompted to confirm that you want to begin the restore. You can click the **Advanced** button to select advanced options (see the NT Backup online help for details), then click **OK** to begin the restore.

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 NAS 300G 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 NAS 300G.

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 (Model G01)" on page 95 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 the NAS 300G 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 (Model G01)" on page 95 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 (Model G01)" on page 95.

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 (Model G01)" on page 95.

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*.

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 the 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 the 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 NAS 300G 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 (Model G01)" on page 95.

Tivoli SANergy

Note: The NAS 300G is enabled for SANergy use. Although the SANergy component is included in the product, you will need to obtain additional licenses from Tivoli to use SANergy client with this appliance.

Tivoli SANergy allows you to deliver shared data access at the speed of a SAN, using Fibre Channel, SCSI, or SSA. It gives multiple computers the power to dynamically share file and data access on SAN-based storage, using standard networks and file systems.

SANergy combines LAN-based file sharing with the very high data transfer speeds of the Fibre Channel, SCSI, and SSA storage networks. The result is high-speed, heterogeneous data sharing without the performance-limiting bottlenecks of file servers and traditional networking protocols.

SANergy extends standard file systems and network services provided by the operating systems that it supports. As an operating system extension built on standard systems interfaces, SANergy fully supports the user interface, management, access control, and security features native to the host platforms. Therefore, it provides you with all the file system management, access control, and security you expect in your network.

With SANergy, applications you have configured into your network can access any file at any time, and multiple systems can transparently share common data. SANergy ensures maximum compatibility with existing and future operating systems, applications, and management utilities.

In addition to the SAN, SANergy also uses a standard LAN for all the meta data associated with file transfers. Because SANergy is based on standard file systems, if your SAN fails, you can continue to access your data through the LAN.

With SANergy, you can reduce or even eliminate the expense of redundant storage and the overhead of data synchronization in multi-host environments. These environments include large-scale web, video, or file servers. Because each system has direct access to the SAN-based storage, SANergy can eliminate your file server as a single point of failure for mission-critical enterprise applications, reducing costly down-time. Also, with SANergy, you can readily manage all your data backup traffic over the storage network, while users have unimpeded LAN access to your existing file servers.

To set up SANergy on your network, use the following steps:
1. Make sure your network is correctly configured for LAN and SAN.
2. Configure your storage system, including disk formatting, partitioning, and volume configuration.
3. Enable SANergy bus management and device assignments. The Meta Data Controller will then be enabled for the appliance operating system.
4. Install additional SANergy licenses on properly configured hardware clients.

Further details on SANergy are contained in the online help.

FAStT MSJ

The FAStT MSJ diagnostic utility allows you to manage and control fibre-channel host bus adapter(s). With FAStT MSJ, you can:

- Retrieve and display general information about the adapters
- Request and display the real-time statistics of adapters
- Diagnose operations on the adapters and attached devices
- Display the NVRAM parameters of adapters (Note that you cannot change the parameters.)
- Monitor alarms and indications of the adapters

The primary purpose of FAStT MSJ in the NAS 300G is to obtain diagnostic information about the fibre channel connections.

You start FAStT MSJ by double-clicking the **IBM NAS Admin** icon. Then, under the **NAS Management** icon, double-click **Storage**, then **NAS Utilities**. And finally, you select **FAStT MSJ**. Once the FAStT MSJ opens, click **Connect**.

For further details on FAStT MSJ, see the online help.

"Appendix E. Fast!UTIL options" on page 129 provides detailed configuration information for advanced users who want to customize the configuration of the FAStT Host Adapter board and the connected devices, using Fast!UTIL to make changes.

System management adapters

There are two types of system management adapters[1]:

- The Integrated System Management Processor (ISMP) integrated on the planar board of each engine of the NAS 300G
- An optional Remote Supervisor Adapter (RSA) that can connect to up to twelve of the ISMPs

The ISMP provides basic operational status about key engine components, such as its processors, power supplies, fans, and so on.

The optional RSA allows you to connect via LAN or modem from virtually anywhere for extensive remote management. The RSA works in conjunction with the ISMP of the NAS 300G and an interconnect cable that connects multiple engines to the ISMP. Remote connectivity and flexibility with LAN capability is provided by Ethernet connection. The RSA enables more flexible management through a Web browser interface, in addition to ANSI terminal, Telnet, and IBM Director.

To use either adapter, and for more information, see "Additional information for the ISMP and RSA" on page 66.

Table 4 on page 65 provides a summary of the features of the ISMP and the RSA.

Remote status includes information on power supply voltages, voltage-regulator module (VRM) readings, temperatures of system components, system power status, power-on hours, fan status, and system state.

The lightpath diagnostics LED status that is available via the ISMP includes:
- Power-supply failure
- Insufficient power for power-supply redundancy
- Exceeded power-supply capabilities
- Non-maskable interrupt occurred
- Over heating
- Fan failure
- Memory error
- Microprocessor failure
- PCI-bus error
- VRM failure
- Planar SCSI failure for system disk or internal tape drive (if any)

---

1. There is a third that might be referred to in some of the documentation that came with your system, but that adapter is not used in the system.

Table 4. ISMP compared to the RSA

Feature	ISMP	RSA
Location	On planar board	Separate PCI adapter option
Light path diagnostics	Remotely reports on	Remotely reports on
LED status of engine	Remotely reports on	Remotely reports on
LED status of HDD in engine	No	No
Remote update of system BIOS	Yes	Yes
Remote update of ISMP BIOS	Yes	No
Remote power on/off	Yes	No
Remote POST (including all POST message ids)	Yes	No
Access to NIC card and fibre-channel status	No	No
Remote access to engine VPD and serial number	Yes	Yes
Multiple login IDs	Yes	Yes
Connect to LAN	No	No
TELNET interface over IP	No	Yes (via LAN connection)
Web-browser interface over IP	No	No
Forwarding of SNMP traps	Yes, to the RSA	Yes (via LAN connection)
Automated server restart	Yes	Yes
Remote Alerts	Yes	No
Configuration	By DOS utility	By DOS utility
Aggregate from other ISMP processors	Yes	Yes

ISMP - RSA communication on a single machine

You will need to follow one of two methods to enable communication between the ISMP and the RSA on a single machine:

1. Using a single ISMP interconnect cable (with dual RJ-11 plugs)
   a. Connect one end of the internal ISMP interconnect cable to the J-54 connector on the system board.
   b. Connect the other end (the RJ-11 socket) of the internal ISMP interconnect cable to the knockout slot on the back panel of the machine until it locks into place.
   c. Connect one connector on the ISMP interconnect cable to the RJ-11 socket you just installed on the back panel (in step 1b).
   d. Connect the other connector to the RJ-11 socket on the RSA.

2. Using two ISMP interconnect cables (each with a single RJ-11 plug)
   a. Connect one end of the internal ISMP interconnect cable to the J-54 connector on the system board.
   b. Connect the other end (with the RJ-11 socket) of the internal ISMP interconnect cable to the knockout slot on the back panel of the machine until it locks into place.
   c. Connect the first ISMP interconnect cable to the RJ-11 socket you just installed on the back panel (in step 2b).
   d. Connect the second ISMP interconnect cable to the RJ-11 socket on the RSA.
   e. Connect the two ISMP interconnect cables with a single Category 5 Ethernet cable (by plugging one end of the Ethernet cable into the "black box" on the first ISMP interconnect cable, and the other end into the "black box" on the second ISMP interconnect cable).

Additional information for the ISMP and RSA

The documentation CD that came with your system contains additional information and software for the ISMP and the RSA. The ISMP configuration program is different than the RSA configuration program. To use the ISMP, complete the following steps:

1. Consult the ISMP user's manual and the README file that is located on the documentation CD.
2. Run the executable to create a bootable floppy disk. The executable is located in:

   `C:\IBM\ASMP\UPDATES\32P0303.EXE`

3. Boot each node of the NAS 300G with floppy disk created in the previous step to configure the ISMP.

The documentation CD that came with your system contains additional information and software for the RSA. To use the RSA, complete the following steps:

1. Consult the RSA user's manual and the README file that is located on the documentation CD.
2. Run the executable to create a bootable floppy disk. The executable is located in:

   `C:\IBM\ASMP\UPDATES\33P2474.EXE`

3. Boot each node of the NAS 300G with floppy disk created in the previous step to configure the ISMP.

Ethernet adapter teaming

This section describes how to enable adapter teaming on the Intel and Alacritech Ethernet adapters

Intel adapters

The Intel Ethernet adapters (Gb Ethernet SX and 10/100 Ethernet) that you install in the PCI slots of the NAS 300G 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 NAS 300G, 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 6. Completing networking, clustering, and storage access setup for the Model G26" on page 39. Additionally, for each team you configure on one 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 NAS 300G 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 Console" on page 12.)
3. From the NAS 300G 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 checkbox 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 integrated Ethernet controller on each NAS 300G node is dedicated to the clustering interconnection between it and another node and cannot be used for teaming.

Alacritech adapter

The Quad-Port 10/100 Ethernet Adapter supports the Cisco Fast EtherChannel (FEC) technology across the four ports on the adapter. You can configure it by clicking successively on **Control Panel**→**Network**→**Adapter**→**Properties**→**Teaming** in the Windows interface.

Fast Etherchannel (FEC) is a proprietary technology developed by Cisco. With FEC, you can create a team of two to four ports on the 4-port 10/100 Ethernet PCI Adapter in to increase transmission and reception throughput. This feature may also be referred to as load balancing, port aggregation, or trunking. When you configure this feature, the adapter ports comprising the FEC team or group create a single high-speed, fault-tolerant link between the engine and the Ethernet switch sharing one IP address. With FEC, fault tolerance and load balancing is provided for both outbound and inbound traffic, unlike other load balancing schemes that only balance outbound traffic.

FEC requires an Ethernet switch with FEC capability. The FEC implementation on the 4-port 10/100 Ethernet Adapter does not support the optional Port Aggregation Protocol (PAgP) feature of FEC-capable Ethernet switches.

Chapter 8. Troubleshooting

This chapter provides basic troubleshooting information to help you resolve some common problems that might occur with the NAS 300G.

If you cannot locate and correct the problem using the information in this section, refer to "Appendix B. Getting help, service, and information" on page 103 for more information. Also, for the latest troubleshooting guidance and symptom-fix tip information, go to the IBM support Web site at

`http://www.ibm.com/storage/support/nas`

This site contains additional information, gathered from field experience, not available when this document was developed.

IBM 5187 Network Attached Storage Model 6RZ

This section gives troubleshooting information for the IBM 5187 Network Attached Storage Model 6RZ (engine).

Note: The information in this section needs to be applied to both engines in the NAS 300G. As an example, when the text reads, "The engine has light-emitting diodes (LEDs) to help you identify problems," this means that each engine in the NAS 300G has LEDs which require your attention.

As another example, the information contained in "Engine troubleshooting charts" on page 74 applies to each of the two engines.

Engine diagnostic tools overview

The following tools are available to help you identify and resolve hardware-related problems:

Note: If you need to remove the engines for inspection, do so one at a time: remove an engine, inspect it, and put it back; then remove the other engine, inspect it, and put it back.

- **POST beep codes, error messages, and error logs**

  The power-on self-test (POST) generates beep codes and messages to indicate successful test completion or the detection of a problem.

  POST error messages and descriptions are given in "Appendix D. Engine POST messages" on page 109.

- **Diagnostic programs and error messages**

  The diagnostic programs are stored in upgradable read-only memory (ROM) on the system board. These programs are the primary method of testing the major components of the NAS 300G engine. See "POST diagnostic programs" on page 119 for more information.

- **Light-path diagnostics**

  The engine has light-emitting diodes (LEDs) on its system board to help you identify problems. These LEDs are part of the light-path diagnostics that are built into the NAS 300G engine. By following the *path of lights*, you can quickly identify the type of system error that occurred. See "Light-path diagnostics" on page 72 for more information.

- **Networking adapter diagnostic tools**
  - **Intel PROSet II**

See "Testing the Ethernet adapters with Intel PROSet II" on page 84.

– **FAStT MSJ**

See "Testing the fibre-channel host adapter with FAStT MSJ" on page 91

- **Troubleshooting charts**

  These charts list problem symptoms, along with suggested steps to correct the problems. See "Engine troubleshooting charts" on page 74 for more information.

- **Support**

  You can register with the following support site to subscribe to e-mail notification of new technical tips and frequently asked questions, obtain downloads, and join forum discussions:

  `http://www.storage.ibm.com/support/nas`

Identifying problems using LEDs

The LEDs are part of the light-path diagnostics built into the NAS 300G engine. The LEDs help you identify the type of system error that occurred. See the following sections for more information.

Power-supply LEDs

The AC and DC power LEDs on the power supply provide status information about the power supply.

Table 5 on page 71 describes the AC and DC power LEDs.

Note: The minimum configuration required for the DC good light to come on is:
- Power supply
- Power backplane
- System board (with pins 2 and 3 on J23 extension cable connected together to bypass the power switch.

Table 5. Power-supply LEDS

AC Good LED	DC Good LED	Description	FRU/action
Off	Off	No power to system or ac problem.	1. **Check ac power to system.** 2. Power supply

On	Off	Standby mode or dc problem.	1. **Check system board cable connectors J32, J33, and J35.** Move jumper on J32's extension cable to pins 2-3 to bypass power control. If the DC Good LED comes on, press **Ctrl+Alt+Delete**. Watch the screen for any POST errors. Check the System Event/Error Log for any listed problems. If the system powers up with no errors:
			  a. **Power switch assembly**
			  b. **System board**
			2. Remove the adapters and disconnect the cables and power connectors to all internal and external devices. Power-on the system. If the DC Good LED comes on, replace the adapters and devices one at a time until you isolate the problem.
			3. Power supply
			4. Power backplane
			5. System board

On	On	Power is OK.	N/A

Light-path diagnostics

You can use the light-path diagnostics built into the NAS 300G engine to identify the type of system error that occurred. Any LEDs that are illuminated remain illuminated during a shutdown as long as the ac power source is good and the power supplies can supply +5V dc current to the NAS 300G engine. This feature helps you isolate the problem, if an error causes the NAS 300G to shut down. See "Light-path diagnostics".

Diagnostics panel

You can use the light path diagnostics to quickly identify the type of system error that occurred. The diagnostics panel is under the "wind tunnel". Any LEDs that are On, remain On when the NAS 300G shuts down as long as the AC power source is stable and the power supplies can provide +5V DC current. This feature helps isolate the problem if an error causes the NAS 300G to shut down.

Figure 1 shows the LEDs on the diagnostics panel on the system board. You need to remove the top cover to view the LEDs.

See "Light-path diagnostics" for information on identifying problems using these LEDs.

MEM	PS1
CPU	PS2
PCI A	PS3
PCI B	NON
PCI C	OVER
VRM	NMI
DASD	TEMP
SP	FAN

REMIND
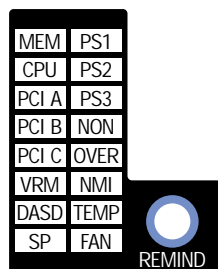
Figure 1. Diagnostics panel LEDs

Light-path diagnostics

Table 6 on page 73 describes the light-path diagnostics LEDs. The system error LED is turned on when an error is detected. If the system error LED (an amber "!" on the lower right corner) is on, remove the cover and check the diagnostic panel LEDs. Table 6 on page 73 is valid only when the system error LED is on.

Notes:
1. If a diagnostic panel LED is on and the information LED panel system error LED is off, there is probably an LED problem. Run LED diagnostics.
2. Check the System Error Log for additional information before replacing a FRU.
3. The DIMM error LEDs, processor error LEDs, and VRM error LEDs turn off when the system is powered off.

Table 6. Descriptions of light-path diagnostics LEDs

Name	Meaning
PS1	Power supply 1 failure.
PS2	Power supply 2 failure.
PS3	Power supply 3 failure.
NON	Non-redundant power.
OVER	The system has exceeded the power capabilities of the installed power supplies.
NMI	Non-maskable-interrupt occurred.
TEMP	System temperature exceeded maximum rating.
FAN	A fan failed or is operating slowly.
MEM	Memory failure. One or more memory DIMMs have failed.
CPU	Microprocessor failure. One or both microprocessors have failed.
PCI A	Error on PCI channel A or system board. **Note:** PCI bus A is often referred to as PCI bus 0.
PCI B	Error on PCI channel B or system board. **Note:** PCI bus B is often referred to as PCI bus 1.
PCI C	Error on PCI channel C or system board. **Note:** PCI bus C is often referred to as PCI bus 2.
VRM	Error on voltage regulator module or on integrated voltage regulator.
DASD	A hot-swap disk drive, backplane, or other part of SCSI channel A has failed.
SP	Integrated System Management Processor detected an error.

Remind button: You can use the remind button to place the front panel system-error light into a remind mode. By pressing the button, you acknowledge the failure but indicate that you will not take immediate action. If a new error occurs, the LED will be on again.

In the remind mode, the system-error LED flashes every 2 seconds. The system-error LED remains in remind mode until one of the following situations occurs:

1. All known problems are resolved
2. The system is restarted
3. A new problem occurs

You can use the remind button to delay maintenance. Also, resetting the system-error LED enables the LED to react to another error. If the LED is still blinking from the first error, it will mask additional errors.

Engine troubleshooting charts

You can use Table 7 to find solutions to problems that have the described symptoms.

If you cannot find the problem in the table, go to "Starting the diagnostic programs" on page 120 to test the NAS 300G engine. If you have run the diagnostic test programs or if running the tests does not reveal the problem, call for service.

The symptom appears in the left column of the table. Instructions and probable solutions to the problem are in the right column. If you have just added new software or a new option and the NAS 300G engine is not working, do the following before using the troubleshooting charts:

- Remove the software or device that you just added.
- Run the diagnostic tests to determine if the NAS 300G engine is running correctly.
- Reinstall the new software or new device.

Table 7. Engine troubleshooting symptoms and actions

Error Symptom	CRU/action
CD is not working correctly.	1. **Clean the CD** 2. Run CD-ROM diagnostic 3. CD-ROM drive
CD-ROM drive tray is not working.	1. **Ensure the appliance is powered ON** 2. Insert the end of a paper clip into the manual tray-release opening 3. Run CD-ROM diagnostic 4. CD-ROM drive
CD-ROM drive is not recognized.	1. **Run Configuration/Setup; enable primary IDE channel** 2. Check cables and jumpers 3. Check for correct device driver 4. System board 5. Run CD-ROM diagnostics 6. CD-ROM drive
Power switch does not work and reset button does work.	1. **Verify that the power-on control jumper on J23 extension cable is on pins 1 and 2** 2. Power switch assembly 3. System board

Table 7. Engine troubleshooting symptoms and actions (continued)

Error Symptom	CRU/action

Diskette drive in-use LED stays on, the system bypasses the diskette drive, or the diskette drive does not work.	1. **If there is a diskette in the drive, verify that:**
	  a. **The diskette drive is enabled in the Configuration/Setup utility program**
	  b. **The diskette is good and not damaged (try another diskette if you have one)**
	  c. **The diskette is inserted correctly in the drive**
	  d. **The diskette contains the necessary files to start the appliance**
	  e. **The program is OK**
	  f. **The cable is installed correctly (correct orientation)**
	2. Run diskette-drive diagnostics
	3. Cable
	4. Diskette Drive
	5. System board

Monitor problems (general).	**Note:** Some monitors have their own self-tests. If you suspect a problem with the monitor, refer to the information that comes with the monitor for adjusting and testing instructions.Suggested action: 1. **Monitor** 2. Run video diagnostics **Note:** If the diagnostics complete successfully, the problem may be a video driver 3. Display adapter/system board
Fixed disk diagnostic does not recognize drives. Test shows fewer drives than are actually installed.	Remove first drive that does not appear and rerun diagnostic. If the remaining drives show up, replace the removed drive.
Fixed disk diagnostic freezes when run.	Remove the drive being tested at the time of the freeze and rerun the diagnostic. If the diagnostic completes successfully, replace the removed drive.

Power problems

Power problems can be difficult to troubleshoot. For example, a short circuit can exist anywhere on any of the power distribution busses. Usually a short circuit causes the power subsystem to shut down because of an overcurrent condition.

Table 8 on page 76 lists the power error messages that you might encounter.

A general procedure for troubleshooting power problems is as follows:

1. Power off the system and disconnect the AC cord(s).

   Attention: Note the special considerations when powering off and powering on the Model G26 . See "Appendix F. Powering off and powering on the NAS 300G" on page 135 for details.

2. Check for loose cables in the power subsystem. Also check for short circuits, for example, if there is a loose screw causing a short circuit on a circuit board.

3. Remove adapters and disconnect the cables and power connectors to all internal and external devices until the NAS 300G engine is at minimum configuration required for power on.

4. Reconnect the AC cord and power on the NAS 300G engine. If the engine powers up successfully, replace adapters and devices one at a time until the

problem is isolated. If the engine does not power up from minimal configuration, replace FRUs of minimal configuration one at a time until the problem is isolated.

Table 8. Power error messages

Message	Action
Power supply ″**X**″ **current share fault** (level-critical; excessive current demand on power supply ″X″)	1. **See "Power problems" on page 75**
Power supply ″**X**″ **DC good fault** (level-critical; power good signal not detected for power supply ″X″)	1. **Replace power supply** ″**X**″
Power supply ″**X**″ **temperature fault**	1. **Replace fan** ″**X**″
Power supply ″**X**″ **removed**	1. **No action required - information only**
Power supply ″**X**″ **fan fault** (level-critical; fan fault in power supply ″X″)	1. **Replace power supply** ″**X**″
Power supply ″**X**″ **12V fault** (level-critical; overcurrent condition detected)	1. **See "Power problems" on page 75**
Power supply ″**X**″ **3.3V fault** (level-critical; 3.3V power supply ″X″ had an error)	1. **See "Power problems" on page 75**
Power supply ″**X**″ **5V fault** (level-critical; 5V power supply ″X″ had an error)	1. **See "Power problems" on page 75**
System over recommended ″**X**″ **current** (level-non-critical; system running too much current on that voltage)	1. **See "Power problems" on page 75**
System running non-redundant power (level-non-critical; system does not have redundant power)	1. **Add another power supply** 2. Remove options from system 3. System can continue to operate without redundancy protection if **1** and **2** above are not followed.
System under recommended voltage for ″**X**″ **v** (level-warning; indicated voltage supply under nominal value; value for ″X″ can be +12, -12, or +5)	1. **Check connections to power subsystem** 2. Replace power supply 3. Replace power backplane
System under recommended voltage on 3.3 v (level-warning; 3.3 volt supply under nominal value)	1. **Check connections to power subsystem** 2. Replace power supply 3. Replace power backplane
System under recommended X current (level-non-critical; system drawing less current than recommended on voltage ″X″)	1. **See "Power problems" on page 75**
″**X**″ **V bus fault** (level-critical; overcurrent condition on ″X″ voltage bus)	1. **Check for short circuit on** ″**X**″ **voltage bus** 2. See "Power problems" on page 75
12V ″**X**″ **bus fault** (level-critical; overcurrent condition on 12 volt ″X″ voltage bus)	1. **Check for short circuit on 12 volt** ″**X**″ **voltage bus** 2. See "Power problems" on page 75
5V fault (level-critical; overcurrent condition on 5 V subsystem)	1. **Check for short circuit on 5 v bus** 2. See "Power problems" on page 75
240 VA fault (level-critical; overcurrent or overvoltage condition in power subsystem)	1. **See "Power problems" on page 75**

Recovering BIOS

If your BIOS has become corrupted, such as from a power failure during a flash update, you can recover your BIOS using the recovery boot block and a BIOS flash diskette.

Note: Note: You can obtain a BIOS flash diskette from one of the following sources:

- Download a BIOS flash diskette from the Web site at
  http://www.ibm.com/storage/support/nas
- Contact your IBM service representative.

The flash memory contains a protected area that cannot be overwritten. The recovery boot block is a section of code in this protected area that enables the NAS 300G to start up and to read a flash diskette. The flash utility recovers the system BIOS from the BIOS recovery files on the diskette.

To recover the BIOS:

1. Power off the NAS 300G and peripheral devices. Disconnect all external cables and power cords. Remove the cover.

   Note: Note the procedure for powering off the unit, as described in "Appendix F. Powering off and powering on the NAS 300G" on page 135.

2. Locate the boot-block jumper block (J16) on the system board. See Figure 2 on page 78.
3. Place a jumper on pins 2 and 3 to enable the BIOS backup page.
4. Insert the BIOS flash diskette into the diskette drive.
5. Restart the NAS 300G.
6. When the NAS 300G completes POST, select **1 -- Update POST/BIOS** from the menu that contains various flash (update) options.
7. When you are asked if you would like to move the current POST/BIOS image to the backup ROM location, type **N**. **Attention:** Typing **Y** will copy the corrupted BIOS into the secondary page.
8. When you are asked if you would like to save the current code on a diskette, select **N**.
9. You will be asked to choose the language you wish to use. Select your language (**0-7**) and press **Enter** to accept your choice. You will be prompted to remove the diskette and press **Enter** to restart the system. Remove the flash diskette from the diskette drive.
10. Power off the NAS 300G.
11. Remove the jumper on the boot-block jumper block, or move it to pins 1 and 2 to return to normal startup mode.
12. Restart the NAS 300G. It should start up normally.

Figure 2 on page 78 shows the location of the boot block jumper on the system board.
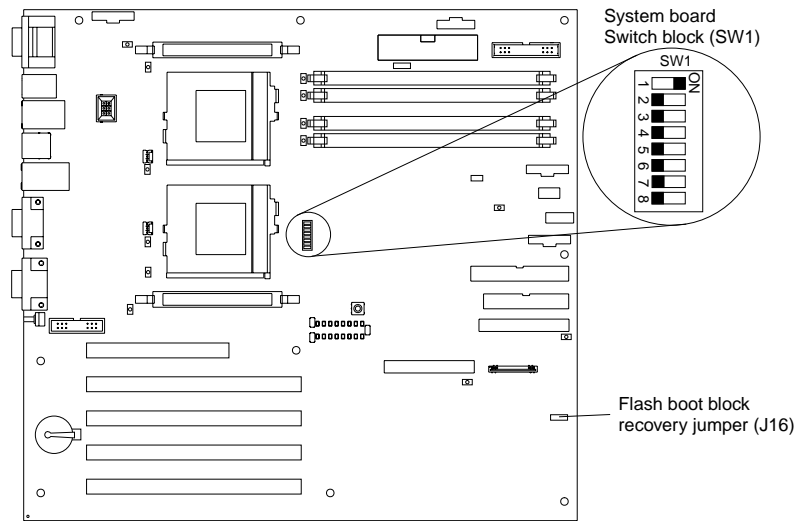
Figure 2. Boot block jumper location

Replacing the battery

IBM has designed this product with your safety in mind. The lithium battery must be handled correctly to avoid possible danger. If you replace the battery, you must adhere to the following instructions.

Note: In the U.S., call 1-800-IBM-4333 for information about battery disposal.

If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.

To order replacement batteries, call 1-800-772-2227 within the United States, and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your IBM reseller or IBM marketing representative.

Note: After you replace the battery, you must reconfigure your appliance and reset the system date and time.

CAUTION:

When replacing the lithium battery, use only IBM Part Number 10L6432 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:
- **Throw or immerse into water.**
- **Heat to more than 100 C (212 F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.
Note: For translations of the safety notice, refer to the multilingual Safety Information on the Documentation CD that came with the appliance.

To replace the battery:

1. Review the information in the section "Before you begin" in the hardware installation guide that came with this appliance, and any special handling and installation instructions supplied with the replacement battery.

2. Turn off the appliance and peripheral devices and disconnect all external cables and power cords; then, remove the appliance cover.

3. Remove the battery:

   a. Use one finger to lift the battery clip over the battery.

   b. Use one finger to slightly slide the battery from its socket. The spring mechanism behind the battery will push the battery out toward you as you slide it from the socket.

   c. Use your thumb and index finger to pull the battery from under the battery clip.

   d. Ensure that the battery clip is touching the base of the battery socket by pressing gently on the clip.
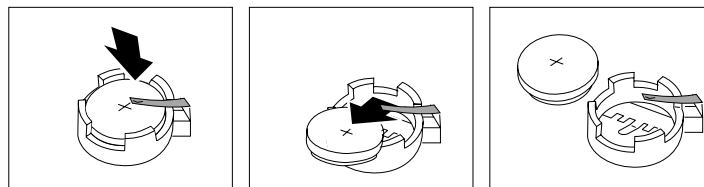
Figure 3. Battery removal

4. Insert the new battery:

   a. Tilt the battery so that you can insert it into the socket, under the battery clip.

   b. As you slide it under the battery clip, press the battery down into the socket.
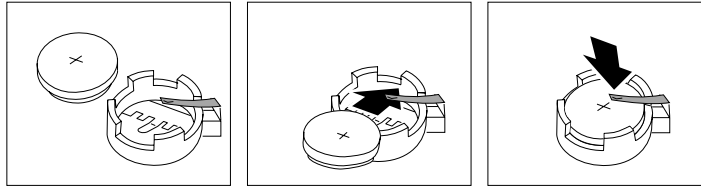
Figure 4. Battery replacement

5. Reinstall the appliance cover and connect the cables.

   Note: Wait approximately 20 seconds after you plug the power cord of the engine into an electrical outlet for the Power Control button to become active.

6. Turn the appliance on.

7. Start the Configuration/Setup Utility program and set configuration parameters.
   - Set the system date and time.
   - Set the power-on password.
   - Reconfigure the engine.

Adapter troubleshooting and diagnostics

This section presents information on troubleshooting and diagnosing the following engine adapters:

- 10/100 integrated Ethernet adapter
- IBM 10/100 PCI Ethernet adapter
- IBM Gigabit Ethernet SX adapter
- Alacritech Quad-Port Ethernet Adapter
- IBM ServeRAID-4Lx SCSI Controller
- Integrated System Management Processor (ISMP)
- Remote Supervisor Adapter (RSA)
- IBM Fast/Wide Ultra SCSI Adapter
- IBM PCI Ultra 160 SCSI Adapter

Integrated Ethernet adapter

This section provides troubleshooting information for problems that might occur with the 10/100 Mbps integrated Ethernet adapter.

Network connection problems

If the Ethernet adapter cannot connect to the network, check the following:

- Make sure that the cable is installed correctly.

  The network cable must be securely attached at all connections. If the cable is attached but the problem persists, try a different cable.

  If you set the Ethernet adapter to operate at 100 Mbps, you must use Category 5 cabling.

  If you directly connect two workstations (without a hub), or if you are not using a hub with X ports, use a crossover cable.

  Note: To determine whether a hub has an X port, check the port label. If the label contains an *X*, the hub has an X port.
- Determine if the hub supports auto-negotiation. If not, try configuring the integrated Ethernet adapter manually to match the speed and duplex mode of the hub.
- Check the Ethernet adapter lights on the operator information panel.

  These lights indicate whether a problem exists with the connector, cable, or hub.
  - The Ethernet Link Status light is On when the Ethernet adapter receives a LINK pulse from the hub. If the light is Off, there might be a bad connector or cable, or a problem with the hub.
  - The Ethernet Transmit/Receive Activity light is On when the Ethernet adapter sends or receives data over the Ethernet Network. If the Ethernet Transmit/Receive Activity light is Off, make sure that the hub and network are operating and that the correct device drivers are loaded.
- Make sure that you are using the correct device drivers, supplied with the NAS 300G engine.
- Check for operating system-specific causes for the problem.
- Make sure that the device drivers on the client and the NAS 300G engine are using the same protocol.
- Test the Ethernet adapter by running the diagnostic program.

Integrated Ethernet adapter troubleshooting chart

Use Table 9 to find solutions to 10/100 Mbps integrated Ethernet adapter problems that have definite symptoms.

Table 9. Integrated Ethernet adapter troubleshooting chart

Ethernet adapter problem	Suggested Action
Ethernet Link Status light is not On.	Check the following: • Ensure that the hub is powered on. • Check all connections at the Ethernet adapter and the hub. • Check the cable. A crossover cable is required unless the hub has an *X* designation. • Use another port on the hub. • If the hub does not support auto-negotiation, manually configure the Ethernet adapter to match the hub. • If you manually configured the duplex mode, ensure that you also manually configure the speed. • Run diagnostics on the LEDs. If the problem remains, go to "Testing the Ethernet adapters with Intel PROSet II" on page 84 to run the diagnostic programs.
The Ethernet Transmit/Receive Activity light is not On.	Check the following: **Note:** The Ethernet Transmit/Receive Activity LED is On only when data is sent to or by this Ethernet adapter. • Ensure that you have loaded the network device drivers. • The network might be idle. Try sending data from this workstation. • Run diagnostics on the LEDs. • The function of this LED can be changed by device driver load parameters. If necessary, remove any LED parameter settings when you load the device drivers.
Data errors	Check the following: • Ensure that you are using Category 5 cabling when operating the NAS 300G engine at 100 Mbps. • Make sure that the cables do not run close to noise-inducing sources like fluorescent lights.
The Ethernet adapter stopped working when another adapter was added to the NAS 300G engine.	Check the following: • Ensure that the cable is connected to the Ethernet adapter. • Ensure that the PCI system BIOS is current. • Reseat the adapter. • Ensure that the adapter you are testing is supported by the NAS 300G engine. Go to "Testing the Ethernet adapters with Intel PROSet II" on page 84 to run the diagnostic programs.
The Ethernet adapter stopped working without apparent cause.	Check the following: • Run diagnostics for the Ethernet adapter. • Try a different connector on the hub. • Reinstall the device drivers. Refer to your operating-system documentation and to the *User's Reference* information. If the problem remains, go to "Testing the Ethernet adapters with Intel PROSet II" on page 84 to run the diagnostic programs.

Troubleshooting the 10/100 PCI Ethernet adapter

You can use Table 10 to find solutions to 10/100 Mbps Ethernet adapter problems that have definite symptoms.

See "Testing the Ethernet adapters with Intel PROSet II" on page 84 for information on testing the adapter.

Table 10. 10/100 PCI Ethernet adapter troubleshooting chart

Ethernet adapter problem	Suggested Action
The adapter cannot connect to the network.	Check the following: 1. Ensure that the network cable is installed correctly. The cable must be securely attached at both RJ-45 connections (adapter and hub). The maximum allowable distance from adapter to the hub is 100 m (328 ft.). If the cable is attached and the distance is within acceptable limits but the problem persists, try a different cable. If you are directly connecting two computers without a hub or switch, make sure you are using a crossover cable. 2. Check the LED lights on the adapter. The adapter has two diagnostic LEDs, one on each side of the cable connector. These lights help you to determine whether there is a problem with the connector, cable, switch, or hub. **ACT/LNK — On** • Adapter and switch is receiving power and cable connection between them is good **ACT/LNK — Off** Check the following: • Adapter not sending or receiving data • Adapter or switch not receiving power • Cable connection between adapter and switch is faulty • Drivers not configured properly **ACT/LNK — Flashing** Normal operation. LED flashes when the adapter sends or receives data. The frequency of the flashes varies with the amount of network traffic **100 — On** Adapter is operating at 100 Mbps **100 — Off** Adapter is operating at 10 Mbps 3. Ensure that you are using the correct drivers. Ensure that you are using the drivers that come with this adapter. Drivers that support previous versions of this adapter do not support this version of the adapter. 4. Ensure that the switch port and the adapter have the same duplex setting. If you configured the adapter for full-duplex, ensure that the switch port is also configured for full-duplex. Setting the wrong duplex mode can degrade performance, cause data loss, or result in lost connections.
Diagnostics pass, but the connection fails or errors occur.	Check the following: 1. For 100 Mbps: • Use Category 5 cabling and ensure that the network cable is securely attached. • Verify the adapter is seated firmly in the slot and connected to a 100BASE-TX hub/switch (not 100BASE-T4). 2. Ensure the duplex mode setting on the adapter matches the setting on the switch

Table 10. 10/100 PCI Ethernet adapter troubleshooting chart (continued)

Ethernet adapter problem	Suggested Action
The LNK LED is not On.	Check the following: 1. Ensure that you loaded the correct network drivers. 2. Check all connections at the adapter and the switch. 3. Try another port on the switch. 4. Ensure that the duplex mode setting on the adapter matches the setting on the switch. 5. Ensure that you have the correct type of cable between the adapter and the hub. 100BASE-TX requires two pairs. Some hubs require a crossover cable while others require a straight-through cable.
The ACT LED is not On.	Check the following: 1. Ensure that you loaded the correct network drivers. 2. The network might be idle. Try accessing a server. 3. The adapter is not transmitting or receiving data. Try another adapter. 4. Ensure that you are using two-pair cable for TX wiring.
Adapter stops working without apparent cause.	Check the following: 1. Run the diagnostics. 2. Try reseating the adapter in its slot, or try a different slot if necessary. 3. The network driver files might be corrupt or missing. Remove and then reinstall the drivers.
The LNK LED is not On when you connect the power.	Check the following: Ensure that the network cable is securely attached at both ends.

Testing the Ethernet adapters with Intel PROSet II

Each NAS 300G engine comes with Intel PROSet II. You can use PROSet to view the following:

- Adapter parameters such as MAC and IP addresses
- Network link status such as speed, duplex mode, and activity
- Device-driver level used for the adapter

You can also use PROSet II to test the 10/100 Ethernet and GB Ethernet PCI adapters for any problems with the adapter hardware, cabling, or network connections. PROSet performs a loopback test on the 10/100 Ethernet and GB Ethernet PCI cards.

To access the PROSet II utility, go into Terminal Services. For instructions on how to invoke Terminal Services, see "Terminal Services and the IBM NAS Administration Console" on page 12. Within Terminal Services do the following steps:

1. Go to the Start menu, select **Settings**, then **Control Panel**.
2. Double-click the INTEL PROSet II icon in the Control Panel to start the INTEL PROSet II utility.
3. In the INTEL PROSet II utility, select the Ethernet adapter you want to test (Gigabit Ethernet PCI adapter or 10/100 Ethernet Adapter).
4. Select the **Diagnostics** tab. A list of available tests is displayed.
5. Select **Run Tests**. You can also select or deselect individual tests with the check boxes. If an error is detected, information about the error is displayed.
6. Repeat Steps 3 through 5 for each Ethernet adapter installed.

For additional information about Intel PROSet, please refer to the online help that accompanies the utility.

Gigabit Ethernet SX adapter

Use Table 11 to find solutions to GB Ethernet adapter problems that have definite symptoms.

See "Testing the Ethernet adapters with Intel PROSet II" on page 84 for information on testing the adapter.

Table 11. Gigabit Ethernet SX adapter troubleshooting chart

Gigabit adapter problem	Suggested Action

No Link or TX/RX Activity	If you cannot link to your switch, check the following:
	1. Check the following LED lights on the adapter:
	
	TX — On
	    The adapter is sending data
	
	RX — On
	    The adapter is receiving data.
	
	Link — On
	    The adapter is connected to a valid link partner and is receiving link pulses.
	
	Link — Off
	    Link is inoperative.
	    • Check all connections at the adapter and link partner
	    • Make sure the link partner is set to 1000 Mbps and full-duplex
	    • Ensure the required drivers are loaded
	
	PRO — Programmable LED
	    Identifies the adapter by blinking. Use the Identify Adapter push-button in INTEL PROSet II to control blinking.
	2. Ensure that the cable is installed correctly. The network cable must be securely attached at all connections. If the cable is attached but the problem persists, try a different cable.

Your computer cannot find the Gigabit Ethernet SX adapter	Check the following: 1. Verify that the adapter is seated firmly in the slot 2. Try a different Gigabit Ethernet SX adapter
Diagnostics pass but the connection fails	Check the following: Ensure the network cable is securely attached
Another adapter stopped working after you installed the Gigabit Ethernet SX Adapter	Check the following: 1. Verify that the cable is connected to the Gigabit Ethernet SX Adapter and not to another adapter. 2. Check for a resource conflict 3. Ensure both adapters are seated firmly in the slot 4. Check all cables
The adapter stopped working without apparent cause	Check the following: 1. Try reseating the adapter 2. The network driver files might be damaged or deleted. Reinstall the drivers 3. Try a different Gigabit Ethernet SX Adapter

Table 11. Gigabit Ethernet SX adapter troubleshooting chart (continued)

Gigabit adapter problem	Suggested Action
LINK LED is not On	Check the following: 1. Ensure that you have loaded the adapter driver 2. Check all connections at the adapter and the buffered repeater or switch 3. Try another port on the buffered repeater or switch 4. Ensure that the buffered repeater or switch port is configured for 1000 Mbps and full-duplex. 5. Try changing the auto-negotiation setting on the link partner, if possible
RX or TX LED is no On	Check the following: 1. Ensure that you have loaded the adapter driver 2. Network might be idle; try logging in from a workstation 3. The adapter is not transmitting or receiving data; try another adapter

Troubleshooting the Alacritech Quad-Port 10/100 Ethernet adapter

Table 12 displays the LED definitions for the Alacritech Quad-Port 10/100 Ethernet adapter LED definitions

Table 12. Alacritech Quad-Port 10/100 Ethernet adapter LED definitions

LED	Indication	Meaning
LNK	Off	Either the adapter or the switch (or both) are not receiving power, or the cable connection between them is faulty.
	Green	The adapter and switch are receiving power. The cable connection between them is good. A 100 Mbps link has been established.
	Amber	The adapter and switch are receiving power. The cable connection between them is good. A 10 Mbps link has been established.
ACT	Off	The adapter is not sending or receiving network data.
	Flashing amber	The adapter is sending or receiving network data.

Testing the Alacritech Quad-Port 10/100 Ethernet adapter

The event log tells you when you should run diagnostics. You can view the event log from the Event Viewer located in the Administrative Tools folder on the Start Menu, located under Programs. When the event log reports that "SLIC*x* has determined that the adapter is not functioning properly," you can run diagnostics on the Alacritech Quad-Port 10/100 Ethernet adapter using the following procedure:

1. Run the SLICuser application from the Start Menu, located under the Program Files folder in the Alacritech Folder.

2. Select the **Diagnostics** tab.

   Note: Running diagnostics disrupts all ports of the adapter.

3. Click **Run**. The adapter will then run through a self-test of the IPP and the selected port of the adapter. A properly functioning board will display a window in which all of its tests have *Passed*.

4. Close the SLICuser utility by clicking **OK**.

Troubleshooting the ServeRAID-4Lx

Error codes and messages display on the screen in a line of text immediately after the adapter BIOS version.

If POST detects changes in the controller configuration or detects a controller hardware problem, messages appear on the screen. Refer to "POST (ISPR) error procedures" on page 88 and correct the problem.

If there is no POST Error or Configuration Error message, the BIOS screen messages resemble the sample shown below. Note that your version may be different from the one shown.

```
 _____
IBM ServeRAID BIOS
Copyright IBM Corp. 1994, 2001. All rights reserved.
BIOS Ver: 4.70.17
 _____
Controller 1 Slot 3, Logical drive=3, Other=0, Firmware=4.70.17, Status=OK
    << Press Ctrl+I to access the Mini-Configuration Program >>

Initializing ServeRAID Controller 1 in Slot 1.
Power-on self-test can take up to 59 Second(s) -- test Passed.
Drive configuration can take up to 6 Minute(s) 0 Second(s) -- test Passed.
```

If there is a POST Error message, the BIOS screen resembles the sample shown below. Refer to "POST (ISPR) error procedures" on page 88 and correct the problem. Note that your version may be different from the one shown. The characters *XXXX* indicate the POST (ISPR) error.

```
 _____
IBM ServeRAID BIOS
Copyright IBM Corp. 1994, 2001.  All rights reserved.
BIOS Ver: 4.70.17
 _____
Controller 1 Slot 3, Logical drive=3, Other=0, Firmware=4.70.17, Status=Failed
    << Press Ctrl+I to access the Mini-Configuration Program >>

Initializing ServeRAID Controller 1 in Slot 1.
Power-on self-test can take up to 59 Second(s) -- test Failed.
Controller is not responding properly - Run Diagnostics.
Error Code: XXXX-YY
```

The sample BIOS screen below shows configuration status and error information.

```
_____
IBM ServeRAID BIOS
Copyright IBM Corp. 1994, 2001. All rights reserved.
BIOS Ver: 4.70.17
_____
Controller 1 Slot 3, Logical drive=3, Other=0, Firmware=4.70.17, Status=OK
    << Press Ctrl+I to access the Mini-Configuration Program >>


_____
Initializing ServeRAID Controller 1 in Slot 1.
Power-on self-test can take up to 59 Second(s) -- test Passed.
Drive configuration-can take up to 6 Minute(s) 0 Second(s) -- test Failed.
Controller POST and Config Error Codes: ISPR = EF10 BCS = 09 ECS = 20.
Following drives not responding (old state: new state: ch SID)

(RDY:EMP: 2:0)

The system has a configuration error due to above condition(s). Press: F4 - Retry
the command F5 - Update Controller configuration to exclude
NON-RESPONDING drives Warning: NON-RESPONDING drives will be set to
DDD, DHS, or EMP state F10 - Exit without change
```

Note: **Do not** replace a ServeRAID-4 controller or a system board containing an imbedded ServeRAID-4 controller for ServeRAID problems unless replacing the controller is listed in Table 13 on page 89.

POST (ISPR) error procedures

The Interrupt Status Port Register (ISPR) Error Procedures list errors, symptoms, and the possible causes. The most probable cause is listed first. Use these procedures to help you solve ServeRAID problems when servicing the computer. A complete list of error codes is in Table 13 on page 89.

EF 10   Default ISPR. No ISPR error present.

9ZXX thru BZXX

SCSI bus error caused either by cables, termination, defective drives, and so on.

1. Isolate the error between SCSI subsystem and controller by disconnecting all SCSI cables from suspect card, and reboot.
    CAUTION:
    Do not press F5. Doing so changes the configuration.
    If an ISPR error is still present, take the following actions until the error is no longer present:
    a. Reseat the controller
    b. Replace the controller

    Note: If the controller detects a configuration change, **do not** choose **Save Changes**. Instead, press **F10** to bypass any options to this effect.

2. If the ISPR error is EF10 after disconnecting cables:
    a. Confirm that the identified channel(s) is the cause of the error by verifying that the error presents itself only when the offending channel is reconnected.
    b. Check termination of identified channel.
    c. Check for proper backplane jumper configuration.
    d. Check for proper cabling configuration in systems that use DASD status cables. Reconnect all cables that you disconnected at the beginning of this procedure.
    e. Replace SCSI cable.
    f. Replace SCSI backplane.

FFFF (or other code not listed)

1. Isolate between SCSI Subsystem and controller by disconnecting all SCSI cables attached to the suspect card, and reboot.

   CAUTION:

   CAUTION: Do not press F5. Doing so changes the configuration.

   If ISPR code is EF10 after disconnecting cables, follow the steps below until the error is eliminated:

   a. Identify which channel is causing the error by reconnecting cables one at a time and rebooting until the error returns.

   b. Disconnect one drive at a time attached to identified channel and reboot each time to determine which drive is causing the problem.

   c. Replace SCSI cable attached to the identified channel.

   d. Replace backplane attached to the identified channel

2. If the original ISPR code is still present after disconnecting all SCSI cables and rebooting, take the following actions until the error is no longer present:

   a. Reseat the controller

   b. Replace the controller

ServeRAID-4Lx problems and actions

Table 13 lists problems and corrective actions associated with the adapter. The table helps you determine which adapters may need to be replaced at the conclusion of troubleshooting procedures.

Note: Do not replace any controllers until you have followed the POST (ISPR) error procedures (see "POST (ISPR) error procedures" on page 88).). Replace a ServeRAID controller only when indicated to do so in the POST (ISPR) error procedures.

XXX in Table 13 is used as a placeholder and may be any letter or number in an actual error message.

Table 13. ServeRAID-4Lx problems and actions

Problem	Action
1XXX (Microcode Checksum Error)	ServeRAID-4 controller
2XXX thru 5XXX (Code DRAM Error)	1. Install download jumpers, flash latest level BIOS and firmware for controller. Remove jumpers. 2. ServeRAID-4 controller
6XXX (Cache DRAM Error) (ServeRAID-4H only)	1. Reseat Daughter card 2. Install download jumpers, flash latest level BIOS and firmware for controller. Remove jumpers. 3. ServeRAID-4 controller
7XXX thru 8XXX (Host/Local PCI Bus Interface Error)	1. Install download jumpers, flash latest level BIOS and firmware for controller. Remove jumpers. 2. ServeRAID-4 controller

Table 13. ServeRAID-4Lx problems and actions (continued)

Problem	Action
9ZXX thru BZXX SCSI Bus error caused by cables, termination, defective drives, and so on). The Z refers to the specific channel or channels that cause the error.	1. Follow indications in the POST error procedures (see "POST (ISPR) error procedures" on page 88). Follow those instructions before continuing with the next steps listed in this table. 2. SCSI cable 3. SCSI backplane 4. Hard drive 5. ServeRAID-4 controller
EFFE (Firmware code corrupt or download jumpers are in place)	1. Flash latest level BIOS and firmware for controller. Remove jumpers. 2. ServeRAID-4 controller
FFFF or other code not listed	1. Follow indications in the POST (ISPR) error procedures ("POST (ISPR) error procedures" on page 88). 2. SCSI cable 3. SCSI backplane 4. Hard drive 5. ServeRAID-4 controller

Testing the ServeRAID 4Lx adapter

You can run all diagnostic operations for the ServeRAID adapters through the IBM ServeRAID Configuration software in the **Advanced Functions** option. You can run subsystem diagnostics through the system diagnostics.

Note: Before running any test, back up the current disk array configuration using the ServeRAID diagnostics test program. Always keep a current backup of the ServeRAID configuration information. Dynamic changes may occur in the configuration due to hot-spare replacement.

The IBM PC ServeRAID Adapter diagnostics test program runs independently of the operating system and is run from diskette. You can obtain a copy from the ServerGuide Diskette Factory or download it from IBM's web site.

To back up the ServeRAID configuration:
1. From the Main Menu, select **Advanced Functions**
2. Select **Backup IPS ServeRaid Config**

You can use the ServeRAID Subsystem Diagnostic program to test the PC ServeRAID Adapter and the devices connected to it. To test the ServeRAID subsystem:

1. Start the ServeRAID Configuration Utility program

2. Select **Advanced Functions** from the Main Menu and press **Enter**

3. Select **IBM ServeRAID Subsystem Diagnostic** from the next menu and press **Enter**

4. Select the diagnostic test that you want to run and press **Enter** . Descriptions of the diagnostic tests available include:
   Run Adapter Self-tests

   Tests the PC ServeRAID Adapter. Restart the server after the self-test completes.

SCSI Device Self-test
Runs diagnostic tests on the SCSI devices attached to the PC ServeRAID Adapter.

Testing the fibre-channel host adapter with FAStT MSJ

Note: Ensure that there is no adapter activity before running the test or data can be lost.

The NAS 300G engine comes with FAStT MSJ for viewing the status of the Fibre Channel connection as well as testing the adapter or cable. To use FAStT MSJ, you should first go into Terminal Services. For instructions on how to invoke Terminal Services, see "Terminal Services and the IBM NAS Administration Console" on page 12.

You access FAStT MSJ by going into the IBM NAS Admin console, selecting **NAS Management** ▸ **Storage** ▸ **NAS Utilities** ▸ **FAStT MSJ**. Then, select **Connect**. A diagnostic panel displays the following general information related to the Fibre Channel adapter which can be useful if you need to place a support call:
- Node name
- Serial number (in hex)
- Loop ID
- BIOS version
- Firmware version number
- Device driver version number
- PCI slot number

FAStT MSJ also provides the NAS 300G engine's world-wide name (WWN) as detailed in "FAStT MSJ" on page 63.

To test the Fibre Channel adapter, select the adapter and then click the **Diagnostic** button. FAStT MSJ can perform fibre loopback and data tests.

For additional information relating to FAStT MSJ diagnostic functions, refer to the online help accessed from its panels.

Checking the FAStT host-bus adapter's fibre-channel connectivity

In addition to the above diagnostic function, you can use FAStT MSJ to determine if the physical fibre channel connections are in place by doing the following steps:

1. Once Connected with FAStT as above, select the **QLA2200 Adapter** icon, and verify that you see all Fibre Controllers that you are physically connected to. If you see a red **X** on the QLA2200 Adapter icon, and the icon is yellow, the adapter cannot register with the 3534 Fibre Channel hub. (A green icon means connections are in place.) Check the fibre cable connections, and if the QLA2200 adapter still does not connect, run the adapter and 3534 Fibre Channel hub diagnostics.
2. If the icon is green, click on the plus sign (+) in front of the adapter icon to see the state of the attached Fibre channel storage controllers. The absence of controllers in the display indicates connection problems.

For additional information relating to FAStT MSJ diagnostic functions, refer to the online help accessed from its panels.

Testing the Integrated System Management Processor

1. Insert the ISMP Utility CD-ROM into the CD-ROM drive and restart the NAS 300G engine. If the engine does not boot from the CD-ROM, use POST/BIOS setup to configure the CD-ROM drive as a boot device.

2. After the engine boots, the main option menu appears. The main menu contains the following selections:

   - `Hardware Status and Information`
   - `Configuration Settings`
   - `Update System Management firmware`

3. Use the up and down arrow keys to select **Hardware Status and Information** and press **Enter**. The Hardware Status and Information menu contains the list of ISMP devices with the following diagnostic test results:

   ```
           Processor Communication   :  Passed
     ->     Built in  Self Test Status  ......    : Passed
            Boot Sector Code Revision ...         :6, Build ID:  RIET62A
            Main Application Code Revision        :4, Build ID:  ILET15A

            Processor Communication   :  Passed
     ->     Built in  Self Test Status  ......    : Passed
            Boot Sector Code Revision ...         :6, Build ID:  WMICT60A
            Main Application Code Revision        :4, Build ID:  WMXT57A
   ```

4. Use the up and down arrow keys to select the device you want to look at in more detail. Press **Enter**. You will see a list of tests and results on the device:

   ```
              Current System Management Processor Status


              Current BIST Results:
                  SRAM Memory Test:                 Passed
                  Serial Port 1 Test :              Passed
                  Serial Port 2 Test:               Passed
                  NVRAM Memory Test                 Passed
                  Realtime Clock Test               Passed
                  Programmable Gate Array Test:     Passed
                  I2C Interface Test:               Passed
                  Main Application Checksum:         Passed
                  Boot Sector Checksum:             Passed


                  Current System Management Adapter Status


              Current BIST Results:
                  SRAM Memory Test:                 Passed
                  Serial Port 1 Test :              Passed
                  Serial Port 2 Test:               Passed
                  NVRAM Memory Test                 Passed
                  Realtime Clock Test               Passed
                  Programmable Gate Array Test:     Passed
                  I2C Interface Test:               Passed
                  Main Application Checksum:         Passed
                  Boot Sector Checksum:             Passed
                  Onboard Ethernet Hardware Test:   Passed
                  PCI EEPROM Initialization Test:   Passed
   ```

5. When you are finished viewing this information, press **Esc** to return to the main option menu. Remove the CD then restart the NAS 300G engine.

Testing the Remote Supervisor Adapter

1. Insert the Remote Supervisor Adapter Support CD into the CD-ROM drive and restart the engine. If the engine does not boot from the CD-ROM, use POST/BIOS setup to configure the CD-ROM drive as a boot device.

2. After the engine boots, the main option menu appears. The main menu contains the following selections:

- Hardware Status and Information
- Configuration Settings
- Update System Management firmware

3. Use the up and down arrow keys to select **Hardware Status and Information** and press **Enter**. The Hardware Status and Information menu contains the list of devices with the following diagnostic test results:

```
      System Management Processor Communication  :  Passed
 ->   Built in  Self Test Status  ......    : Passed
      Boot Sector Code Revision ...         :16, Build ID:  CNET15A
      Main Application Code Revision        :16, Build ID: TUET15A
```

4. Use the up and down arrow keys to select the device you want to look at in more detail. Press **Enter**. You will see a list of tests and results on the device:

```
         Current System Management Processor Status

            Current BIST Results:
               SRAM Memory Test:                  Passed
               Serial Port 1 Test :               Passed
               Serial Port 2 Test:                Passed
               NVRAM Memory Test                  Passed
               Realtime Clock Test                Passed
               Programmable Gate Array Test:      Passed
               I2C Interface Test:                Passed
               Main Application Checksum:         Passed
               Boot Sector Checksum:              Passed


            Current System Management Adapter Status

            Current BIST Results:
               SRAM Memory Test:                  Passed
               Serial Port 1 Test :               Passed
               Serial Port 2 Test:                Passed
               NVRAM Memory Test                  Passed
               Realtime Clock Test                Passed
               Programmable Gate Array Test:      Passed
               I2C Interface Test:                Passed
               Main Application Checksum:         Passed
               Boot Sector Checksum:              Passed
               Onboard Ethernet Hardware Test:    Passed
               PCI EEPROM Initialization Test:    Passed
```

5. When you are finished viewing this information, press **Esc** to return to the main option menu. Remove the CD then restart the engine.

Testing SCSI Adapters

The SCSI adapters are used for tape backup operations. They may be configured during engine boot time by entering **Ctrl-A** when prompted. This invokes the BIOS SCSI Select utility. Follow the on-screen directions when this utility appears. The adapters are tested during the boot process.

Chapter 9. Using the Recovery and Supplementary CDs

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 58 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 (Model G01)

The Recovery CD Set (three CDs, labeled as "Recovery CD 1," "Recovery CD 2," and "Recovery CD 3") contains the preload image for this appliance and is used to recover the preloaded image on the appliance. You must start the appliance using the Recovery Enablement Diskette before you can boot from Recovery CD 1.

CAUTION:
The Model G01 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 an appliance, perform 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. Attach a keyboard and display to the appliance.
2. Insert the Recovery Enablement Diskette into the diskette drive of the Model G01 and restart the appliance. When the Recovery Enablement Diskette has

completed loading and modifying the appliance startup sequence, the appliance will begin a continuous beep. Do not continue with this procedure until the appliance begins the beep.

> **Important**
>
> The Recovery Enablement Diskette enables the Model G01 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.

3. Remove the Recovery Enablement Diskette from the diskette drive of the appliance.
4. Place Recovery CD 1 in the CD-ROM drive of the Model G01 and restart the appliance.
5. If you installed additional processor memory on the appliance, the BIOS configuration program will appear. Click **Continue** on the first screen, click **Continue** again, click **Exit Setup**, and finally, click **Yes, save and exit Setup**.
6. The recovery process will begin automatically. Follow the instructions provided by the image restoration software, and the original manufacturing preload will be restored. During the restoration of the preload, you will be prompted to insert the other recovery CDs into the CD-ROM drive. Once the preload image is restored, the Model G01 restarts automatically.
7. If you installed additional processor memory, the BIOS configuration program will now appear a second time. Click **Continue** on the first screen, click **Continue** again, click **Exit Setup**, and finally, click **Yes, save and exit Setup**. You may now detach the keyboard and display from the appliance and allow the recovery process to complete automatically.

> **Important**
>
> - After the Model G01 restarts, a series of configuration and system preparation programs that finish configuring the appliance 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 the Model G01. Do not connect to or configure the appliance for at least 15 minutes after system restart. This notice applies only to the first time the Model G01 is started after using the Recovery CD Set.
> - Logical Disk 0 will be configured to have a 6-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 Model G01, contains the Maintenance partition, but for a replacement hard disk drive would not contain any other partitions), will be unchanged.

8. Reinstall all software updates you had installed on the appliance. Or, if the Recovery CD Set you used in this procedure is a newer version than the one you received with the Model G01, reinstall only those software updates that are newer than those on the Recovery CD Set.

Using the Recovery Enablement Diskette and Recovery CD (G26)

The Recovery CD Set (three CDs, labeled as "Recovery CD 1," "Recovery CD 2," and "Recovery CD 3") contains the preload image for this appliance and is used to recover the preloaded image on either node. You must start the (failed) node using the Recovery Enablement Diskette before you can boot from Recovery CD 1.

CAUTION:
The Model G26 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, perform 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. Attach a keyboard and display to the node.
2. On the other (working) node of the Model G26, 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**.
3. 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 G26.
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 G26 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 node using the Recovery Enablement Diskette.

5. Remove the Recovery Enablement Diskette from the diskette drive of the node.
6. Place Recovery CD 1 in the CD-ROM drive of the failed node and restart the node.
7. If you installed additional processor memory on the failed node, the BIOS configuration program will appear. Click **Continue** on the first screen, click **Continue** again, click **Exit Setup**, and finally, click **Yes, save and exit Setup**.
8. The recovery process will begin automatically. Follow the instructions provided by the image restoration software, and the original manufacturing preload will be restored. During the restoration of the preload, you will be prompted to insert the other recovery CDs into the CD-ROM drive. Once the preload image is restored, the node restarts automatically.

9. If you installed additional processor memory, the BIOS configuration program will now appear a second time. Click **Continue** on the first screen, click **Continue** again, 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 the Model G26. 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 G26 is started after using the Recovery CD Set.
> - Logical Disk 0 will be configured to have a 6-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 unchanged.

10. Reinstall all software updates you had installed on the node. Or, if the Recovery CD Set you used in this procedure is a newer version than the one you received with the Model G26, 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:

    a. Start a Terminal Services session to the node and click the **IBM NAS Admin** icon. From the IBM NAS Administration console that appears, select **Computer Management** and **Disk Management**.

    b. Start a *Windows 2000 for NAS* user interface session to the node and select **Disks and Volumes**. Select **Disks and Volumes** again, and then provide your administrator user name and password when prompted.

    Once Disk Management has started, perform these steps:

    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. 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`, and file system `FAT32`.

12. On the failed (now recovered) node, follow the procedures for configuring a joining node located in "Roadmap for setting up and configuring the NAS 300G" on page 3 (and described in detail in other chapters). 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.

Using the Supplementary CD

The Supplementary CD contains documentation and copies of key software applications that are preinstalled on the NAS 300G. Table 14 includes the names of the directories found on the Supplementary CD and a description of the contents of the directory.

Table 14. 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 NAS 300G. To install the Advanced Appliance Configuration console (on another network-attached workstation running Windows 98, Windows NT, or Windows 2000), run lpv2setup.exe 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	Diskette images for the Recovery Enablement Diskette and the IBM NAS AutoRAID diskette. To create the Recovery Enablement Diskette, run RecovDsk.bat and insert an HD 1.44 floppy diskette into drive A: when prompted. To create the IBM NAS AutoRAID diskette, run IBM_NAS_AutoRAID.exe and insert an HD 1.44 floppy diskette into drive A: when prompted. Note that the NAS 300Gsupports two internal hard disk drives. Please read the file readme.txt in the root directory and readme.txt in this directory for more information about the diskette images and how to create diskettes from the images. **Attention:** Starting the NAS 300G with the IBM NAS AutoRAID diskette will remove all RAID configuration changes from your ServeRAID adapter and restore the RAID configuration to its factory default configuration. All data stored in your ServeRAID arrays will be lost. Use this diskette only if you want to reset the NAS 300G to factory default settings. After using the diskette, you must use the Recovery CD (described earlier in this chapter) to restore the preloaded software image on the system drive.
I386	Windows Powered installation files. If you add device drivers, OS features, and so on, you may be prompted to insert the Windows Powered CD-ROM. If so, insert the Supplementary CD, and specify path x:\i386, where x is the drive letter assigned to the CD-ROM drive.
W2KSP2	Windows Powered Service Pack 2, which is preloaded on the NAS 300G. 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.

Table 14. Supplementary CD directories (continued)

Directory Name	Contents
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 the NAS 300G. 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 NAS 300G 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.

Appendix A. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States or other countries or both:

IBM
IBM Director
ServeRAID
ServerGuide
TotalStorage

Intel, MMX, LANDesk, Pentium, Pentium II Xeon, and Pentium III Xeon are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Lotus and Domino are trademarks of Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

NetWare is a trademark of Novell, Inc.

Persistent Storage Manager is a trademark of Columbia Data Products, Inc.

Tivoli and NetView are trademarks of Tivoli Systems Inc. in the United States, other countries, or both.

UNIX is a registered trademark in the United States and other countries and is licensed exclusively through The Open Group.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Getting help, service, and information

If you need help, service, technical assistance, or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

IBM maintains pages on the World Wide Web where you can get information about IBM products and services and find the latest technical information.

Table 15 lists some of these pages.

Table 15. IBM Web sites for help, services, and information

http://www.ibm.com	Main IBM home page
http://www.storage.ibm.com	IBM Storage home page
http://www.storage.ibm.com/support/nas	IBM NAS Support home page

You might also want to visit the Web pages of other companies for information about other operating systems, software, and accessories. The following are some other Web sites you might find helpful:

http://www.tivoli.com
http://www.cdpi.com

Services available and telephone numbers listed are subject to change without notice.

Service support

With the original purchase of an IBM hardware product, you have access to extensive support coverage. During the IBM hardware product warranty period, you may call the IBM Support Center (1 800 426-7378 in the U.S.) for hardware product assistance covered under the terms of the IBM hardware warranty. See "Getting help by telephone" on page 105 for Support Center telephone numbers in other countries.

The following services are available during the warranty period:
- Problem determination: Trained personnel are available to assist you with determining if you have a hardware problem and deciding what action is necessary to fix the problem.
- IBM hardware repair: If the problem is determined to be caused by IBM hardware under warranty, trained service personnel are available to provide the applicable level of service.
- Engineering change management: Occasionally, there might be changes that are required after a product has been sold. IBM or your reseller, if authorized by IBM, will make Engineering Changes (ECs) available that apply to your hardware.

Be sure to retain your proof of purchase to obtain warranty service.

Please have the following information ready when you call:
- Machine type and model
- Serial numbers of your IBM hardware products
- Description of the problem

- Exact wording of any error messages
- Hardware and software configuration information

If possible, be at your NAS device when you call.

A compatible monitor, keyboard, and mouse are required for many service activities. Before you have the NAS device serviced, be sure to attach these components to the device, either directly or indirectly through a console switch.

The following items are not covered:
- Replacement or use of non-IBM parts or nonwarranted IBM parts

   Note: All warranted parts contain a 7-character identification in the format IBM FRU XXXXXXX.
- Identification of software problem sources
- Configuration of BIOS as part of an installation or upgrade
- Changes, modifications, or upgrades to device drivers
- Installation and maintenance of network operating systems (NOSs)
- Installation and maintenance of application programs

Refer to your IBM hardware warranty for a full explanation of IBM's warranty terms.

Before you call for service

Some problems can be solved without outside assistance, by using the online help, by looking in the online or printed documentation that comes with your network-attached storage appliance, or by consulting the support Web page noted in Table 15 on page 103. Also, be sure to read the information in any README files that come with your software.

Your network-attached storage appliance comes with documentation that contains troubleshooting procedures and explanations of error messages. The documentation that comes with your appliance also contains information about the diagnostic tests you can perform.

If you receive a POST error code or beep code when you turn on your Network Attached Server appliance, refer to the POST error-message charts in your hardware documentation. If you do not receive a POST error code or beep code, but suspect a hardware problem, refer to the troubleshooting information in your hardware documentation or run the diagnostic tests.

If you suspect a software problem, consult the documentation (including any README files) for the operating system or application program.

Getting customer support and service

Purchasing an IBM network-attached storage appliance entitles you to standard help and support during the warranty period. If you need additional support and services, a wide variety of extended services are available for purchase that address almost any need; see "Appendix C. Purchasing additional services" on page 107 for information.

Getting help online: http://www.ibm.com/storage/support/nas

Be sure to visit the support page that is specific to your hardware, complete with
FAQs, parts information, technical hints and tips, technical publications, and
downloadable files, if applicable. This page is at:
http://www.ibm.com/storage/support/nas.

Getting help by telephone

During the warranty period, you can get help and information by telephone through
the IBM Support Center. Expert technical-support representatives are available to
assist you with questions you might have on the following:
* Setting up your network-attached storage appliance
* Arranging for service
* Arranging for overnight shipment of customer-replaceable parts

In addition, if you purchased a network-attached storage appliance, you are eligible
for IBM up and running support for 90 days after installation. This service provides
assistance for:
* Setting up your network-attached storage appliance
* Limited configuration assistance

Please have the following information ready when you call:
* Machine type and model
* Serial numbers of your appliance and other components, or your proof of
  purchase
* Description of the problem
* Exact wording of any error messages
* Hardware and software configuration information for your system

If possible, be at your computer when you call.

In the U.S. and Canada, these services are available 24 hours a day, 7 days a
week. In the U.K., these services are available Monday through Friday, from 9:00
a.m. to 6:00 p.m. In all other countries, contact your IBM reseller or IBM marketing
representative.[2]

---

2. Response time will vary depending on the number and complexity of incoming calls.

Appendix C. Purchasing additional services

During and after the warranty period, you can purchase additional services, such as support for IBM and non-IBM hardware, operating systems, and application programs; network setup and configuration; upgraded or extended hardware repair services; and custom installations. Service availability and name might vary by country.

Warranty and repair services

You can upgrade your standard hardware warranty service or extend the service beyond the warranty period.

Warranty upgrades in the U.S. include:

* On-site service to premium on-site service

    If your warranty provides for on-site service, you can upgrade to premium on-site service (4-hour average on-site response, 24 hours a day, 7 days a week).

You also can extend your warranty. Warranty and Repair Services offers a variety of post-warranty maintenance options. Availability of the services varies by product.

For more information about warranty upgrades and extensions:
* In the U.S., call 1-800-426-4343.
* In Canada, call 1-800-465-7999.
* In all other countries, contact your IBM reseller or IBM marketing representative.

Appendix D. Engine POST messages

This appendix identifies and describes POST messages that you might encounter, and gives corrective actions where applicable.

Note: The information in this appendix applies to each engine in the appliance. For example, when the text reads, "When a monitor and keyboard is attached to the appliance," that means that a monitor and keyboard has been attached to either of the two engines.

Power-on self-test (POST)

When you turn on your NAS 300G, its engine performs a power-on self-test (POST) to check the operation of appliance components and some of the options installed in the appliance.

If POST finishes without detecting any problems when a monitor and keyboard are not attached to the appliance, you will hear one long and three short beeps. When a monitor and keyboard are attached, you will hear one short beep. Any other series of beeps indicates a problem, and an error message appears on your screen. See "POST beep code descriptions" for more information.

Notes:
1. If you have a power-on password or administrator password set, you must type the password and press **Enter**, when prompted, before POST will continue.
2. A single problem might cause several error messages. When this occurs, work to correct the cause of the first error message. After you correct the cause of the first error message, the other error messages usually will not occur the next time you run the test.

POST beep code descriptions

Beep codes are sounded in a series of beeps. For example, a 1-2-4 beep code sounds like one beep, a pause, two consecutive beeps, another pause, and four more consecutive beeps.

The possible types of beep codes that your appliance might emit include the following:

No beeps
> If no beep occurs after your appliance completes POST (that is, after the system POST complete (OK) light on the operator information panel is illuminated), call for service.

Continuous beep
> The recovery enablement disk has booted, your startup (boot) microprocessor has failed, or your system board or speaker subsystem might contain a failing component. If the system continues through POST with no errors, call for service. If no video appears, the startup processor has failed; replace the startup processor.

One short beep
> When a monitor and keyboard is attached to the appliance, one beep indicates that your appliance successfully completed POST. POST detected no configuration or functional errors. One beep also occurs after your appliance completes POST if you enter an incorrect power-on password.

109

Two short beeps

POST encountered an error. The Configuration/Setup Utility program will display additional information; follow the instructions that appear on the screen. See "POST error messages" on page 114 for descriptions of the text messages that might appear.

Three short beeps

A system memory error has occurred. This combination occurs only if the video Basic Input/Output System (BIOS) cannot display the error message. Replace the failing memory module.

Repeating short beeps

The system board might contain a failing component, your keyboard might be defective, or a key on the keyboard might be stuck. Ensure that:
1. Nothing is resting on the keyboard and pressing a key.
2. No key is stuck.
3. The keyboard cable is connected correctly to the keyboard and to the correct connector on the appliance.

Running the diagnostic tests can isolate the appliance component that failed, but you must have your system serviced. If the error message remains, call for service.

Note: If you just connected a new mouse or other pointing device, turn off the appliance and disconnect that device. Wait at least 5 seconds; then, turn on the appliance. If the error message goes away, replace the device.

One long and one short beep

POST encountered an error on a video adapter. If you are using the integrated video controller, call for service. If you are using an optional video adapter, replace the failing video adapter.

One long and two short beeps

A video I/O adapter ROM is not readable, or the video subsystem is defective. If you hear this beep combination twice, both the system board and an optional video adapter have failed the test. This beep combination might also indicate that the system board contains a failing component.

One long and three short beeps

This series of beeps has two meanings. The first means that the POST has completed without detecting errors, when a monitor and keyboard is not attached. However, when a monitor is attached, and you hear this series, it means the system-board video subsystem has not detected a monitor connection to the appliance. Ensure that the monitor is connected properly to the appliance. If the problem persists, replace the monitor.

Two long and two short beeps

POST does not support the optional video adapter. This beep combination occurs when you install a video adapter that is incompatible with your appliance. Replace the optional video adapter with one that the appliance supports or use the integrated video controller.

Table 16 on page 111 describes the codes and specifies the action to take.

POST beep codes

Table 16. POST beep codes

Symptom	FRU/action
1-1-2 (Processor register test failed)	**Processor**
1-1-3 (CMOS write/read test failed)	1. **Battery** 2. System board
1-1-4 (BIOS EEPROM checksum failed)	**System board**
1-2-1 (Programmable Interval Timer failed)	**System board**
1-2-2 (DMA initialization failed)	**System board**
1-2-3 (DMA page register write/read failed)	**System board**
1-2-4 (RAM refresh verification failed)	1. **DIMM** 2. System board
1-3-1 (1st 64K RAM test failed)	**DIMM**
1-3-2 (1st 64K RAM parity test failed)	1. **DIMM** 2. System board
2-1-1 (Secondary DMA register failed)	**System board**
2-1-2 (Primary DMA register failed)	**System board**
2-1-3 (Primary interrupt mask register failed)	**System board**
2-1-4 (Secondary interrupt mask register failed)	**System board**
2-2-2 (Keyboard controller failed)	1. **System board** 2. Keyboard
2-2-3 (CMOS power failure and checksum checks failed)	1. **Battery** 2. System board
2-2-4 (CMOS configuration information validation failed)	1. **Battery** 2. System board
2-3-1 (Screen initialization failed)	1. **Jumper on J14** 2. System board
2-3-2 (Screen memory failed)	**System board**
2-3-3 (Screen retrace failed)	**System board**
2-3-4 (Search for video ROM failed)	**System board**
2-4-1 (Video failed; screen believed operable)	**System board**

Table 16. POST beep codes (continued)

Symptom	FRU/action
3-1-1 (Timer tick interrupt failed)	**System board**
3-1-2 (Interval timer channel 2 failed)	**System board**
3-1-3 (RAM test failed above address OFFFFH)	1. **DIMM** 2. System board
3-1-4 (Time-Of-Day clock failed)	1. **Battery** 2. System board
3-2-1 (Serial port failed)	**System board**
3-2-2 (Parallel port failed)	**System board**
3-2-3 (Math coprocessor failed)	**Processor**
3-2-4 (Failure comparing CMOS memory size against actual)	1. **DIMM** 2. Battery
3-3-1 (Memory size mismatch occurred; see the Hardware Installation Guide.)	1. **DIMM** 2. Battery
3-3-2 (Critical SMBUS error occurred)	1. **Disconnect the server power cord from outlet, wait 30 seconds and retry.** 2. System board 3. DIMMs 4. DASD backplane 5. Power supply 6. Power supply backplane 7. 12 C cable
3-3-3 (No operational memory in system)	1. **Install or reseat the memory modules, then do a 3 boot reset.** (See the *Hardware Installation Guide*.) 2. DIMMs 3. Memory board 4. System board
Two Short Beeps (Information only, the configuration has changed)	1. **Run diagnostics** 2. Run Configuration/Setup
Three Short Beeps	1. **DIMM** 2. System board
One Continuous Beep	1. **Processor** 2. System board
Repeating Short Beeps	1. **Keyboard** 2. System board
One Long and One Short Beep	1. **Video adapter (if present)** 2. System board

Table 16. POST beep codes (continued)

Symptom	FRU/action
One Long and Two Short Beeps	1. **Video adapter (if present)** 2. System board
Two Long and Two Short Beeps	Video adapter

Table 17. POST no-beep codes

No Beep Symptom	FRU/action
No beep and the system operates correctly.	1. **Check speaker cables** 2. Speaker 3. System board
No Beeps occur after successfully completing POST (The Power-On Status is disabled.)	1. **Run Configuration/Setup, set the Start Options Power-On Status to enable.** 2. Check speaker connections 3. System board
No AC power(Power supply AC LED is off)	1. **Check the power cord.** 2. Power supply (If two are installed, swap them to determine if one is defective.) 3. Power backplane 4. Hot-swap power AC inlet box
No beep and no video	**See** *the Hardware Installation Guide.*
System will not power-up (Power supply AC LED is on)	**See** *the Hardware Installation Guide.*

POST error messages

Table 18 provides information about the POST error messages that can appear during startup.

Note that these diagnostic error messages require the attachment of a monitor, keyboard, and mouse (before you power on the system) to enable you to see them.

In the following error messages, *X* can be any number or letter.

Table 18. POST error messages

Error code/Symptom	Meaning	FRU/action
062	Three consecutive boot failures using the default configuration	1. **Run Configuration/Setup** 2. Battery 3. System board 4. Processor
101, 102	System and processor error	**System board**
106	System and processor error	**System board**
111	Channel check error	1. **Failing ISA Adapter** 2. DIMM 3. System board
114	Adapter read-only memory error	1. **Failing Adapter** 2. Run Diagnostics
129	Internal cache error	1. **Processor** 2. Optional processor (if installed)
151	Real-time clock error	1. **Run Diagnostics** 2. Battery 3. System board
161	Real-time clock battery error	1. **Run Configuration/Setup** 2. Battery 3. System board
162	Device Configuration error	1. **Run Configuration/Setup** **Note:** Be sure to load the default settings and any additional desired settings; then, *save the configuration.* 2. Battery 3. Failing Device 4. System board
163	Real-time clock error	1. **Run Configuration/Setup** 2. Battery 3. System board
164	Memory configuration changed	1. **Run Configuration/Setup** 2. DIMM
175	Hardware error	**System board**

Table 18. POST error messages (continued)

Error code/Symptom	Meaning	FRU/action
176	Computer cover or cable cover was removed without a key being used	1. **Run Configuration/Setup** 2. System board 3. C2 Security Switch
177, 178	Security hardware error	1. **Run Configuration/Setup** 2. System board
184	Power-on password corrupted	1. **Run Configuration/Setup** 2. System board
185	Drive startup-sequence information corrupted	1. **Run Configuration/Setup** 2. System board
186	Security hardware-control logic failed	1. **Run Configuration/Setup** 2. System board
187	VPD serial number not set	1. **Set serial number in Setup** 2. System board
188	Bad EEPROM CRC #2	1. **Run Configuration/Setup** 2. System board
189	An attempt was made to access the appliance with invalid passwords	**Run Configuration/Setup, enter the administrator password**
201	Memory test error	**If the appliance does not have the latest level of BIOS installed, update the BIOS to the latest level and run the diagnostic program again.** 1. DIMM 2. System board
229	Cache error	1. **Run Configuration/Setup** 2. Processor 3. Second Processor
262	DRAM parity configuration error	1. **Battery** 2. System board
289	DIMM has been disabled by the user or system	1. **Run Configuration/Setup, if disabled by user** 2. Disable DIMM, if not disabled by user
301	Keyboard or keyboard-controller error	1. **Keyboard** 2. System board
303	Keyboard controller error	1. **System board** 2. Keyboard
602	Invalid diskette boot record	1. **Diskette** 2. Diskette drive 3. Cable 4. System board

Table 18. POST error messages (continued)

Error code/Symptom	Meaning	FRU/action
604	Diskette-drive error	1. **Run Configuration/Setup and diagnostics** 2. Diskette Drive 3. Drive cable 4. System board
605	Unlock failure	1. **Diskette drive** 2. Drive cable 3. System board
662	Diskette-drive configuration error	1. **Run Configuration/Setup and Diagnostics** 2. Diskette Drive 3. Drive Cable 4. System board
762	Coprocessor configuration error	1. **Run Configuration/Setup** 2. Battery 3. Processor
962	Parallel-port error	1. **Disconnect external cable on parallel port.** 2. Run Configuration/Setup 3. System board
11XX	System-board serial port 1 or 2 error	1. **Disconnect external cable on serial port.** 2. Run Configuration/Setup 3. System board
0001200	Machine-check architecture error	1. **Processor** 2. Optional Processor
0001295	ECC circuit check	1. System board 2. Processor
1301	I^{2}C cable to front panel not found	1. **Cable** 2. Front panel 3. Power switch assembly 4. System board
1302	I^{2}C cable from system board to power on and reset switches not found	1. **Cable** 2. Power Switch Assembly 3. System board
1303	I^{2}C cable from system board to power backplane not found	1. **Cable** 2. Power backplane 3. System board
1304	I^{2}C cable to diagnostic LED board not found	1. **Cable** 2. Diagnostic LED Board 3. Power Switch Assembly 4. System board

Table 18. POST error messages (continued)

Error code/Symptom	Meaning	FRU/action
1600	The Service Processor is not functioning	1. **Ensure that a jumper is not installed on J-51** 2. Remove the AC power to the system, wait 20 seconds and then reconnect the AC power. Wait 30 seconds; then, power-on the appliance. 3. System board 4. Processor/PCI board
1601	The system is able to communicate to the Service Processor, but the Service Processor failed to respond at the start of POST	Suspected part: 1. **Remove the AC power to the system, wait 20 seconds, and reconnect the AC power. Wait 30 seconds and power on the system.** 2. Flash update the service processor. 3. System board 4. Processor/PCI board
1762	Hard-disk-drive configuration error	1. **Run Configuration/Setup** 2. Hard disk cables 3. Hard disk adapter 4. Hard disk drive 5. SCSI backplane 6. System board
178*X*	Hard-disk-drive error	1. **Run diagnostics** 2. Hard disk cables 3. Hard disk adapter 4. Hard disk drive 5. System board
1800	No more hardware interrupts available for PCI adapter	1. **Run Configuration/Setup** 2. Failing adapter 3. System board
1962	Drive does not contain a valid boot sector	1. **Verify that a bootable operating system is installed.** 2. Run diagnostics 3. Hard disk drive 4. SCSI backplane 5. Cable 6. System board
5962	IDE CD-ROM configuration error	1. **Run Configuration/Setup** 2. CD-ROM drive 3. CD-ROM power cable 4. IDE Cable 5. System board 6. Battery
8603	Pointing-device error	1. **Pointing device** 2. System board

Table 18. POST error messages (continued)

Error code/Symptom	Meaning	FRU/action
00019501	Processor 1 is not functioning	1. **Check VRM and processor LEDs** 2. VRM 1, VRM 2 3. Processor 1 4. Processor board 5. System board
00019502	Processor 2 is not functioning	1. **Check VRM and processor LEDs** 2. VRM 2 3. Processor 2 4. System board
00019701	Processor 1 failed BIST	1. **Processor 1** 2. System board
00019702	Processor 2 failed BIST	1. **Processor 2** 2. System board
00180100	No room for PCI option ROM	1. **Run Configuration/Setup** 2. Failing adapter 3. System board
00180200	No more I/O space available for PCI adapter	1. **Run Configuration/Setup** 2. Failing adapter 3. System board
00180300	No more memory (above 1 MB for PCI adapter)	1. **Run Configuration/Setup** 2. Failing adapter 3. System board
00180400	No more memory (below 1 MB for PCI adapter)	1. **Move the failing adapter to slot 1 or 2** 2. Run Configuration/Setup 3. Failing adapter 4. System board
00180500	PCI-option ROM checksum error	1. **Remove failing PCI card** 2. System board
00180600	PCI built-in self-test failure; PCI-to PCI-bridge error	1. **Run Configuration/Setup** 2. Move the failing adapter to slot 1 or 2 3. Failing adapter 4. System board
00180700, 00180800	General PCI error	1. **System board** 2. PCI card
01295085	ECC checking hardware test error	**Processor**
01298001	No update data for processor 1	1. **Ensure that all processors are the same stepping level and cache size.** 2. Processor 1

Table 18. POST error messages (continued)

Error code/Symptom	Meaning	FRU/action
01298002	No update data for processor 2	1. **Ensure that all processors are the same stepping level and cache size.** 2. Processor 2
01298101	Bad update data for processor 1	1. **Ensure that all processors are the same stepping level and cache size.** 2. Processor 1
01298102	Bad update data for processor 2	1. **Ensure that all processors are the same stepping level and cache size.** 2. Processor 2
I9990301	Fixed boot sector error	1. **Hard disk drive** 2. SCSI backplane 3. Cable 4. System board
I9990305	Fixed boot sector error, no operating system installed	**Install the operating system to the hard disk drive**
I9990650	AC power has been restored	1. **Check power cable** 2. Check for interruption of power supply

Event/error logs

The POST error log contains the three most recent error codes and messages that the system generated during POST. The System Event/Error Log contains all error messages issued during POST and all system status messages from the Advanced System Management Processor. In event of a POST error, check the System Event/Error Log as it may indicate the most recent errors commonly associated with typical hardware failures. It may not detect all hardware failures but many times will provide an indicator as to the nature of key failures.

To view the contents of the error logs, start the Configuration/Setup Utility program, then select **Event/Error Logs** from the main menu.

POST diagnostic programs

The appliance diagnostic programs are stored in upgradable read-only memory (ROM) on the system board. These programs are the primary method of testing the major components of your appliance.

Diagnostic program error messages indicate that a problem exists; they are not intended to be used to identify a failing part. Troubleshooting and servicing of complex problems that are indicated by error messages should be performed by trained service personnel. For a list of error messages and associated actions that you can take, see Table 18 on page 114.

Sometimes the first error to occur causes additional errors. In this case, the appliance displays more than one error message. Always follow the suggested action instructions for the *first* error message that appears.

The following sections contain the error codes that might appear in the detailed test log and summary log when running the diagnostic programs.

The error code format is as follows:

`fff-ttt-iii-date-cc-text message`

where:

fff   is the three-digit function code that indicates the function being tested when the error occurred. For example, function code 089 is for the microprocessor.

ttt   is the three-digit failure code that indicates the exact test failure that was encountered.

iii   is the three-digit device ID.

date   is the date that the diagnostic test was run and the error recorded.

cc   is the check digit that is used to verify the validity of the information.

text message
        is the diagnostic message that indicates the reason for the problem.

Text messages

The diagnostic text message format is as follows:

`Function Name: Result (test specific string)`

where:

Function Name
        is the name of the function being tested when the error occurred. This corresponds to the function code (fff) given in the previous list.

Result can be one of the following:

> **Passed**
>   The diagnostic test has completed without any errors.
>
> **Failed** The diagnostic test has discovered an error.
>
> **User Aborted**
>   You stopped the diagnostic test before it is complete.
>
> **Not Applicable**
>   You specified a diagnostic test for a device that is not present.
>
> **Aborted**
>   The test could not proceed because of the system configuration.
>
> **Warning**
>   A possible problem was reported during the diagnostic test, such as when a device that is to be tested is not installed.

Test Specific String
        This is additional information that you can use to analyze the problem.

Starting the diagnostic programs

To start the diagnostic programs:

1. Ensure you have connected a monitor, keyboard, and mouse to your NAS 300G.

Notes:

  a. When you *do not* have a monitor, keyboard, and mouse attached and the NAS 300G engine passes POST, one long and three short beeps sound.

  b. When you *have* a monitor, keyboard, and mouse attached and the NAS 300G engine passes POST, one beep sounds. If the NAS 300G fails POST, a series of beeps sound (see "POST beep code descriptions" on page 109 for more details) and an error message appears on the monitor screen.

2. Power on the NAS 300G and watch the screen.

3. When the message `F2 for Diagnostics` appears, press **F2**. If a POST error is encountered, a series of beeps sound and an error message appears on the monitor screen.

4. Type in the appropriate password; then, press **Enter**. If a system error is encountered, the Configuration/Setup screen appears. Press **Esc** to start the Diagnostic program.

    Note: To run the diagnostic programs, you must start the NAS 300G with the highest level password that is set. That is, if an administrator password is set, you must enter the administrator password, not the power-on password, to run the diagnostic programs.

5. Select either **Extended** or **Basic** from the top of the screen. (*PC-Doctor 2.0* with a copyright statement appears at the bottom of this screen.)

6. When the Diagnostic Programs screen appears, select the test you want to run from the list that appears; then, follow the instructions on the screen.

    Notes:

  a. Press **F1** while running the diagnostic programs to obtain `Help` information. Also press **F1** from within a help screen to obtain online documentation from which you can select different categories. To exit `Help` and return to where you left off, press **Esc**.

  b. If the NAS 300G engine stops during testing and you cannot continue, restart the NAS 300G engine and try running the diagnostic programs again.

  c. If you run the diagnostic programs with either no mouse or a USB mouse attached to your NAS 300G engine, you will not be able to navigate between test categories using the **Next Cat** and **Prev Cat** buttons. All other functions provided by mouse-selectable buttons are also available using the function keys.

  d. You can test the USB keyboard by using the regular keyboard test. The regular mouse test can test a USB mouse. Also, you can run the USB hub test only if there are no USB devices attached.

  e. You can view NAS 300G engine configuration information (such as system configuration, memory contents, interrupt request (IRQ) use, direct memory access (DMA) use, device drivers, and so on) by selecting **Hardware Info** from the top of the screen.

  f. You cannot use the diagnostics program to test adapters. Use the procedure outlined in "Adapter troubleshooting and diagnostics" on page 81.

When the tests have completed, you can view the Test Log by selecting **Utility** from the top of the screen.

If the hardware checks out OK but the problem persists during normal NAS 300G operations, a software error might be the cause. If you suspect a software problem, refer to the information that comes with the software package.

Viewing the test log

The test log will not contain any information until after the diagnostic program has run.

Note: If you already are running the diagnostic programs, begin with step 4

To view the test log:

1. Ensure a monitor, keyboard, and mouse is connected to the NAS 300G.
2. Power on the NAS 300G engine and watch the screen.

   If the NAS 300G engine is on, shut down your operating system and restart the engine.
3. When the message `F2 for Diagnostics` appears, press **F2**.

   If a power-on password or administrator password is set, you will be prompted for it. Type in the appropriate password, then press **Enter**.
4. When the Diagnostic Programs screen appears, select **Utility** from the top of the screen.
5. Select **View Test Log** from the list that appears; then, follow the instructions on the screen.

   The system maintains the test-log data while the NAS 300G is powered on. When you turn off the power to the NAS 300G, the test log is cleared.

Diagnostic error message tables

Table 19 describes the error messages that might appear when you run the diagnostic programs.

Important: If diagnostic error messages appear that are not listed in Table 19, make sure that your appliance has the latest levels of BIOS, Advanced System Management Processor, and diagnostics microcode.

In the following error codes, if *XXX* is 000, 195, or 197, *do not* replace a part. These error codes have the following meanings:

000   The test passed.

195   Esc was pressed to end the test.

197   This is a warning error and may not indicate a hardware failure.

For all other error codes, replace the part or perform the actions indicated.

Table 19. Diagnostic error messages

Error Code	Meaning	FRU/action
001-*XXX*-000	Failed core tests	**System board**
001-*XXX*-001	Failed core tests	**System board**
001-250-000	Failed System board ECC	**System board**
001-250-001	Failed Processor board ECC	1. **Processor/PCI board** 2. System board
005-*XXX*-000	Failed Video test	**System board**
011-*XXX*-000	Failed COM1 Serial Port test	**System board**
011-*XXX*-001	Failed COM2 Serial Port test	**System board**

Table 19. Diagnostic error messages (continued)

Error Code	Meaning	FRU/action
014-XXX**-000**	Failed Parallel Port test	**System board**
015-XXX**-001**	Failed USB test	**System board**
015-XXX**-015**	Failed USB external loopback test	1. **Make sure parallel port is not disabled** 2. Re-run USB external loopback test 3. System board
015-XXX**-198**	USB device connected during the USB test	1. **Remove USB devices from USB1 and USB2** 2. Re-run USB external loopback test 3. System board
020-XXX**-000**	Failed PCI Interface test	**System board**
020-XXX**-001**	Failed Hot-Swap Slot 1 PCI Latch test.	1. **PCI hot-swap latch assembly** 2. System board
020-XXX**-002**	Failed hot-swap slot 2 PCI latch test	1. **PCI hot-swap latch assembly** 2. System board
020-XXX**-003**	Failed hot-swap slot 3 PCI latch test	1. **PCI hot-swap latch assembly** 2. System board
020-XXX**-004**	Failed hot-swap slot 4 PCI latch test	1. **PCI hot-swap latch assembly** 2. System board
030-XXX**-000**	Failed internal SCSI interface test	**System board**
035-XXX**-099**	No adapters were found	**If the adapter is installed, recheck the connection.**
035-XXX**-**S**99**	Failed RAID test on PCI slot S	**Note:** Check the System Error Log before replacing a part. 1. **Adapter** 2. SCSI backplane 3. Cable
035-XXX**-**SNN	NN = SCSI ID of failing hard disk	**Note:** Check the System Error Log before replacing a part.**Hard disk drive with SCSI ID** NN **on RAID adapter in PCI slot** S**.**
035-253-S**99**	RAID adapter initialization failure; ServeRAID Adapter in slot S is not configured properly	1. **Obtain the basic and extended configuration status** 2. Adapter 3. SCSI backplane 4. Cable
075-XXX**-000**	Failed power supply test	**Power supply**
089-XXX**-001**	Failed microprocessor test	1. **VRM 1** for microprocessor 1 2. Microprocessor 1
089-XXX**-002**	Failed test for optional microprocessor	1. **VRM 2** 2. Optional microprocessor 2
166-250-000	System Management failed: (I2C cable is disconnected. Reconnect I2C cable between Remote Supervisor Adapter and system board.)	1. **Reseat the I2C cables between Remote Supervisor Adapter (in PCI slot 1/J44) and system board (J45)** 2. I2C cables

Table 19. Diagnostic error messages (continued)

Error Code	Meaning	FRU/action
166-198-000	System Management aborted: (Unable to communicate with the Remote Supervisor Adapter. It may be busy. Run the test again). (Communication with the Remote Supervisor Adapter has failed).	1. **Re-run the Diagnostic Test** 2. Fix other error conditions and retry. These include other Failed System Management tests and items logged in the optional Remote Supervisor Adapter's System Error Log 3. Disconnect all server and option power cords from the unit, wait 30 seconds, reconnect, and retry. 4. Remote Supervisor Adapter, if installed 5. System board
166-201-001	System Management failed: (I2C Bus Error(s)) (ISMP indicates I2C errors on bus 0. Potential FRUs: Memory DIMMs, system board)	1. **If installed, reseat I2C cable between Remote Supervisor Adapter (in PCI slot 1/J44) and system board** 2. Reseat memory DIMMs 3. Memory DIMMS 4. System board
166-201-002	System Management failed: (I2C Bus Error(s)) (ISMP indicates I2C errors on bus 2. Potential FRUs: LED front panel, system board).	1. **Reseat I2C cable between operator information panel and system board (J39)** 2. Operator information panel 3. System board
166-201-003	System Management failed: (I2C Bus Error(s)) (ISMP indicates I2C errors on bus 3. Potential FRUs: power backplane, system board).	1. **Reseat cables between power backplane and system board** 2. Operator information panel 3. System board
166-201-004	System Management failed: (I2C Bus Error(s)) (ISMP indicates I2C errors on bus 4. Potential FRUs: DASD backplane, system board).	1. **If installed, reseat I2C cable between Yugo and DASD backplane and DASD I2C on system board (J0)** 2. System board
166-201-005	System Management failed: (I2C Bus Error(s)) (ISMP indicates I2C errors on bus 0, 1, or 5. Potential FRUs: Memory DIMMs, CPUs, system board).	1. **Reseat Memory DIMMs** 2. Reseat processors 3. Memory DIMMs 4. Processors 5. System board
166-260-000	System Management failed: (Unable to restart Remote Supervisor Adapter). Restart Remote Supervisor Adapter Error. After restarting, Remote Supervisor Adapter communication was lost. Unplug and cold boot to reset the Remote Supervisor Adapter).	1. **Disconnect all server and option power cords from server, wait 30 seconds, reconnect, and retry.** 2. Reseat the Remote Supervisor Adapter in PCI slot 1/J44). 3. Remote Supervisor Adapter

Table 19. Diagnostic error messages (continued)

Error Code	Meaning	FRU/action
166-342-000	System Management failed: Remote Supervisor Adapter BIST indicate failed tests).	1. **Ensure that the latest firmware levels for the Remote Supervisor Adapter and BIOS** 2. Disconnect all server and option power cords from the unit, wait 30 seconds, reconnect, then retry. 3. Remote Supervisor Adapter
166-400-000	System Management failed: System management hardware on system board failed) (ISMP Self Test Result failed tests: *x* where *x* = Flash, RAM, or ROM).	1. **Re-flash or update firmware for ISMP** 2. System board
180-*XXX*-000	Diagnostics LED failure	**Run the diagnostics LED test for the failing LED.**
180-*XXX*-001	Failed front LED panel test	
180-*XXX*-002	Failed diagnostics LED panel test	1. **System board** 2. Power-switch assembly
180-*XXX*-005	Failed SCSI backplane LED test	1. **SCSI backplane** 2. SCSI backplane cable 3. System board
180-*XXX*-006	Memory Board LED test	Suspected part: 1. **Memory** 2. Processor/PCI board 3. System board
180-361-003	Failed fan LED test	1. **Fans** 2. System board
201-*XXX*-0*NN*	Failed Memory test	1. **DIMM Location DIMM1 - DIMM4 where *NN* can be a value from 01 to 04. 01 = DIMM2, 02 = DIMM1, 03 = DIMM4, 04 = DIMM3** 2. System board
201-*XXX*-999	Multiple DIMM failure; see error text for failing DIMMs	1. **See error text for failing DIMMs** 2. System board
202-*XXX*-001	Failed system cache test	1. **VRM 1** 2. Microprocessor 1
202-*XXX*-002	Failed system cache test	1. **VRM 2** 2. Microprocessor 2
206-*XXX*-000	Failed diskette drive test	1. **Cable** 2. Diskette drive 3. System board
215-*XXX*-000	Failed IDE CD-ROM test	1. **CD-ROM drive cables** 2. CD-ROM drive 3. System board
217-198-*XXX*	Could not establish drive parameter	1. **Check cable and termination** 2. SCSI backplane 3. Fixed disk

Table 19. Diagnostic error messages (continued)

Error Code	Meaning	FRU/action
217-*XXX***-000**	Failed BIOS hard disk drive test **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array.	**Hard disk drive 1**
217-*XXX***-001**	Failed BIOS hard disk drive test **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array.	**Hard disk drive 2**
217-XXX-002	Failed BIOS hard disk drive test. **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array	**Hard disk drive 3**
217-*XXX***-003**	Failed BIOS hard disk drive test **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array.	**Hard disk drive 4**
217-*XXX***-004**	Failed BIOS hard disk drive test **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array.	**Hard disk drive 5**
217-*XXX***-005**	Failed BIOS Fixed Disk test **Note:** If RAID is configured, the hard disk drive number refers to the RAID logical array.	**Hard disk drive 6**
264-*XXX***-0NN**	Failed tape-drive test	1. **Tape cartridge, if user executed the read/write tape drive test (***XXX* **= 256)** 2. SCSI or power cable connected to tape drive with SCSI ID *NN*. 3. Tape drive with SCSI ID *NN* (Refer to the Help and Service Information appendix of the tape drive's user guide). 4. System board or SCSI Controller (Run SCSI controller diagnostic to determine if the SCSI bus is functioning correctly.)
264-*XXX***-999**	Errors on multiple tape drives	**See error messages/text in the PC Doctor error log for detailed information on each individual tape drive error.**
301-*XXX***-000**	Failed Keyboard test	**Keyboard**
405-*XXX***-000**	Failed Ethernet test on controller on the system board	1. **Verify that Ethernet is not disabled in BIOS** 2. System board

Table 19. Diagnostic error messages (continued)

Error Code	Meaning	FRU/action
405-*XXX***-00***N*	Failed Ethernet test on adapter in PCI slot N	1. **Adapter in PCI slot** *N*. 2. System board
415-*XXX***-000**	Failed modem test	Suspected part: 1. **Cable** 2. Modem **Note:** Ensure that the modem is present and attached to appliance. 3. System board

Appendix E. Fast!UTIL options

This appendix provides detailed configuration information for advanced users who want to customize the configuration of the FAStT Host Adapter and the connected devices. However, customizing the configuration is not recommended, as the adapter was configured specifically for the NAS 300G.

The board can be configured using Fast!UTIL. Access Fast!UTIL by pressing **Alt + Q** during the adapter BIOS initialization (it may take a few seconds for the Fast!UTIL menu to appear). If you have more than one FAStT Host Adapter, Fast!UTIL prompts you to select the adapter you want to configure. After changing the settings, Fast!UTIL restarts your system to load the new parameters.

Attention: If the configuration settings are incorrect, your FAStT Host Adapter board might not function properly.

Configuration settings

This is the first selection on the Fast!UTIL Options menu. These settings configure the Fibre Channel (FC) devices and the FAStT Host Adapter to which they are attached.

Host adapter settings

From the Configuration Settings menu in Fast!UTIL, select **Host Adapter Settings**. The default settings for the FAStT Host Adapter are listed in Table 20 and described in the following paragraphs.

Table 20. Host adapter settings

Setting	Options	Default
Host Adapter BIOS	Enabled or Disabled	Disabled
Frame Size	512, 1024, 2048	2048
Loop Reset Delay	0-15 seconds	5 seconds
Adapter Hard Loop ID	Enabled or Disabled	Disabled
Hard Loop ID	0-125	125

Host Adapter BIOS
> When this setting is disabled, the ROM BIOS on the FAStT Host Adapter is disabled, freeing space in upper memory. This setting must be enabled if you are booting from an FC disk drive attached to the FAStT Host Adapter. The default is Disabled.

Frame Size
> This setting specifies the maximum frame length supported by the FAStT Host Adapter. The default size is 1024. If using F-Port (point-to-point) connections, change this setting to 2048 for maximum performance.

Loop Reset Delay
> After resetting the loop, the firmware does not initiate any loop activity for the number of seconds specified in this setting. The default is 5 seconds.

Adapter Hard Loop ID
> This setting forces the adapter to attempt to use the ID specified in the Hard Loop ID setting. The default is Disabled.

Hard Loop ID

> If the Adapter Hard Loop ID setting is enabled, the adapter attempts to use the ID specified in this setting. The default ID is 0.

Selectable boot settings

Though you can access this option from the Configuration Settings menu, do not change the settings as booting from Fibre Channel is not supported.

Restore default settings

You can access this option from the Configuration Settings menu. It restores the FAStT Host Adapter default settings.

Raw NVRAM data

This option displays the adapter's NVRAM contents in hexadecimal format. This is a QLogic troubleshooting tool; you cannot modify the data.

Advanced adapter settings

You can access this option from the Configuration Settings menu. The default settings for the FAStT Host Adapter are listed in Table 21 and described in the following paragraphs.

Table 21. Advanced adapter settings

Setting	Options	Default
Execution Throttle	1-256	256
Fast Command Posting	Enabled or Disabled	Enabled
>4 GByte Addressing	Enabled or Disabled	Disabled
LUNs per Target	0, 8, 16, 32, 64, 128, 256	0
Enable LIP Reset	Yes or No	No
Enable LIP Full Login	Yes or No	Yes
Enable Target Reset	Yes or No	Yes
Login Retry Count	0-255	30
Port Down Retry Count	0-255	30
Drivers Load RISC Code	Enabled or Disabled	Enabled
Enable Database Updates	Yes or No	No
Disable Database Load	Yes or No	No
IOCB Allocation	1-512 buffers	256 buffers
Extended Error Logging	Enabled or Disabled	Disabled

Execution Throttle

> Specifies the maximum number of commands executing on any one port. When a port's execution throttle is reached, no new commands are executed until the current command finishes executing. The valid options for this setting are 1-256. The default (optimum) is 256.

Fast Command Posting

> Decreases command execution time by minimizing the number of interrupts. The default is Enabled.

>4 GByte Addressing.
    Enable this option if the system has more than 4 GB of memory available.
    The default is Disabled.

LUNs per Target
    Specifies the number of LUNs per target. Multiple LUN support is typically
    for redundant array of independent disks (RAID) boxes that use LUNs to
    map drives. The default is 0.

Enable LIP Reset
    Determines the type of loop initialization process (LIP) reset that is used
    when the operating system initiates a bus reset routine. When this setting is
    yes, the driver initiates a global LIP reset to clear the target device
    reservations. When this setting is no, the driver initiates a global LIP reset
    with full login. The default is No.

Enable LIP Full Login
    Instructs the ISP chip to log in to all ports after any LIP. The default is Yes.

Enable Target Reset
    Enables the drivers to issue a Target Reset command to all devices on the
    loop when a SCSI Bus Reset command is issued. The default is Yes.

Login Retry Count
    Specifies the number of times the software tries to log in to a device. The
    default is 30 retries.

Port Down Retry Count
    Specifies the number of times the software retries a command to a port
    returning port down status. The default is 30 retries.

Drivers Load RISC Code
    When this setting is enabled, the host adapter uses the RISC firmware that
    is embedded in the software driver. When this setting is disabled, the
    software driver loads the RISC firmware found on the system. The default is
    Enabled.

    Note: The driver being loaded must support this setting. If the driver does
            not support this setting, the result is the same as disabled regardless
            of the setting. Leaving this option enabled guaranties a certified
            combination of software driver and RISC firmware.

Enable Database Updates
    When enabled, it allows the software to save the loop configuration
    information in flash memory when the system powers down. The default is
    No.

    Note: This option usually applies to Windows NT and Windows 2000
            operating environments.

Disable Database Load
    When enabled, the device database is read from the Registry during driver
    initialization. When disabled, the device database is created dynamically
    during driver initialization. The default is No.

IOCB Allocation
    Specifies the maximum number of buffers from the firmware's buffer pool
    that are allocated to any one port. The default is 256 buffers.

Extended Error Logging
> Provides additional error and debug information to the operating system. When enabled, events are logged into the Windows NT or Windows 2000 Event Viewer. The default is Disabled.

Extended Firmware Settings

You can access this option from the Configuration Settings menu. The default settings for the FAStT Host Adapter are listed in Table 22 and described immediately following the table.

Table 22. Extended firmware settings

Setting	Options	Default
Extended Control Block	Enabled or Disabled	Enabled
RIO Operation Mode	0, 1, 2, 3, 4	0
Connection Options	0, 1, 2, 3	3
Class 2 Service	Enabled or Disabled	Disabled
ACK0	Enabled or Disabled	Disabled
Fibre Channel Tape Support	Enabled or Disabled	Disabled
Fibre Channel Confirm	Enabled or Disabled	Disabled
Command Reference Number	Enabled or Disabled	Disabled
Read Transfer Ready	Enabled or Disabled	Disabled
Response Timer	0-255	0
Interrupt Delay Timer	0-255	0

Extended Control Block
> Enables all other extended firmware settings. The default is Enabled.

RIO Operation Mode
> Specifies the reduced interrupt operation (RIO) modes, if supported by the software driver. RIO modes allow posting multiple command completions in a single interrupt (see Table 23). The default is 0.

Table 23. RIO operation modes

Option	Operation mode
0	No multiple responses
1	Multiple responses, 16 bit handles, interrupt host
2	Multiple responses, 32 bit handles, interrupt host
3	Multiple responses, 16 bit handles, delay host interrupt
4	Multiple responses, 32 bit handles, delay host interrupt

Connection Options
> Defines the type of connection (loop or point to point) or connection preference (see Table 24). The default is 3.

Table 24. Connection options

Option	Type of connection
0	Loop only
1	Point-to-point only

Table 24. Connection options (continued)

2	Loop preferred, otherwise point to point
3	Point-to-point, otherwise loop

Class 2 Service
> Enables Class 2 service parameters to be provided during all automatic logins (loop ports). The default is Disabled.

ACK0 Determines the type of acknowledge (ACK) used. When this setting is enabled, sequence ACK is used. When this setting is disabled, frame ACK is used. The default is Disabled.

> **Note:** The Class 2 Service setting must be enabled to use the ACK0 setting.

Fibre Channel Tape Support
> This setting is reserved for Fibre Channel tape support. The default is Disabled.

Fibre Channel Confirm
> This setting is reserved for Fibre Channel tape support. The default is Disabled.

Command Reference Number
> This setting is reserved for Fibre Channel tape support. The default is Disabled.

Read Transfer Ready
> This setting is reserved. The default is Disabled.

Response Timer
> Contains the value (in 100-microsecond increments) used by a timer to limit the time waiting accumulating multiple responses. For example, if this field is 8, the time limit is 800 microseconds. The default is 0.

Interrupt Delay Timer
> Contains the value (in 100-microsecond increments) used by a timer to set the wait time between accessing (DMA) a set of handles and generating an interrupt. The default is 0.

Scan Fibre Channel Devices

Use this option to scan the FC loop and list all the connected devices by loop ID. Information about each device is listed, for example, vendor name, product name, and revision. This information is useful when configuring your FAStT Host Adapter and attached devices.

Fibre Disk Utility

This option scans the FC loop bus and lists all the connected devices by loop ID. You can select a disk device and perform a low-level format or verify the disk media.

CAUTION:
Performing a low-level format destroys all data on the disk.

Loopback Data Test

This option performs a data test using an FC loop or a loopback connector.

CAUTION:
Performing this test will disrupt data if tested in a FC loop.

Select Host Adapter

Use this setting to select a specific FAStT Host Adapter if you have multiple FAStT Host Adapters in your system.

Appendix F. Powering off and powering on the NAS 300G

The clustering function requires special considerations when you need to power off and power on the NAS 300G. This section gives the details for those considerations.

Powering off the NAS 300G when clustering is active

1. Make note of the order in which you shut down the nodes.

   You shut the nodes down one at a time, and in the powering on procedure you start the nodes in the opposite order in which you powered them off.

2. On the node you want to shut down last (the second node), click **Cluster Administration**, located in IBM NAS Admin, in the Cluster Tools folder. If prompted for a cluster name, enter the name of the cluster, and then click **Open**. Make sure that all resources are in the online state.

3. With all clustered resources in the online state, on the node you want to shut down first (the first node), go to **Start**, **Shut Down** and select **Shut down** from the drop down menu. Click **OK**.

4. On the second node, in Cluster Administrator, wait for all resources to fail over to that node and return to the online state.

5. Once all resources are in the online state, and the first node has shut down, on the second node go to **Start**, **Shutdown** and select **Shut down** from the drop down menu. Click **OK**.

6. You may power down any network hubs or switches that are used exclusively by the NAS 300G. If they are used by other network attached devices, do not power these off.

7. You may also power off any Uninterruptible Power Supplies (UPS) that regulate power for the NAS 300G, provided that no other equipment that you wish to keep powered on is plugged into the same UPS.

Powering on the NAS 300G when clustering is active

1. Power on any UPS that you powered off in the powering off procedure, and allow it to return to normal operation.

2. Power on any network hubs or switches that you powered off in the powering off procedure.

3. Power on the node that you shut down last in the powering off procedure.

4. Once the node comes up, start Cluster Administrator on that node and make sure that all resources are in an online state or shortly return to that state.

5. If no problems exist and all clustered resources are online, power on the node that you shut down first in the powering off procedure. Each resource for which that node is the preferred owner will fail back to that node and return to an online state.

Recovering from a corrupted Quorum drive

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 event log 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.

Appendix G. Customer Replaceable Unit (CRU) list

Table 25 contains the CRU list for this product.

Table 25. CRU list

CRU number	System part
38P8355	TOP COVER
37L0305	92 MM X 38 FAN (2)
00N7259	SLIM HARD DISK DRIVE BEZEL FILLER ASSEMBLY
19K0614	18.2 GB SLIM HARD DISK DRIVE
37L0311	POWER SUPPLY WITH MOUNTING, 270 WF
38P7582	FRONT BEZEL
36L8645	12.7 MM DISKETTE DRIVE
06P5263	24X CDROM
00N7213	CARD ASSEMBLY, FRONT SWITCH CARD
06P5931	FRAME ASSEMBLY
25P2127	SYSTEM BOARD
33L3325	512 MB RDIMM MEMORY
25P2605	1133 MHZ/133-512K PROCESSOR
24P6893	VOLTAGE REG. MOD.
06P5924	BAFFLE, AIR
007248	REAR 92 MM X 38 FAN
38P7771	CABLE, 10FT. CAT-5 UPT ENET
38P7576	10 FT CAT5 ETHERNET CROSSOVER CABLE FRU
38P8356	TOP COVER SERVICE LABEL
10L7095	PCI FAST/WIDE ULTRA SCSI ADAPTER
09N7292	NETFINITY FAStT HOST ADAPTER
06P5067	REMOTE SUPERVISOR ADAPTER
03K9319	RSA INTERCONNECT CABLE RS485 PEER
02K6555	RSA AC ADAPTER
06P3609	NETFINITY 10/100 ETHERNET ADAPTER
06P3709	NETFINITY 1GB ETHERNET ADAPTER
00N6407	BLANK 5.25 HDD BEZEL (SNAP MOUNT)
06P5923	BAFFLE
00N7193	MISC RACK HARDWARE KIT
00N7211	BRACKET, CABLE MGMT CHASSIS ATTACH (2)
00N7242	CABLE MANAGEMENT ARM ASSEMBLY (2)
00N7245	CABLE MANAGEMENT ARM ASSEMBLY (2)
06P5922	POWER CABLE
06P5978	SIGNAL CABLE
6952301	POWER CORD
14F0033	POWER CORD

Table 25. CRU list (continued)

CRU number	System part
13F9940	POWER CORD
13F9979	POWER CORD
13F9997	POWER CORD
14F0015	POWER CORD
14F0051	POWER CORD
14F0069	POWER CORD
14F0087	POWER CORD
1838574	POWER CORD
6952300	POWER CORD
02K0546	POWER CORD
36L8880	POWER CORD
36L8886	POWER CORD
06P2215	SCSI LVD/SE ADAPTER
38P7829	10/100 ENET 4 PORT ADAPTER
00N7691	CORD, JUMPER 1M
06P5864	CABLE, RSA
09N9581	CABLE, RS485 BUS
38P7771	CABLE, 10FT CAT-5 UTP STRAIGHT THROUGH

IBM Glossary of Storage Networking Terms

This glossary includes terms and definitions from:

- *The American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018. Definitions are identified by the symbol (A) after the definition.
- The *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronics Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

Numerics

10BASE2. The IEEE 802.3 Ethernet standard that supports a transmission rate of 10 Mbps using RG 58 A/U and RG 58 C/U coaxial cable and BNC connectors. 10BASE2 is sometimes called thin Ethernet or thinnet.

10BASE5. The IEEE 802.3 Ethernet standard that supports a transmission rate of 10 Mbps using a 50-ohm coaxial cable with Type N connectors over a distance of up to 500 m (1640 ft) without using repeaters. 10BASE5 is sometimes called thick Ethernet or thicknet.

10BASE-FL. The IEEE 802.3 Ethernet standard that supports a transmission rate of 10 Mbps using optical fiber.

10BASE-T. The IEEE 802.3 Ethernet standard that supports a transmission rate of 10 Mbps using two twisted-pair wires (Category 3 telephone wiring). 10BASE-T is the most widely deployed 10-Mbps Ethernet transmission protocol in use today.

100BASE-T. The IEEE 802.3 Ethernet standard that supports a transmission rate of 100 Mbps using 2 twisted-pair wires (Category 5 telephone wiring).

A

access control. In computer security, the process of ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.

access control list (ACL). (1) In computer security, a collection of all access rights for one object. (2) In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights; for example, a list associated with a file that identifies users who can access the file and identifies their access rights to that file.

accessory. An IBM designation for a separately orderable part that (a) has no type number, (b) is for purchase only, and (c) does not receive normal IBM maintenance.

active-backup. A type of bond group that provides high availability. Two or more ports are combined under a logical bond group with one link active and the other link or links left idle. The idle links are ready to take over in the event that the currently active link fails. See bond group.

active dispatcher node.   The engine within a load-balancing group that functions as the load balancer for that group. Because each NAS engine can have multiple physical and bonded interfaces, there can be more than one load-balancing engine per set of engines. Each load-balancing engine acts as an active backup for another load-balancing engine within that set. Alternatively, there can be only one active load-balancing engine per set of engines and one passive backup (standby) load-balancing engine.

actual data transfer rate.   The average number of bits, characters, or blocks per unit of time transferred from a data source and received by a data sink.

adapter address.   The hexadecimal digits that identify an adapter.

adaptive cut-through switching.   A mode of operation for LAN switches in which they will automatically alternate between cut-through switching and store-and-forward switching depending on user-configurable, per port, error-rate thresholds.

advertise.   To pass routing reachability information along from one router to another.

all-routes broadcast frame.   A frame that has bits in the routing information field set to indicate that the frame is to be sent to all LAN segments in the network (across all bridges, even if multiple paths allow multiple copies of the frame to arrive at some LAN segments). The destination address is not examined and plays no role in bridge routing.

all-stations broadcast frame.   A frame whose destination address bits are set to all ones. All stations on any LAN segment on which the frame appears will copy it. The routing information, not the destination address, determines which LAN segments the frame appears on. All-stations broadcasting is independent of all-routes broadcasting; the two can be done simultaneously or one at a time.

alternate adapter.   In a personal computer that is used on a LAN and that supports installation of two network adapters, the adapter that uses alternate (not standard or default) mapping between adapter-shared RAM, adapter ROM, and designated computer memory segments. The alternate adapter is usually designated as adapter 1 in configuration parameters. Contrast with primary adapter.

alternate memory mapping.   The mapping between adapter-shared RAM, adapter ROM, and the designated computer memory segments for an alternate network adapter.

ASM (see advanced system management).

assigned disk.   A disk that is mapped to a logical drive.

asynchronous.   A class of data transmission service whereby all requests for service contend for a pool of dynamically allocated ring bandwidth and response time.

asynchronous data transfer.   A physical transfer of data to or from a device that occurs without a regular or predictable time relationship following execution of an I/O request. Contrast with synchronous data transfer.

asynchronous transfer mode (ATM).   A transfer mode in which the information is organized into cells; it is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic. ATM is specified in international standards such as ATM Forum UNI 3.1.

asynchronous transmission.   A method of transmission in which the time intervals between characters do not have to be equal. Start and stop bits are added to coordinate the transfer of characters.

ATM (see asynchronous transfer mode).

attach.   To make a device a part of a network logically. Not to be confused with connect, which implies physically connecting a device to a network. Contrast with connect.

attachment.   A port or a pair of ports, optionally including an associated optical bypass, that are managed as a functional unit. A dual attachment includes two ports: a port A, and a port B. A single attachment includes a Port S.

attachment feature.   (1) The circuitry by which some host processors or controllers are connected to a LAN access unit or connection point. (2) A feature that can be added to enhance the capability, storage capacity, or performance of a product, but is not essential for its basic work; for example, an adapter that allows a device to attach to a network.

attachment unit interface (AUI).   Also known as thick Ethernet, thicknet or 10BASE5. This type of Ethernet connector has a 15-pin D type connector.

attention (ATTN).   An occurrence external to an operation that could cause an interruption of the operation.

AUI (see attachment unit interface).

authentication.   In computer security, verification of the identity of a user or the user's eligibility to access an object.

auto-removal.   The removal of a device from data-passing activity without human intervention. This action is accomplished by the adapter in the device, and can be initiated by a network management program.

B

balun.   A transformer used to connect balanced cables, such as twisted-pair cables, to unbalanced cables, such as coaxial cables, by matching the electrical characteristics of the cables.

bandwidth aggregation.   The ability to establish more than one communication channel per connection.

bandwidth augmentation.   The ability to add another communication channel to an already existing communication channel.

bandwidth-distance product.   The parameter specified for bulk fiber that defines the distance that a signal at a defined frequency can be transmitted with a specified loss, usually half the power at zero frequency. Use of a fiber with a bandwidth-distance product of 500 MHz-km would support 250 MHz for a distance of 2 km.

baseband LAN.   A local area network in which data are encoded and transmitted without modulation of a carrier (T).

Basic Input/Output System.   The personal computer code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

baud.   (1) A unit of signaling speed equal to the number of discrete conditions or signal events per second; for example, one baud equals one-half dot cycle per second in Morse code, one bit per second in a train of binary signals, and one 3-bit value per second in a train of signals each of which can assume one of eight different states (A). Contrast with bits per second. (2) In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud.

BIOS (see Basic Input/Output System).

bit-time.   (1) The time required to transmit 1 bit on the network. For example, the IBM PC Network bit-time equals 500 nanoseconds (ns). (2) The reciprocal of the line data rate (or network data transfer rate).

bits per second (bps).   The rate at which bits are transmitted per second. Contrast with baud.

block delay time.   The time delay permitted for received frames to be assembled into blocks for retransmission.

bond group.   A logical collection of two or more physical ports (on a per engine basis only) that becomes one interface on the network. You can create two kinds of bond groups in the NAS appliance: aggregated links (see link aggregration) and active-backup.

bonded interface (see bond group).

bonding.   The act of combining two or more physical ports to create one logical network interface with one associated IP address. Bonding can improve performance by either increasing bandwidth (see link aggregation) or providing port backup (see active-backup).

bootstrap.   (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage (T). (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device (A).

bps (see bits per second).

broadcast frame.   A frame that is simultaneously transmitted to more than one destination. A broadcast frame is forwarded by all bridges, unless otherwise restricted.

broadcast topology. A network topology in which all attaching devices are capable of receiving a signal transmitted by any other attaching device on the network.

buffer storage. (1) A special-purpose storage or storage area allowing, through temporary storage, the data transfer between two functional units having different transfer characteristics. A buffer storage is used between non-synchronized devices, or where one is serial and the other is parallel or between those having different transfer rates. Synonymous with buffer (T). (2) In word processing, a temporary storage in which text is held for processing or communication (T).

building cable. The permanently installed cable within a building that interconnects offices to wiring closets, wiring closets to wiring closets, and wiring closets to computer rooms of building entrances.

building entrance. The entry point in a building where external communication cables are interconnected with internal building cables.

C

cache. A high-speed buffer storage that contains frequently accessed instructions and data to reduce access time.

cascade. To connect in a series or in a succession of stages so that each stage derives from or acts upon the product of the preceding stage.

catenet. A network in which hosts are connected to networks and the networks are interconnected by gateways. The Internet is an example of a catenet.

CDDI (see Copper Distributed Data Interface).

Challenge Handshake Authorization Protocol (CHAP). A password protection protocol that describes how to authenticate incoming data calls. The password is encrypted over the access line.

CHAP (see Challenge Handshake Authorization Protocol).

CIFS (see Windows networking).

client. A computer system or process that requests access to the data, services, or resources of a server (another computer system or process). Multiple clients may share access to a common server. Synonym for requester.

client-server model. A common way to describe network services and the model user processes (programs) of those services.

closed network. Synonym for closed path.

closed path. A network in which all of the cable paths and wiring closets are directly or indirectly connected. Synonymous with closed network.

cluster. In high-availability cluster multiprocessing (HACMP), a set of independent systems (called nodes) that are organized into a network for the purpose of sharing resources and communicating with each other. .

collision avoidance. In carrier sense multiple access with collision avoidance (CSMA/CA), the sending of a jam signal and waiting a variable time before transmitting data, to avoid two or more simultaneous transmissions.

Common Internet File System (CIFS). A protocol that enables collaboration on the Internet by defining a remote file-access protocol that is compatible with the way applications already share data on local disks and network file servers (MS).

configuration list. In a LAN, a list of all of the names and addresses of stations attached to a LAN segment.

connect. In a LAN, to physically join a cable from a station to an access unit or network connection point. Contrast with attach.

connection-oriented. The communication process that proceeds through three well-defined phases: connection establishment, data transfer, and connection release. Examples are: X.25, Internet TCP, and ordinary telephone calls.

connection-oriented network. A network which requires that a setup procedure be executed to establish an information channel between two logical nodes before they can interchange information.

control port. An alternate port that you can use to access the configuration when the data ports are not available.

control unit. A processor electronics assembly in a storage controller that exposes LUNs to the storage network and connects internally to the storage controllers disk drives. A storage controller can have 1 to *n*, but typically has one for each path group.

Copper Distributed Data Interface (CDDI). A proposed ANSI standard that defines a dual counter-rotating ring which operates at a rate of 100 Mbps over Category 5 copper wire.

coprocessor. A secondary processor used to speed up operations by handling some of the workload of the main CPU.

CRC (see cyclic redundancy check).

CRU (see customer-replaceable unit).

customer-replaceable unit (CRU). An assembly or part that a customer can replace in its entirety when any of its components fail. Contrast with field-replaceable unit (FRU).

cyclic redundancy check (CRC). (1) A redundancy check in which the check key is generated by a cyclic algorithm (T). (2) A system of error checking performed at both the sending and receiving station after a block-check character has been accumulated.

D

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data port. Ethernet ports used for storage-traffic and configuration purposes.

DASD queue. A queue that resides on a direct access storage device (DASD).

data store. An abstraction for a repository where data is kept, independent of underlying implementation. Data stores can be block based (a LUN or set of LUNs); file based (a local or remote file system); or relational (a database). Since IBM TotalStorage™ NAS family appliances are file based, all of their datastores must be kept in file systems, directories, or files which are kept on LUNs.

data bus. A bus used to communicate data internally and externally to and from a processing unit, storage, and peripheral devices (A). (See bus.)

data integrity. (1) The condition that exists as long as accidental or intentional destruction, alteration, or loss of data does not occur (T). (2) Preservation of data for its intended use.

DDP (see distributed data processing).

default route. A route, in the routing table, that is used when no other route is specified or appropriate.

device address. (1) In data communication, the identification of any device to which data can be sent or from which data can be received. (2) The first subchannel address recognized by a channel-attached device.

device identifier (ID). An 8-bit identifier that uniquely identifies a physical I/O device.

device parity protection. A function that protects data stored on a disk unit subsystem from being lost because of the failure of a single disk unit in the disk unit subsystem. When a disk unit subsystem has device parity protection and one of the disk units in the subsystem fails, the system continues to run. The disk unit subsystem reconstructs the data after the disk unit in the subsystem is repaired or replaced. See RAID and RAID-5.

DHCP (see Dynamic Host Configuration Protocol).

diagnostic diskette. A diskette containing diagnostic modules or tests used by computer users and service personnel to diagnose hardware problems.

direct access storage device (DASD).   A mass-storage medium on which a computer stores data. Contrast with random access memory (RAM).

Direct Memory Access (DMA).   A technique in which an adapter bypasses a computer's CPU, and handles the transfer of data between itself and the system's memory directly.

distributed data processing (DDP).   Synonym for distributed processing.

DLR (see dynamic link routine).

DMA (see Direct Memory Access).

DNS (see domain name system).

Domain Name System (DNS).   In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

drive bay.   A receptacle into which you insert a disk drive module in an appliance. The bays are in storage units that can be physically located in a separate rack from the appliance.

dual inline memory module (DIMM).   A small circuit board with memory-integrated circuits containing signal and power pins on both sides of the board.

Dynamic Host Configuration Protocol (DHCP).   A protocol defined by the Internet Engineering Task Force (IETF) that is used for dynamically assigning IP addresses to computers in a network.

dynamic link routine (DLR).   A program or routine that can be loaded by an application or as part of a program.

E

EIA (see Electronic Industries Association).

EISA (see Extended Industry Standard Architecture).

ELAN (see emulated LAN).

electromagnetic interference.   A disturbance in the transmission of data on a network resulting from the magnetism created by a current of electricity.

Electronic Industries Association (EIA).   An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

Electronic Industries Association (EIA) unit.   A unit of measure equal to 4.45 cm (1.75 in).

electrostatic discharge (ESD).   An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

EMC.   Electromagnetic compatibility.

emulate.   To imitate one system with another, primarily by hardware, so that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated system (A).

emulated LAN (ELAN).   A specific implementation of a virtual LAN, as it relates to LAN Emulation in ATM networks. An ELAN consists of one or more LAN Emulation clients (LECs) that share the same LAN Emulation Server and Broadcast and Unknown Server (LES/BUS). LECs gain membership in an ELAN based on configurable policies. Like devices on traditional LANs, each ELAN member has a MAC address and can use the LES/BUS to send unicast and broadcast packets to other members based on MAC addresses.

emulation.   (1) The use of a data processing system to imitate another data processing system, so that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated system. Emulation is usually achieved by means of hardware or firmware (T). (2) The use of programming techniques and special machine features to permit a computing system to execute programs written for another system.

engine. The unit that contains the processors that respond to requests for data from clients. This is where the operating software for the TotalStorage Model G25 appliance resides.

equivalent paths. A collection of paths to the storage device. The paths have no switchover time penalty when changing from one path group to another while accessing the storage device.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition (A) (I).

ESD (see electrostatic discharge).

ESM (see environmental service monitor).

Ethernet. A standard protocol for a 10-Mbps baseband local area network (LAN) that allows multiple access and handles contention by using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method.

Ethernet network. A baseband LAN with a bus topology in which messages are broadcast on a coaxial cable using a carrier sense multiple access/collision detection (CSMA/CD) transmission method.

event message. Synonym for call-progress event message.

executable statement. A statement that specifies one or more actions to be taken by a computer program at execution time; for example, instructions for calculations to be performed, conditions to be tested, flow of control to be altered (T).

expansion slot. In personal-computer systems, one of several receptacles in the rear panel of the system unit into which a user can install an adapter.

extended configuration services. Configuration services that reside outside a CP processor. Extended configuration services keeps a local cache of transmission group locations. Extended configuration services do not handle activation and deactivation. See configuration services.

Extended Industry Standard Architecture (EISA). The PC bus standard that extends the AT bus (ISA bus) to 32 bits and provides busmastering. It was announced in 1988 as a 32-bit alternative to the Micro Channel that would preserve investment in existing boards. PC and AT cards (ISA cards) can plug into an EISA bus.

F

failback. The restoration of the appliance to its initial configuration after detection and repair of a failed network or appliance component.

failover. (1) The automatic recovery of resources in the event of a network outage, or failure of the hardware or software. (2) A cluster event where the primary database server or application server switches over to a backup system due to the failure of the primary server.

failover group. A type of virtual network interface. It is a collection of physical and bonded interfaces that provide backup for each other. Each member of the failover group must have the same front-end and backend connectivity.

failure. (1) The termination of the ability of a functional unit to perform its required function. (2) An uncorrected hardware error. Failures are either recoverable or not recoverable by the software or the operator. The operator is always notified when failures occur. Contrast with error.

Fast Ethernet. An Ethernet standard that provides a data rate of 100 Mbps.

feature code. A code used by IBM to process hardware and software orders.

Federal Communications Commission (FCC). A board of commissioners appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign communications by wire and radio originating in the United States.

fiber optic cable (see optical cable).

Fiber Optic Inter-Repeater Link (FOIRL). An IEEE standard for fiber optic Ethernet.

FIC (see File Image Capture).

Field-replaceable unit (FRU).   An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit may contain other field replaceable units. Contrast with customer-replaceable unit (CRU).

File Image Capture (FIC).   Function that takes a file system clone and a read-only copy of the certain read-write (active) file system. File Image Capture reflects the state of the file system at the time it was created.

File Image Restore.   Function that allows a file system to revert to the state and contents of a previous File Image Capture. This function can be used to recover a corrupted file system.

File Transfer Protocol (FTP).   In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

FIR (see File Image Restore).

firewall.   A logical barrier around systems in a network. A firewall consists of hardware, software, and a security policy that control the access and flow of information between secure or trusted systems and nonsecure or untrusted systems.

fixed-length record.   A record having the same length as all other records with which it is logically or physically associated.

flash memory.   A memory chip that holds its content without power but must be erased in fixed blocks rather than single bytes.

floating virtual connection (FVC).   The ability to resume a virtual connection on a port other than the port connection on which the original virtual connection was established.

frame alignment error.   An error in a frame, indicated by a frame check sequence (FCS) indicator. When excessive or missing bits occur during the reception of a frame, the frame is misaligned.

free disk.   A physical disk that is not assigned as a hot-spare, as a standby hot-spare, or to a logical drive.

FRU (see field-replaceable unit).

FTP (see File Transfer Protocol).

FVC (see floating virtual connection).

G

gateway.   A device that acts as a router, but occurs at the transport layer, to transfer packets between networks.

group definition.   A list of directory numbers.

group definition ID.   The identifier of a group definition.

group SAP.   A single address assigned to a group of service access points (SAPs).

group separator (GS) character.   The information separator intended to identify a logical boundary between groups.

H

hard failure.   An error condition on a network that requires that the network be reconfigured or that the source of the error be removed before the network can resume reliable operation. Synonym for hard error.

hertz (Hz).   A unit of frequency equal to one cycle per second.

Note: In the United States, line frequency is 60 Hz or a change in voltage polarity 120 times per second; in Europe, line frequency is 50 Hz or a change in voltage polarity 100 times per second.

higher level. In the hierarchical structure of a data station, the conceptual level of control or processing logic, above the data link level that determines the performance of data link level functions such as device control, buffer allocation, and station management.

host. (1) In TCP/IP, any system that has at least one internet address associated with it. A host with multiple network interfaces may have multiple internet addresses associated with it. The host can be (a) a client, (b) a server, or (c) both a client and a server simultaneously. (2) In Fibre Channel, any system that has at least one worldwide name associated with it. A host with multiple network interfaces may have multiple worldwide names associated with it.

host application program. An application program processed in the host computer.

host attachment. A mode of SNA communication in which the processor acts as a secondary SNA device.

host computer. (1) In a computer network, a computer that usually performs network control functions and provides end users with services such as computation and database access (T). (2) The primary or controlling computer in a multiple computer installation or network. (3) A computer used to prepare programs for use on another computer or on another data processing system; for example, a computer used to compile, link edit, or test programs to be used on another system. (4) Synonym for host processor.

hot-spare disk. A physical disk that is automatically mapped to a logical drive if one of the logical drive's disks goes offline.

HTTP (see Hypertext Transfer Protocol).

Hypertext Transfer Protocol. In the Internet suite of protocols, the protocol that is used to transfer and display hypertext documents.

I

IBM Disk Operating System (DOS). A disk operating system based on MS-DOS that operates with all IBM-compatible personal computers.

IETF (see Internet Engineering Task Force).

iLUN. iSCSI client logical-unit number.

initial microcode load (IML). The action of loading the operational microcode.

initialize. In a LAN, to prepare the adapter (and adapter support code, if used) for use by an application program.

inoperative. The condition of a resource that has been active, but is no longer active. The resource could have failed or could have been suspended while a reactivate command was being processed.

interference. (1) The prevention of clear reception of broadcast signals. (2) The distorted portion of a received signal. (3) In optics, the interaction of two or more beams of coherent or partially coherent light.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet. The IETF consists of numerous working groups, each focused on a particular problem. Internet standards are typically developed or reviewed by individual working groups before they can become standards.

Internet Protocol (IP). A protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network.

Internetwork Packet Exchange (IPX). The routing protocol used to connect Novell's servers or any workstation or router that implements IPX with other workstations. Although similar to TCP/IP, it uses different packet formats and terminology.

interrupt level. The means of identifying the source of an interrupt, the function requested by an interrupt, or the code or feature that provides a function or service.

IOPS. Input/output operations.

IP (see Internet Protocol).

IPX. Internetwork Packet Exchange

IRQ. Interrupt request.

iSCSI. A technology that enables the SCSI transport protocol over an IP network by connecting clients (initiators) and servers to storage.

iSCSI client. A device that creates and sends SCSI commands to the target IBM IP Storage appliance.

iSCSI client logical-unit number (iLUN). A unique number that is assigned to each VLUN. The iLUN for a single client starts at zero and increments sequentially.

J

jumper. A connector between two pins on a network adapter that enables or disables an adapter option, feature, or parameter value.

jumper cable. Synonym for patch cable.

K

Kerberos. Pertaining to the security system of the Massachusetts Institute of Technology's Project Athena. It uses symmetric key cryptography to provide security services to users in a network.

L

LAN (see local area network).

local area network. A network in which a set of devices are connected to one another for communication and that can be connected to a larger network.

LAN emulation client (LEC). A LAN emulation component that represents users of the emulated LAN.

LAN emulation configuration server (LECS). A LAN emulation service component that centralizes and disseminates configuration data.

LAN multicast. Sending of a transmission frame that is intended to be accepted by a group of selected data stations on the same local area network.

LAN Segment Number. The identifier that uniquely distinguishes a LAN segment in a multi-segment LAN.

LAN-to-LAN. An access mode for connecting remote LAN sites.

large-scale integration (LSI). The process of integrating large numbers of circuits on a single chip of semiconductor material.

LBG (see load-balancing group).

LDAP (see Lightweight Directory Access Protocol).

Lightweight Directory Access Protocol. In TCP/IP, a protocol that enables users to locate people, organizations, and other resources in an Internet directory or intranet directory.

limited broadcast. Synonym for single-route broadcast.

link aggregation. A type of bond group that combines the bandwidth of two or more ports to serve as one IP address. The bond group distributes data across the bonded ports by using an algorithm. See bond group.

LIP. Loop initialization process

load-balancing group (LBG). A type of virtual network interface that comprises a set of physical and bonded interfaces. A set of nodes within a virtual server that has layer-2 front-end connectivity can be collectively identified by a unique IP address and grouped into a load-balancing group (LBG). The intent of such a grouping is to enable all

nodes in the LGB to share the file serving load. A unique IP address and DNS host name combination identify each load-balancing group. Depending on the front-end connectivity, you can configure a node to be a member of more than one load-balancing group.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with universally administered address.

logical connection. In a network, devices that can communicate or work with one another because they share the same protocol.

logical drive. A unit of virtual storage that is made available to the network through VLUNs and iLUNs. It is made up of one or more physical disks that are combined using RAID 0, 1, 1E, 5, or 5E technology.

logical node. Logical nodes exist and operate in the physical context of the primary devices. There are different types of logical nodes and each is associated with a specific protocol stack.

loop. A closed unidirectional signal path connecting input/output devices to a system.

Low-smoke fire-retardant zero halogen. Describes materials that are not flammable and do not emit large amounts of smoke or toxic gasses when burnt.

Low-smoke zero halogen. Describes materials that do not emit large amounts of smoke or toxic gasses when burnt.

LSFR0H (see Low-smoke fire-retardant zero halogen).

LS0H (see Low-smoke zero halogen).

M

macro. An instruction that causes the execution of a predefined sequence of instructions in the same source language.

main storage. Program-addressable storage from which instructions and other data can be loaded directly into registers for subsequent execution or processing (A) (I).

management information base (MIB). SNMP units of managed information that specifically describe an aspect of a system, such as the system name, hardware number, or communications configuration. A collection of related MIB objects is defined as a MIB.

megahertz (MHz). A unit of measure of frequency. One megahertz = 1 000 000 hertz.

MES (see miscellaneous equipment specification).

MIB. Management information base.

MIB browser. In the Simple Network Management Protocol (SNMP), a small PC or workstation application that can load MIB definitions, query or set data items in a managed node, and decode returned values and results in an easily readable form.

microinstruction. An instruction for operations at a level lower than machine instructions (T).

microprogram. A sequence of microinstructions. Microprograms are mainly used to implement machine instructions (T).

migrate. To move to a changed operating environment, usually to a new release or version of a program, system, or device.

miscellaneous equipment specification (MES). Any equipment that is added after the time of the initial order.

mode field diameter. A measure of the width of the guided optical power's intensity distribution in the core and the cladding of a single-mode fiber.

modulation. (1) The process by which a characteristic of a carrier is varied in accordance with a characteristic of an information-bearing signal (T). (2) The process by which a message signal is impressed upon a carrier signal so that the carrier is altered to represent the message signal.

multicast address (see LAN multicast).

multimode optical fiber. (1) A graded-index or step-index optical fiber that allows more than one bound mode to propagate (E). Contrast with single-mode optical fiber. (2) In FDDI, an optical fiber waveguide usually characterized by a core diameter of 50 to 100 micron that will allow a large number of modes to propagate.

multiplexing. In data transmission, a function that permits two or more data sources to share a common transmission medium so that each data source has its own channel (A) (I).

N

N (see Newton).

nanosecond (ns). One thousand millionth of a second.

NAS. Network-attached storage.

NDMP (see network data management protocol).

network-attached storage (NAS). A task-optimized storage device directly attached to a network that works independent of the general-purpose file servers.

network data management protocol (NDMP). An open standard protocol for enterprise-wide network-based backup for network attached storage.

network file system (NFS). A protocol, developed by Sun Microsystems, Incorporated, that allows any host in a network to mount another host's file directories. After a file directory is mounted, the it appears to reside on the local host.

network information services (NIS). A set of UNIX network services (for example, a distributed service for retrieving information about the users, groups, network addresses, and gateways in a network) that resolve naming and addressing differences among computers in a network.

network interface.

newton (N). The force that when applied to a body having a mass of one kilogram gives it an acceleration of one meter per second per second (1 m/s(2)).

NFS (see network file system).

NI (see network interface).

NIS (see network information services).

non-broadcast frame. A frame containing a specific destination address and that can contain routing information specifying which bridges are to forward it. A bridge will forward a non-broadcast frame only if that bridge is included in the frame's routing information.

non-canonical. In this form, the most significant bit of an octet is transmitted first.

ns (see nanosecond).

O

ODI (see Open Data-Link Interface).

Open Data-Link Interface (ODI). A common interface for network drivers developed by Novell. It allows multiple transport protocols to run on one network adapter.

optical cable.   A fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications (E).

optical fiber.   Any filament made of dielectric materials that guides light, regardless of its ability to send signals.

optical fiber coupler.   (1) A device whose purpose is to distribute optical power among two or more ports (A). (2) A device whose purpose is to couple power between a fiber and a source or detector (A).

P

packet internet groper (PING).   In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply.

parity check.   (1) A redundancy check by which a recalculated parity bit is compared to the pre-given parity bit (T). (2) A check that tests whether the number of ones (or zeros) in an array of binary digits is odd or even (A).

passive hub.   A hub that adds nothing to the data being transmitted through it.

path.   The connection between a storage port and the WWN (World Wide Name): target : LUN of a storage device.

path group.   A collection of equivalent paths. Storage devices may have one, two or *n* path groups.

PCI (see Peripheral Component Interconnect).

PCNFS (see personal-computer network file system).

PCNFSD (see personal-computer NFS daemon).

PCMCIA (see Personal Computer Memory Card International Association).

PDC (see primary domain controller).

PDU.   Power distribution unit.

Peripheral Component Interconnect (PCI).   A local bus for PCs from Intel that provides a high-speed data path between the CPU and up to 10 peripherals (video, disk, network, and so on). The PCI bus coexists in the PC with the ISA or EISA bus. ISA and EISA boards still plug into an ISA or EISA slot, while high-speed PCI controllers plug into a PCI slot.

Persistent Storage Manager (PSM).   Columbia Data Products software that creates multiple point-in-time persistent True Image data views of any or all system and data volumes residing on the NAS. All persistent images survive system a power loss or a planned or unplanned reboot. Each instance of PSM seamlessly handles 250 concurrent images of up to 255 independent volumes for a total of 63,750 independent data images.*

personal-computer NFS daemon (PCNFSD).   A daemon that manages user authentication and print spooling.

Personal Computer Memory Card International Association (PCMCIA).   An organization that standardizes credit-card size memory and I/O adapters for personal computers.

PING (see packet internet groper).

pinout.   Information that specifies which signal, signal line, or cable wire maps to each pin on a module, card, or cable connector. A module is usually keyed to allow for pin number identification.

PPS (see per port switching).

primary adapter.   In a personal computer that is used on a LAN and that supports installation of two network adapters, the adapter that uses standard (or default) mapping between adapter-shared RAM, adapter ROM, and designated computer memory segments. The primary adapter is usually designated as adapter 0 in configuration parameters. Contrast with alternate adapter.

promiscuous mode.   In a local area network (LAN), a method of processing and monitoring LAN frames that does not discriminate based on address.

PSM (see Persistent Storage Manager).

Q

QoS.   Quality of service.

R

RAID (see redundant array of independent disks).

RAID-5.   The RAID method used by the high-performance models of the IBM 9337 Disk Array Subsystem. See redundant array of independent disks and device parity protection.

RAM (see random access memory).

random access memory (RAM).   A temporary storage location in which the central processing unit (CPU) stores and executes its processes. Contrast with direct access storage device.

redundant array of independent disks (RAID).   A method of protecting data loss due to disk failure based on the Redundant Array of Independent Disks specification published by the University of California in 1987. See device parity protection and RAID-5.

remote procedure call (RPC).   A facility that a client uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation.

S

Samba.   A UNIX implementation of CIFS that enables Windows networking-file-system protocol to communicate with UNIX operating systems.

SAN.   Storage Area Network.

SCSI (see small computer system interface).

shared LAN.   A LAN in which the total bandwidth is shared among all nodes attached to the LAN segment.

shared RAM.   Shared memory provided by an adapter with onboard memory and requiring use of system CPU.

shielded twisted pair (STP).   A cable medium consisting of a telephone wire wrapped in a metal sheath to eliminate external interference.

Simple Mail Transfer Protocol (SMTP).   In the Internet suite of protocols, an application protocol for transferring mail among users in the Internet environment. SMTP specifies the mail exchange sequences and message format. It assumes that the Transmission Control Protocol (TCP) is the underlying protocol.

Simple Network Management Protocol (SNMP).   In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single system image (SSI).   A system architecture in which a cluster of engines provides an external view of the system such that it appears as a single entity in terms of administration, client-side attachment or both.

single-mode optical fiber.   An optical fiber in which only the lowest-order bound mode (which can consist of a pair of orthogonally polarized fields) can propagate at the wavelength of interest. Contrast with multimode optical fiber.

single-route broadcast.   The forwarding of specially designated broadcast frames only by bridges which have single-route broadcast enabled. If the network is configured correctly, a single-route broadcast frame will have exactly one copy delivered to every LAN segment in the network. Synonym for limited broadcast.

small computer system interface (SCSI).   A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SMTP (see Simple Mail Transfer Protocol).

SNMP (see Simple Network Management Protocol).

splitter.   In a local area network (LAN), a passive device used at a node to connect two or more branches (T).

standby hot-spare disk.   A physical disk that is automatically mapped to a logical drive when no suitable hot-spare disk is available.

Storage Area Network (SAN).   A dedicated storage network tailored to a specific environment, combining servers, storage products, networking products, software, and services.

storage controller.   A device (such as a RAID Controller) that creates and manages other storage devices.

storage device.   A LUN that terminates a collection of ports on the storage network.

storage network.   Provides shared access to a set of LUNs across one to *n* storage client networks.

storage network device.   A type of hub, switch, director or router on the Fibre Channel fabric that is directly connected to the storage client network. A storage network device is part of the fabric infrastructure, but does not directly provide LUNs.

storage client network.   A classic interconnected Fibre Channel fabric with a single Fibre Channel fabric name.

storage port.   A Model G25 engine's connection point to a storage client network. A storage port is a member of a single fabric.

storage unit.   Hardware that contains one or more drive bays, power supplies, and network interface. Some storage units contain RAID controllers; their storage unit is accessed by the appliance.

store-and-forward.   A mode of operation for a LAN switch in which it completely checks every frame before forwarding, so customers can use the switch to isolate erroneous frames generated on one segment so they do not traverse the switch onto another segment.

STP (see shielded twisted pair).

SVN (see switched virtual network).

switched LAN.   A LAN that has a dedicated connection for each user whereby the full bandwidth is available to the workstation.

switched virtual networks (SVN).   A comprehensive approach for building and managing switched-based networks. It combines the virtues of LAN switching, bridging, routing, ATM switching and other switched services.

synchronous data transfer.   A physical transfer of data to or from a device that has a predictable time relationship with the execution of an I/O request.

synchronous transmission.   A method of transmission in which characters are synchronized by the transmission of initial sync characters and a common clock signal.

T

tape device.   A collection of tape units that come from one model type and serial number (such as all the LUNs of a tape library).

tape unit.   A tape drive or a robotics controller that is visible over a storage network. A tape unit is a member of a single storage network (of 1 to *n* fabrics), but can have 1 to *n* equivalent paths.

target.   A collection of logical units that are directly addressable on the network. The target corresponds to the server in a client-server model.

TCP (see Transmission Control Protocol).

TCP/IP (see Transmission Control Protocol/Internet Protocol).

Telnet.   In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

timeout. A time interval that is allotted for certain operations to occur, for example, a response to polling or addressing before system operation is interrupted and must be restarted.

Tivoli Storage Manager (TSM). A client/server product that provides storage management and data access services in a heterogeneous environment.

Transmission Control Protocol (TCP). In TCP/IP, a host-to-host protocol that provides transmission in an internet environment. TCP assumes Internet Protocol (IP) is the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). The Transmission Control Protocol and the Internet Protocol, which together provide reliable end-to-end connections between applications over interconnected networks of different types.

True Image data view. A data view that allows the file to be restored in the event of accidental deletion. It consists of 'point-in-time' images that provide a near-instant virtual copy of an entire storage volume.

TSM (see Tivoli Storage Manager).

twinaxial cable. A three-conductor cable with the two inner conductors serving to carry the signal energy, and the outer conductor serving as ground. The three conductors are insulated from each other.

U

universal serial bus (USB). A serial interface standard for telephony and multimedia connections to personal computers.

unshielded twisted pair (UTP). A cable medium with one or more pairs of twisted insulated copper conductors bound in a single plastic sheath.

USB (see universal serial bus).

V

VLAN (see virtual local area network).

VLU. Volume logical unit.

VLUN (see virtual logical unit).

virtual connection. A connection set up between two points that appears to the user to be available as a dedicated connection. This phantom connection can be maintained indefinitely or can be ended at will. The three states of a virtual connection are up, down or suspended.

virtual local area network (VLAN). A logical association of switch ports based upon a set of rules or criteria such as MAC addresses, protocols, network address, or multicast address. This permits resegmentation of the LAN without requiring physical rearrangement.

virtual logical unit (VLUN). A subset of a logical drive.

virtual port. Logical construct that corresponds to a logical adapter for a switched network port. A virtual port organizes outgoing switched logical links by specifying incoming call acceptance criteria, by dynamically building and relating logical adapters with selected hardware adapter ports, and by specifying adapter-related data link control (DLC) profiles for use with those logical adapters.

VNI. Virtual network interface.

volume. (1) Unit of storage on disk, tape, or other data recording media. (2) A logical disk visible to the appliance over a storage network. A member of a single storage network of 1 to n fabrics. It can have 1 to n path groups of 1 to n equivalent paths.

W

Windows Internet Name Service (WINS). Program that provides a distributed database for registering and querying dynamic NetBIOS names to IP address mapping in a routed network environment.*

WINS (see Windows Internet Naming Service).

Windows networking. Networking file-system protocol for the Windows operating system.

X

Xmodem. A public-domain asynchronous data link control (DLC) protocol that provides packet numbering and checksum error control for the transfer of binary files.

Index

Special Characters

(ISMP) Integrated System Management Processor   64

A

adapter troubleshooting and diagnostics   81
administering the appliance   9
administrative functions, advanced   51
Advanced Appliance Configuration Utility   11
Alacritech SLICuser   2

B

battery, replacing   78
beep codes   109
BIOS
    recovering   77
boot block jumper   77

C

CDs, Recovery and Supplementary   95
Cluster Services   2
clustering   39
    configuration requirements   5
    installation steps
        cluster configuration   42
        joining a domain   41
        networking setup   39
        shared storage setup   29
    powering off and powering on the NAS 300G when
        clustering is active   135
configuring the appliance   9

D

diagnostic programs
    description   119
    error messages   122
diagnostic tools   69
diagnostics panel   72
disaster recovery   56
discovery of appliances   15

E

error log   119
error messages   114
Ethernet adapter teaming   67
event log   119

F

families and groups   16
Fast!UTIL options   129
FAStT Host Adapter, customizing   129

FAStT MSJ   2, 63

H

help
    online   105
    telephone   105

I

IAACU (IBM Advanced Appliance Configuration
  Utility)   11
IAACU Agent   14
IAACU Console   14
IBM 5187 Network Attached Storage Model 6RZ
  (engine)   69
IBM Advanced Appliance Configuration Utility
  (IAACU)   11
IBM Advanced Appliance Configuration Utility agent
  (IAACU)   2
IBM Director Agent   2
integrated Ethernet adapter
    troubleshooting   81
Integrated System Management Processor (ISMP)   64
Intel PROSet II   84

K

keyboard, monitor, and mouse (using for setup and
  configuration)   9

L

LEDs
    diagnosing problems using   70
    diagnostics panel   72
    power supply   70
light-path diagnostics   72
log
    event/error   119

M

managing the appliance   9
messages
    diagnostic programs   119, 122
    POST   114
Microsoft Cluster Services   2
Microsoft Services for UNIX   2
Microsoft Windows 2000 for Network Attached Storage
  GUI   2
Microsoft Windows Terminal Services   2

N

NAS Administration console   13
NAS Backup Assistant   51

W

warranty and repair 107
Web sites 103
Windows 2000 for Network Attached Storage,
  administration tasks 22
Windows 2000 for Network Attached Storage
  (Web-based interface) 11

IBM ®