Network Attached Storage RAID Server

NAS-3200/NAS-3400

User's Manual

Safety Approvals

υ CE Marking

υ FCC Class A

FCC Compliance

This equipment has been tested and complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. If not installed and used in accordance with proper instructions, this equipment might generate or radiate radio frequency energy and cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measurers:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Safety Precautions

Before getting started, read the following important cautions.

1. Be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and place all electronic components in any static-shielded devices. Most electronic components are sensitive to static electrical charge.

2. Disconnect the power cords from the NAS server before making any installation. Be sure both the system and the external devices are turned OFF. Sudden surge of power could ruin sensitive components. Make sure the NAS server is properly grounded.

3. Do not open the system's top cover. If opening the cover for maintenance is a must, only a trained technician is allowed to do so. Integrated circuits on computer boards are sensitive to static electricity. To avoid damaging chips from electrostatic discharge, observe the following precautions:

   ü Before handling a board or integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. This will help to discharge any static electricity on your body.

   ü When handling boards and components, wear a wrist-grounding strap, available from most electronic component stores.

Copyright

Revision

User's Manual for PLANET Network Attached Storage RAID Server

Model: NAS-3200/NAS-3400

Rev: 3.0 (September, 2003)

Part No. EM-NAS3KV3

Table of Contents

Chapter 1

Introduction

To accommodate the increasing storage demands for enterprise, small business, SOHO, and home use, PLANET provides reliable and affordable solutions, the NAS-3200 and the NAS-3400. Regardless of the operating systems installed in your network, the NAS servers have straightforward setup procedures and can be installed in any existing network environment using its simple and intuitive management interface.

1.1 Features

- 2 or 4 ATA-66/100 hot swappable IDE trays
- Provides scalability up to 500GB or 1TB
- NAS-3200 supports RAID 0, 1 and NAS-3400 supports RAID 0, 1, 5, and 5+hot spare with on-line rebuild
- External UPS support through COM port
- Gigabit Ethernet support
- Two RJ-45 ports for redundant network connection
- Multi-protocol system support for Microsoft, Apple, UNIX/LINUX, and Novell networks
- Powerful utility for data backup and replication
- Multi-language support and user friendly web management interface
- SNMP MIB II support
- Fully integrated ability for Windows 2000 domains, NT 4.0 domains, and UNIX NIS domains
- File level ACL (Access Control List) support for Windows, Macintosh, and UNIX clients
- Rich log records for easy diagnostics
- 3rd Party Backup Application Support: Veritas Backup Exec, CA BrightStor, and Dantz Retrospect

1.2 Package Contents

The following items should be included:
- NAS Server unit
- 2 or 4 HDD trays
- Power cord
- CD-ROM (includes user's manual, utilities)
- Quick Installation Guide

If any of the above items are damaged or missing, please contact your dealer immediately.

1.3 Physical Details

Front View

NAS-3200
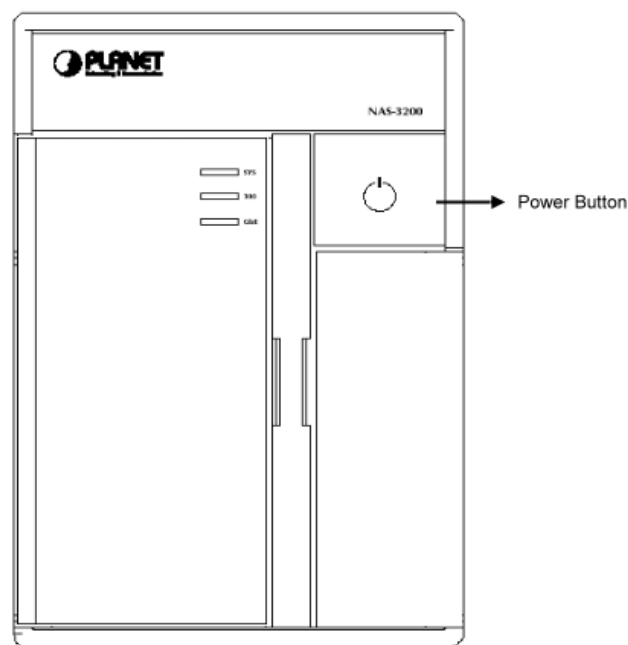
Power button: When the A/C power cable is in socket, the NAS-3200 will start to initiate. Press this button once to shutdown the NAS-3200. Press once again to switch on the server.

NAS-3400
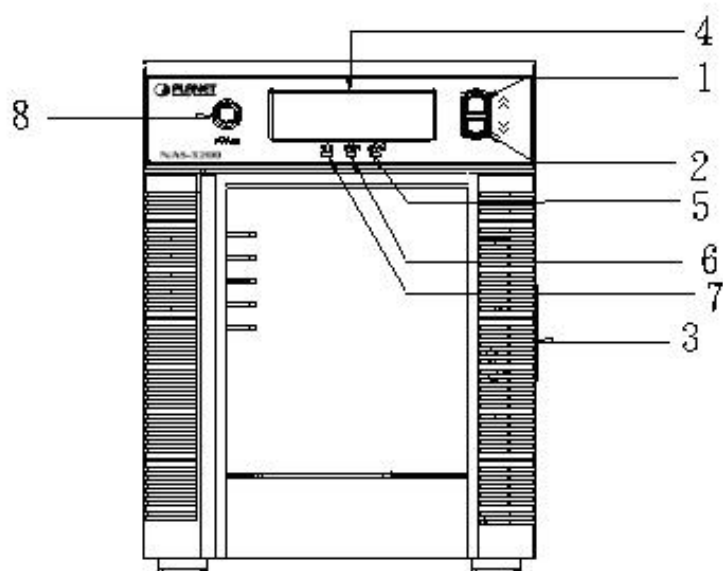
1	Up select button	**2**	Down select button
3	HDD Door	**4**	LCD display
5	Link/Active LED of GbE LAN port	**6**	Link/Active LED of 100 LAN port
7	LED of System Status/Alert	**8**	Power Control Button

Attention:

1. When the NAS server is operating, press power button continuously over 4 seconds to shut it off immediately. This shut-off activity should happen only when the NAS server is hung; otherwise it may make the server non-operational or damage the drives.

2. Once the power button is pressed, it takes around 20 seconds for shutdown.

LED definition:

LED	Color	Function
SYS	Green	Indicating system status. 1. One flash per 0.5 second: the system is booting. 2. One flash per 1.0 second: the system is being shutdown. 3. One flash per 2.0 second: the system is rebuilding. 4. Always on：the system is ready.
	Orange	Indicating system alert. 1. When system is booting, the Yellow LED will turn on for 1 second while BIOS is doing POST (power on self test), then the LED turns to green. 2. One flash per 1.0 second：one or two Fans fail. Fan 1 is the CPU fan. Fan 2 is the chassis fan. 3. One flash per 2.0 second: CPU is over heating.
100	Green	On: LAN is connected at 100Mbps speed. Blink: Transmitting or receiving data through the LAN.
	Orange	On: LAN is connected at 10Mbps speed. Blink: Transmitting or receiving data through the LAN.
GbE	Green	On: LAN is connected at 1000Mbps speed. Blink: Transmitting or receiving data through the LAN.
	Orange	On: LAN is connected at 10/100Mbps speed. Blink: Transmitting or receiving data through the LAN.

Rear View

NAS-3200
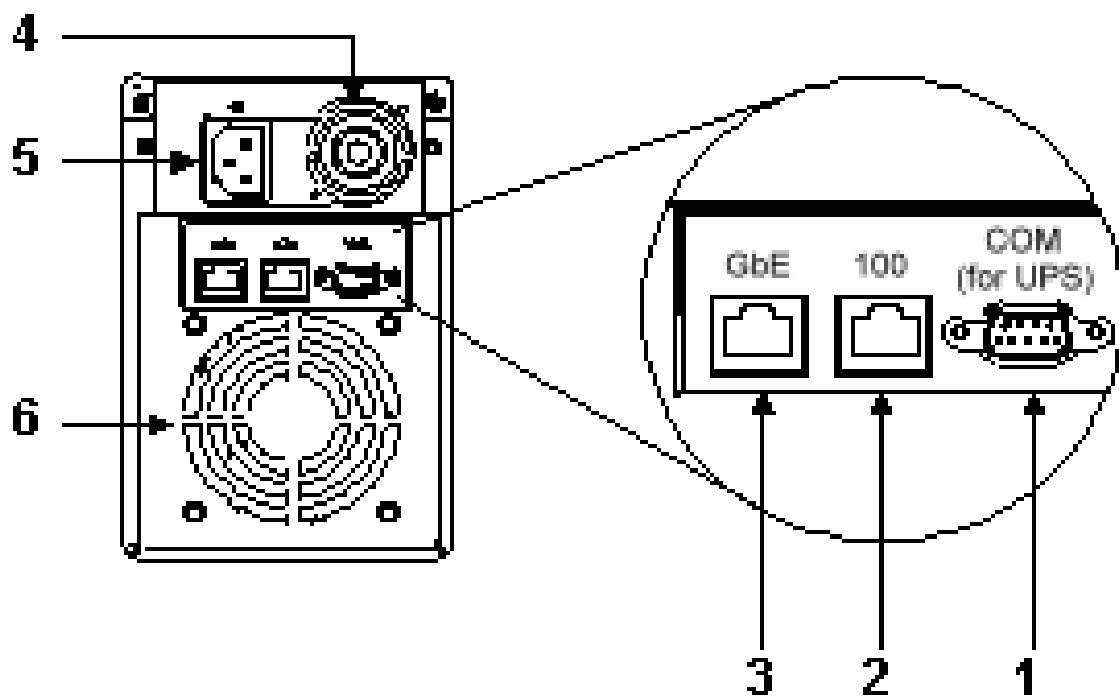
1. **COM (for UPS):** The NAS-3200 uses a DB-9 connector for its serial port connection. The pin assignments of this connector are as follows:
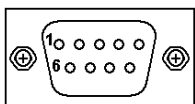
Pin #	Signal Name
1	DCD, Data carrier detect
2	RXD, Receive data
3	TXD, Transmit data
4	DTR, Data terminal ready
5	GND, ground
6	DSR, Data set ready
7	RTS, Request to send
8	CTS, Clear to send
9	RI, Ring indicator

2. **100:** 10/100M Ethernet port

3. **GbE:** 10/100/1000M Ethernet port

4. FAN of power supply

5. AC inlet of power supply

6. Chassis FAN

NAS-3400
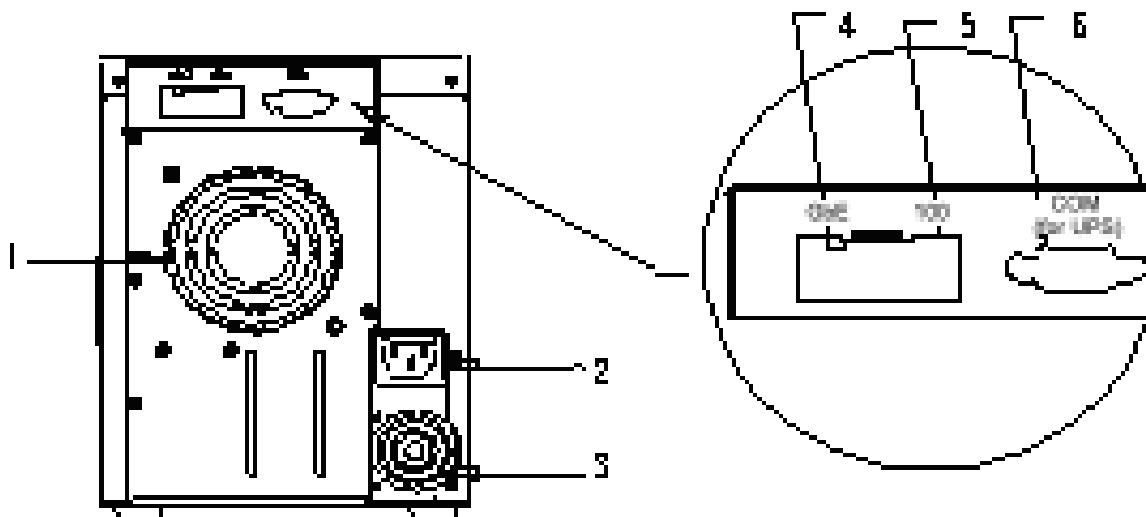
1. Chassis FAN

2. AC inlet of power supply

3. FAN of power supply

4. **GbE:** 10/100/1000M Ethernet port

5. **100:** 10/100M Ethernet port

6. **COM (for UPS):** The NAS-3400 uses a DB-9 connector for its serial port connection. The pin assignments of this connector are as follows:
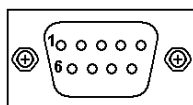
Pin #	Signal Name
1	DCD, Data carrier detect
2	RXD, Receive data
3	TXD, Transmit data
4	DTR, Data terminal ready
5	GND, ground
6	DSR, Data set ready
7	RTS, Request to send
8	CTS, Clear to send
9	RI, Ring indicator

Chapter 2
Installation

2.1 Hardware Installation Procedures

Before start using NAS server, please follow the procedures below to complete the hardware Installation.

Step 1: Install at least one hard disk via hot-swappable drive tray. Insert the tray to the left driver bay of NAS-3200 or to the top driver bay of NAS-3400 (these driver bays are considered as the disk 1 of respective NAS servers). Note that it is strongly recommended to use brand new hard disks and all HDDs must be set to master mode.

Step 2: Connect one end of an Ethernet cable to the LAN port located on the NAS server rear panel and attach the other end to a hub or switch.

Step 3: Connect the provided power cord to the power supply of the NAS server.

Step 4: The orange system LED is continuously on for 2 seconds, then the green system LED flash rapidly (one flash per 0.5 second) indicating the NAS server is booting.

Step 5: The continuous green LED indicates the NAS server is ready to use.

2.2 Installing Hard Drives to HDD Trays

The hot-swappable HDD trays of NAS server can be used to install 3.5" IDE hard drive each. You don't' need to turn off the server when replacing a failed hard drive. The hard drive must be 3.5" ATA66/100 IDE compliance. The hot-swappable drive tray connects to the backplane. The backplane is the printed circuit board behind the bay.

Note:

1. Do not use any other drive tray that is not designed for NAS server, or a serious damage might be caused.

2. For best flexibility, the NAS server is designed to fit most types of hard drive form various hard disk drive vendors. But each of them might have slightly different mechanical dimension. We strongly recommend applying hard drives with the same type or with the same dimension to NAS server.

Install hard drive to hot-swappable drive tray

1. Open HDD door, press plastic locker trigger of tray downward to release tray handle. See figure 1 and figure 2.

2. Remove the empty hot-swappable drive tray by pulling the tray handle. Slide the tray off the tray bay. See figure 1 and figure 2.
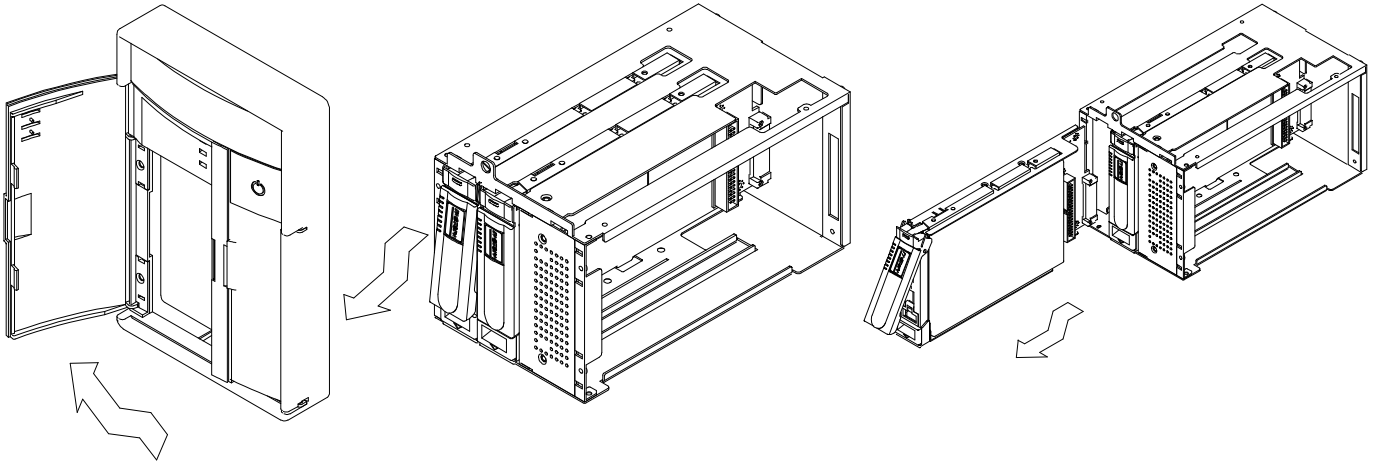
Figure 1
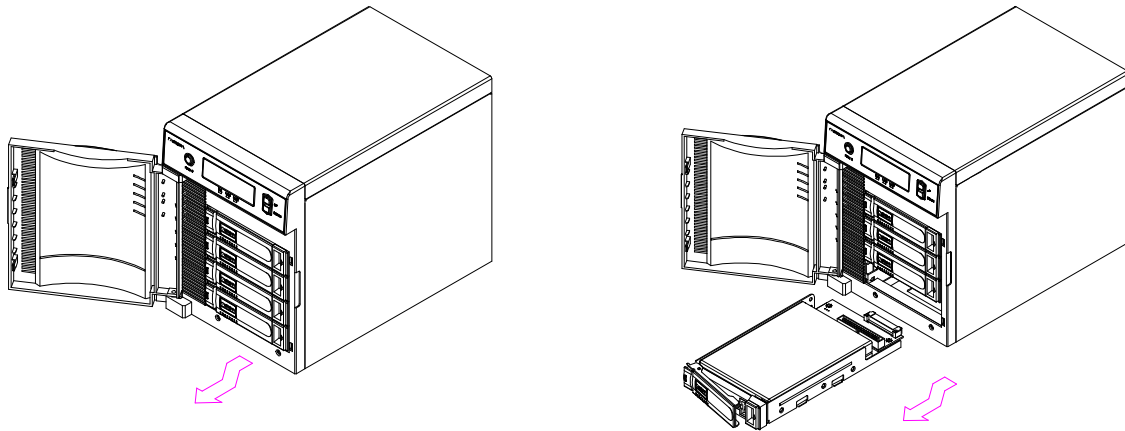
Figure 2

3. Loosen 4 screws that firmly mounted the HDD drive onto the drive tray. Disconnected the cable of old or damage HDD drive from the tray backplane. Then, pull the HDD drive out of the tray drive bay. See figure 3.

4. Mount the new HDD drive(s) into the empty slot. Connect the cable of tray backplane into new HDD. Secure the HDD drive by mounting 4 screws on each side of the drive tray. See figure 3.
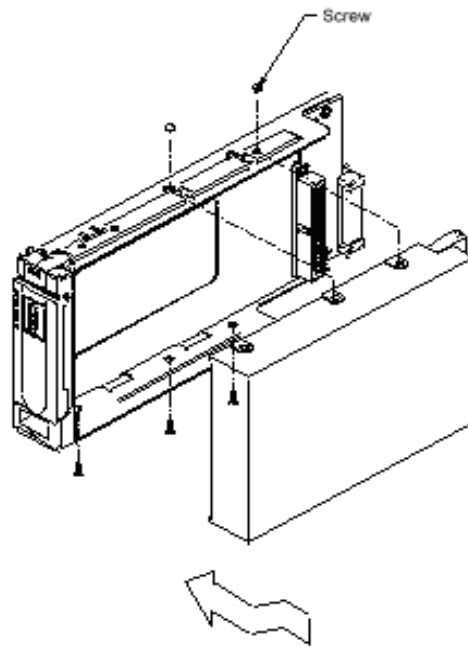
Figure 3

5. Gently push the hot-swappable drive tray into NAS server until the tray connects to the backplane.

6. Push the drive tray handle toward to the close position. See figure 4 and figure 5.
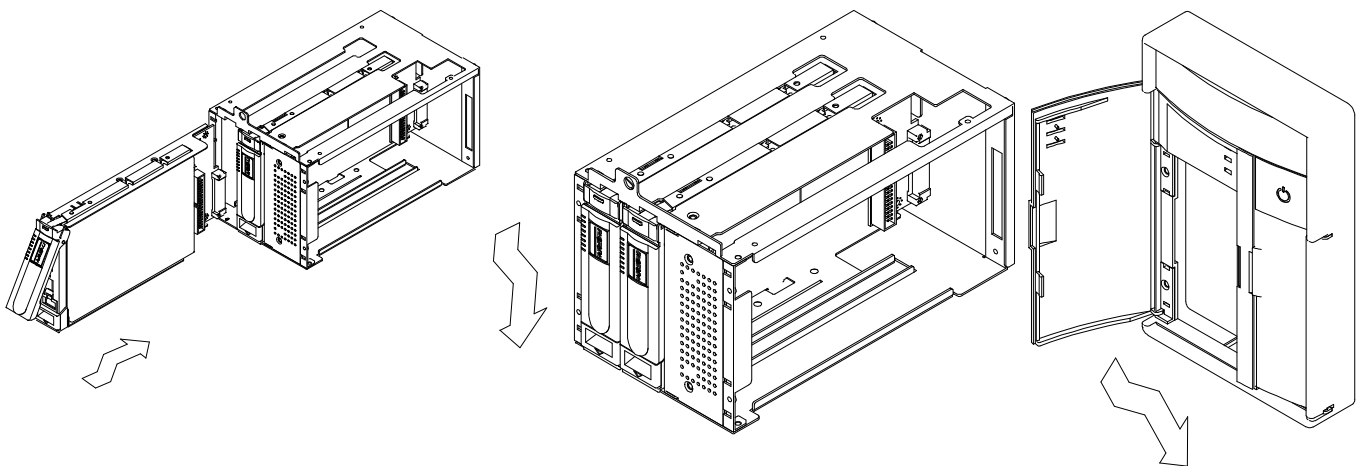
Figure 4
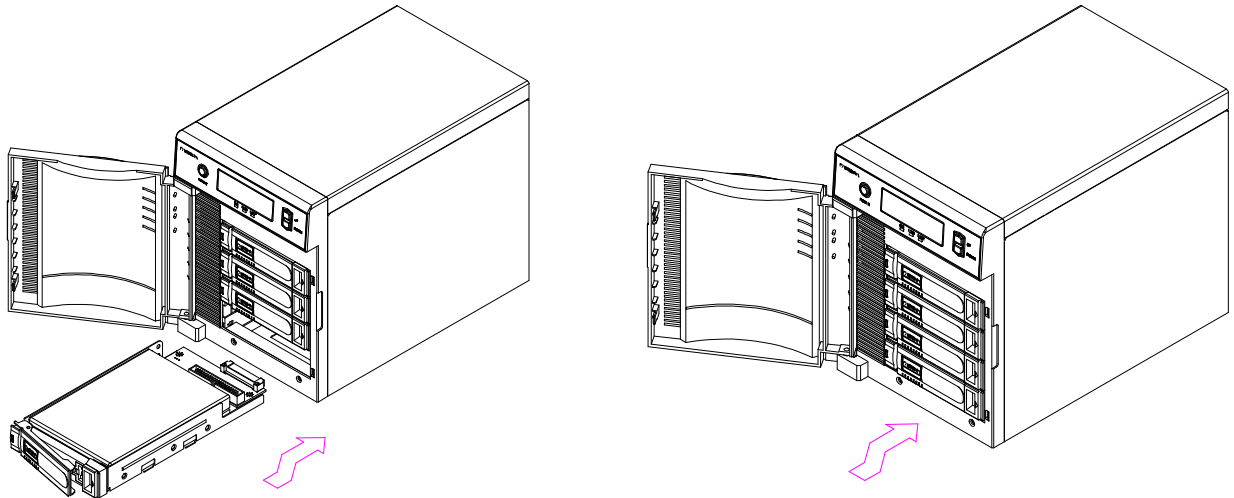
Figure 5

Verify the HDD status

1. When the HDD orange LED is continuously on, the drive is failed or not installed.

2. When the HDD orange/green LED is off, the drive tray is in bad connection.

3. When the HDD green LED flash rapidly, the drive is accessing by host.

HDD Status LED
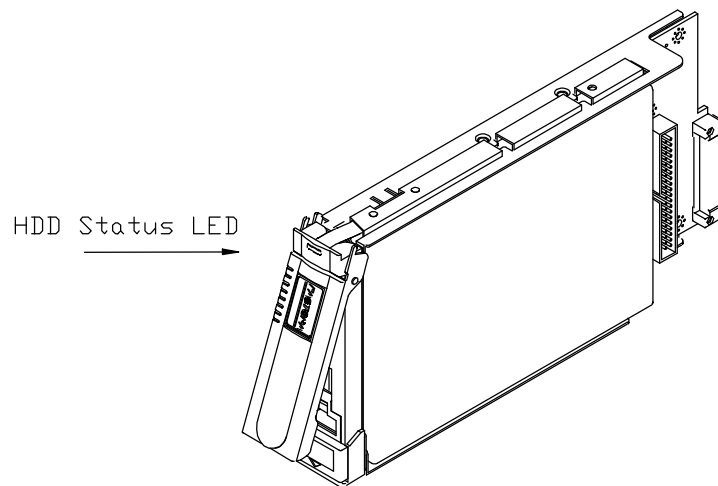
Figure 6

2.3 Setting Up the NAS Server

After connecting the NAS server to a power cord and the LAN, power it up and follow the procedures below to set up the server via PLANET NAS-3000 series Assistant. The demonstration is running in windows system. PLANET NAS-3000 series Assistant also provides MAC OS 9 and

OS X version, please refer to Appendix 4 for details.

1. Choose a computer in the same network as NAS server running Microsoft Windows 98/ME/NT /2000/XP and an IE5.0 (or above) web browser installed.

2. Insert the bundled CD in the CD-ROM drive to initiate the autorun program. Once completed a menu screen will appear as follows:

3. Click on the "NAS-3000 series Assistant" hyperlink to activate the program.

    If the above screen is not shown, you can start the installation as follows.
    A. Click on **Start Menu/ Run.**
    B. Enter "E:\UTILITY\Assistant\Windows\NAS3000SeriesAssistant.exe" in the appeared box, where "E" is the letter of your CD-ROM drive.
    C. Click on "OK" button.

4. PLANET NAS-3000 series Assistant will automatically search and list all available NAS servers on the LAN. The Server Status column will show current status of the server.
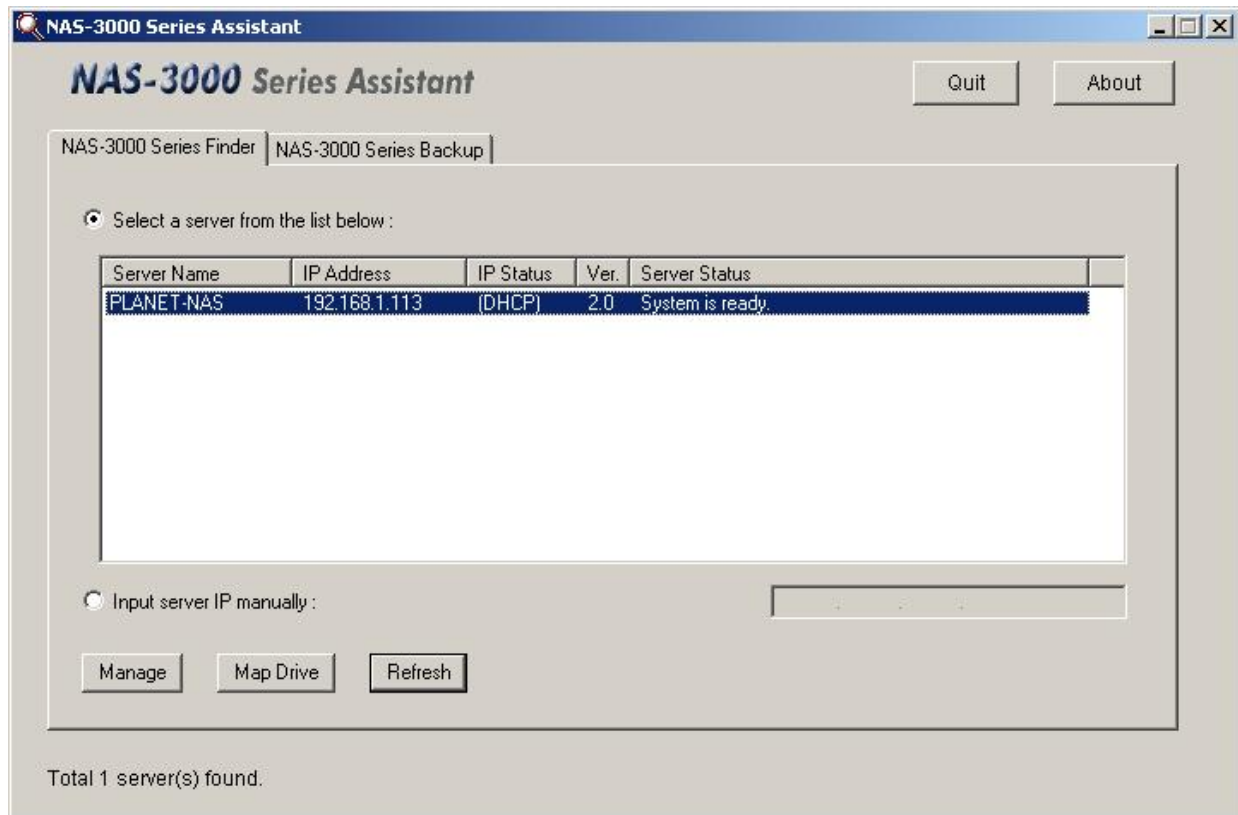
Suppose you want to set up a server called PLANET-NAS for the first time. By default the system obtains the network configuration information through the DHCP server. If a DHCP server does exist on the LAN, its IP Status will show DHCP, referring that the NAS server has correctly received IP from DHCP server. Please double click the server name or click the Manage button, and PLANET NAS-3000 series Assistant will automatically activate the browser, connect to the server's IP address, and then start the Quick Configuration.

5. If there is no DHCP server on the LAN, or the client that runs PLANET NAS-3000 series Assistant does not belong to the same network as NAS server, the IP Status column will show Unknown instead.
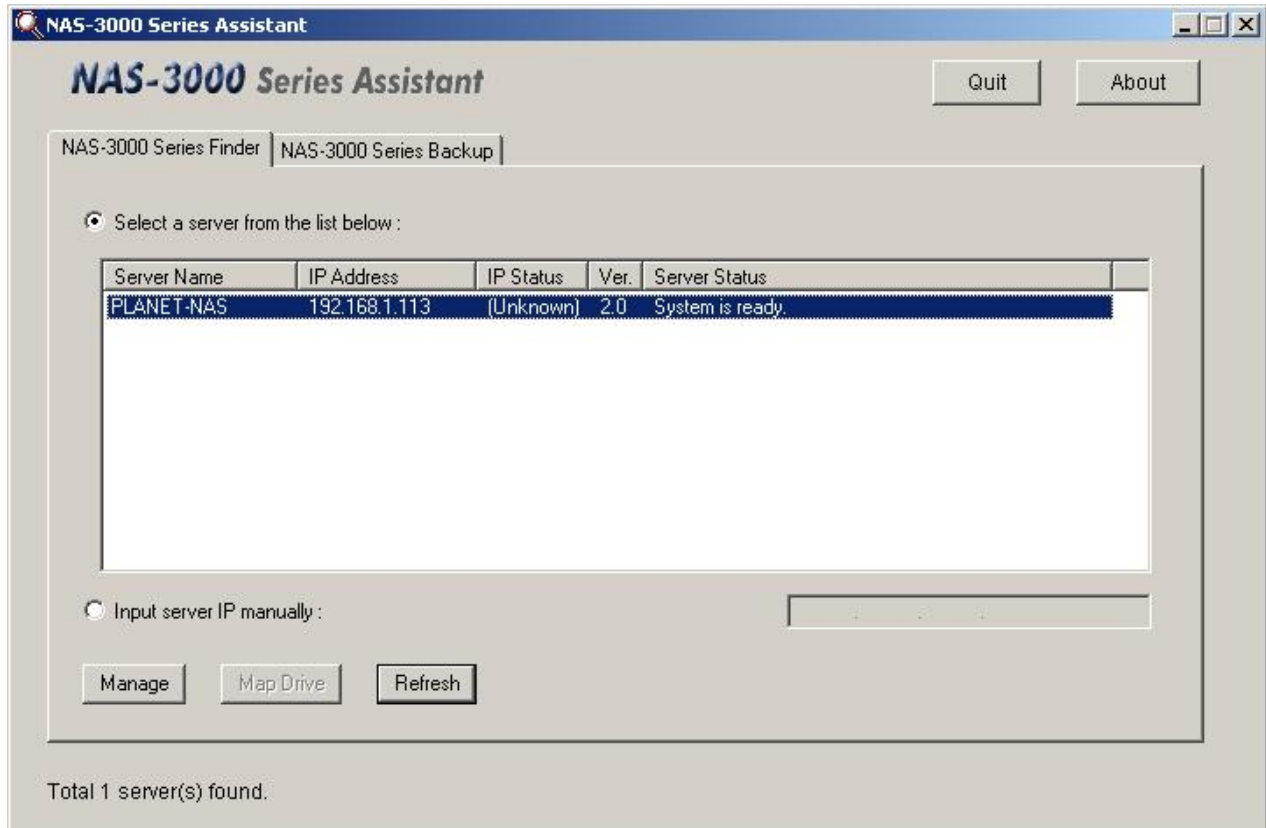
Double-click on the server name PLANET-NAS to open the network configuration screen. Input password into System administrator password field; the default value is blank. You can either select Get Network Configuration through DHCP to automatically configure the network through the DHCP server, or choose Use Manual Configuration and enter the IP address, domain name, subnet mask, gateway, and DNS server. The setup program will get the network configuration for your reference. If the information is not enough, click on Suggestion; the setup program will check available IPs on the LAN and provide a suggested IP address.

6. Click *Apply* to confirm the network settings. The program will automatically activate the browser and connect to the server's IP address, then start the Quick Configuration.

2.4 Turn off the NAS Server

There are two ways to turn off the NAS server.

1. When the NAS server is running, you can turn it off by pressing the power control button once. The NAS server will shutdown automatically after around 20 seconds. Do not press the power button continuously for over 4 seconds, for this action will turn off the power immediately and may cause the server non-operational or corrupt the drives.

2. You can turn off (shutdown) the NAS server via Toolkits option of its web management interface

Quick Configuration

The NAS server offers a simple and easy-to-use approach, which called NAS-3000 Series Manager, for administration. Use this manager to configure the server, system and network parameters, including Windows, UNIX, Novell and Apple Macintosh network settings, as well as the hard disk configuration.

When you install the NAS server for the first time, PLANET NAS-3000 series Assistant will complete the IP configuration of the server, then automatically activate the web browser to connect to the server. The Quick Configuration page with basic configuration options will appear. Please follow the instructions to complete all steps.
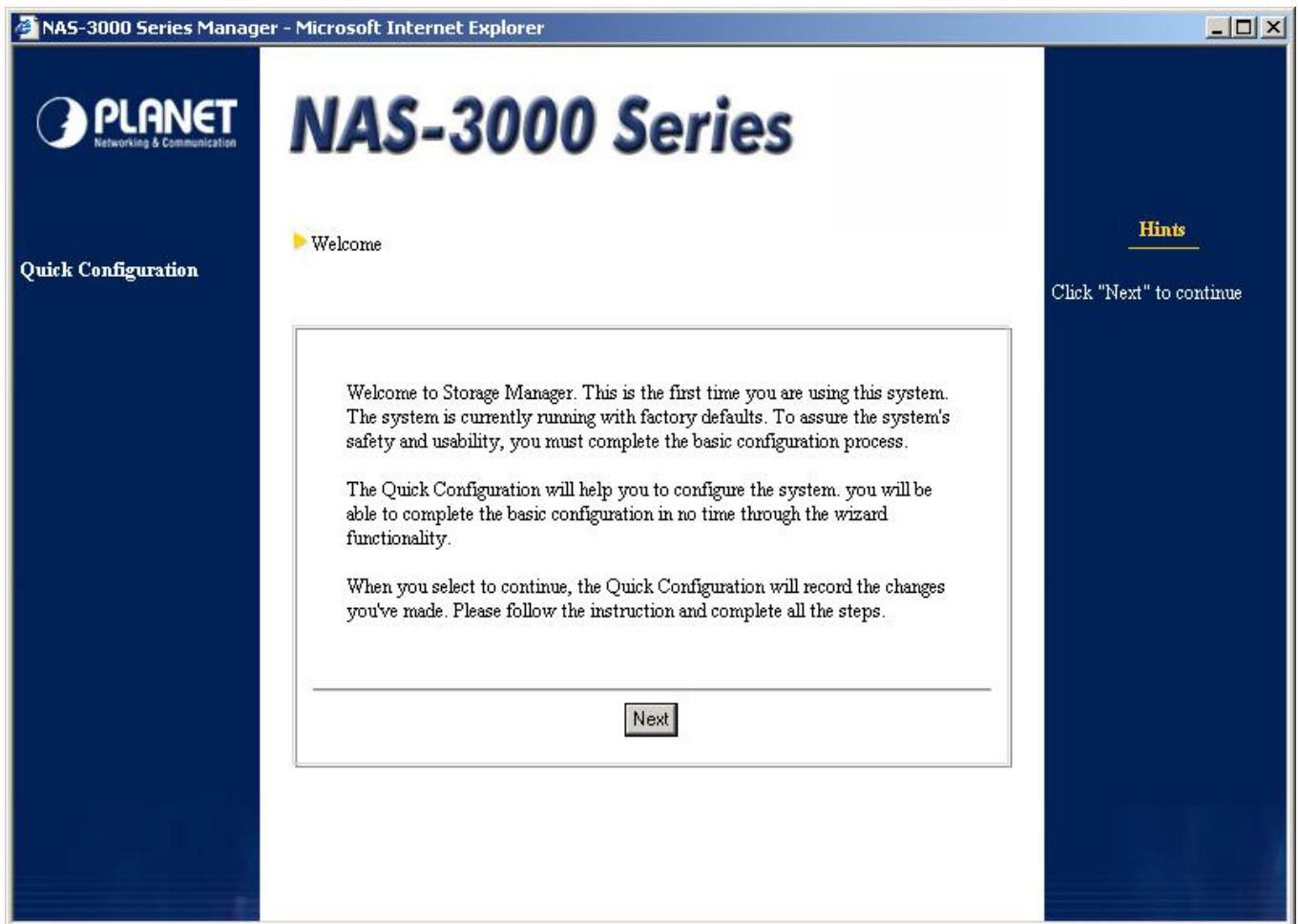
Note:

1. There are always hints on the right side of the screen during setup procedures. You can

obtain some useful information of every screen there.

2. This system only supports Microsoft IE 5.0 browsers or above. Netscape or other browsers are not supported.

Step 1: Enter the root password

Since this is the first time using this system, the system will prompt for changing the default root (system administrator) password. Make a note of this password for future access to the NAS server.

The password is case sensitive, and up to 12 displayable characters can be entered, including letters, numbers, signs, and space, etc. However, the password of root cannot be empty. After entering the password, please confirm your choice by re-entering it in the Confirm password field.

Step 2: Basic server configuration

System administrator can change the default server name here and further configure the network settings. Please note that the server name must be unique, meaning that no other server in the network should have the same name. The name is not case-sensitive and cannot exceed 15 characters. The first character must be a letter; the other characters can be letters, numbers, the underscore or minus sign.

This system supports up to four domain names and three DNS servers. The length of the domain name cannot exceed 64 characters. If the existing DHCP server has already created multiple domain names and DNS server setup while NAS server obtains its network settings from DHCP server, this page will capture the first item from the DHCP server. The system administrator must specify other items manually.

Step 3: LAN port 1

Next, please setup the IP address of the first network card. This page will show the setup information previously defined in PLANET NAS-3000 series Assistant, and system administrator can make additional change here.

If the LAN includes a DHCP server, click "Get network configuration through DHCP". Otherwise, choose "Use manual configuration", and fill out the related settings. Filling out the column with a red star sign on the right is mandatory, while filling out the column with the orange star is recommend by the system.

Step 4: Enter the system date and time

Use a 24-hour format to enter the system date and time, as well as the correct time zone. The NAS server will automatically adjust itself if daytime saving time (DST) is applicable to the selected time zone. There is no need for extra setup.

To activate network time synchronization, please choose "Enable network time synchronization", in the "Period" pull down menu, choose the appropriate period, and then fill out the hostname or IP in the Primary time server field. If a spare time server is available, fill out its hostname or IP in the Secondary time server field. When the primary time server is failed, the NAS server will try to synchronize the time with the secondary time server.
Note: Please find below NTP server web address for your reference to set the time server.

http://www.eecis.udel.edu/~mills/ntp/clock1a.html

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Step 5: Select a language

You can perform all the language settings on this page. Please choose a display language for NAS-3000 Series Manager, event notification emails, and the code page for different kinds of client.

In Display Language column, when selecting Browser Default Language, NAS-3000 Series Manager will automatically display the same language as the browser of the client when system administrator or general user is connected to NAS-3000 Series Manager.

For some languages at least 2 sorting methods are available for the administrator to choose. The sorting method is used to sort information on NAS-3000 Series Manager, such as shared folders and user accounts. The sorting method can be chosen from the "Sort by:" pull-down menu.

Encoding for Windows/ Apple/ Novell will be applied for the three clients, and allow them to access the server correctly with the defined encoding when Unicode is not available. After selecting the encoding for Windows/ Apple/ Novell, please select the appropriate encoding for NFS clients under the same locale language.

Once Quick Configuration is complete, NAS-3000 Series Manager will use that language. If you do not know the correct code page of your Windows client, enter the command "chcp" in the command prompt and press Enter to retrieve the correct code page information.

Note:

1. Inconsistent codepage settings between the system and the clients will result in incorrect display on accessing the data. The system codepage must be the same with that of the clients.

2. If the administrator set a single-byte language (code page), such as English, for Windows clients, an error will occur when the client attempts to save double-byte files or folder names (e.g. Traditional Chinese) on the NAS server, and some files cannot be deleted once saved. In this case, the system administrator must use the Server Configurationà Language Setup to change the code page to double-byte encoding; only then can the file be properly accessed and deleted.

Step 6: Enter a recipient for notification

NAS server can notify the system administrator of important events via e-mail. Enter a SMTP

server and the primary e-mail address 1. When an important event occurs, the system administrators will be informed via e-mail and can respond immediately, thus ensuring system safety. You have the option to send a test message after setup to make sure you have entered a valid configuration.

Due to the excessive amount of junk mail pervading the Internet, many providers do not allow their SMTP servers to be used by outside users. We therefore strongly recommend using the SMTP server of your e-mail domain (the address 1, address 2). E.g., if you use root@abc.com, select the SMTP server belonging to this provider, for example mail.abc.com.

Note: if you enter the host name (e.g. mail.abc.com) of the SMTP server, instead of the IP address (e.g. 192.168.1.1), please also enter the DNS address to ensure the notification emails can be sent to administrators.

Step 7: Cache setup

In order to improve data access performance, you can select to turn on "Disk write cache" support on this page. It is suggested that an UPS is accompanied with the server if this option is turned on to prevent from data loss when abnormal power failure occurs.

Step 8: Completing Quick Configuration
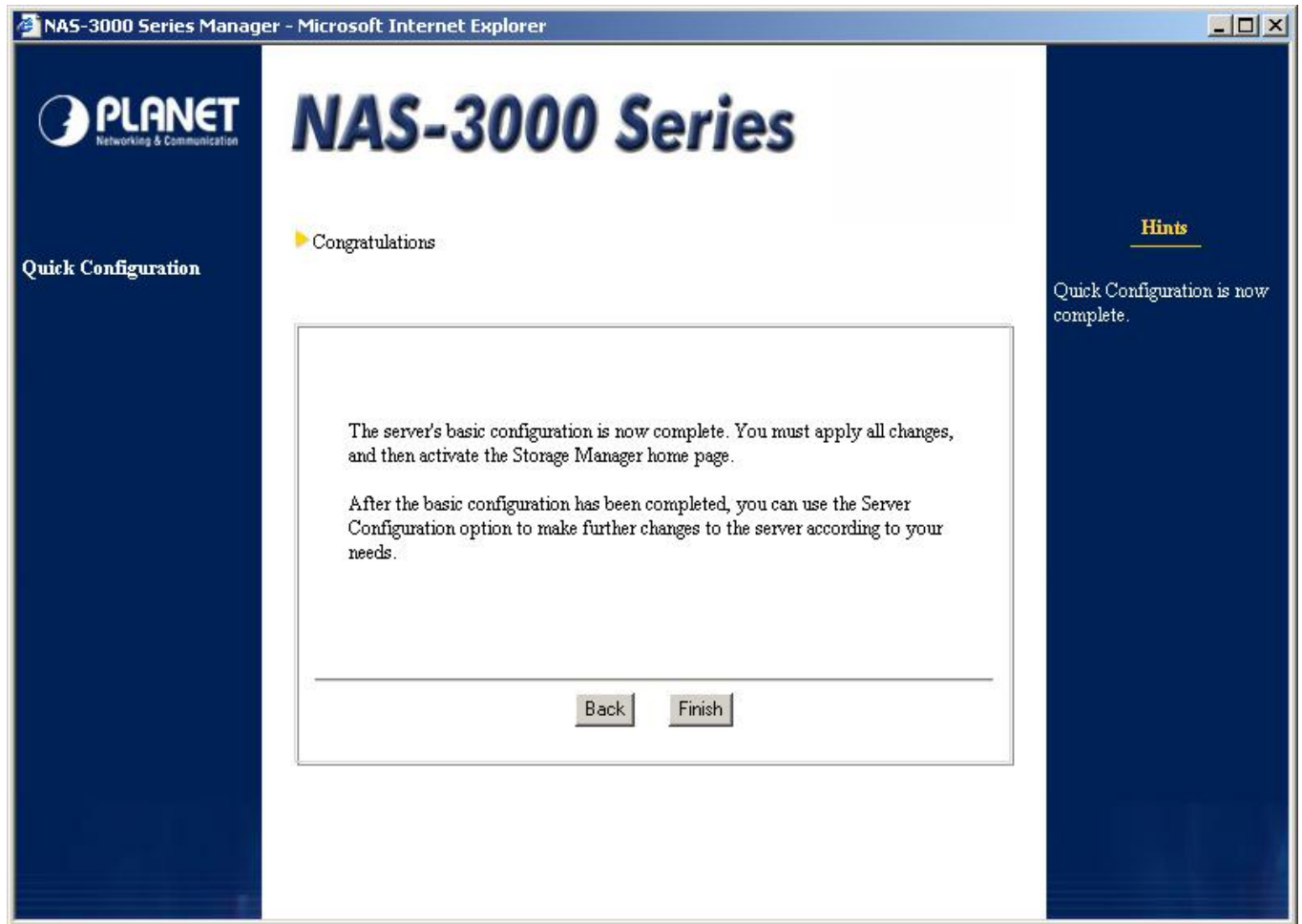
Once you have completed the Quick Configuration, the NAS server should operate properly on the LAN. Click "Finish" to apply all settings and activate NAS-3000 Series Manager.

Chapter 4

Using NAS-3000 Series Manager

After the Quick Configuration is complete, the NAS server will open the web-based NAS-3000 Series Manager program, where the system administrator can further edit the settings of the server.

Note:

1. NAS-3000 Series Manager does not include a Back option, but lists all of the configurable items on the left-hand side of the browser window. When you are done with one screen, simply select the next item you wish to configure from the list on the left.

2. If no entry modification in NAS-3000 Series Manager for 15 minutes, you will automatically be logged out, and will have to log in again to continue.

4.1 Server Information

You can obtain information about your NAS server here.

General tab

Shows system version and manufacturer information.

Configuration tab

Shows the current configurations of the server. You can change these settings under Server Configuration.

Status tab

Shows the current operation status of the server, including network port (s) and hard disk usage. If an error occurs on the server, such as network card malfunction or hard disk failure, the information on this page will be immediately updated, and a notification message will be sent via e-mail to the system administrator.
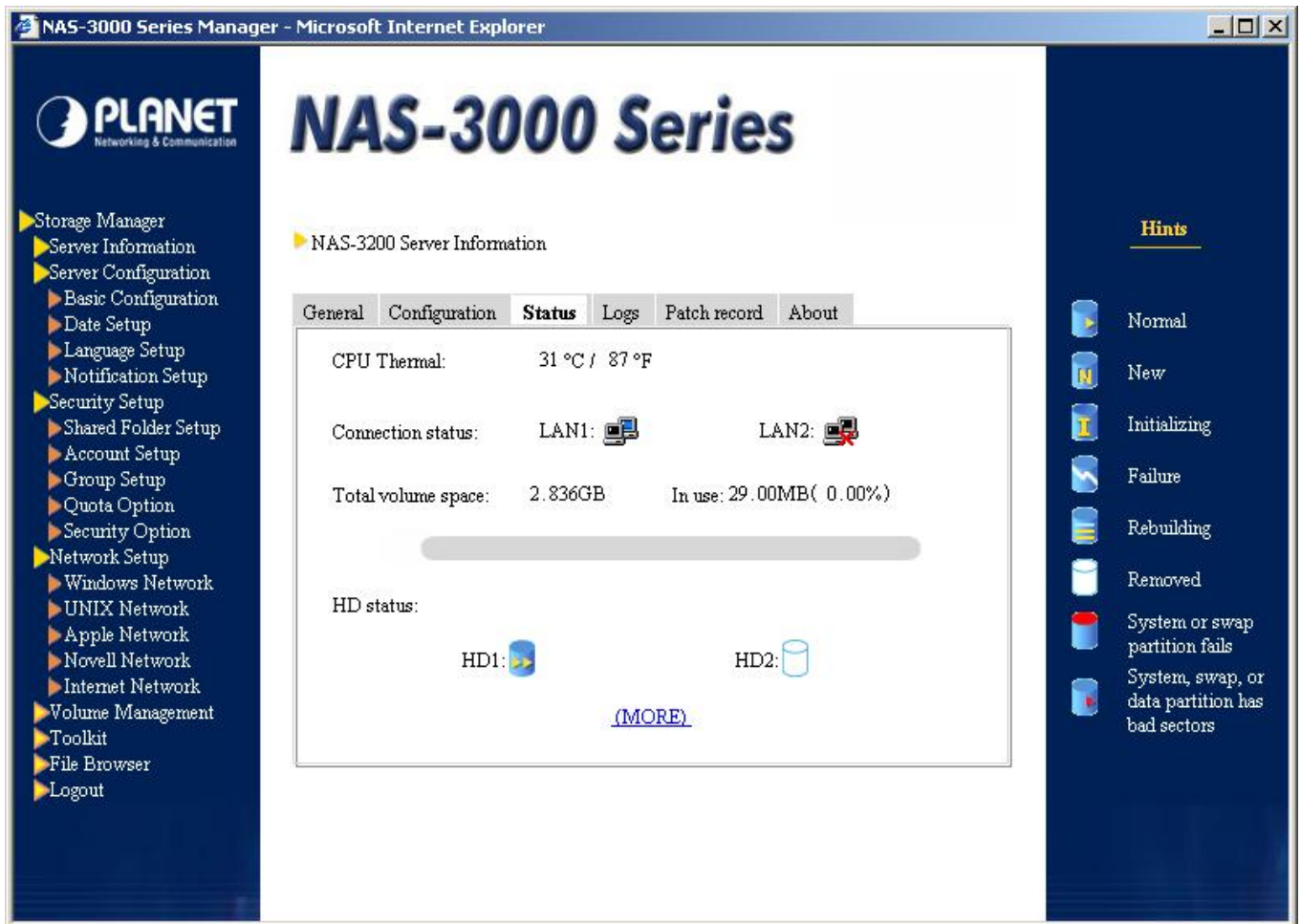
Moreover, when the hard disk is at "Damages in system area" or "With bad sectors" status, you can check the bad sector details of the hard disk by moving the mouse over the hard disk graphics on this page. When bad sectors occur on the hard disk, the NAS server provides a Dynamic Bad Sector Recovery (DBSR) mechanism by reserving a space on each partition of the hard disk for mapping bad sectors when bad sectors are used and recovering data in the future, so the file can be protected against access failure.

    i. Bad sector mapping: If a HDD bad sector is used when writing data to an existing volume, the bad sector will be automatically mapped to the reserved space. Any request for the data in the future will be redirected to the mapped space.

    ii. Bad sector recovery: On a RAID1 volume, if a HDD bad sector occurs on an existing data entry, when reading the data, the system will still generate the correct data by calculating the RAID1 consistency and map the data to a reserved space. Any request for the data in the future will be redirected to the mapped space.

Icon description:

 The disk is normally operating.

 The disk is newly added to NAS server.

 The NAS server is initialing the disk.

 The disk is failed and needs to be replaced.

 The NAS server is rebuilding the disk.

 The disk is removed.

 The system or swap partition fails.

 There are bad sectors in the disk.

System log tab

Shows the system log, connection log and current connection log.
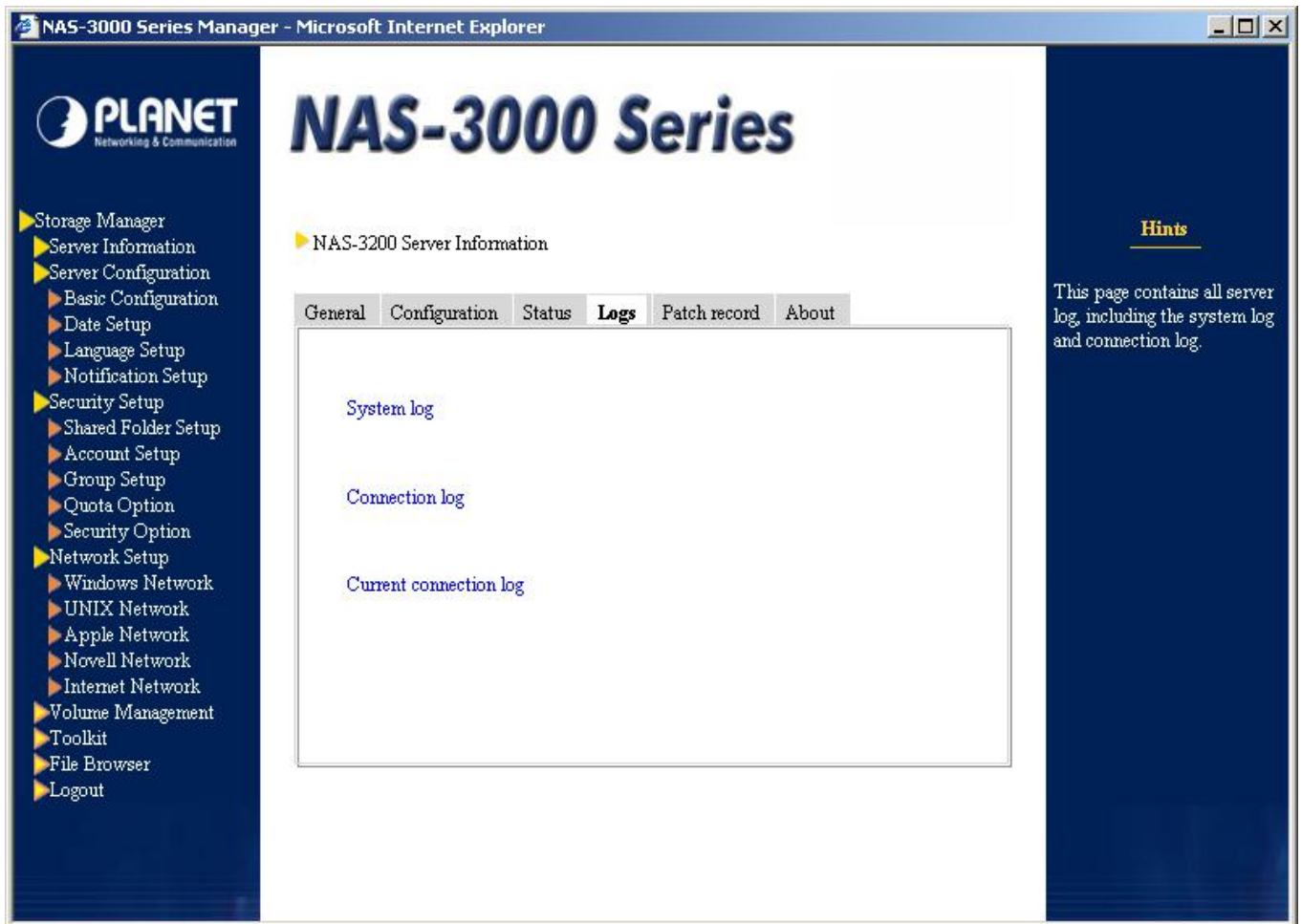
Patch record tab

This page allows you to review the patched programs and version information for the server.
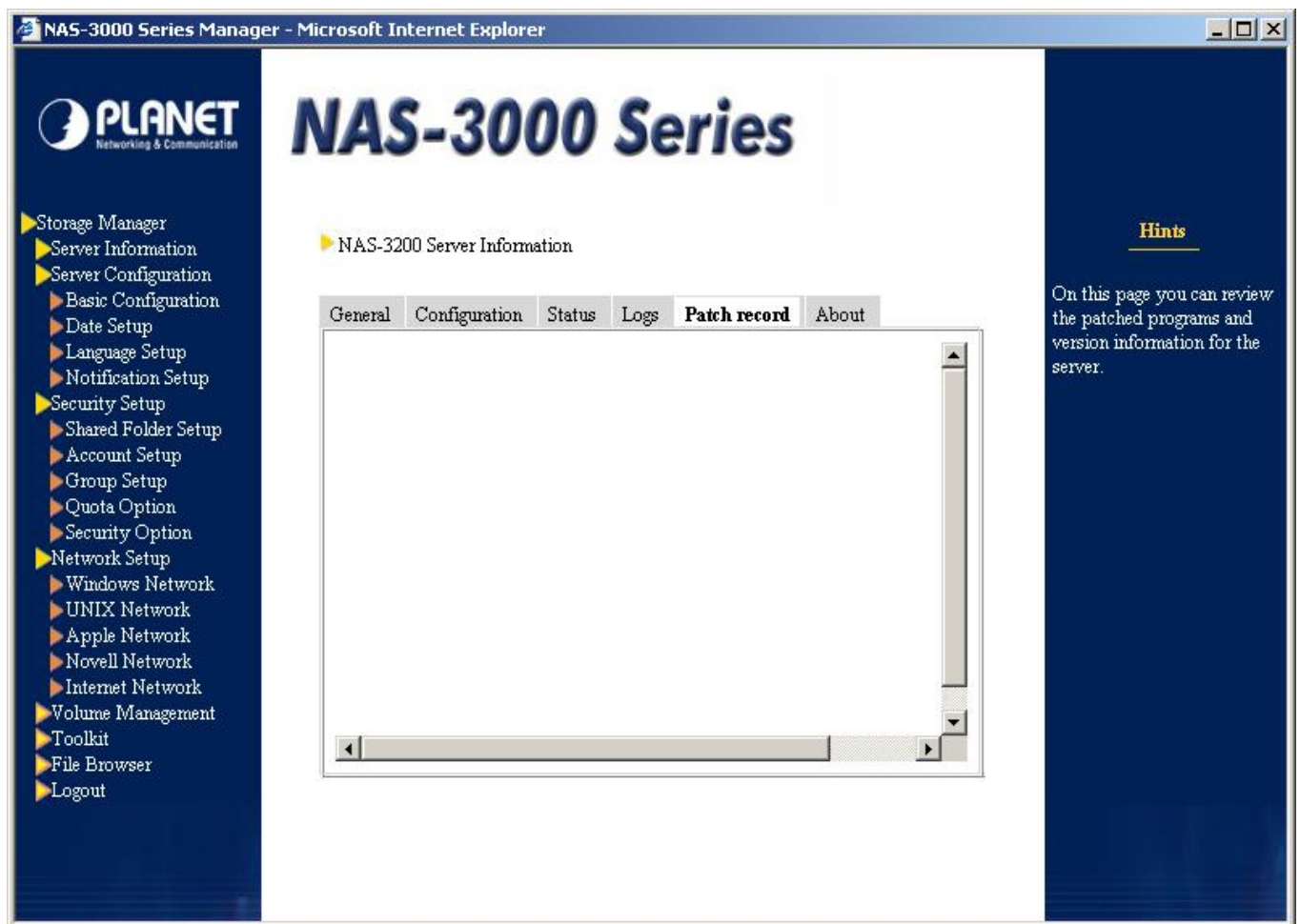
4.2 Server Configuration

4.2.1 Basic Configuration

General tab

System administrator can change the server name here and further configure the network settings. Please note that the server name must be unique, meaning that no other server in the network should have the same name. The name is not case-sensitive and cannot exceed 15 characters. The first character must be a letter; the other characters can be letters, numbers, the underscore or minus sign.

This system supports up to four domain names and three DNS servers. The length of the domain name cannot exceed 64 characters. If the existing DHCP server has already created multiple domain names and DNS server setup while NAS server obtains its network settings from DHCP server, this page will capture the first item from the DHCP server. The system administrator must specify other items manually.

LAN Port 1 tab

If the LAN includes a DHCP server, click "Get network configuration through DHCP". Otherwise, choose "Use manual configuration", and fill out the related settings. Filling out the column with a red star sign on the right is mandatory, while filling out the column with the orange star is recommend by the system.

LAN Port 2 tab
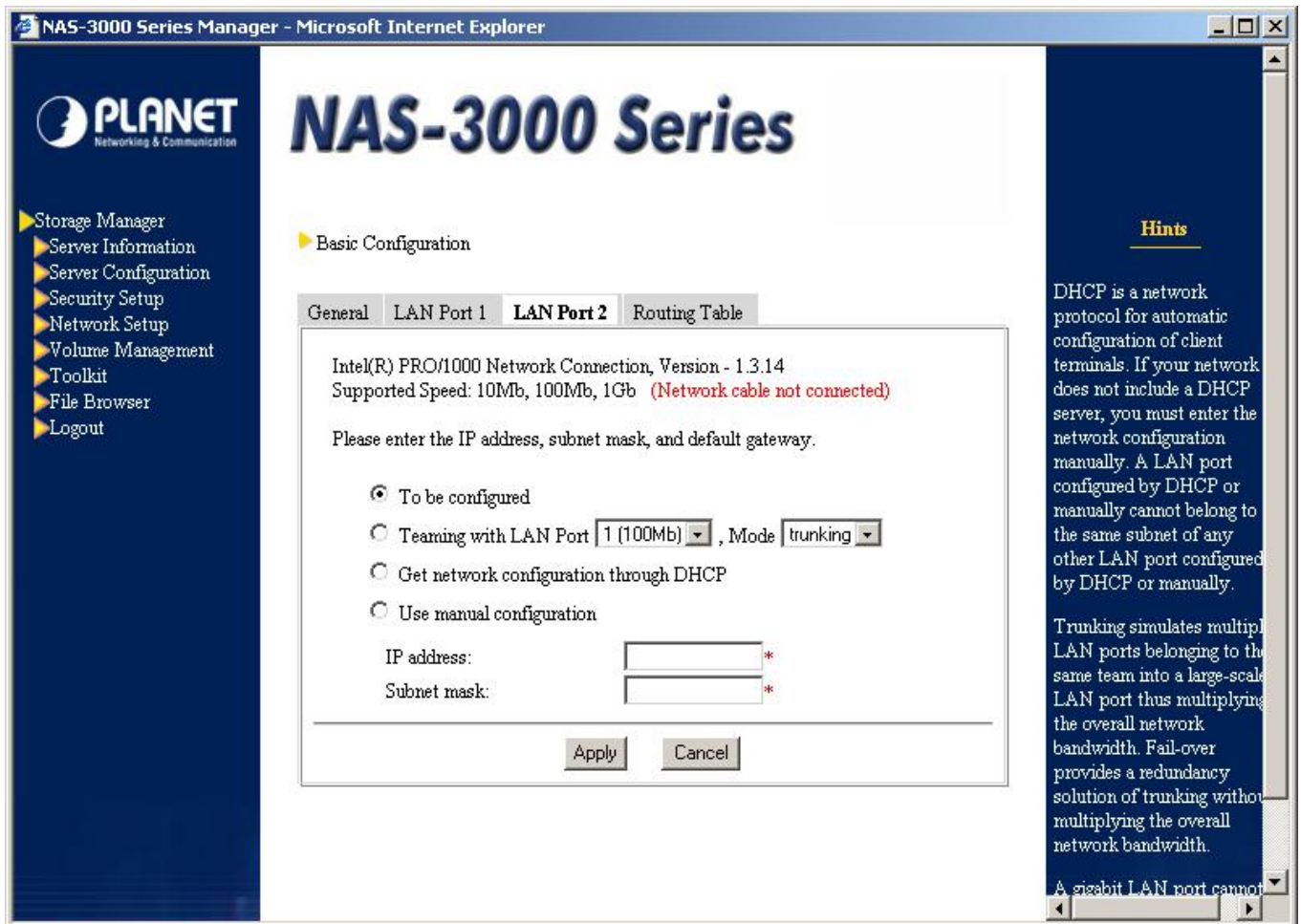
There are two available teaming modes can be configured in NAS-3000 Series Manager: trunking and fail-over. But NAS-3200 and NAS-3400 only support fail-over mode because a gigabit LAN port cannot trunk with a non-gigabit port.

The "Fail-over" mode provides a redundancy solution. Should any LAN port fail, the other port in the same team would take over its job and continue to provide services. Multiple network adapters with different bandwidths can be teamed as "Fail-over". In this case the network adapter with larger bandwidth will be used as the master network adapter. When the master network adapter fails, the other network adapter will take over the service.

Or, if a network has more than two subnets, system administrator can setup each network card separately into different subnet IP address to achieve the "Load Balancing" effect.

Note: If the two LAN ports are not configured in "Fail-over" mode, you must assign two IP addresses in different subnet to the cards respectively, thus when choosing network type through DHCP, please make sure if the subnet has any DHCP server available for use.

Routing table tab
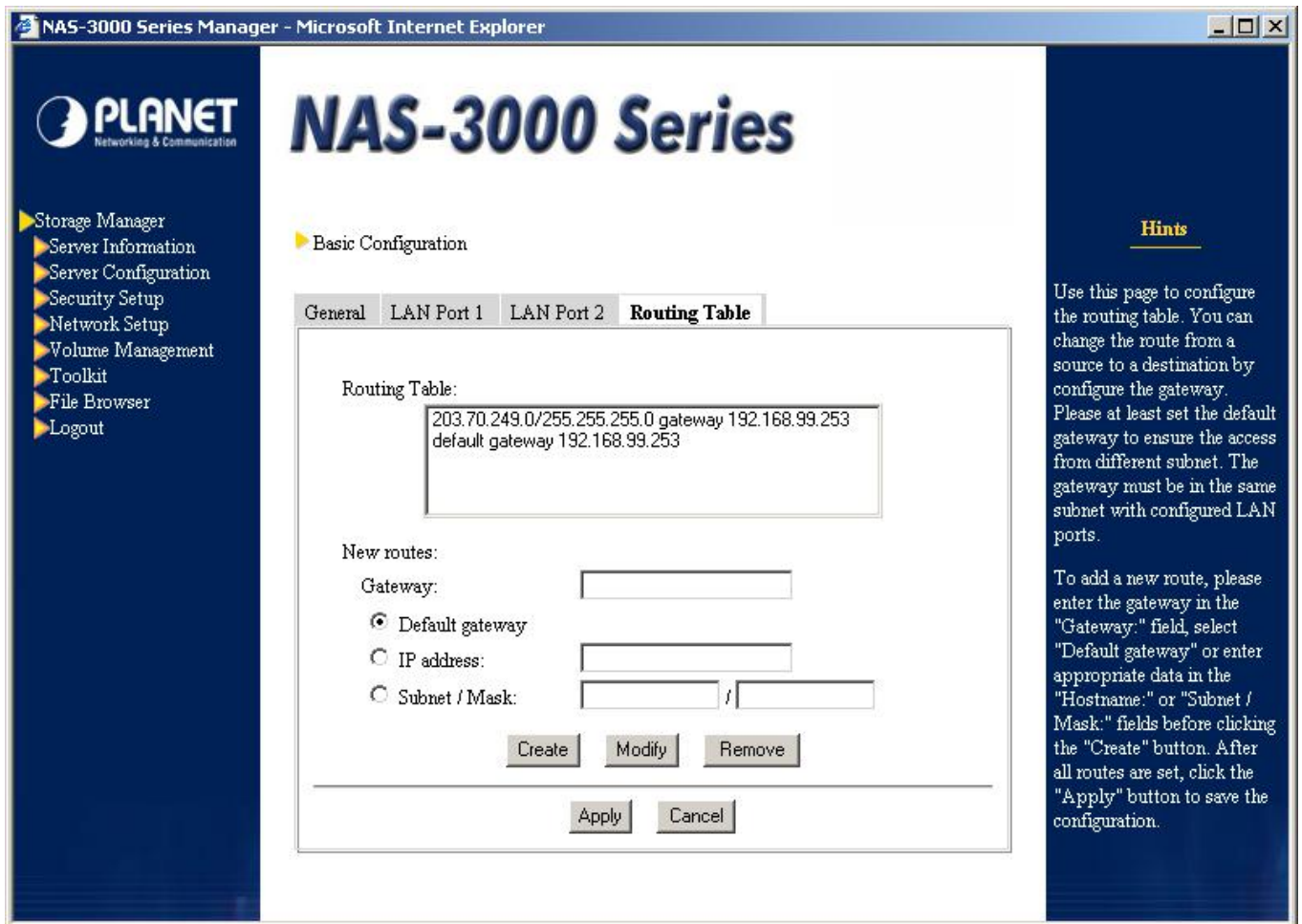
Use this page to configure the routing table. To add a new route, please enter the gateway in the "Gateway" field. You can select "Default gateway" or enter appropriate data in the "IP address" or "Subnet/Mask" fields, then click "Create" button. After finish adding all route records, click "Apply" button to save the configuration.

4.2.2 Date Setup

Use a 24-hour format to enter the system date and time, as well as the correct time zone. The NAS server will automatically adjust itself if daytime saving time (DST) is applicable to the selected time zone. There is no need for extra setup.

To activate network time synchronization, please choose "Enable network time synchronization", in the "Period" pull down menu, choose the appropriate period, and then fill out the hostname or IP in the Primary time server field. If a spare time server is available, fill out its hostname or IP in the Secondary time server field. When the primary time server is failed, the NAS server will try to synchronize the time with the secondary time server.

4.2.3 Language Setup

You can perform all the language settings on this page. Please choose a display language for NAS-3000 Series Manager, event notification emails, and the code page for different kinds of client.

In Display Language column, when selecting Browser Default Language, NAS-3000 Series Manager will automatically display the same language as the browser of the client when system administrator or general user is connected to NAS-3000 Series Manager.

For some languages at least 2 sorting methods are available for the administrator to choose. The sorting method is used to sort information on NAS-3000 Series Manager, such as shared folders and user accounts. The sorting method can be chosen from the "Sort by:" pull-down menu.

Encoding for Windows/ Apple/ Novell will be applied for the three clients, and allow them to access the server correctly with the defined encoding when Unicode is not available. After selecting the encoding for Windows/ Apple/ Novell, please select the appropriate encoding for NFS clients under the same locale language.

Once Quick Configuration is complete, NAS-3000 Series Manager will use that language. If you do not know the correct code page of your Windows client, enter the command "chcp" in the command prompt and press Enter to retrieve the correct code page information.

Note:

1. Inconsistent codepage settings between the system and the clients will result in incorrect display on accessing the data. The system codepage must be the same with that of the clients.

2. If the administrator set a single-byte language (code page), such as English, for Windows clients, an error will occur when the client attempts to save double-byte files or folder names (e.g. Traditional Chinese) on the NAS server, and some files cannot be deleted once saved. In this case, the system administrator must use the Server Configuration à Language Setup to change the code page to double-byte encoding; only then can the file be properly accessed and deleted.

4.2.4 Notification Setup

NAS server can notify the system administrator of important events via e-mail. Enter a SMTP server and the primary e-mail address 1. When an important event occurs, the system administrators will be informed via e-mail and can respond immediately, thus ensuring system safety. You have the option to send a test message after setup to make sure you have entered a valid configuration.

Due to the excessive amount of junk mail pervading the Internet, many providers do not allow their SMTP servers to be used by outside users. We therefore strongly recommend using the SMTP server of your e-mail domain (the address 1, address 2). E.g., if you use root@abc.com, select the SMTP server belonging to this provider, for example mail.abc.com.

Note: if you enter the host name (e.g. mail.abc.com) of the SMTP server, instead of the IP address (e.g. 192.168.1.1), please also enter the DNS address to ensure the notification emails can be sent to administrators.

4.3 Security Setup

In this section, the administrator can define users and user groups to access certain files and folders on the NAS server.

4.3.1 Shared Folder Setup

Shared Folder tab
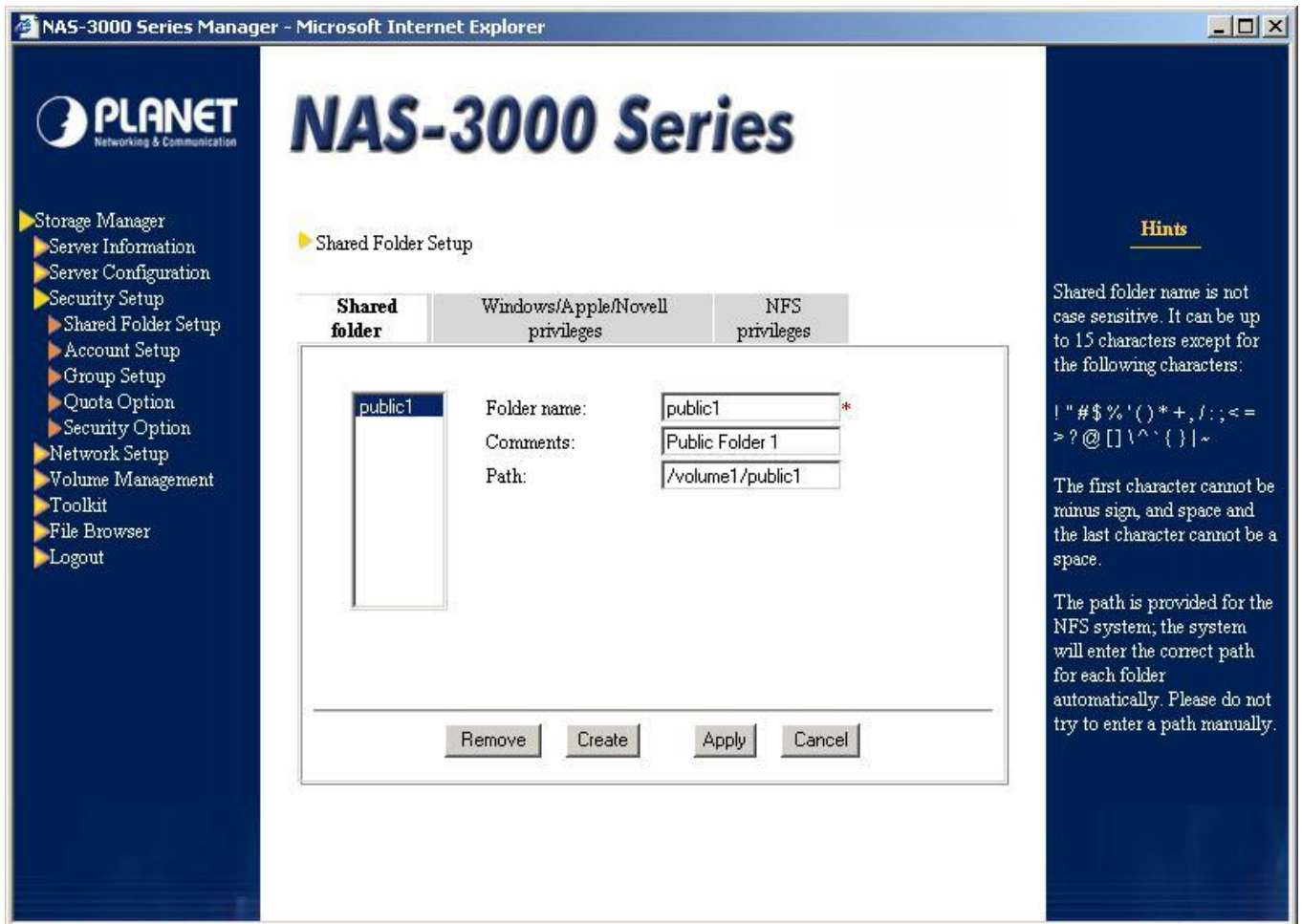
The administrator can use this option to add, modify or delete shared folders and select whether folders can be exported via NFS to allow UNIX access only.

Shared folder name is not case sensitive. It can be up to 15 characters except for the following characters:

! " # $ % ' ( ) * + , / : ; < = > ? @ [ ] \ ^ ` { } | ~!

Besides, the first character cannot be minus sign, and space; the last character cannot be space.

Note: NAS server allows up to 32 shared folders, not including the home folders of "users" group accounts.

The option "Path" is only available for NFS and cannot be edited manually. The system will automatically enter the path "/volume*n*/Shared_Folder_Name" for each shared folder on the NAS server. For example, if you create a shared folder called "test" on a volume on the NAS server, the system will automatically assign the path "/volume1/test". The administrator cannot change this default value.

Once the shared folder is created, the system administrator must use the "Windows/Apple/Novell

Privileges" or "NFS Privileges" tabs to choose users and their access privileges. All files stored in the shared folder will have the same privileges.

Default shared folders

By default, NAS-3000 Series Manager will create a shared folder named "publicn" on each individual volume, whereas n represents the disk volume. For example, if there are 2 volumes on a NAS server, the folders will be named "public1", and "public2" respectively. However, if system administrator segments the storage space into multiple volumes, then the system will automatically create a "publicn" shared folder for each volume.

The name, description, and path of this folder (/volumen/publicn) cannot be changed by the administrator. By default, any user logged into the NAS server has full read/write access privileges to this public folder. System administrator can change the user access rights of this shared folder through "Windows/Apple/Novell privileges" or "NFS privileges" tabs.

Adding a shared folder

To add a folder, please follow the steps:

1. Click on "Create". The "New Shared Folder Setup" page will appear.
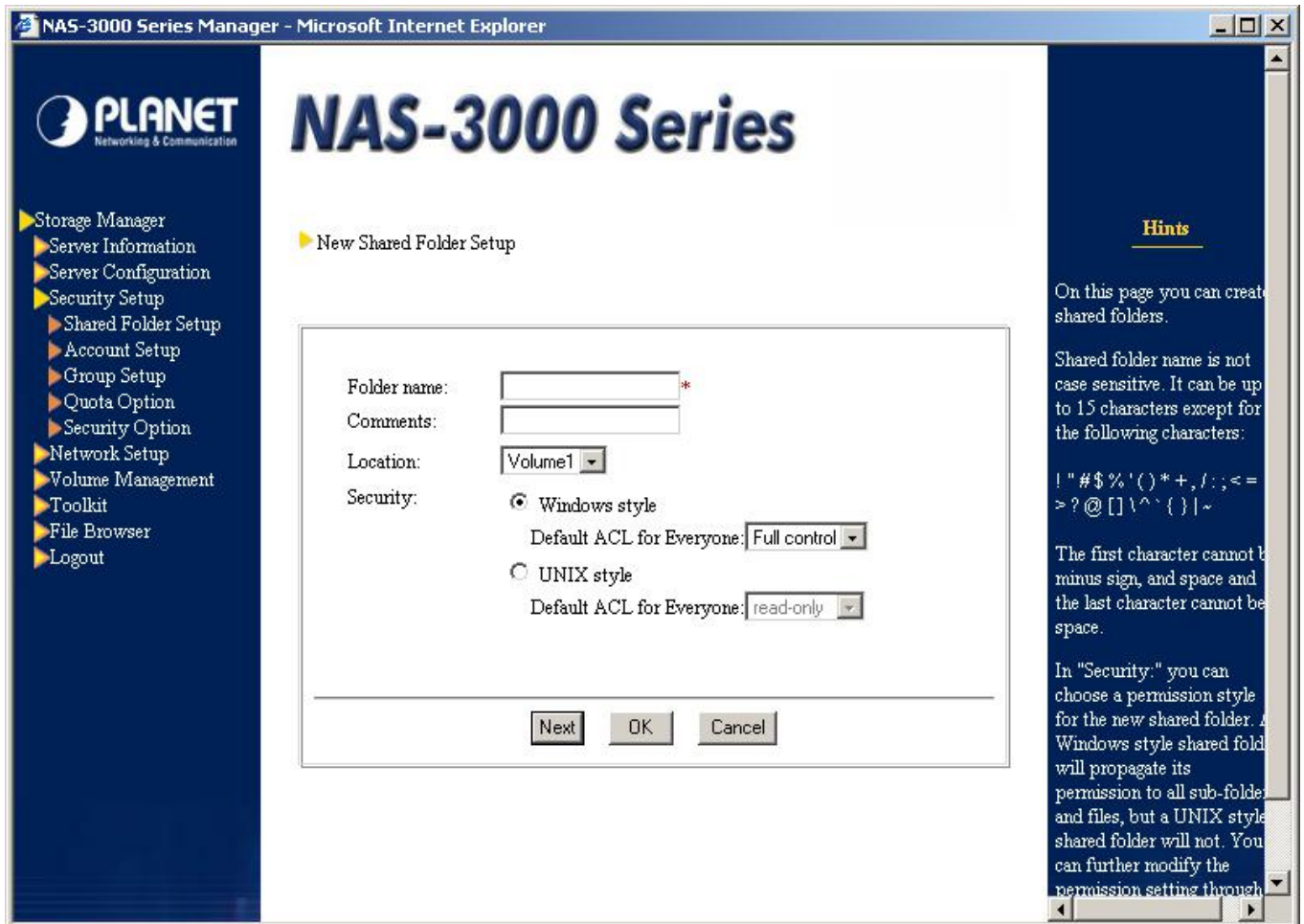
2. Enter "Folder name" and "Comments" fields for the folder.

3. Select a proper location from "Location" drop down menu to place this folder.

4. Choose a permission style for this new shared folder in "Security" field.

5. Click on "OK" to complete the configuration, or click on "Next" to add another new shared folder.

After the shared folder is setup, it does not matter if the shared folder is Window compatible or UNIX compatible. All the users with proper privileges can press the right button on the shared folder under Windows' network neighborhood to reset the privileges.

Note: When Windows 98 clients connect to the NAS server through Windows "My Network Places" or the Mac OS X clients through "Samba", they can only access shared folders with folder name as many as 12 characters. Thus when sharing with these clients, the length of the shared folders' name should not exceed 12 characters.

Modifying a shared folder

Click on a existing folder name to display the information pertaining to this folder in the right windowpane. To rename the folder or modify its description, make the necessary changes on the right and then click "Apply".

Deleting a shared folder

To delete a shared folder, select the desired folder (use Ctrl for multiple and Shift for continuous selection) in the list on the left pane, then click "Remove". The default shared folders "publicn" cannot be deleted.

Windows/ Apple/ Novell User Privileges tab
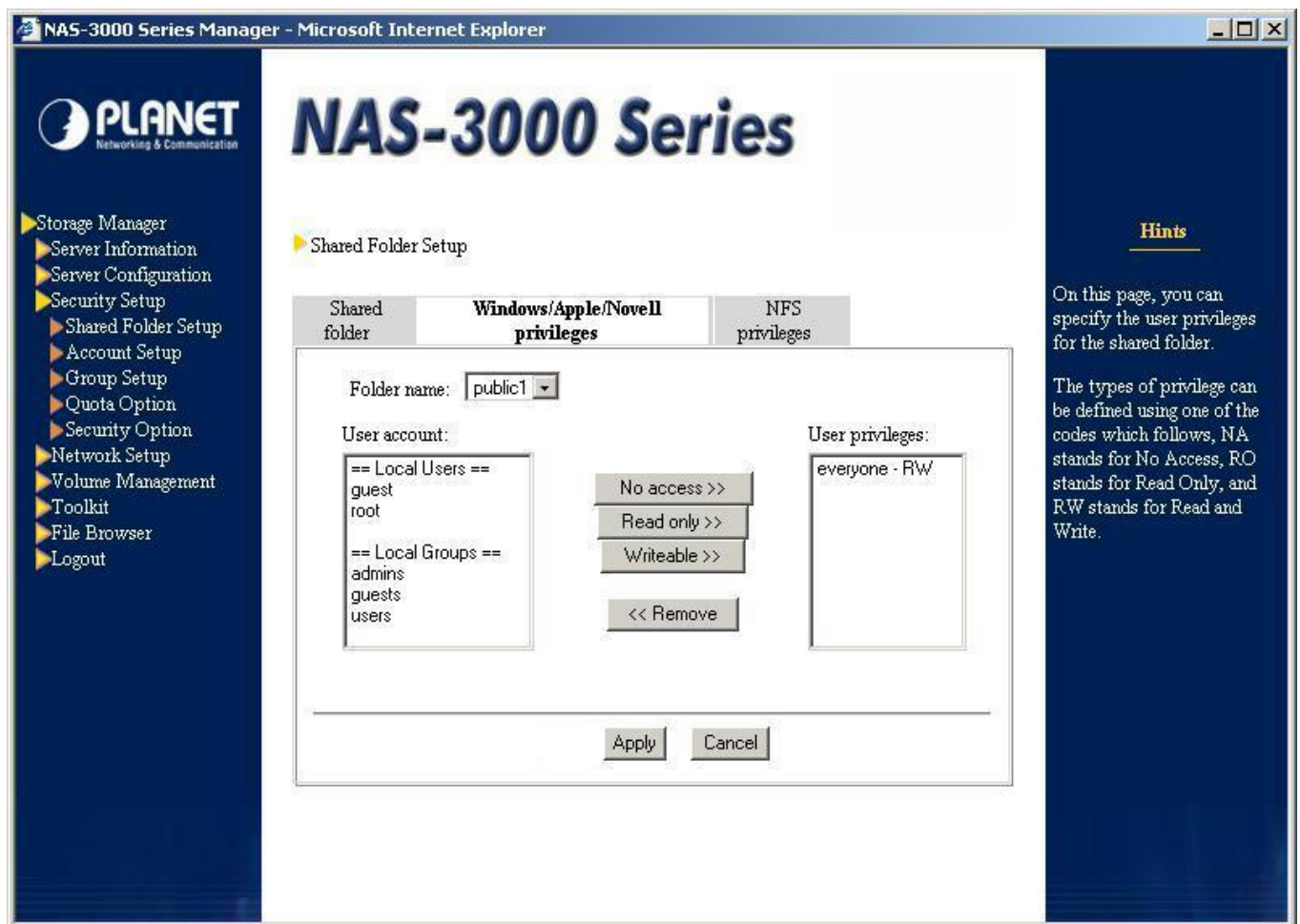
The system administrator can use this page to assign access privileges for local users/groups (i.e. Windows/Apple/Novell clients with accounts on the NAS server) and Windows domain users/groups. Use the drop down menu to choose a folder in the "Folder name" list, the "User privileges" column will show all the users or groups entitled to access the selected folder.

Note: Mac and Windows clients can share the same folder. However, since Mac and Windows systems handle file associates in different ways, the access to the files supported by both Mac and Windows systems such as "pdf" and "html" may be restricted.

For example, when a Windows client saves an html file to the NAS server, a Mac client cannot double-click this file on the server to open the file by automatically launching the web browser. Because the way Windows system saves "Associated file type" differs from that of Mac, Mac system does not know with what program it can open the html file created in Windows.

There are two solutions for it:

1. Re-establish the associate of this file on the Mac client.

2. Launch the program used for executing the file on the Mac client first. In this case launch IE or Netscape and then open the file with the browser. Alternatively, use "save as" to save the file on the Mac client so that the new file will be saved in the Mac format. To open the file, simply double-click it.

When the Windows client cannot directly execute files saved by the Mac client, the same solution can also be applied.

Modifying User Privileges

To change existing user privileges, e.g. from "Writeable" to "Read only", select the user whose privileges you wish to change in the "User privileges" column, then select "Read only" in the center column, and click "Apply" to confirm your selection.

Adding user privileges

To add user or group privileges under a particular folder, please follow the steps:

1. Select a user or user group in the "User account:" column (use Ctrl for multiple and Shift for continuous selection).

2. Click on "No access", "Read Only" or **"Writeable"**.

3. Press "Apply" to complete.

Note: if this NAS server is added to the Windows domain, and (1) system administrator has previously added certain Windows domain user account to Local account or (2) there is an account in both NAS server and Windows domain with the same name, then the users account list on the left will not show the account number in NT Domain Users but only in Local Users to prevent system administrator from confusion caused repeated setup of access rights for the same user.

Deleting User Privileges

To delete user or group privileges, please follow the steps:

1. Use the mouse to select a user or user group in the "User privileges" column (use Ctrl for multiple and Shift for continuous selection).

2. Then click "Remove".

3. Press "Apply" to complete.

Note:

1. When setting Windows/Novell/Apple user privileges for the shared folders, make sure to avoid possible conflicts. Root, for example, is a member of the admins group. To avoid conflicts, you must not set the privileges for root to read only, while admins is set to writeable.

   In the event of conflicts in access privileges, the system will authorize users/groups in the following order: no access (N/A), readable and writeable (RW) and read-only (RO). For example, if the access privilege of the root account (belonging to the admins group) is set as "N/A" and that of the admins groups is "RW," the access privilege of root for this folder will be "N/A." If the privilege for everyone is set to writeable and the user root to read only, the system will assign writeable privileges to everyone as soon as you click "Apply".

2. The NAS server supports the ACL (Access Control List), i.e. users can click the right mouse button on a file and set the access privilege. Please refer to the last section of this chapter Using Access Control List (ACL) for details.

The system administrator can use NAS-3000 Series Manager's Security Setupà Shared Folder Setup page to set the access privileges for every shared folder.

NFS Privileges tab
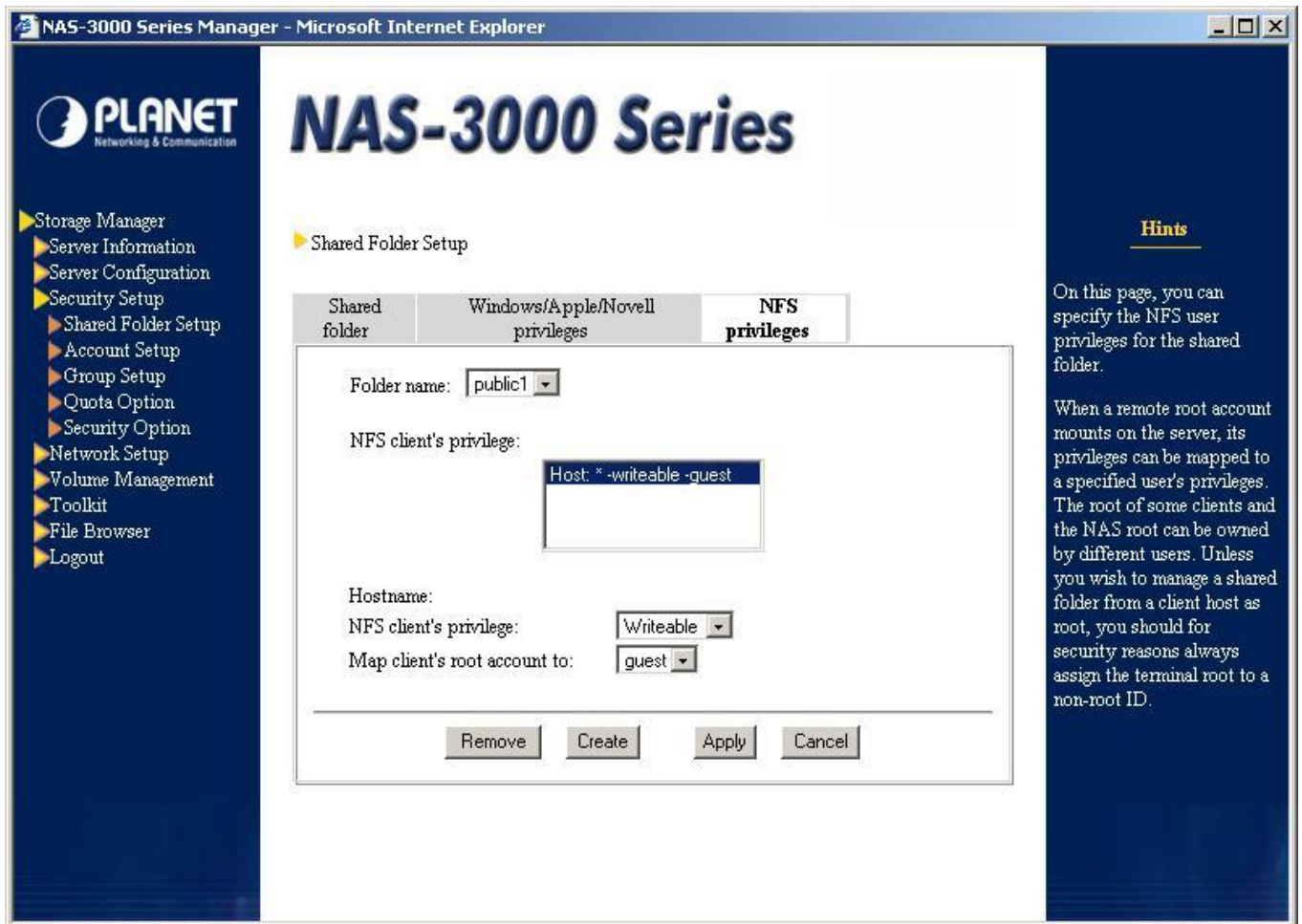
Use this option to set NFS (Solaris, FreeBSD or Linux and other UNIX family clients) access privileges for shared folders.

Enter the Shared Folder Setup à NFS Privileges page, and select the desired shared folder in the Folder name column. The NFS client's privilege column below will show the hosts and subnets or net groups with access privileges and the type of permission granted.

NFS client's privilege consists of three components:

1. The first component is the subject sharing a folder, either a host, subnet, or a net group. The entry Host:* means the folder is shared between all hosts.

2. The second component is the share mode, such as read only or writeable.

3. The third element is a local user name. The administrator root of a NFS client can only access the folder with this ID.

The root of some clients and the NAS root can be owned by different users. Unless you wish to manage a shared folder from a client terminal as root, you should always assign the terminal root to a non-root ID for security reasons.

Adding NFS user privileges

To add NFS user privilege settings, click on "Create". A new page will appear. Enter the "hostname", "subnet mask" (e.g. 192.168.1.0 / 255.255.255.0), or "net group" (only available if the NAS server joins the NIS domain). Under "Map client's root account to" column, choose a local user, and then set the "NFS client's privilege" to read only or writeable. Click "OK" to confirm your selection and return to the previous page, or click "Next" to add another client.

Note:

When setting user privileges for the NFS hosts, subnets or net groups, try to avoid possible conflicts. E.g., if host A belongs to net group AAA, do not set the access privilege of host A to read only while setting AAA to writeable.

Conflicts will be dealt with in the following manner:

1. If a single host setting conflicts with Host*, the single host setting is used.

2. If a single host setting conflicts with the subnet setting, the single host setting is used.

3. When a single host setting conflicts with a net group, the entity which first received its user privilege has priority. If the net group AAA has already been set to writeable, you cannot later set the single host A to read only.

Deleting NFS User Privileges

To delete the user privileges of a NFS client, select the desired item on "NFS client's privilege" column (use Ctrl for multiple and Shift for continuous selection), and click "Remove".

Modifying NFS User Privileges

To modify existing privileges, select the desired item on "NFS client's privilege" column, remove it and add a new privilege.

4.3.2 Account Setup

The NAS server supports up to 20480 user accounts (Including accounts on the local machine, Windows, and NIS server). Three types of users can access a NAS server:

1. Local users, with an account on the local machine.

2. Users with Windows domain or Active Directory accounts

3. Users with accounts on a UNIX NIS server

Local Accounts tab
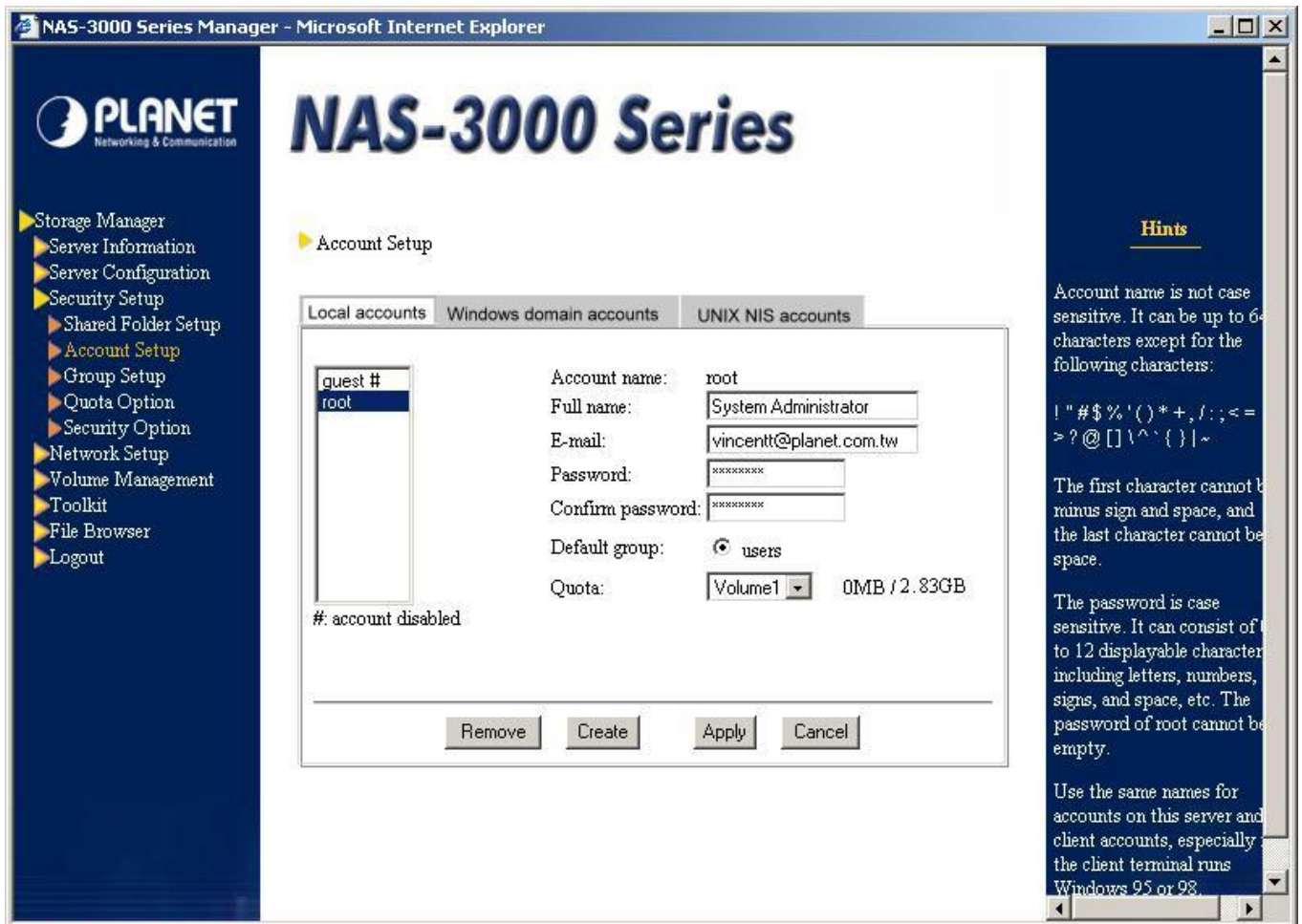
The system administrator can setup accounts for Windows, Mac and Novell users on the NAS server (the local machine). When these clients attempt to access the NAS server, they only need to enter their account name and password to gain access.

The system administrator can add, modify and delete user accounts. Account name is not case sensitive. It can be up to 64 characters except for the following characters:

! " # $ % ' ( ) * + , / : ; < = > ? @ [ ] \ ^ ` { } | ~

Besides, the first character cannot be minus sign and space, and the last character cannot be space. The password is case-sensitive and can consist of 0 to 12 displayable characters, including letters, numbers, signs, and spaces.

Note:

The passwords for some clients, such as Windows 98 clients and Novell clients, are not case-sensitive while the passwords for other clients, such as Win NT/2000, UNIX, and Mac clients are. Therefore, please make sure the account passwords for the local machines are case-sensitive so that they will be suitable for all clients

Mac clients only allow passwords of up to 8 characters. Thus, when setting passwords for Mac

clients on the NAS server, please limit the length of passwords to 8 characters or less.

Default local accounts

There are two preset accounts on the server: *root* and *guest.*

1. *root*: This is the default account for the system administrator and belongs to both the *admins* and *users* group. As a first step in the server setup, please setup a password for this account.

2. *guest*: This open account belongs to the *guests* group and has no password and quota restriction by default. Its purpose is to give access to all users on the LAN, so that they may access the NAS server's guest folders, such as public*n*. For the unauthorized Windows 98 clients, the system will automatically connect them to server with the account *guest*. For other Windows NT/2000/XP, Novell and Mac clients, users can enter *guest* as the user name (no password is needed) to connect to the server..

However, due to security reasons, the system administrator might not want all unauthorized users, e.g. users without an account on the NAS server or other account servers on the same LAN, to access the shared folders of the NAS server. By adding a password to the guest account, unrestricted access is disabled.

Note: Account server, e.g. a Windows domain controller on an NT domain, Windows 2000 Active Directory Service or a NIS server on a UNIX domain.

Adding user accounts

To add a new local user, click "Create". The "New Account Setup" dialog appears. Enter the "account name", the "full name" of the user, an e-mail address and a password. Under "Default group", select whether the user will receive his/her own home folder. If yes, select the "users" group; if no, select "guests".

After a new account has been created under "users" group, the system will set up a home folder named "home" for this account. Only the user can access his home folder. If a Windows client accesses the NAS server through the Network Neighborhood, he will see a folder named "home." The user has full read and write privileges to that folder. When the system has more than one volume, system administrator must specify in which volume to store the home folder of this account in the "User home volume". The default location can be setup in the "Security Option" page. System administrator can also change it.

The system administrator can proceed to setup the disk quota for each account. The default quota for newly created user specified in the "Security Option" page will be displayed here. Please change it according to your own need. Please note the disk quota will be applied to every volume. This means that if there are three volumes in the NAS server, and system administrator grants 100MB quota to a user, this user will have 100MB quota of storage space in each volume, and totally 300 MB quota on the NAS server.

Note:

If the quota set by the administrator for a new account differs from the default quota granted to the user in the "Default Privilege Settings" page, the user quota on future created volumes will be based on that in the "Default Privilege Settings" page. Thus the administrator must change the quota manually.

The preset value for the guest and root accounts is unrestricted. If, for security reasons, the administrator wishes to restrict disk quota for guest users without proper accounts on the NAS server or any account server, simply setup a quota for the guest account in the Security Setupà Quota Option page. The system administrator can also use this page to change the quota of each account or specify quota in each volume of a user in a flexible way. .

When a Windows NT 4.0/2000, Novell or Mac user accesses the NAS server, the Windows operating system will ask for the NAS server or Windows account and password to confirm his or her identity. In the case of Windows 98, Windows will automatically retrieve the identity of the client and only request a password. If the Windows user account is not the same as the account on the NAS server, the client cannot log in on the server. The system administrator must therefore keep the NAS server accounts and Windows accounts synchronized.

Deleting local users

To delete a local user, simple select the account on the left side (use Ctrl for multiple and Shift for continuous selection), then click "Remove".

Modify user account detail

To modify the details of a user account, select an account from the user list on the left side of the page, make changes on the right, and click the "Apply" button below.

Windows Domain Accounts tab
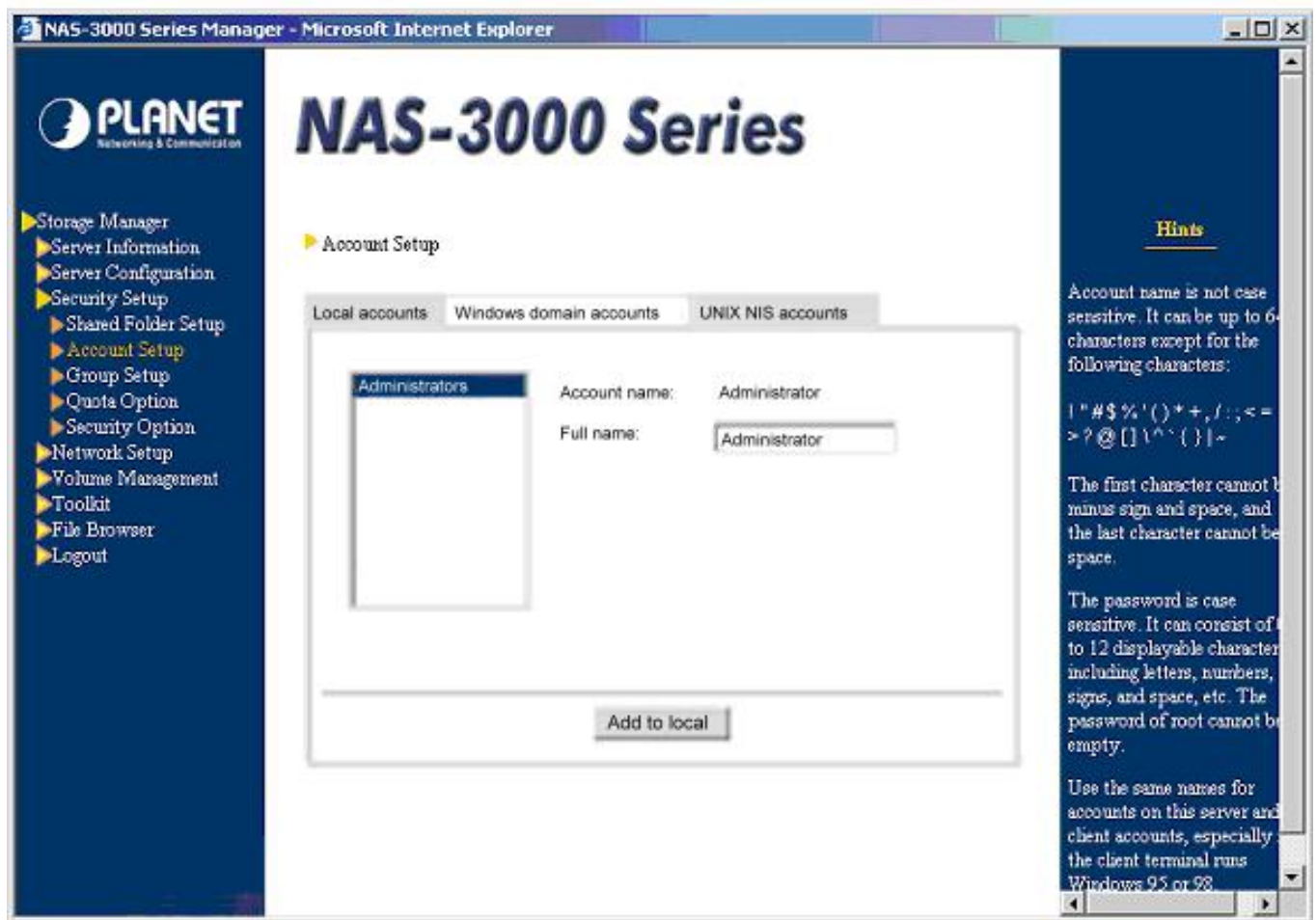
If a Windows domain exists in the network, the system administrator only has to add the NAS server to the Windows domain to take advantage of the Windows domain controller privilege settings and grant all accounts on the Windows domain access right to the NAS server's storage space. When these clients need to access the server, they can do so by entering their Windows domain account name and password.

Once the NAS server is joining into a Windows domain, a new tab called "Windows domain accounts" will become available on this page, containing a copy of all user accounts. Only the account names will be copied here, without passwords and other information. When a client attempts to access the NAS server, the server will forward the account and password information to the Windows domain for verification. If the user passes the authentication, access will be granted. If the Windows domain controller does not authorize the user, the account is verified against the list of local users. Access is granted, if the login data corresponds to a local user. If a user has an account "user1" on both the Windows domain and the NAS server, but with different passwords, access is granted if either one of the two passwords is provided. The system administrator should, however, avoid allowing accounts existing on the Windows domain to be created on the NAS server. A situation where different users share the same account name should also be avoided.

The NAS server will read the Windows domain account list every 60 minutes; any changes on the

Windows domain will also appear on the NAS server.

By default, Windows domain accounts do not have home folders. If you wish to assign a home folder to this type of account, simply select the desired account on the left (use Ctrl for multiple and Shift for continuous selection), then click on "Add to local". The selected accounts will appear in the list of local users. By default, they are part of the "guests" group. First setup the passwords for the accounts, then transfer these accounts from the "guests" group to the "users" group, and select the "User home volume" location.

Additionally, Windows domain account will directly apply the default settings for all newly created users defined in "Security Option". The system administrator can setup hard disk quota for each individual NT domain account in "Quota Option".

Note:

1. For security reasons, the Windows domain does not allow other domains to retrieve the user passwords on it; when the account information in the "Windows domain accounts" tab are added to the "local accounts", the system will not able to duplicate the user passwords on Windows domain directly to the local machine. The system administrator will have to add passwords for these accounts on the "Local accounts" tab manually. Therefore, please set the same passwords here as the ones on Windows domain.

2. This system allows group names with a maximum of 15 displayable characters. After having been added to a Windows domain, any group name on the domain with more than 15 characters will not be duplicated by the system onto the NAS server. Only one warning message will be shown and inform the system administrator of all unduplicated accounts. If the NAS server is part of the Windows domain, the system administrator has to avoid adding any group on the domain with a name exceeding 15 characters, otherwise the system will not be able to duplicate this group to the NAS server, nor will a warning message appear.

UNIX NIS Accounts tab
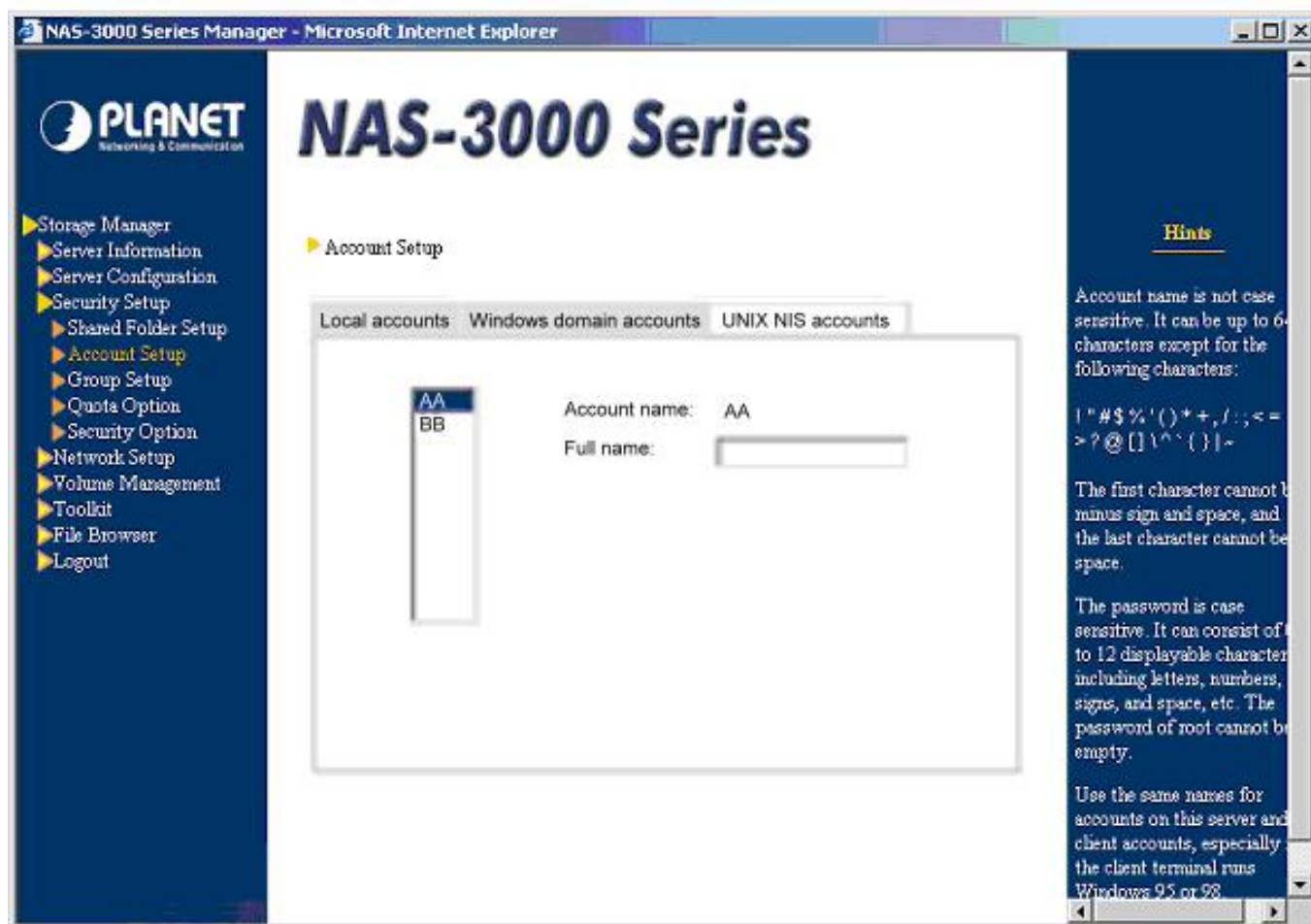
If the network already contains a UNIX NIS domain, the system administrator can simply add the NAS server to the UNIX NIS domain to retrieve access settings from the NIS server.

Once the system administrator adds the NAS server to a UNIX NIS domain (see *Network Setupà UNIX NIS*), a new tab entitled "UNIX NIS Accounts" will appear on this page, containing all the users retrieved from the NIS server. These accounts will directly apply the default quota set up for a new user in the "Security Option" page. The system administrator can also set hard disk quota individually for each NIS domain account in the "Quota Option" page.

When adding new users In some UNIX platforms, the system allows creating an according group with the same name, and since the NAS server only allows up to 1,024 user groups, it is suggested you don't create the according groups when creating new users in the UNIX platform to avoid failure of the NAS server adding to the NIS domain.

4.3.3 Group Setup

User Group tab
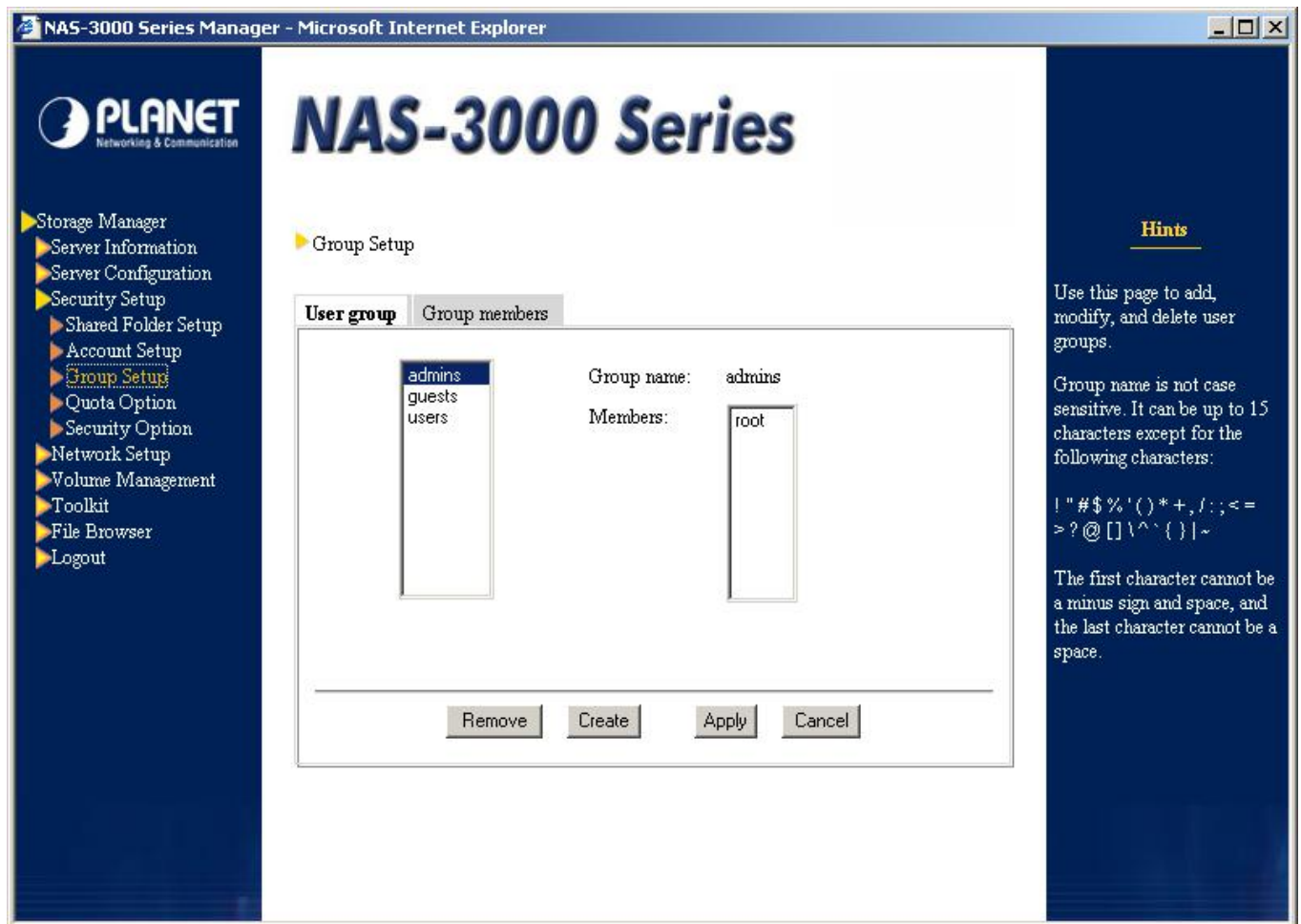
Use this page to add, modify or delete user groups. NAS server allows up to 2048 user groups (including user groups on the local machine, Windows domain and NIS server).

Group name is not case sensitive. It can be up to 15 characters except for the following characters:

! " # $ % ' ( ) * + , / : ; < = > ? @ [ ] \ ^ ` { } | ~

Besides, the first character cannot be minus sign and space, and the last character cannot be spaces.

Default user groups

The system includes three default groups:

1. *admins*: this is the system administrator group. Only members of this group can change system settings. "root" is the default member of this group.

2. *users*: this is the user group. Each member of this group has his/her own home folder. "root" is the default member of this group.

3. guests: unlike the members of the "users" group, those of "guests" do not have their own home folders, instead, they can access the public folders on the NAS server. The account "guest" is the default member of this group.

Note: Users can only belong to either the "users" or the "guests" group, not to both. Suppose a company has two departments A and B. Department A has purchased a NAS server for their employees to store and share information. Part of the space should be made available to department B. In this case, the system administrator can setup accounts for each member of department A and B, then group the department A accounts under "users" and the members of department B under "guests". That way the employees of department A will have their own home folders, while the members of department B will be able to access only those folders for which they have access privileges.

Adding user groups

To add a new group, click *"Create"*. The "New Group Setup" page appears. Enter a name for the group, and select the members of the group in the "Not members" list (use Ctrl for multiple and Shift for continuous selection). Click on "Add" to add the selected members. Select "OK" to confirm the operation, or "Next" to add more groups.

Deleting user groups

To delete a group, select the group in the list (use Ctrl for multiple and Shift for continuous selection), and then click "Remove".

Group members tab
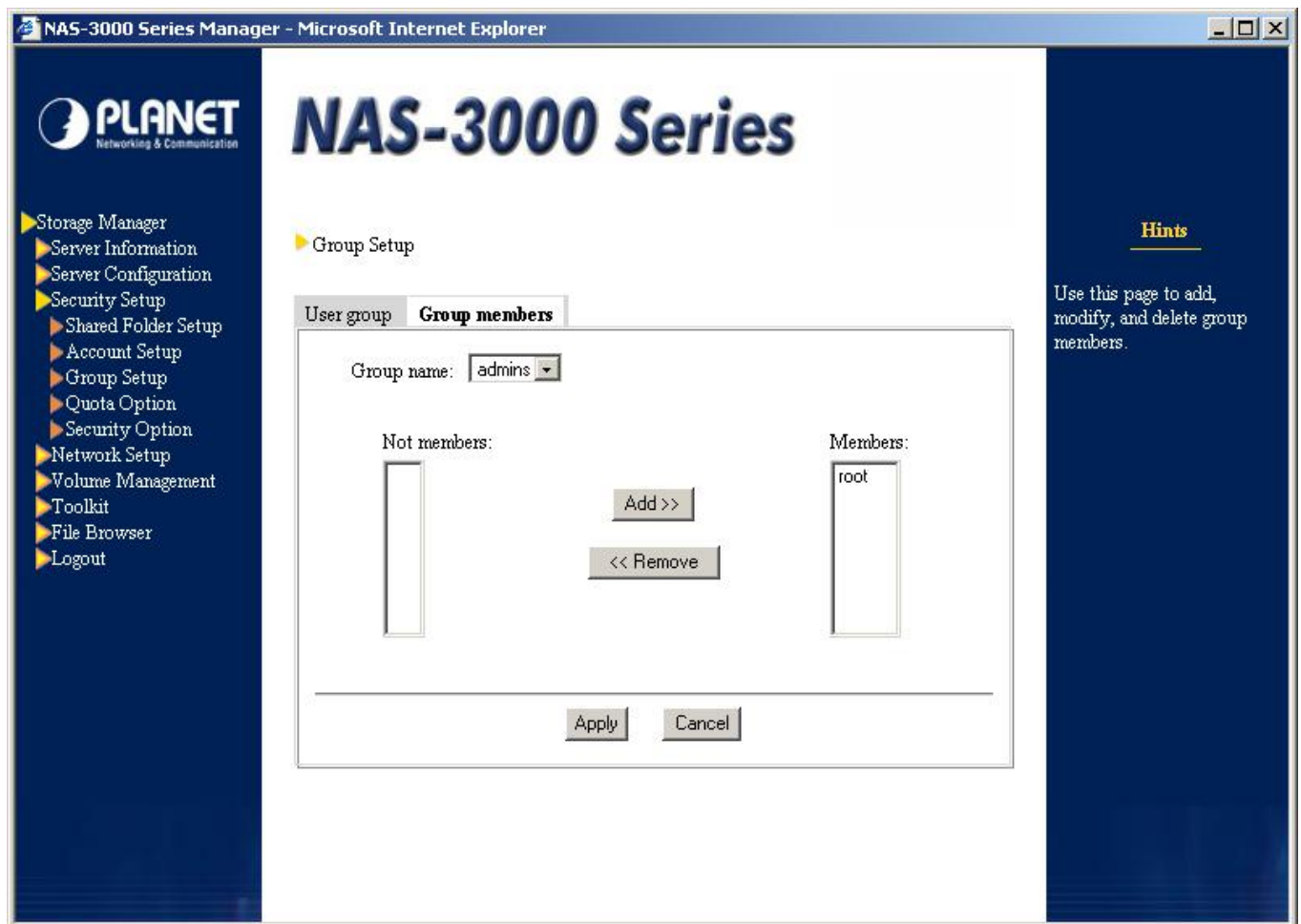
Use this page to add, modify, and delete group members. The "Members" field contains existing members. Users not belonging to this group are listed on the left "Not members" field.

If this NAS server belongs to a Windows domain and (1) the system administrator has previously moved Windows domain users in the "Account Setup" page to the local accounts or (2) both NAS server and Windows domain have the account with the same name, those NT domain users will NOT appear in the list of members but Local Users to avoid multiple selection and assignment to a group of the same user.

Adding group members

To add a new group member, select the target group from the list, and then select the members you wish to add in the "Not members" list (use Ctrl for multiple and Shift for continuous selection). Then click "Add".

Note that all users must belong either to the "users" or the "guests" group. If the system administrator uses this page to move a member from the "guests" group to the "users" group, the account will automatically be removed from the "guests" group, and vice versa. However, accounts belonging to "guests" or "users" group can be assigned to other groups, including the predefined "admins" group, or any other group set up by the administrator.

Deleting group members

To remove a member from a group, select the name from the list of members (use Ctrl for multiple and Shift for continuous selection), then click "Remove".

Note: If a user is connected to the server while the administrator is modifying the user's security settings, these changes will not be applied immediately, but only after the user logs out and back in again.

Moving group members

To move a user account to another group, you should delete this account from the original group and then add it to the new group.

Rules for moving group members as follows:

To: / From:	guests	users	admins
guests		Allowed	Not allowed
Users	Allowed		Allowed
admins	Not allowed	Allowed	

Note: Moving an account from the "users" to the "guests" group will remove the home folder of that account, as well as its data. Be careful in making this change.

Although the "root" account belongs to both the "admins" and the "users" group, there is no home folder for this account. Moreover, the system administrator cannot move "root" account into the "guests" group. The "guest" account can only belong to the "guests" group. The system administrator cannot move it to the "users" or "admins" group.

4.3.4 Quota Option

User quota tab

You can modify user quota on this page.

Please follow the steps below to modify user quota:

1. Select the user account you want to modify in the "User Name:" pull down menu.

2. Select the volume item to be changed in the "Current [In Use/Quota](MB):" list.

3. In "Setting New Quota:" either enter new quota or select "unrestricted."

4. Click the "Set>>" button, and repeat the steps above if there are more than one volume item to setup.

5. If you want to cancel any setting, select the item form the "New Quota(MB):" list, and click the "<<Cancel" button.

6. Click "Apply" to confirm.

Note: The "Current [In Use／Quota] (MB)" list indicates the quota and the space used in each volume by the current account. The symbol "*" in this list means the account is assigned the maximum quota.

Volume quota tab

You can modify user quota in every volume on this page.

Please follow the steps to modify volume quota:

1. Select a volume in the "Volume quota." pull down menu.

2. Select the user account to be modified in the "Current [In Use/Quota](MB):" list.

3. In "Setting New Quota:" either enter new quota or select "unrestricted."

4. Click the "Set>>" button, and repeat the steps above if there are more than one volume item to setup.

5. If you want to cancel any setting, select the item form the "New Quota(MB):" list, and click the "<<Cancel" button.

6. Click "Apply" to confirm.

Note: Please note that the setting will be separated into different pages according to the number of accounts. If the account you are going to perform does not appear on the page, please select the page number at the bottom of the page to go to other page

4.3.5 Security Options

The system administrator can use this page to modify the preferences of newly created shared folders and user accounts.

Default settings for newly created folders

1. Privileges for everyone: ◯ writeable ◯ read-only ◯ no access

   New folders can be exported to Windows/Mac/Novell either with full read and write permissions, i.e. writeable, with write protection, i.e. read-only, or no access right, i.e. no access.

2. NFS exported as: ◯ writeable ◯ read-only ◯ no access

   This setting determines whether NFS users have by default full read and write permissions, i.e. writeable, can only read newly created folders, i.e. read-only, or no access right, i.e. no access.

Default settings for newly created accounts

1. Default group: ◯ users ◯ guests

   Here you can choose to which group newly created users belong by default. If you want new accounts to automatically have a home folder, choose "users", otherwise, choose "guests".

2. Default quota: ◯ [_____] MB ◯ unrestricted

   With this setting you can limit the amount of storage space allotted to new users, or choose not to attach any restrictions, i.e. unrestricted.

3. Default home volume: [Volume   ]

If the newly created account belongs to "Users" group, please select the volume in which its home folder will be saved.

Note: If a user is online, all the user privilege changes under "System privileges setting" will not be effective at once but only after the user has logoff and login again.

4.3.6 Using Access Control List (ACL)

The NAS server allows users of different platforms to access the files simultaneously. However, different platforms themselves have different design of the access right control for files and folders. The ACL implements an appropriate mapping among platforms to provide consistent behavior of file level access control.

Windows mapping table

ACL entry of **NAS server**		Corresponding access right of **Windows**
●: stands for the entry is checked		
Traverse Folder / Execute File	●	Full Control
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	
Write Extended Attributes	●	
Delete Subfolders and Files	●	
Delete	●	
Read Permissions	●	
Change Permissions	●	
Take Ownership	●	
Traverse Folder / Execute File	●	Modify

Permission	Mark	Permission Level
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	
Write Extended Attributes	●	
Delete Subfolders and Files		
Delete	●	
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		Read & Execute
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File		
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		Read
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File		Write
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data	●	
Create Folders / Append Data	●	

Write Attributes	●	
Write Extended Attributes	●	
Delete Subfolders and Files		
Delete		
Read Permissions		
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		List Folder Contents (Folders only)
Write Attributes		
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		

UNIX mapping table

ACL entry of **NAS server**		Corresponding access right of **UNIX**
●: stands for the entry is checked		
▲: only applicable for folders		
Traverse Folder / Execute File	●	
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	7
Write Extended Attributes	●	
Delete Subfolders and Files	●▲	
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File		6
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	

Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	
Write Extended Attributes	●	
Delete Subfolders and Files	●▲	
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		1
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions		
Change Permissions		
Take Ownership		
Traverse Folder / Execute File		
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		4
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File		2
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	
Write Extended Attributes	●	
Delete Subfolders and Files	●▲	
Delete		

Read Permissions		
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		5
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	3
Write Extended Attributes	●	
Delete Subfolders and Files	●▲	
Delete		
Read Permissions		
Change Permissions		
Take Ownership		

Mac mapping table

ACL entry of **NAS server**		Corresponding access right of **Mac**
●: stands for the entry is checked		
▲: only applicable for folders		
Traverse Folder / Execute File	●	Read & Write
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	
Write Extended Attributes	●	

Delete Subfolders and Files	●▲	
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data	●	
Read Attributes	●	
Read Extended Attributes	●	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		Read only
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions	●	
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data	●	
Create Folders / Append Data	●	
Write Attributes	●	Write only
Write Extended Attributes	●	(For folders only)
Delete Subfolders and Files	●	
Delete		
Read Permissions		
Change Permissions		
Take Ownership		
Traverse Folder / Execute File	●	
List Folder / Read Data		
Read Attributes		
Read Extended Attributes		
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes		No access
Write Extended Attributes		
Delete Subfolders and Files		
Delete		
Read Permissions		
Change Permissions		
Take Ownership		

4.4 Network Setup

Use this section to set the network types supported by the NAS server. The default setting allows for simultaneous use of Windows, UNIX, and Mac networks. You may change the defaults according to your needs.

4.4.1 Windows Network

The system administrator can choose to enable Windows networking so that the Windows clients can access the shared folders of the NAS server. To do so, select "Enable Windows networking", and then select "Workgroup" or "Domain" below.

If "Workgroup" is selected, type the workgroup name and then press "Apply".

If "Domain" is selected, type the Windows domain name in the "Domain:" field, in the "Account name:" and "Password:" fields type in the authentication data of the Windows account that belongs to the Administrator group, and then click "Apply" to complete.

Please note that in the "Domain:" field, you can type a fully qualified domain name (up to 63 characters) or NetBIOS domain name (up to 15 bytes).

Applying Windows domain Privilege Settings

After the server has successfully joined in a Windows domain, a new tab will appear on the *Security Setup à Account Setup* screen, called "Windows Domain Accounts", containing a copy of all user accounts. (For setup instructions, see *Security Setup à Account Setup à Windows Domain Accounts*).

In the future when a Windows or Mac client attempts to access the NAS server, the server will forward the entered account and password to the Windows domain controller for authentication. If the authentication passes, access right to the NAS server will be granted. However, if the authentication fails, the NAS server will take over the authentication task and grant the user access right if the entered account and password corresponds to a local user.

Note:
1. After moving a NAS server from a Windows domain, or workgroup to another domain or workgroup, the NAS server may still appear in the original domain or group in the Windows clients' My Network Places. This is a restriction of the My Network Places module itself and does not involve a breach of security: the server does in fact not exist any longer in the original domain or workgroup.
2. When NAS server is added into the Windows domain, if Windows domain controller is not able to operate properly, Windows client users will not be able to access the NAS server. This is the limitation of Windows. Setting multiple Windows domain controllers can eliminate the chance of happening.
3. For security reasons, an existing root account on the Windows domain will not be merged with the root account of the NAS server. In other words, if a client attempts to log into the NAS server with the root account, he must enter the NAS root password to gain access as system administrator.
4. Once a NAS server is part of a domain, only users in the same Windows domain can access the server. Members of other domains or workgroup cannot access the server. E.g., if your NAS server is part of a Windows domain A*,* and the Windows in this domain knows an account *user1* with the password *123.* If the client to which this account belongs to another domain *B*, the client will still not be able to access to NAS server, even when providing the correct login information on the account.

Synchronization settings

After the NAS server successfully joins in the Windows domain, there will be an additional tab named "Synchronization settings" appearing next to the existing tab "Windows Network". In this page you can setup how the user and group data of the NASserver will be synchronized with the Windows domain controller.

Synchronize with schedule

You can choose to synchronize data between the NAS server and the Windows domain controller every fixed period or at a certain time everyday. To do so, select an appropriate time from the pull-down menus and then click the "Apply" button to finish the setting.

Please note that when the account number is large, to ensure every scheduled synchronization can complete and to keep the server efficiency, the interval between 2 synchronizations should not be too long.

Synchronize immediately

Select the check box before the option "Synchronize immediately" and then click "Apply", the NAS server will synchronize data with Windows domain controller right away.

WINS Server

If there is a WINS server in the Windows network, please fill in the IP address of the WINS server.

4.4.2 UNIX Network
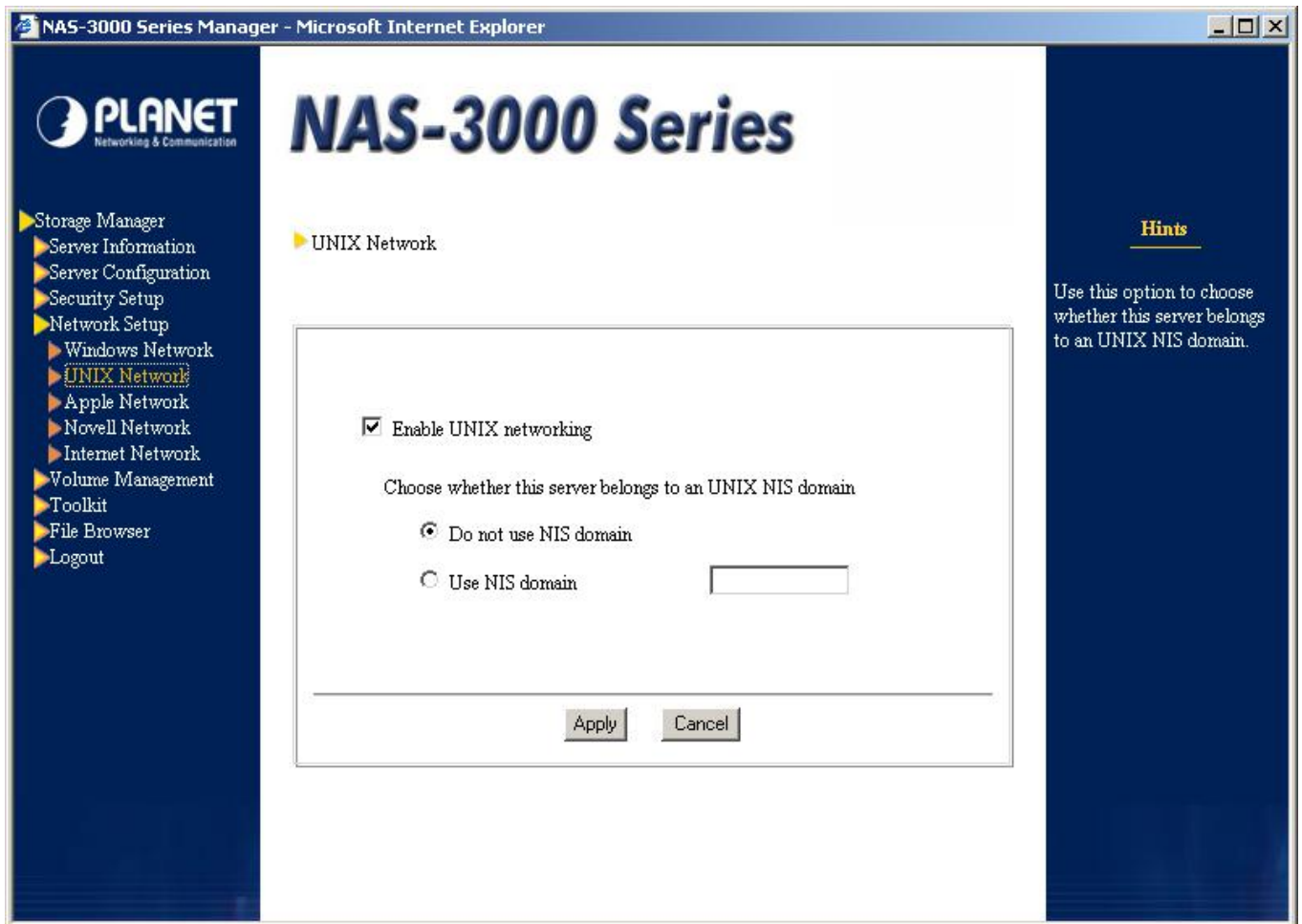
The system administrator can decide whether to make the NAS server available for NFS client. If yes, please select "Enable UNIX Networking".

If there is a NIS server in the UNIX network, use this option to select whether the server should be part of a NIS domain. If yes, you must enter a domain name.

After joining a NIS domain, a new tab called "UNIX NIS Accounts" will appear under *Security Setupà Account Setup*, showing all available user accounts on the NIS server. System administrator can setup hard disk quota for these users in the *Security Setupà Quota Option* page.

4.4.3 Apple Network
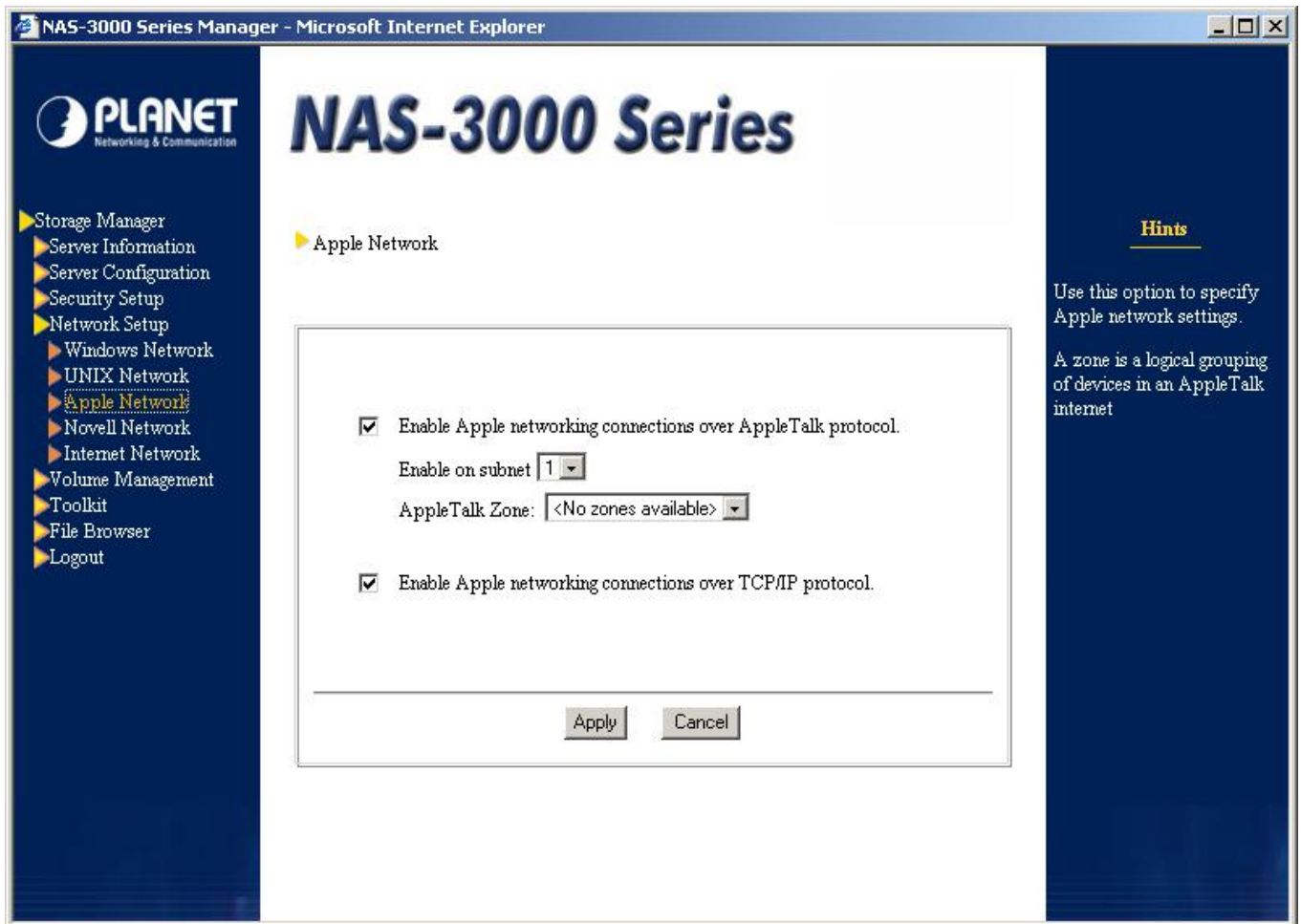
Use this option to select whether the server should use AppleTalk or TCP/IP, thus allowing or preventing Mac clients from accessing the NAS server.

This system also supports "Zone", a logical group of devices in an AppleTalk network. When the system detects the first subnet that has an AppleTalk Zone, it will display these zones on this page. A system administrator can add the NAS server to one of the zones.

Note:

1. If the NAS server is set up as having multiple subnets, this system only supports Mac client in one single subnet to read/write from the server through AppleTalk or TCP/IP protocol. Mac clients in another subnet can only read/write through TCP/IP protocol. Due to this limitation, this system can only support the Zone in a single subnet.

2. When a Mac client, for example a Mac OS 9.0.2 client, is trying to browse an English web site and sees many "cross" marks appear, please close "Smartview" from the "Control Panel".

3. Mac clients will not be able to save any single file larger than 2GB onto the NAS server.

4. When a Mac client deletes a file on the NAS server, the file is not actually deleted. So the available HDD space shown on the "Server Information/Status" page is not enlarged. To release the space, use "Empty Trash" on the Mac client.

4.4.4 Novell Network

Use this page to specify whether to support a Novell network or not. If the NAS server is set up as having multiple subnets, this page will display multiple tabs such as "Subnet 1", "Subnet 2", etc. allowing system administrator to setup Novell environment within each subnet.

If you want to allow access by Novell clients, enter the correct values for "Frame Type" and "Network Number". The "Internal network number" must be unique and should be set automatically to avoid conflicts.

Note:

1. When selecting automatic configuration of the "Internal Network Number", make sure the server's IP address is not in conflict with other servers.

2. When adding the filer to the network where a Novell server is already set up, you have to make sure the Novell server has the same "External Network Number" and "Frame Type" settings with the filer. "Auto-detect" setting on the Novell server is not recommended.

3. In the Netware Services network, the system will automatically add _NW to the original server name.

4. Novell clients cannot use the *root* account to access the NAS server. For the system

administrator *root* to access the server from Novell clients, please use the "*supervisor*" account and the root password of the NAS server to log in (there's no need to create this account on the NAS), or create another *admins* group account on the server.

5. Novell clients will not be able to save any single file larger than 2GB onto the NAS server.

6. The Windows Client service for Netware will automatically change small letters into capitals in the background, which can cause errors with some double byte characters, but this problem will not happen with Novell client 4.8 for Windows NT/2000, or 3.3 for Windows 98.

4.4.5 Internet Network

Internet Network tab
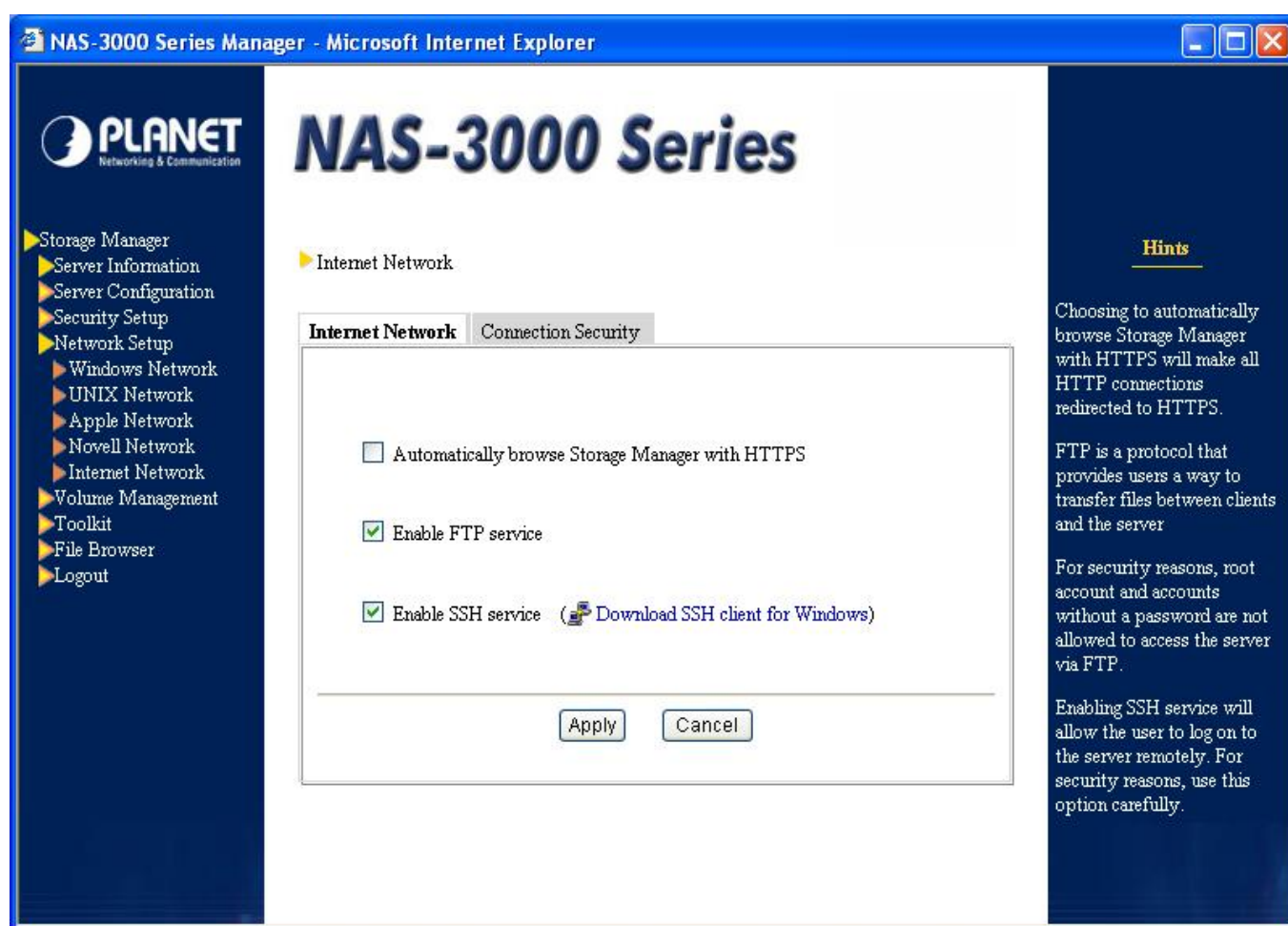
The system administrator can make Internet related configurations on this page.

Automatically browse Storage Manager with HTTPS

HTTPS is a protocol encrypted with SSL that makes data transmission between clients and the

server more secure.

To automatically browser the **NAS-3000 Series Manager** with HTTPS, check the option "Automatically browse Storage Manager with HTTPS", and all HTTP connections will be redirected to HTTPS.

Enable FTP service

FTP is a network protocol that allows user to transfer files between clients and server. For security reasons, "root" account and other accounts without password configured are not allowed to access NAS server via FTP.

Enable SSH service

SSH service is currently available only for the system vendor to do remote diagnosis.

Connection Security tab

This page allows administrators to define the FTP access privileges. Select "FTP" in the

"Connection Type", then enter appropriate information in "Hostname" or "Subnet/Mask" fields. Select "Allow" or "Deny" from "Access privileges", then click "Create" to add this record. After all privileges are set, click "Apply" button to save the configuration.

4.5 Volume Management

The system administrator can add or delete volumes in the system according to his/her own needs.

4.5.1 Volume Setting
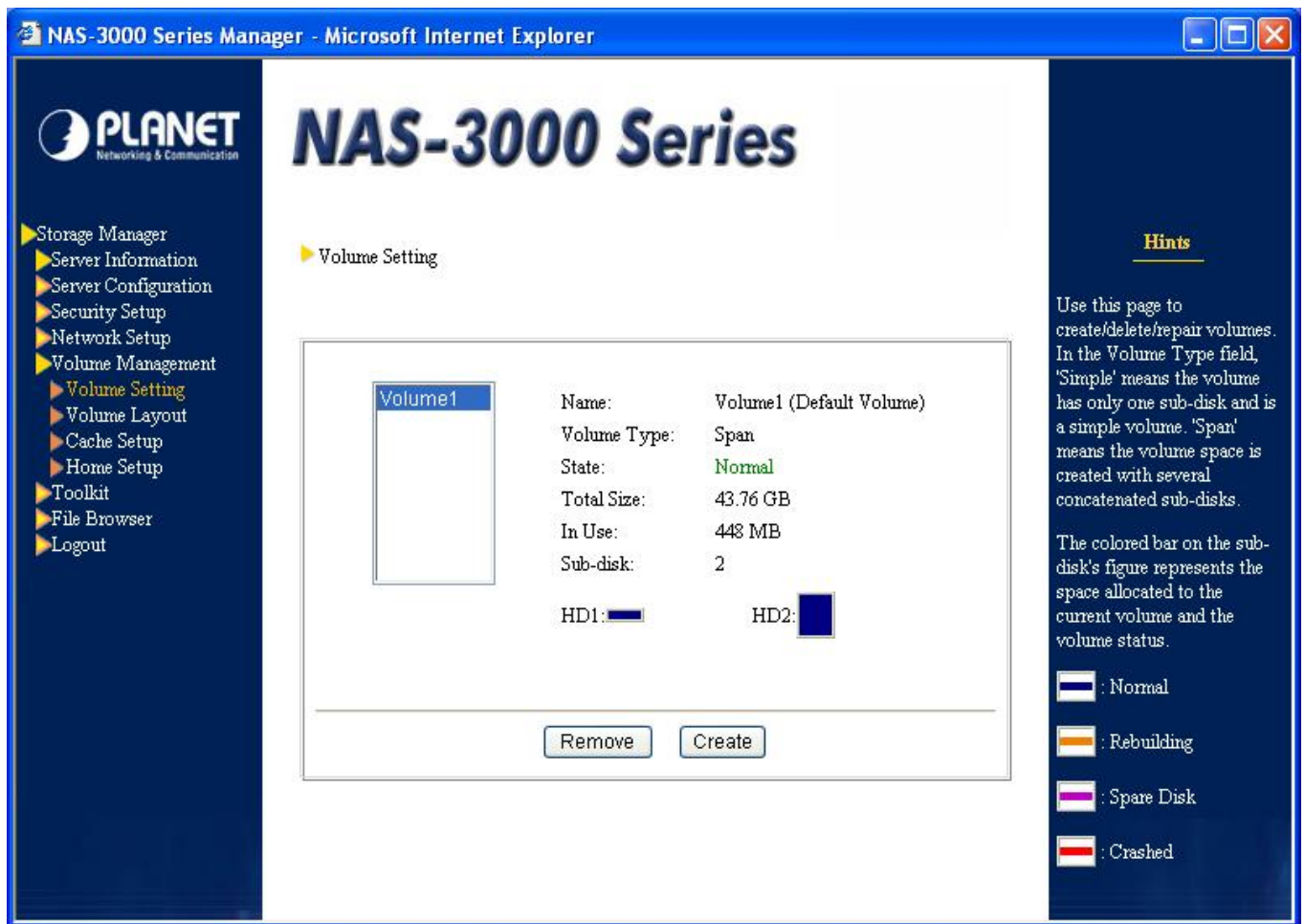
System administrator can change, remove, or repair volume on this page without restarting the server for the setting to take effect.

Create volume

1. Click on "Create" button to create a new volume and select the "Volume Type" you want to create. There are four options for NAS-3200 and six options for NAS-3400 in "Volume Type" field.

Simple

The NAS server will create an independent volume on each available hard disk with its available capacity, and the volume does not have data redundant mechanism.

Span

Select this option to make the selected disks as a concatenated, single volume.

RAID 0

A RAID 0 volume takes all hard disk for one large hard disk, and performs parallel and multiple read and write, thus it has better performance than *Non-RAID* volume. RAID 0 volume is applicable for severs with two hard disks, and the hard disks must be identical in size. If 2 different capacity hard disks are chosen to create a RAID 0 volume, the capacity of the smaller one will be adopted to create the volume.

RAID 1

A RAID 1 volume duplicates data from one hard disk to another to ensure data security and integrity. The actual available space is only half of the total space. This level of RAID ensures high level of data security, but because it only has 50% utilization rate, the cost is relatively higher than other volume types. RAID 1 volume is applicable for severs with two hard disks, and the hard disks must be identical in size. If 2 different capacity hard disks are chosen to create a RAID 1 volume, the capacity of the smaller one will be adopted to create the volume.

RAID 5 (NAS-3400 only)

This configuration includes a backup option. It treats multiple disks as one virtual disk to increase access speed. It uses parity mode to store redundant data on a space equal to the size of one disk for later data recovery. The actual available storage space in a system with n disks is thus n-1 hard disks.

RAID 5 with Spare (NAS-3400 only)

RAID 5 with Spare adds one spare disk to the RAID 5 array, allocating one for redundancy and the second one as a spare. The actual available storage space in a system with n disks is thus n-2 hard disks.

2. If you choose to create a RAID 1, RAID 5, or RAID 5 with Spare volume, you must specify which option you want the consistency or parity data of the volume to be created. The volume will be available for access in a short time when consistency or parity is built in the background. If the consistency of parity is built in the foreground, all processes must be finished before the volume can be accessed.

3. The "Available Space (GB):" list indicates space in each hard disk that has not yet been

allocated. Please determine which hard disk storage space will make up the volume.

4. Select the size from the "Size to use:" pull down menu.

5. Click the "Add>>" button.

6. Repeat step 4 to step 6, or press "Ctrl" fro multiple selections or "Shift" for continuous selections in step 4.

7. Click "OK" to confirm and start creating the volume.

After a volume is created, the default public*n* shared folder will also be created. You can now create shared folders in this volume and grant access right to the client users.

Note:

1. "Size to use" is measured in the unit of "GB," i.e., gigabyte, and the smallest unit is decided by dividing the size of the hard disk by 20 to get the nearest whole number. For example, if the size of a hard disk is less than 40 GB, the smallest unit is 1GB, while the size of the hard disk is greater than or equal to 40GB and less than 60GB, the smallest unit is 2 GB, etc.

2. Regardless of the hard disk size, the option "1GB" will always be shown in the "Size to use:" menu.

3. The size of a single volume can be up to 8 TB.

4. After a volume is created, the "In Use:" size will reveal 1% of that volume. This space is reserved by default for the administrator to do the necessary operations such as accessing the web UI or reading/writing/deleting data on the NAS server after the system is full.

Re-create volume

If a volume is crashed due to any failed disk, the volume structure could be recovered by clicking the "Re-create" button.

The re-creating function can only re-create the original structure of the crashed volume: share folders and users' home folders, and set it as the default volume if it originally was setup as such. It cannot restore any lost data in these shared folders.

Before you start recreating, please make sure the failed disk is replaced with a new one.

Note:

1. When a volume crashes, all data in users' home folders on the crashed volume will also be destroyed. However, the structure of the folders will be moved to the next available volume, and the original folder structure will be moved back after the crashed volume is re-created.

2. When a volume crashes while there is no other volume available, the data in users' home folders on the crashed volume will be destroyed and the users' accounts will be transferred into the *guests* group. There will be no home folders for these accounts if the volume is re-created in the future since the accounts in the *guests* group don't have a home folder.

Repair volume

For RAID 1 and RAID 5 Volumes

When any of the sub-disks that compose the volume with data protection mechanism, such as RAID 1 or RAID 5, the status of the volume will become "degrade."

When a volume becomes "degrade," a "Repair" button will appear on the bottom of the page if there is available hard disk space on the hard disks that don't compose the degraded volume, and you can follow the steps below to repair the volume:

1. Click "Repair".

2. Choose the hard disk space to be used in the "Available Space" list.

3. Click the "Add>>" button.

4. Click "Repair" to confirm.

Note:

1. To ensure the data protection mechanism still provides the highest level of safety, you can only select the hard disk on which the volume is not created while repairing volume space.

2. If there is no available hard disk space on the NAS server when a volume becomes "degrade" status, please replace the bad hard disk that makes the volume "degrade," and the NAS server will repair the volume automatically after the new hard disk is inserted

For RAID 5 with Spare Volume

When the spare sub-disk fails

When the spare sub-disk that compose the "RAID 5 with Spare volume fails, the status of the volume will becomes "Spare sub-disk abnormal," in this case please replace the spare disk for the NAS server to automatically repair the volume.

When the non-spare sub-disk fails

When any of the non-spare sub-disks that compose the "RAID 5 with Spare volume fails, the spare sub-disk will take over the failed sub-disk and repair the volume automatically, and after the repair finishes, the failed sub-disk will becomes the spare sub-disk, and the volume therefore becomes "Spare sub-disk abnormal," please replace the spare disk in this case

Note: "Spare sub-disk" stands for a hard disk space on a hard disk that composes the "RAID 5 with Spare" volume, while "spare disk" stands for the hard disk with the "spare sub-disk" on it.

Check file system

If the NAS server is improperly shut down or powered off, consistency check and parity check will be applied on RAID 1, RAID 5, and RAID 5 with Spare volume(s) when the server is rebooted. And if the hard disk is improperly removed on the parity check stage, the "Volume Setting" page will show the following message:

The system has detected that the volume needs file system checking. Press Check to begin the process.

Please click the "Check" button to start the file system check and recovery.

The integrity of file system will decide whether the data on the NAS server is read correctly. Even though file system check is applied after any improper shutdown, it may still lead to data lost. Hence it is strongly recommended that The NAS server be shut down properly.

4.5.2 Volume Layout
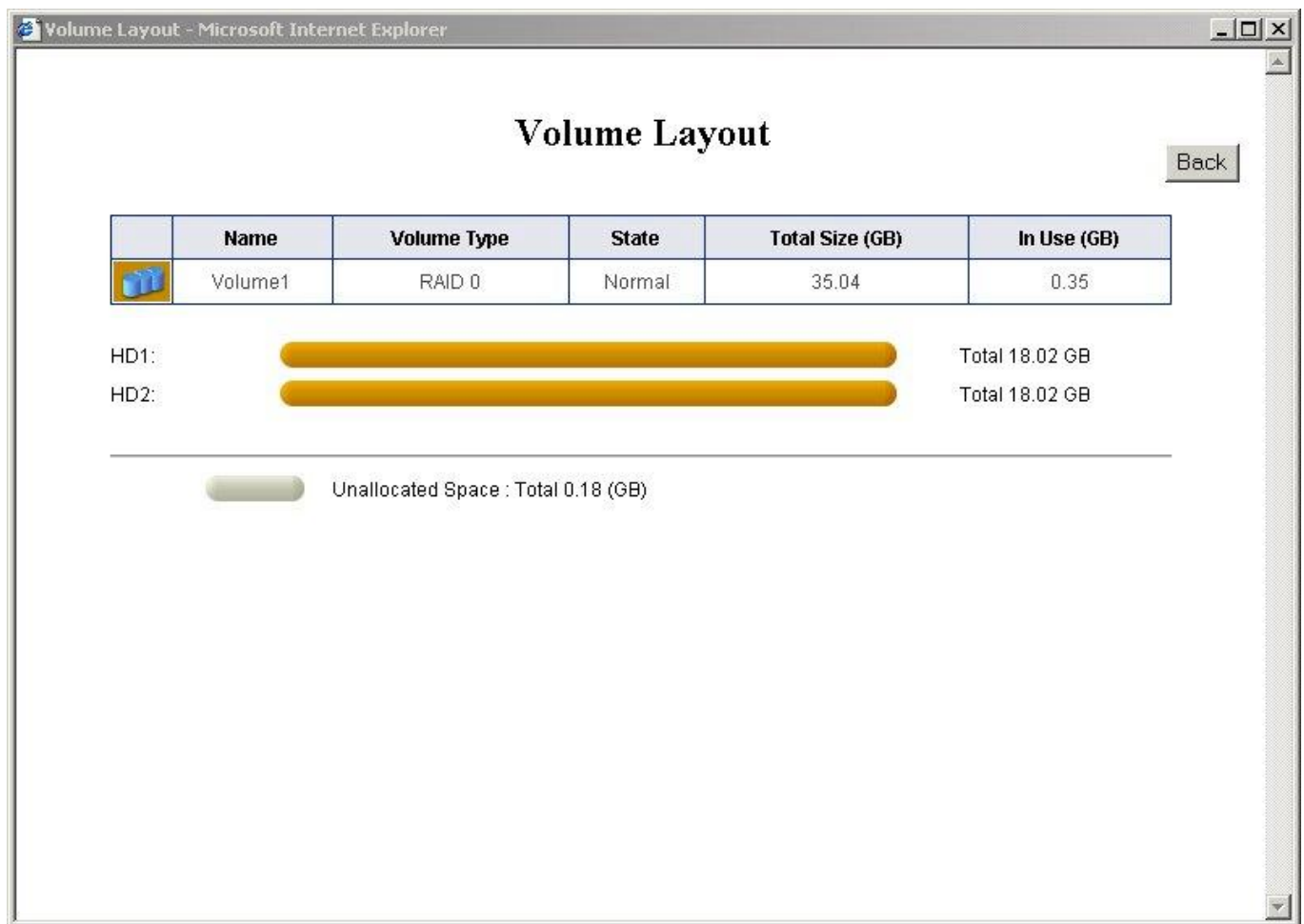
This page shows the status of volume layout in the NAS server.

4.5.3 Cache Setup
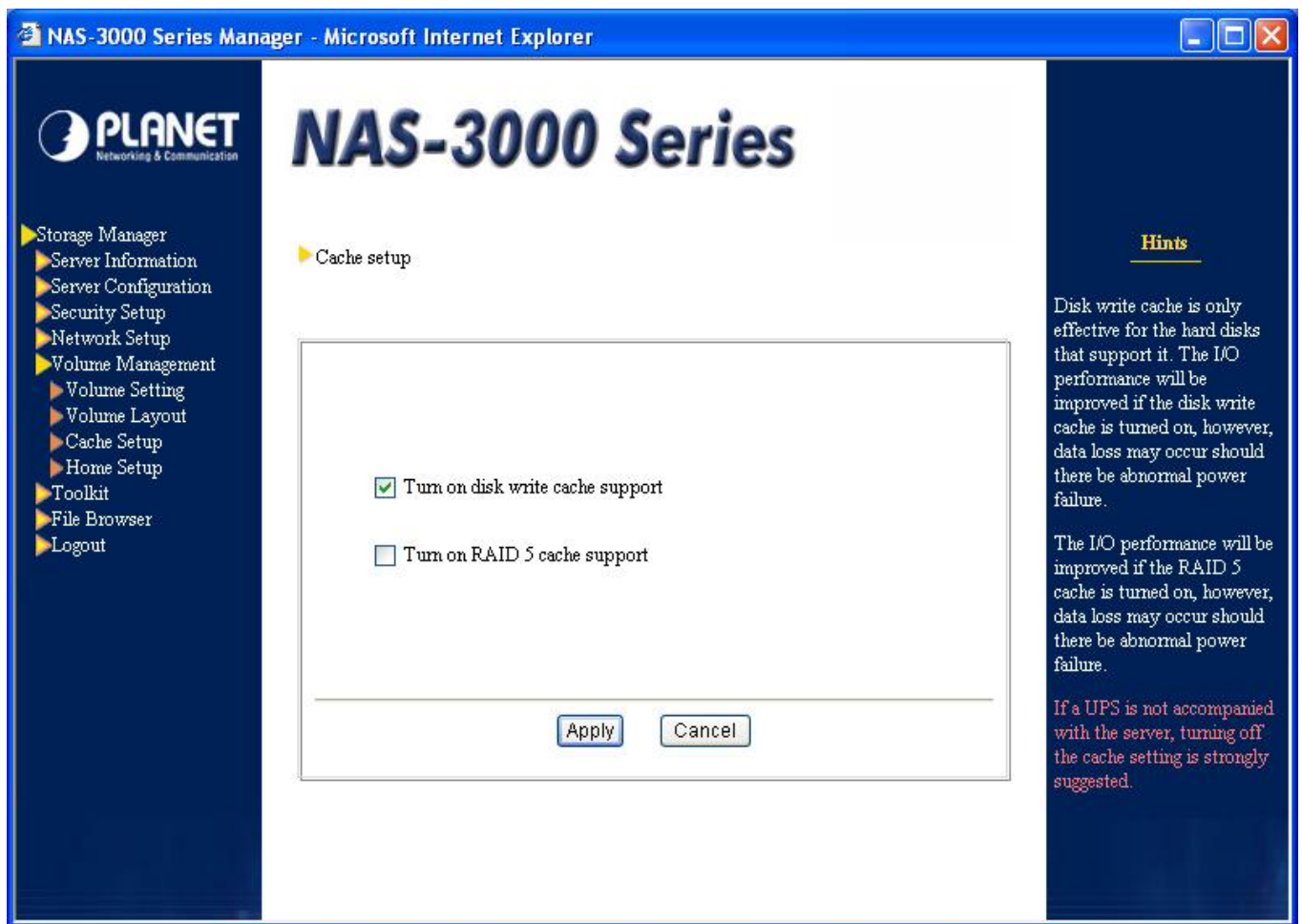
Turn on disk write cache support

System administrator can enable or disable the hard disk write cache here.

This setup will take effect only if the server hard disk supports cache memory. If the hard disk write cache is enabled, the system read/write performance will improve, but it may result in data loss if any unanticipated power failure occurs. If the system utilizes UPS, then we suggest that you enable this selection. To check if the hard disk supports the cache memory, contact your hard disk dealer.

Turn on RAID 5 cache support

A RAID 5 volume requires more frequent data requests to compute parity, and to improve the I/O efficiency, the NAS server supports RAID 5 device-layer cache so data can be stored in memory temporarily for faster access.

However, it is suggested UPS is accompanied with the NAS server when this option is turned on to avoid data loss when unanticipated power failure occurs.

Note:

1. You have to reboot the NAS server to make the RAID 5 Cache setting effective, and it will be applied only to the selected volume(s).

2. If the NAS server doesn't have any RAID 5 volume when you apply the "Turn on RAID 5 cache support "option, the RAID cache support will be turned on automatically on all future created RAID 5 volumes.

4.5.4 Home Setup

When adding a new account into the "Users" group, the system will automatically create a home folder for this account. System administrator must specify the volume to store the home folder. But it is possible to save many accounts into certain volume causing the volume to carry heavy load or have inadequate space. This "Home Setup" page enables system administrator to easily manage user home folders.

After selecting a volume in "Volume Name", the system will display accounts' home folders in the selected volume in the "Current User (home size)" column. Select accounts that require moving of home folders, select destination in "Move to Volume" and click "Move to". After confirmation then

click "Apply".

Note:

1. Administrator cannot move users' home folders to other volumes when any user is accessing his/her own data online.

2. The setting will be separated into different pages according to the number of accounts. If the account you are going to perform does not appear on the page, please select the page number at the bottom of the page to go to other pages.

4.6 Toolkit

4.6.1 LED Management
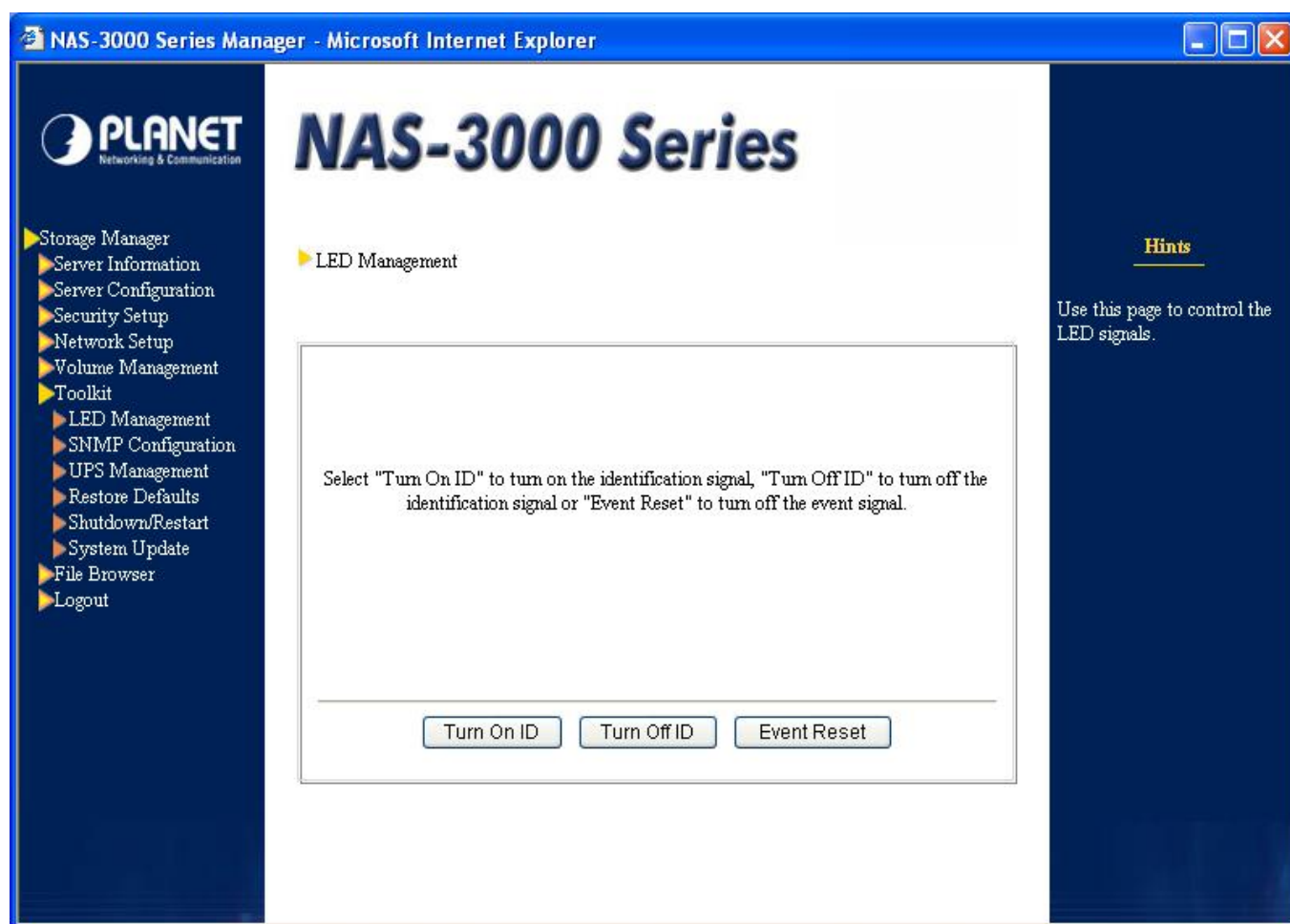
This page is preserved for future use.

4.6.2 SNMP Configuration
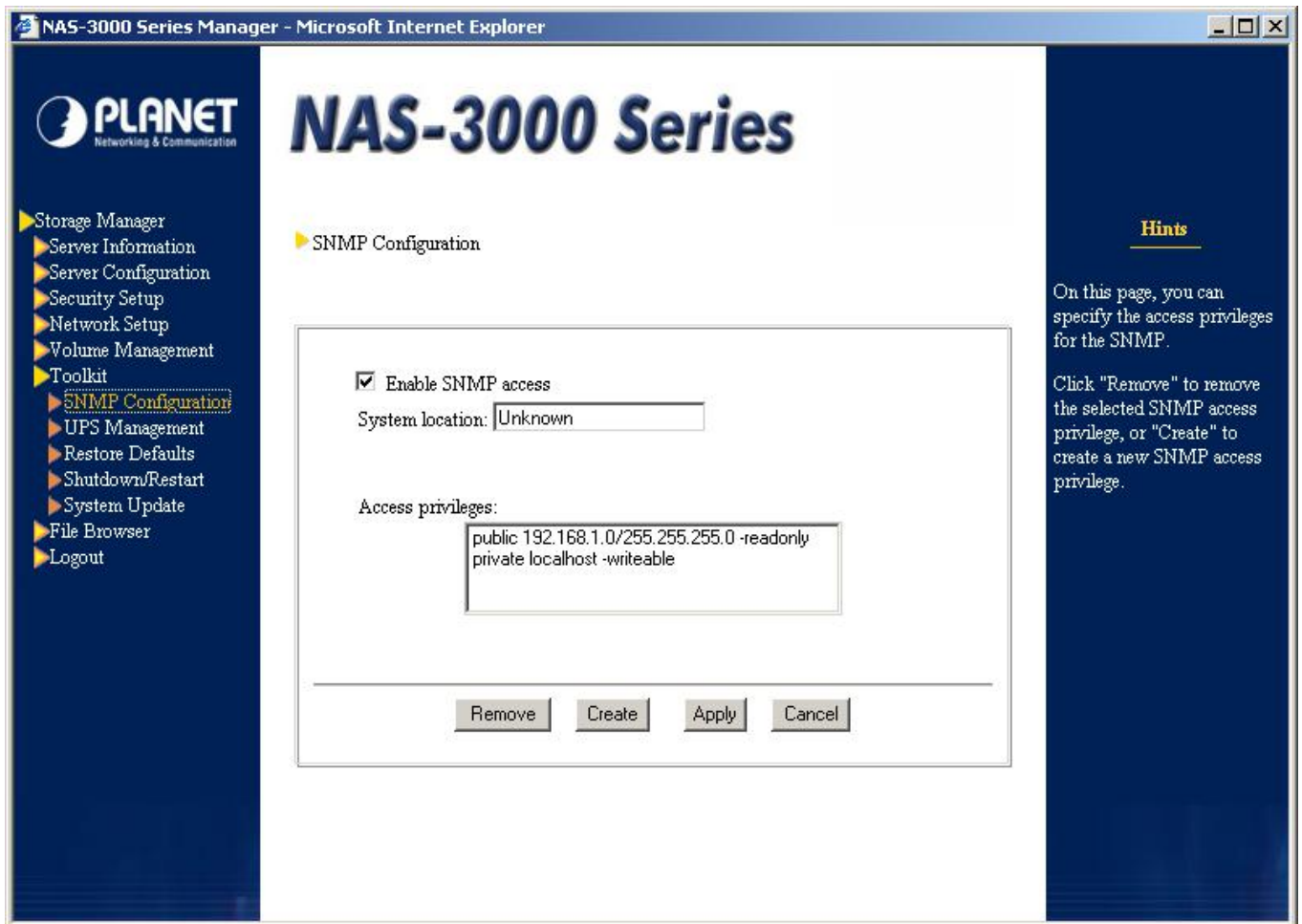
Use this option to enable SNMP access. To do this, select "Enable SNMP access" and in the column "System location", enter the geographical location of the NAS server; then click "Apply".

Each entry in "Access privileges" consists of three elements:

1. The first component is the community the NAS server belongs to, to be chosen by the system administrator.

2. The second component is the host or subnet of this community.

3. The third element is the NAS server access privileges of the community's host or subnet through SNMP

Adding SNMP Access Privileges
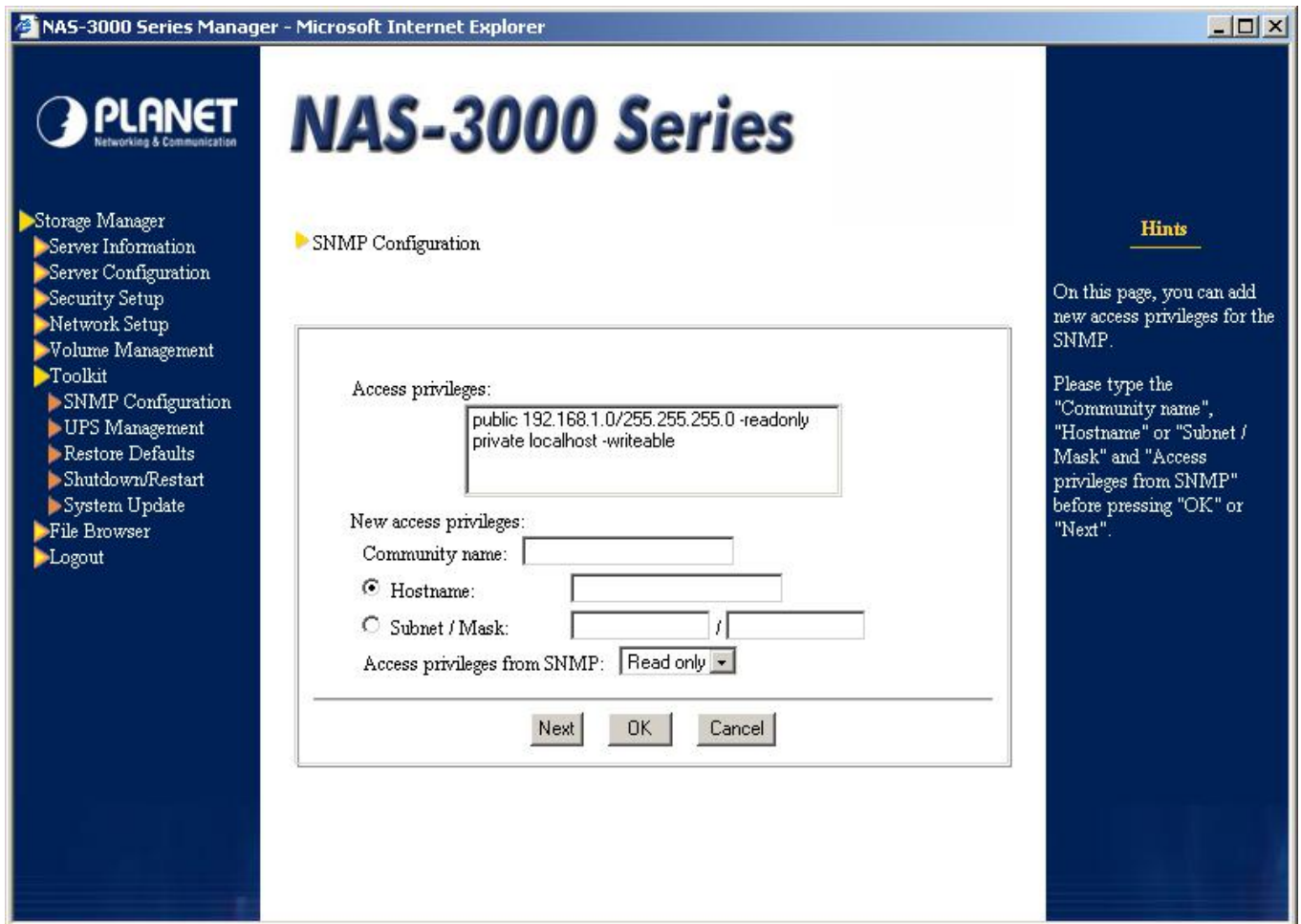
To add SNMP access privileges, click on "Create". A new dialog will appear, where you can select a community name along with the host and Subnet /Mask (e.g. 192.168.1.0/255.255.255.0) belonging to this community. Then select the "Access privileges from SNMP": either "read only", or "writeable". "Read only" means the community hosts can only read information through SNMP, "writeable" means the community's hosts can also modify some read and write fields. Click "OK" to confirm or "Next" to add more privileges.

Removing SNMP Access Privileges

To remove SNMP access, select an option under "Access privileges" (use Ctrl for multiple and Shift for continuous selection), and then click "Remove".

Modifying SNMP Access Privileges

To modify existing privileges, select an option under "Access Privileges", remove it and add a new privilege.

4.6.3 UPS Management
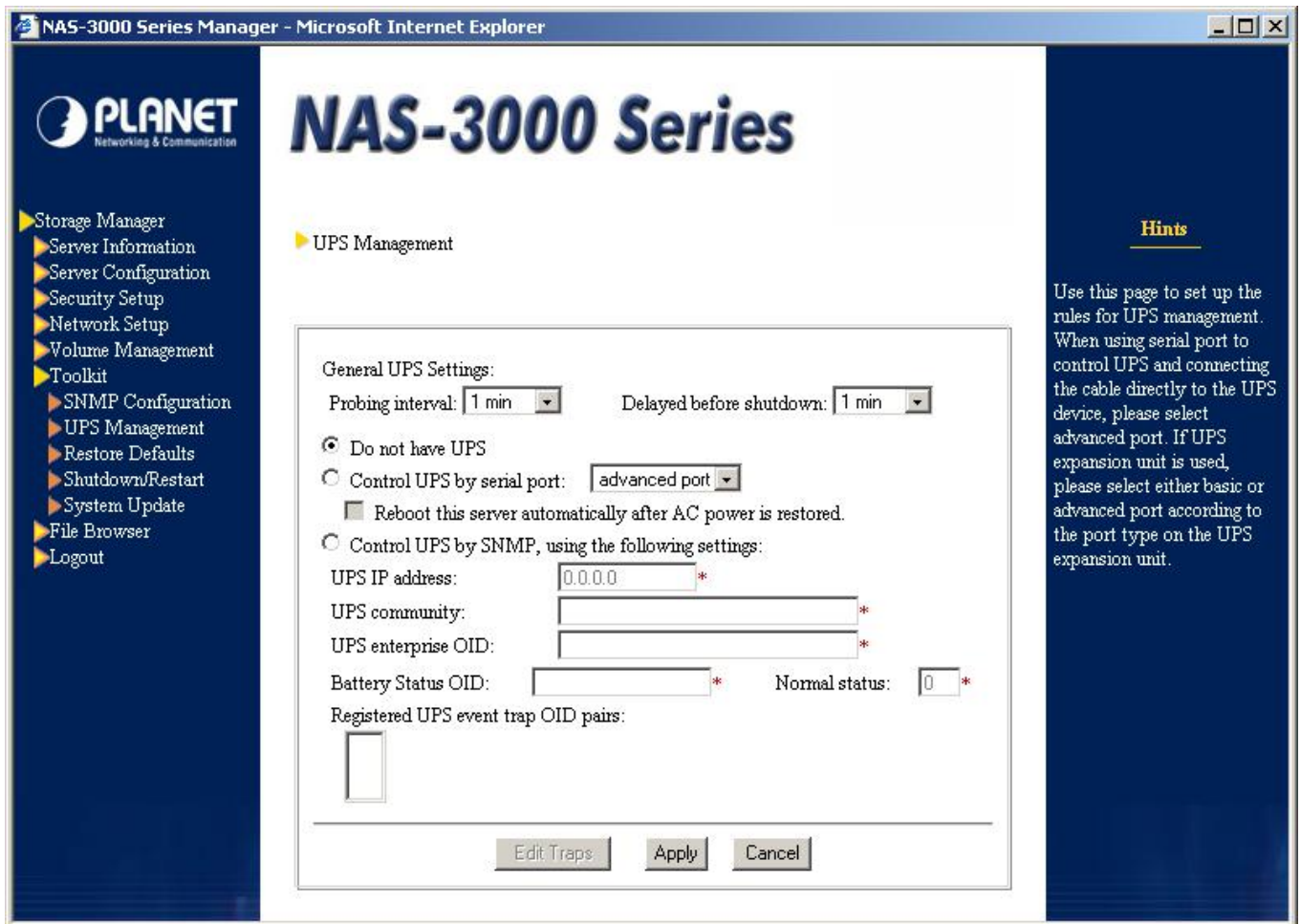
The NAS server currently supports only APC Smart Series UPS, either via serial connection or SNMP.

Control UPS by serial port

Connect the power cable of NAS server to the UPS and connect APC RS-232 cable to COM port on rear panel of the server. In **NAS-3000 Series Manager**, go to *Toolkità UPS Management* to configure "Probing interval" and "Delayed before shutdown".

Select "Control UPS by serial port", and choose "advanced port" or "basic port" from the pull-down menu on the right side. Click "Apply" to finish.

If the power cable of the NAS server and APC RS-232 cable are connected to the UPS directly, select "advanced port"; if more APC RS-232 cables are connected to the expansion unit for multiple servers to share the same UPS and the NAS server has to be connected to the basic port on the expansion unit, select "basic port".

Note:

1. When APC UPS expansion unit is used, please use the proper APC RS-232 cable to connect. If "advanced port" is selected, make sure that the 940-0024C cable is connected, and if "basic port" is selected, please connect the 940-0020B cable.

2. Advanced port provides automatic response function so that the system will detect when it does not find any UPS. Basic port does not have this function.

The system performs scheduled detection of UPS power supply according to "Probing interval". The system will take the following actions if there is anything abnormal with UPS:

1. AC power failed: If AC power failed, the system will delay shutdown according to the settings in "Delayed before shutdown". If the event is cleared during this period, the system will not shut down.

2. Low battery: If UPS battery is low, the system will shut down in five seconds. If the event is cleared during this period, the system will not shut down.

3. Overloaded: If UPS power supply is overloaded, the system will shutdown based on the setting of "Delayed before shutdown". If the event is cleared during this period, the system will not shut down.

4. When the cable is connected to Advanced port, the system will shut down five seconds after UPS timeout. If the event is cleared during this period, the system will not shut down.

Auto boot the NAS server after AC power restores

If you want the UPS to boot the NAS server automatically when AC power restores, please select the option "Reboot this server automatically after AC power is restored".

Note: If the option is selected, when AC power fails, the NAS server will shut down based on the setting of "Delayed before shutdown:", and then the UPS will shut down after 3 minutes. Thus if other machines share the same UPS with the NAS server, they will also lose power when the UPS shuts down, in this case, please properly configure the "Delayed before shutdown:" option of other machines.

Control UPS by SNMP

1. Connect the power cord of the NAS server to the UPS and the UPS to the network. Select proper values for "Probing interval" and "Delayed before shutdown".

2. Select "Control UPS by SNMP, using the following settings:".

3. UPS IP address and UPS community

   UPS equipped with SNMP faculties will be assigned an IP address. Enter this IP address in the respective column. In the SNMP user interface of the UPS terminal certain communities will be

registered, each community containing one or more host names and IP addresses. These hosts can be trusted and can read information from the UPS. If you want to control the UPS via SNMP, you must register the NAS server in one of the communities listed, then enter the name of the community in the "UPS community" field.

4. UPS enterprise OID

This setting can be found in the MIB file of the UPS. If the UPS supports SNMP access, the manufacturer has added an MIB file to the documentation. Download the file from the manufacturer's web site if necessary. Look in the file for the "Private Enterprise Number". APC's Private Enterprise Number is 318, so the value of this field should read *1.3.6.1.4.1.318*, whereby *1.3.6.1.4.1* is static and must not be changed. You can also use an SNMP program such as HP OpenView to browse through the MIB file and retrieve the "Private Enterprise Number".

5. Battery Status OID

This setting refers to the "battery status OID" in the MIB file. The value for the APC UPS is *1.3.6.1.4.1.318.1.1.1.2.1.1*. Enter this value, or the short form *1.1.1.2.1.1*, if you are using an APC product.

6. Normal status

The "battery status OID" (see above) obtained from the MIB file represents a number of states, e.g., 2 for "battery normal", 1 and 3 for "unknown" or "low battery" respectively.

After items 5 and 6 are filled up, the system will probe the UPS in the interval chosen above and shut down in 5 seconds if abnormal battery status is detected.

7. Registered UPS event trap OID pairs

A UPS with SNMP faculties usually has a trap function, used to detect anomalies in the UPS status without waiting for the scheduled probing signal. Click "Edit trap" to add or delete event trap OIDs for your UPS.
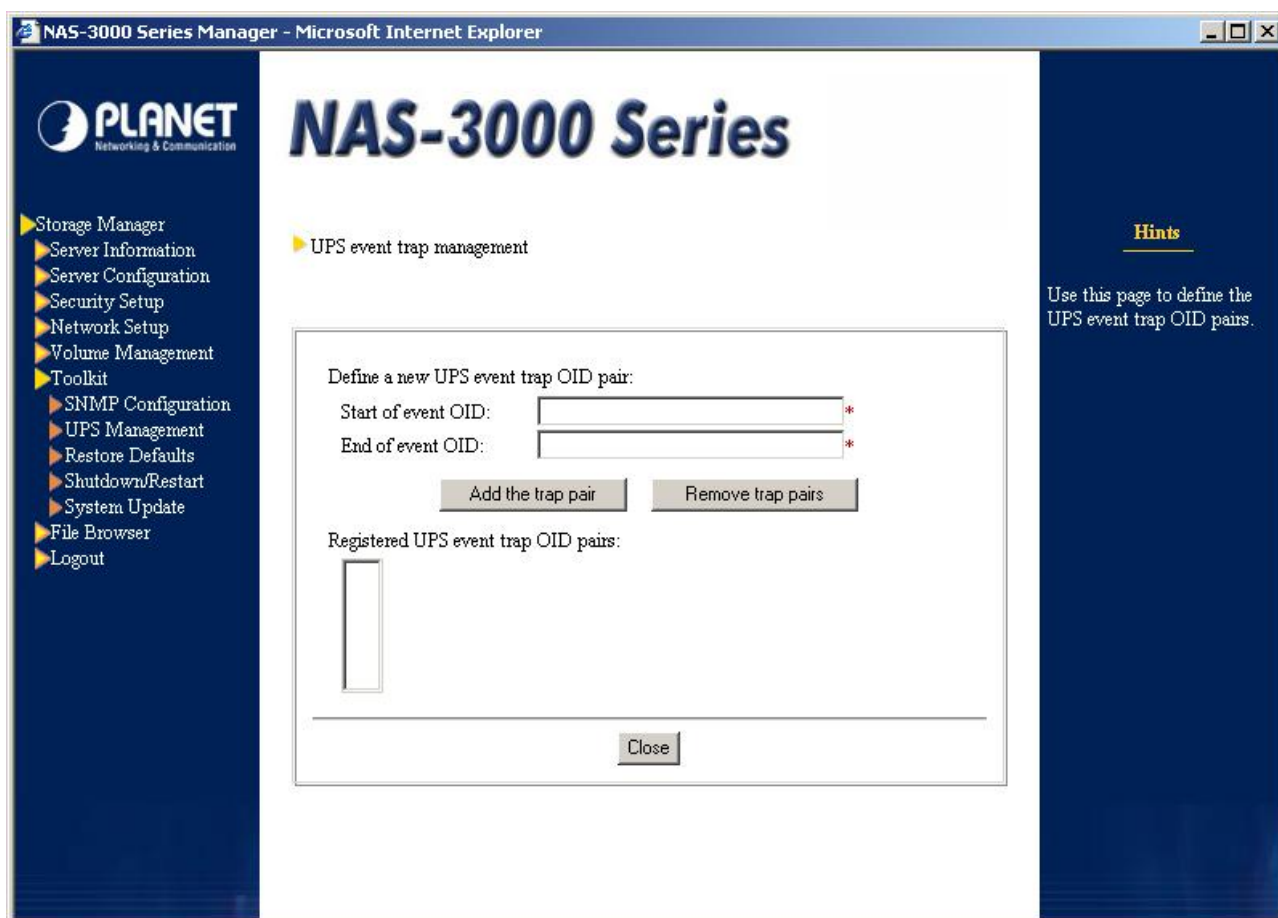
In "Start of event OID", enter the critical event trap OID. Alternatively, use an SNMP program such as HP OpenView to browse through the MIB file and obtain the trap OID. The value 1.3.6.1.4.1.318.0.5 for example stands for A/C power failed, switching to battery.

In the field "End of event OID", enter the informational trap OID, e.g. 1.3.6.1.4.1.318.0.9 for A/C power restored. This field is optional, since many critical events do not permit resuming and require a system shutdown. Retrieve both values for "Start of event OID" and "End of event OID" for the MIB documentation of your UPS manufacturer.

Note: After making the configuration above, the system will periodically probe the UPS status based on the "Probing interval", and shut down in the time as defined in "Delayed before shutdown" when abnormal events defined in "Registered UPS event trap OID pairs" occur.

4.6.4 Restore Defaults
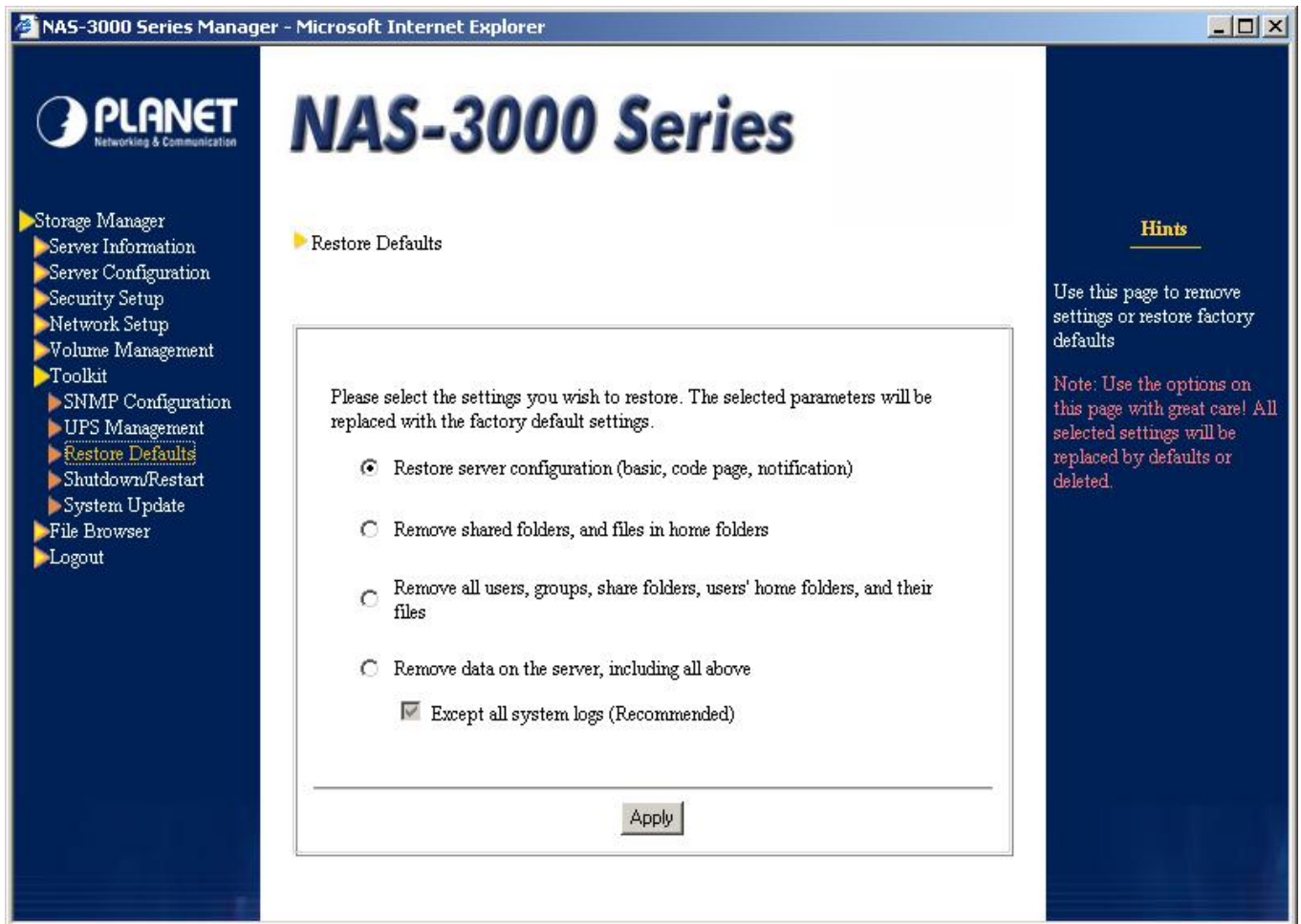
The system administrator has the option to restore factory defaults for all settings, or remove all user settings in the system. Four options are available:

1. Restore Server Configuration (basic, code page, notification).

2. Remove shared folders, and files in home folders.

3. Remove all users, groups, shared folders, users' home folders, and their files.

4. Remove data on the server, including all above.

Note:

1. Be careful when using the options on this page. All selected settings will be replaced by defaults or deleted.

2. If you choose to apply the first (Restore Server Configuration) or the fourth (Remove server) option, you must go through "Quick Configuration" again.

4.6.5 Shutdown/ Restart
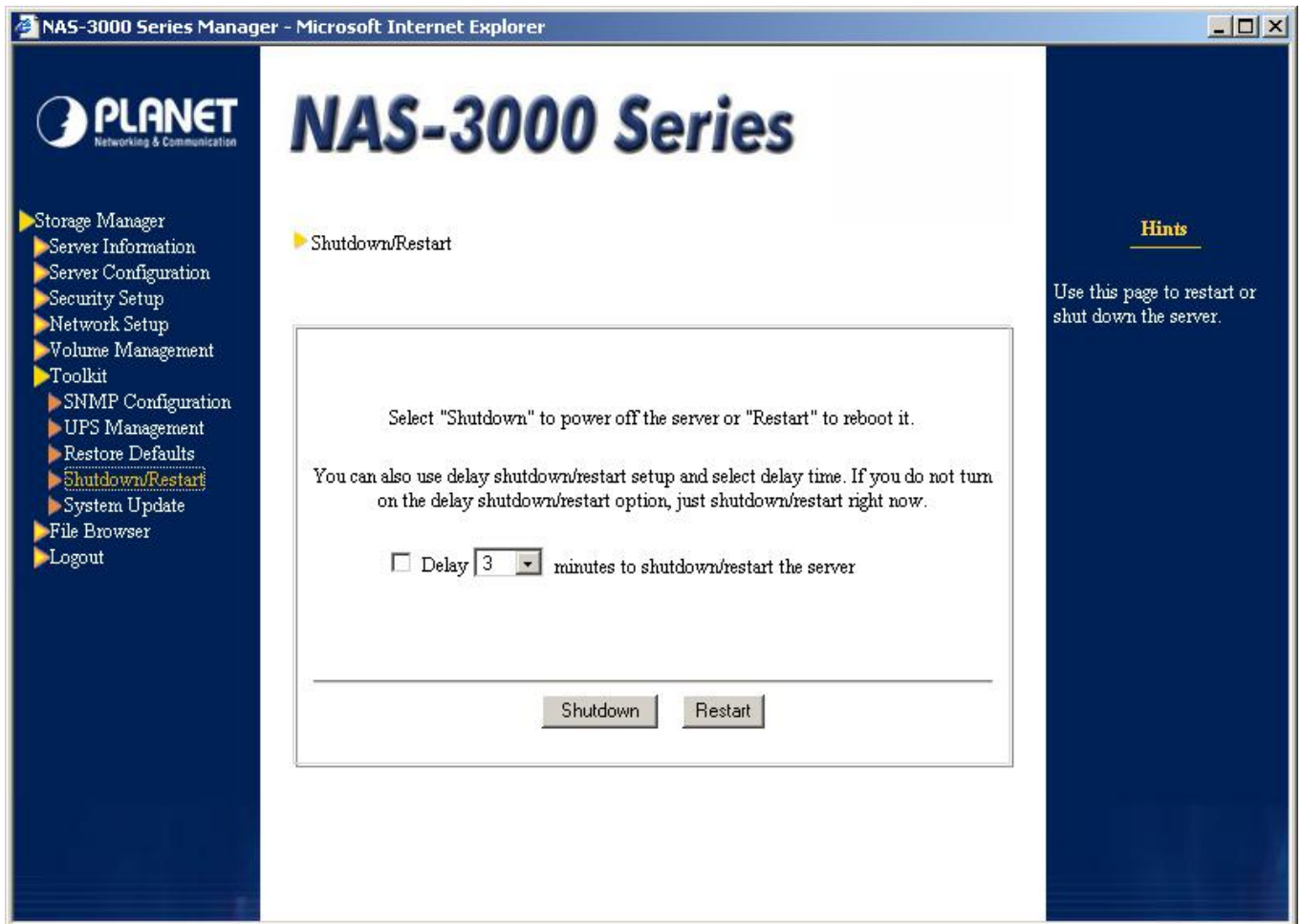
Use this page to "Shutdown or Restart" the server. You can also use the power switch on the NAS server. To preserve data integrity, never unplug the server before it has been properly shut down. System administrator can select the option "Delay xxx minutes to shutdown/restart the server" and the setup will be executed after the time specified.

Wait for the power LED to go off and the server to halt operation completely before unplugging and moving the server.

4.6.6 System Update
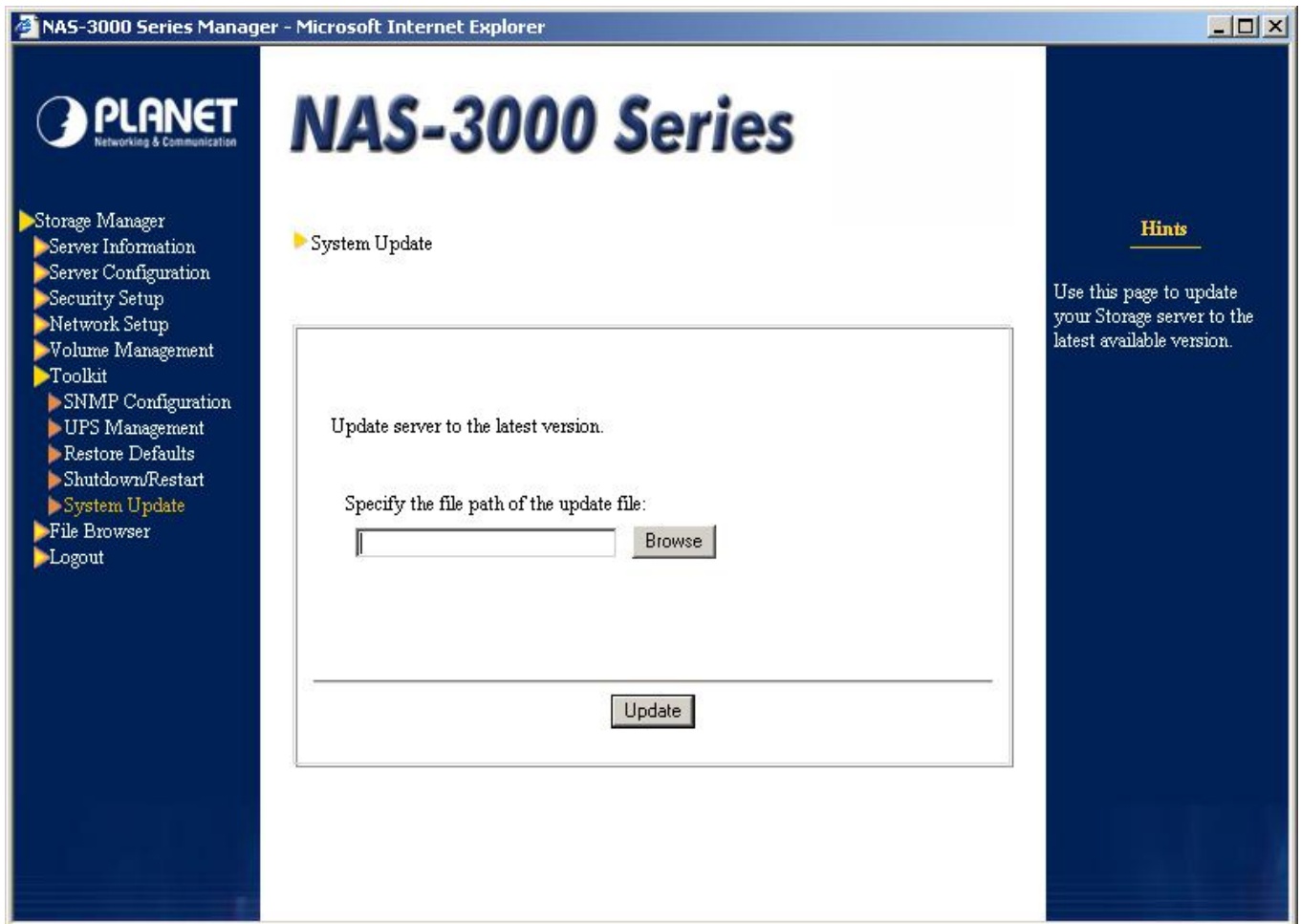
Once you have obtained the OS upgrade, follow these steps to update your system:

1. Copy the update file (assume its name as "update.pat") from any client computer to any shared folder in the NAS server.

2. Click "Browse" to select name and path of system update file.

3. Click on "Update". The update process will start immediately and the system will restart automatically upon completion.

Note:

1. System update will not affect the files saved on the server. However, we still strongly recommend that the administrator backup all the files on the server before updating the system.

2. The server cannot be accessed while the upgrade is running.

3. When the system is being updated, do not close **NAS-3000 Series Manager** window, turn off the server or remove the AC power, to avoid errors in the system operation.

4. During the upgrade, the browser on the client terminal will loose the connection to the system. Close the browser and wait for the upgrade to complete before re-connecting to NAS server. (The system will send an e-mail message informing the administrator that the server is back on line).

4.7 File Browser
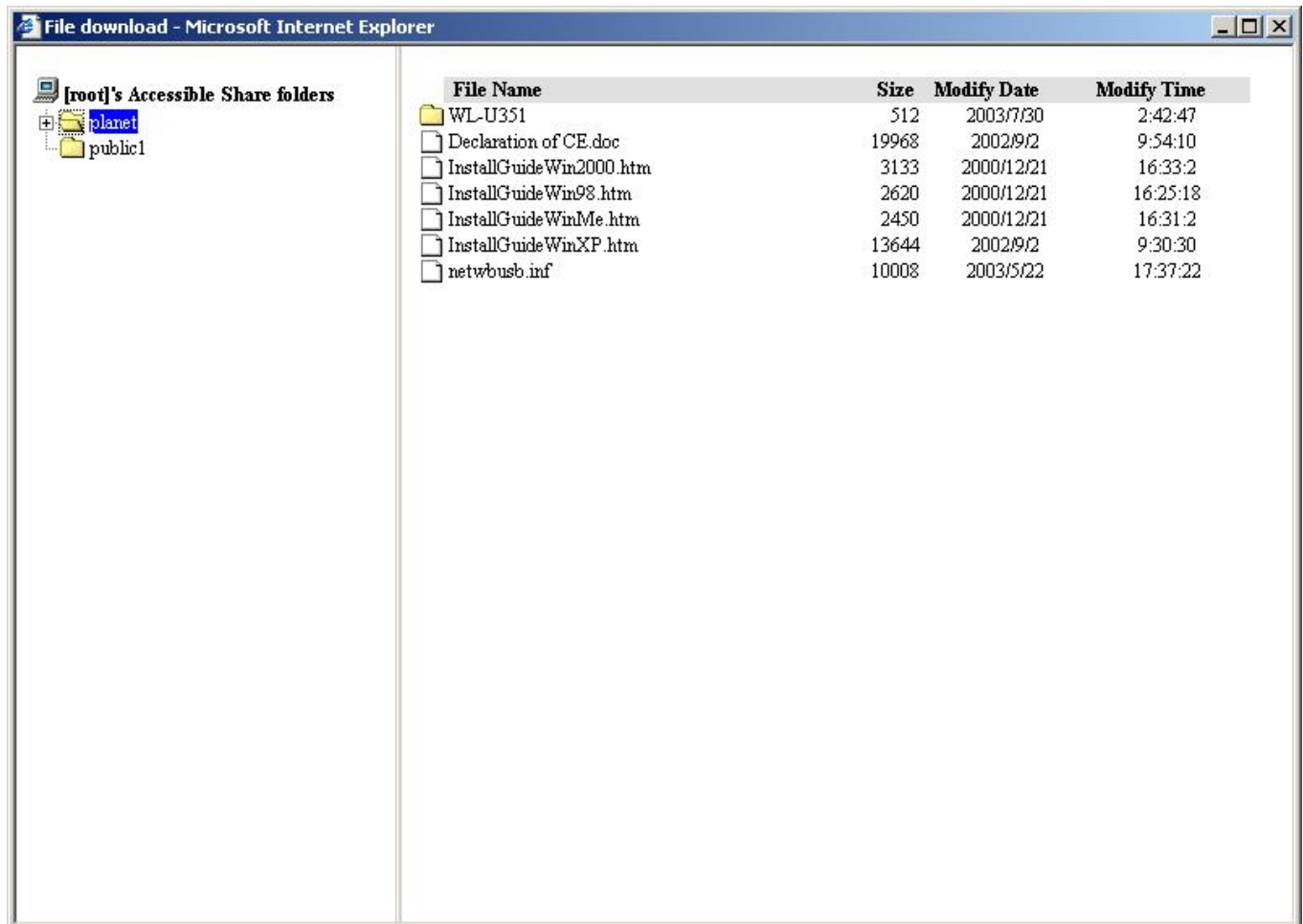
This function allows users to have remote access to files in the server through the Internet (HTTP protocol). The user can login to NAS server and browse all the folders and files in each shared folder the user has access rights.

Note: To make sure files/folders on the NAS server can be displayed correctly on this page, please upgrade the IE browser version to 5.5 or above.

4.8 Logout
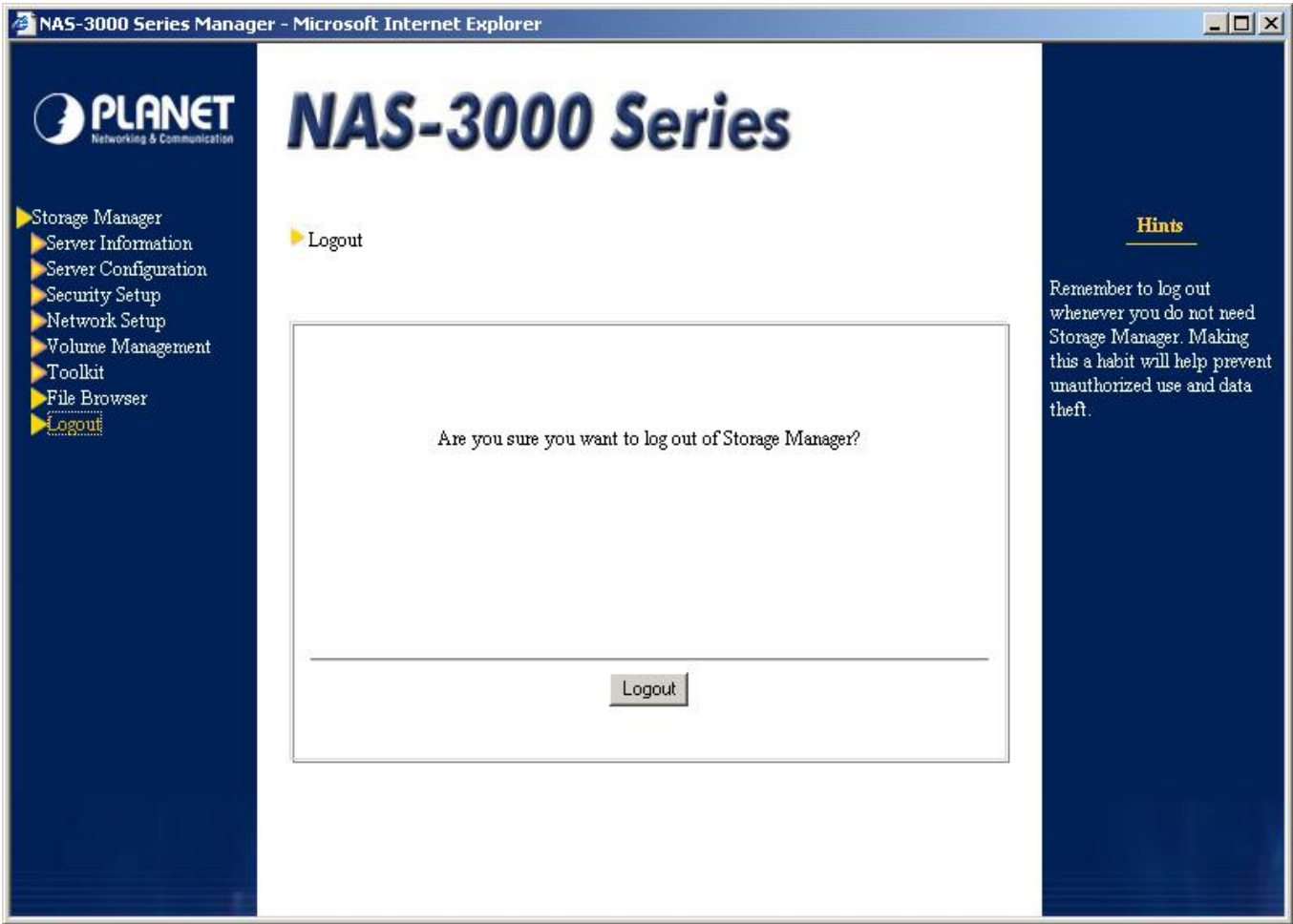
In the interest of safety, remember to log out whenever you complete the management operation.

Using Backup Utility

PLANET NAS-3000 series Backup is a backup tool integrated in PLANET NAS-3000 series Assistant. The system administrator can use it to backup data from the NAS server to other storage devices on the LAN, or to restore previously backed up data back to the NAS server.
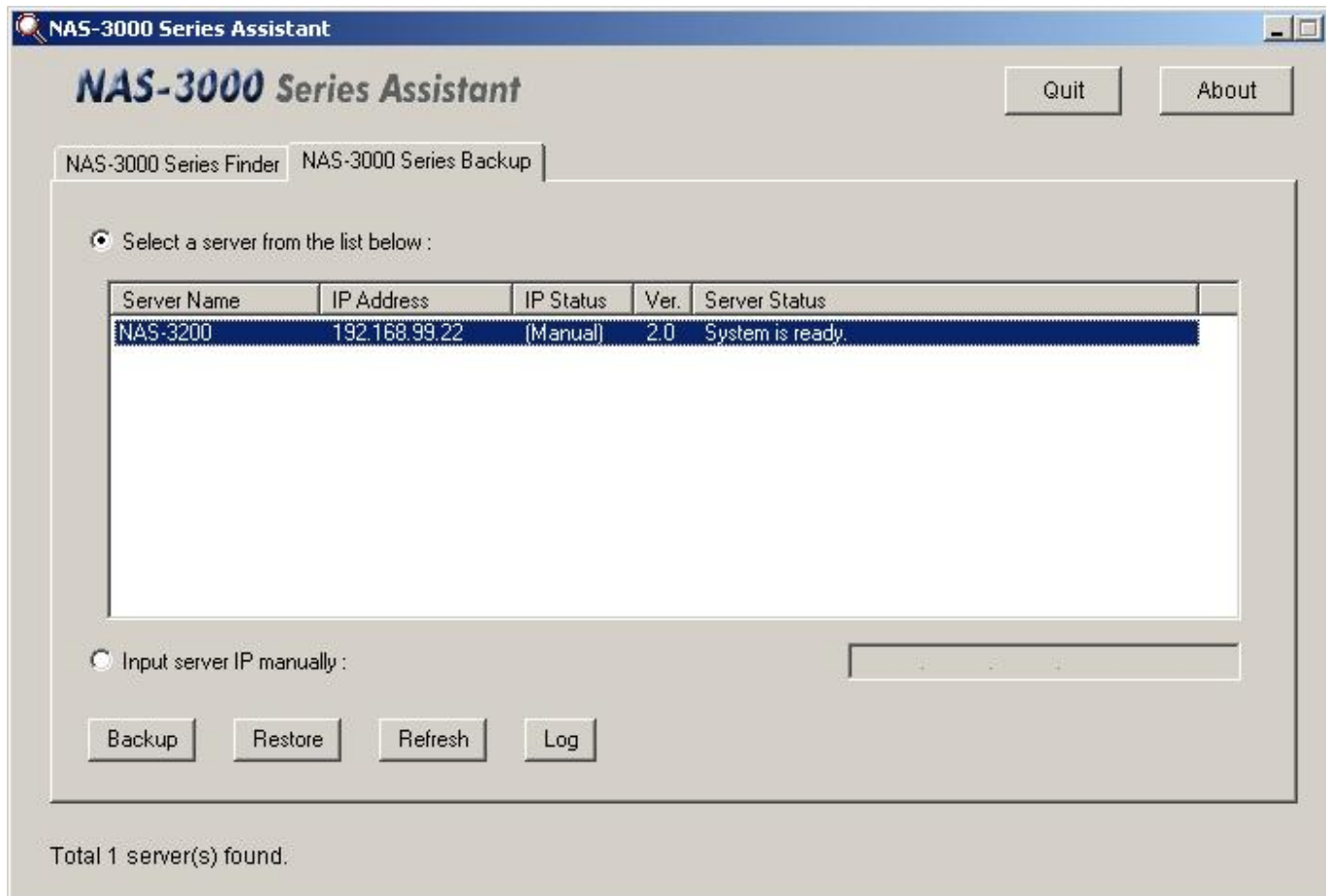
There are four types of data available for the administrator to backup and restore:

1. System information: including basic configuration, network time synchronization, time zone setup, language setup, notification setup, security option, Apple network, Novell network, Internet network, SNMP configuration, UPS management, and cache setup.

2. User accounts and groups: including account and group setup, root password, Windows network, and UNIX network.

3. User accounts, groups, and data: including shared folder setup, account and group setup, root password, Windows network, UNIX network, and data on selected shared folders and user

home folders.

4. System information, user accounts, groups and data: all data on the server, including the configurations and data mentioned above.

5.1 Backing up data

To backup data, follow the steps:

1. Activate PLANET NAS-3000 series Assistant, click the NAS-3000 series Backup tab, and select the server to be backed up from the server list, or select "Input server IP manually" and input the server IP.
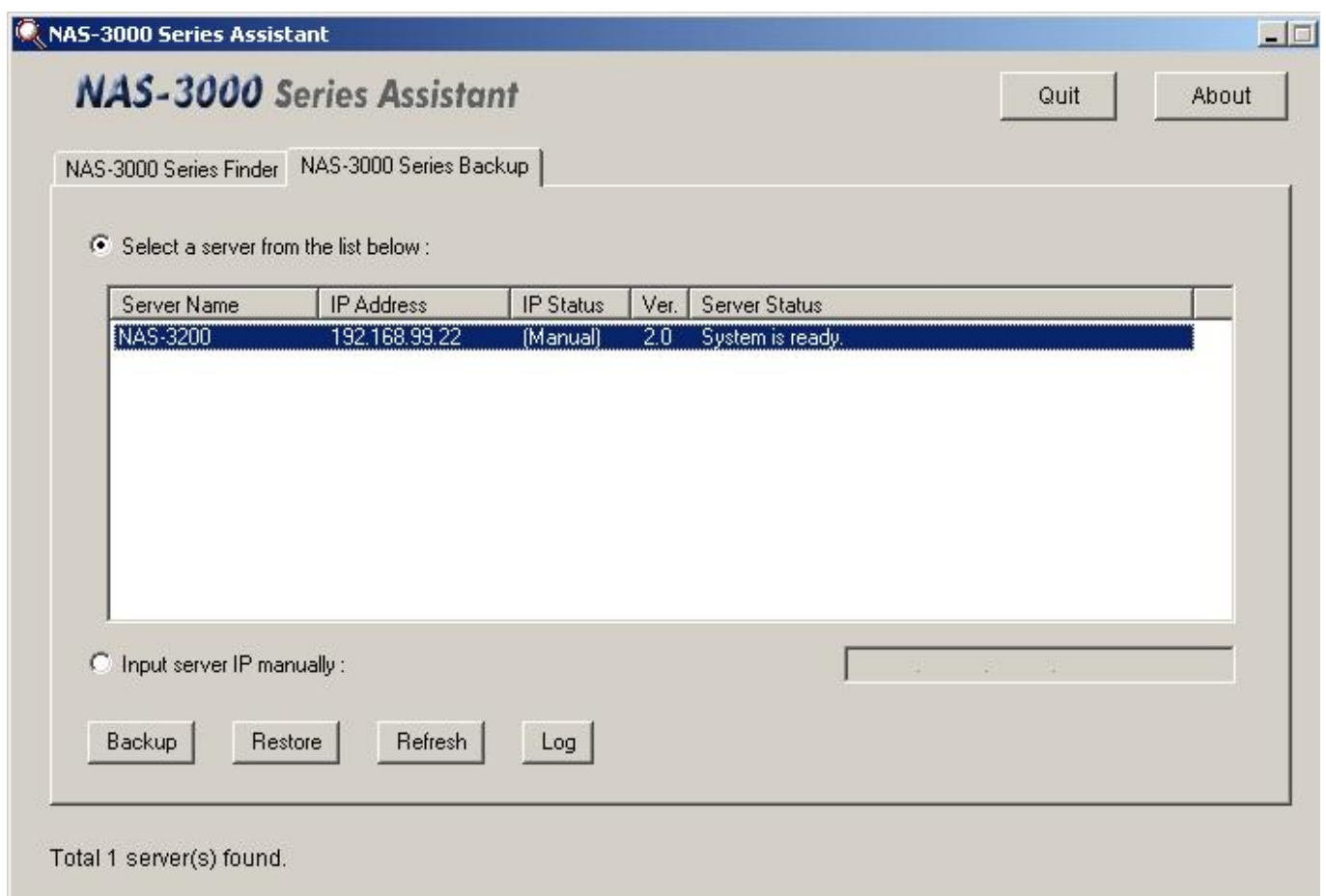
2. Click on the "Backup" button to open the backup window.
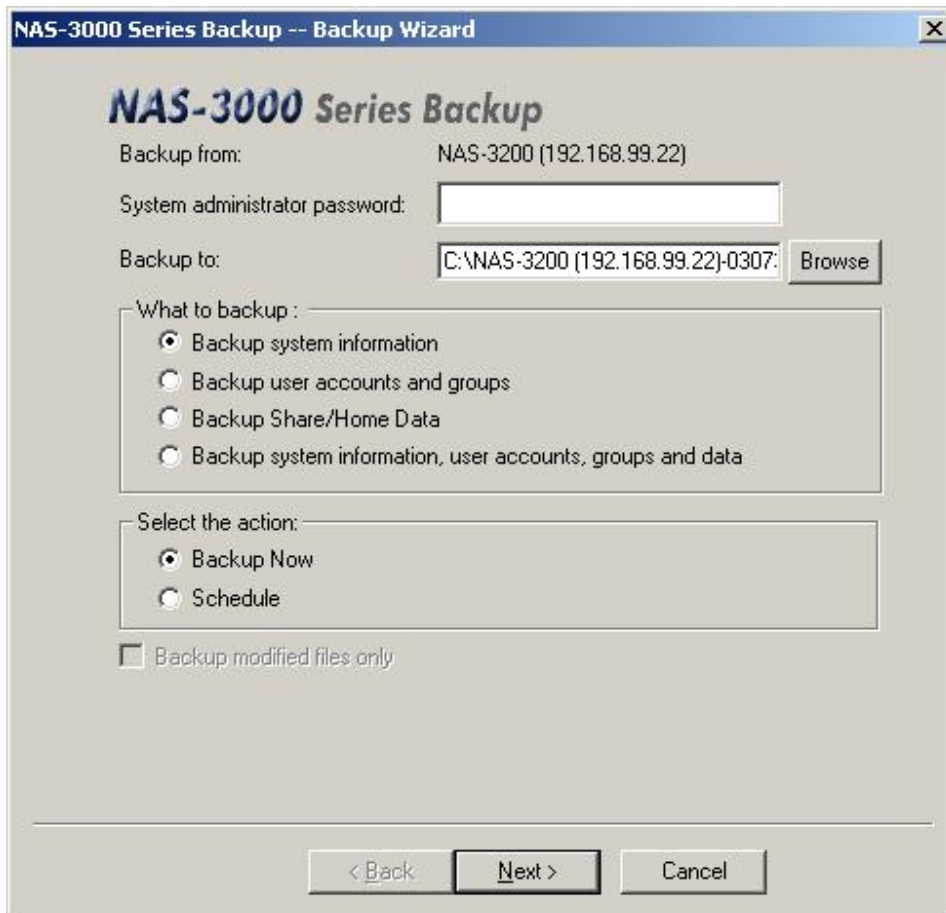
3. Enter the "System administrator password".

4. Click the "Browse" button to choose the backup path. By default the backup file is named as "server_name-mmddhhss.bkp", where mmddhhss stands for month-day-hour-minute of the backup time. The administrator can also specify the file name manually.

5. Choose the backup item from the "What to backup:" list.

If the 3rd or 4th item is selected, an additional option "Backup modified files only" is available for the administrator to choose.

Note: If the 2nd, 3rd, or 4th item is selected from the "What to backup:" list, user quota will not be backed up. In the future when the backup data is restored back to the NAS server, user quota will be set as "unrestricted", and administrator has to manually set the quota if needed.

6. Choose "Backup Now" in the "Select the action:" list and click the "Next" button.

If the 1st or 2nd backup item is selected, the backup will start right after clicking the "Next" button, however, if the 3rd or 4th is selected, the administrator can further choose which shared folders to backup.
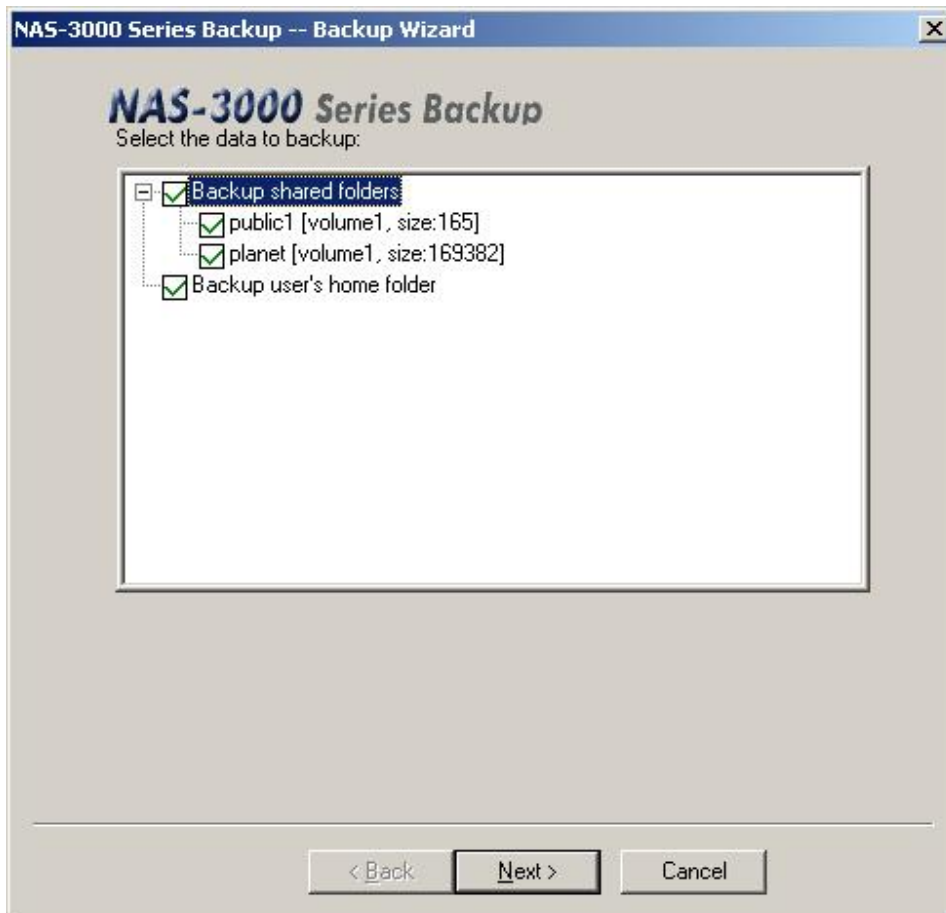
7. Check the shared folders to be backed up and click the "Next" button for the backup to begin.

Note: FAT/FAT32 does not support files larger than 4GB. When running PLANET NAS-3000 series Backup on Windows 98 clients with FAT/FAT32, or backing up files from the NAS server to another devices running Windows 98 with FAT/FAT32, the system will automatically divide the backup file into several 4GB-size files, and name the extension of each file in the order of ".bkp", ".001", ".002", etc. Please store these files in the same directory. When restoring the data back onto the NAS server in the future, the administrator only needs to specify the ".bkp" file, and other related files will also be restored automatically without manually restoring every single file.

5.2 Scheduling Backup

5.2.1 Scheduling a Backup

You have complete flexibility in scheduling a custom backup with the following steps:

1. Repeat step 1 to step 5 mentioned above.

When using Schedule to backup data, by default the file name is "Server_Name-mmddhhss.bkp", where mmddhhss stands for month-day-hour-minute of the backup time. The system administrator can also specify the file name, however, to ensure every scheduled backup can be reserved without being overwritten, if the specified file name doesn't

fit the system predefined format, an additional "-mmddhhss" will be appended to the file name.

2. Choose "Schedule" from the "Select the action:" list and click the "Next" button to go to the schedule setup window.

3. Make proper selections from "Schedule Task", "Start time" and "Schedule Task Daily" options. If you want to make further settings, click the "Advanced" button to enter the advanced settings window.
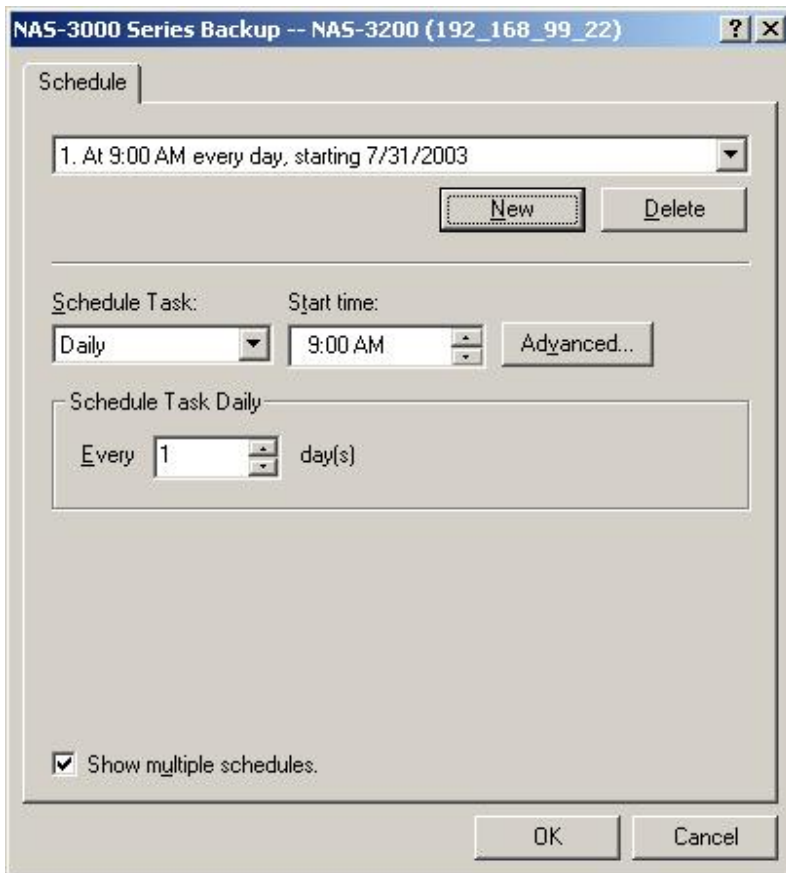
4. After finishing setting, click "OK" to close the setup window.

Now you can close the Backup Program. Windows will perform the backups according to the schedule.

5.2.2 Scheduling Multiple Backups

You can also schedule multiple backups to perform backups according to different schedules. For example, if you want to backup "system information" at 12 o'clock on Mondays and "user accounts and groups" at 6 PM on Tuesdays, you can set up two different schedules, so the backups will be done accordingly.

To schedule multiple backups, follow the steps:

1. Create the first schedule according to the description on the "Scheduling a Backup" section.

   Take the server named "NAS-3200" for example, after the schedule is created, PLANET NAS-3000 series Backup will generate the following items:

   i. A schedule item "NAS-3000 series Backup—NAS-3200" on Schedule Task of Windows system's Control Panel.

   ii. A configuration file "NAS-3200.bkc" on the directory where the Windows OS is installed. This profile will record the time to perform schedule backup and the backup item.

2. Rename the following items:

   i. Rename the schedule item "NAS-3000 series Backup—NAS-3200" to an identifiable name, for example, "NAS-3000 series Backup—NAS-3200-schedule1".

   ii. Rename the configuration file "NAS-3200.bkc" to an identifiable name, for example, "NAS-3200-schedule1.bkc."

   iii. Right-click "NAS-3000 series Backup—NAS-3200-schedule1" and choose "Properties". Change the configuration file name "NAS-3200.bkc" that appears on "Run" field to "NAS-3200-schedule1.bkc". Please note that the changed name of the configuration file should be identical with the exact configuration file so that the schedule task can perform correctly.
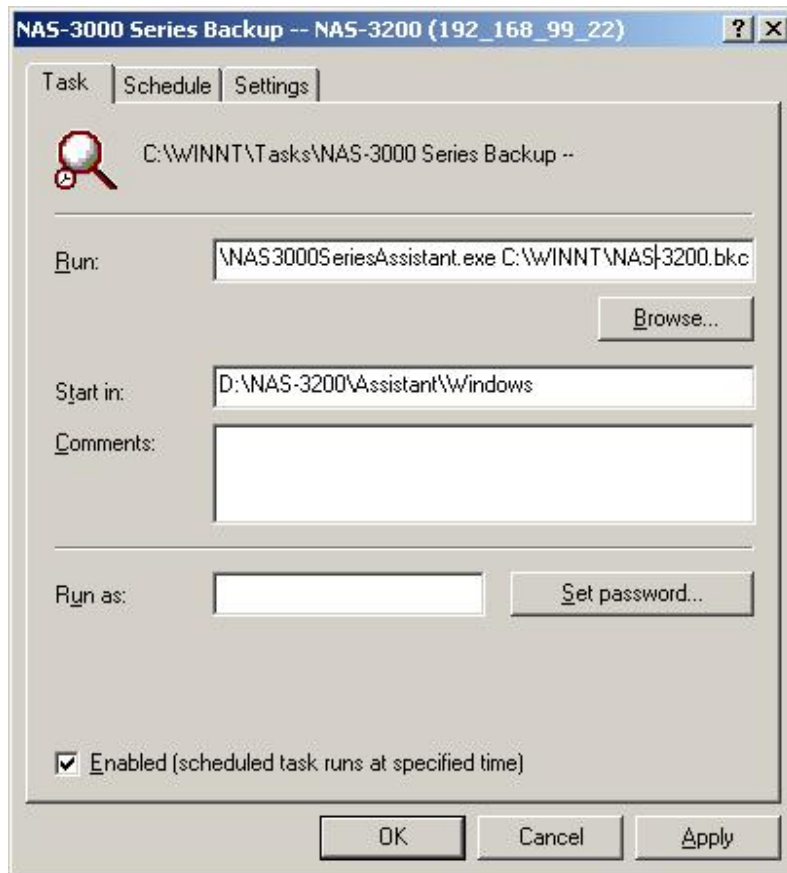
5.2.3 Deleting Schedule

If you want to delete predefined schedule, go to the schedule page, check the "Show multiple schedules" on the bottom. Press the "Delete" button to delete the schedule.

If you have set up multiple schedules, you can only delete the last created schedule from the schedule setup page. If you want to delete all schedules, go to Schedule Task on Windows system's Control Panel to delete all created schedules directly.

5.3 Restoring data back to the server

Follow the steps below to restore data to the server:

1. Activate PLANET NAS-3000 series Assistant, click the NAS-3000 series Backup tab, and select the server to restore data to from the server list, or select "Input server IP manually" and input the server IP.
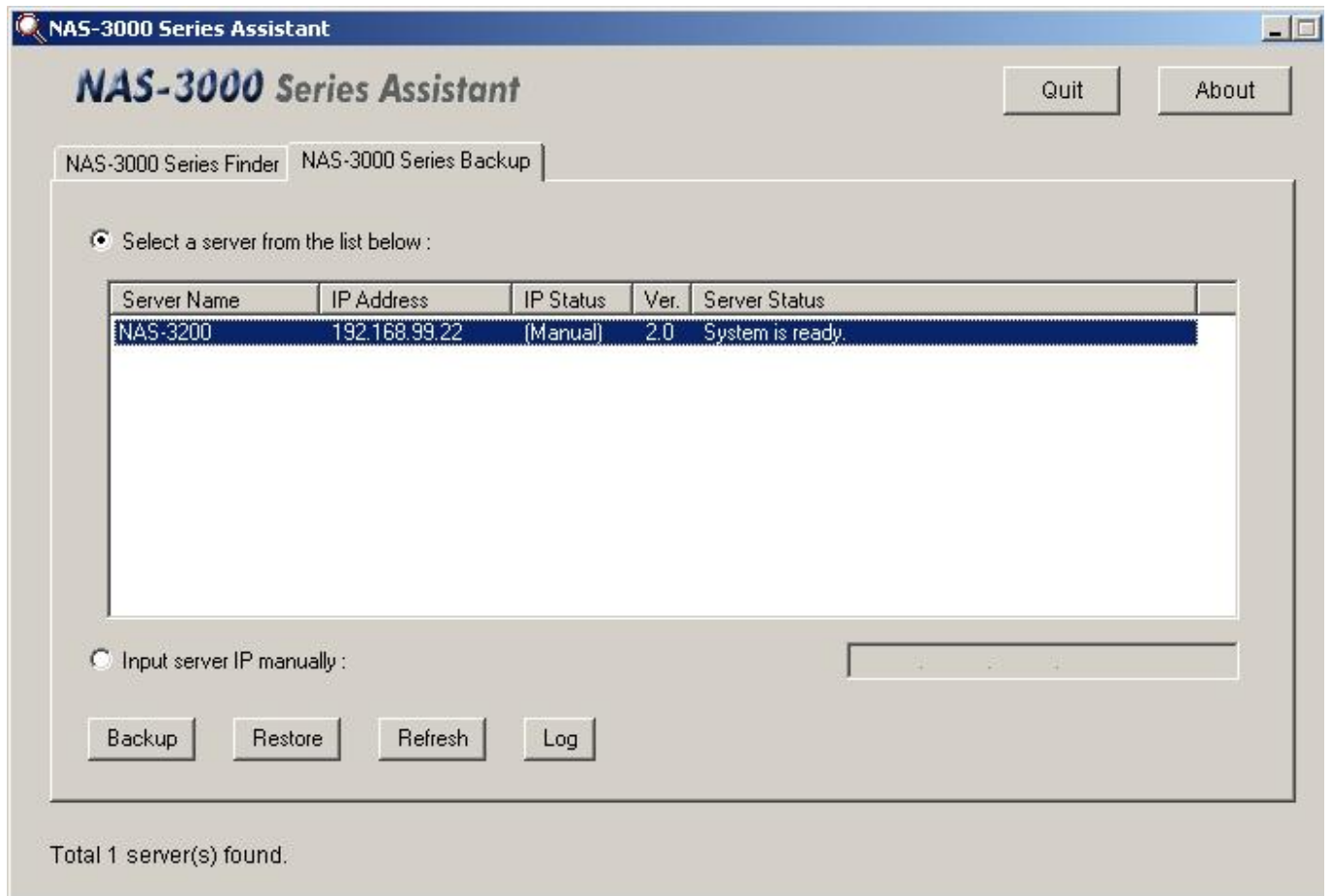
2. Click the "Restore" button to run the restoration wizard.
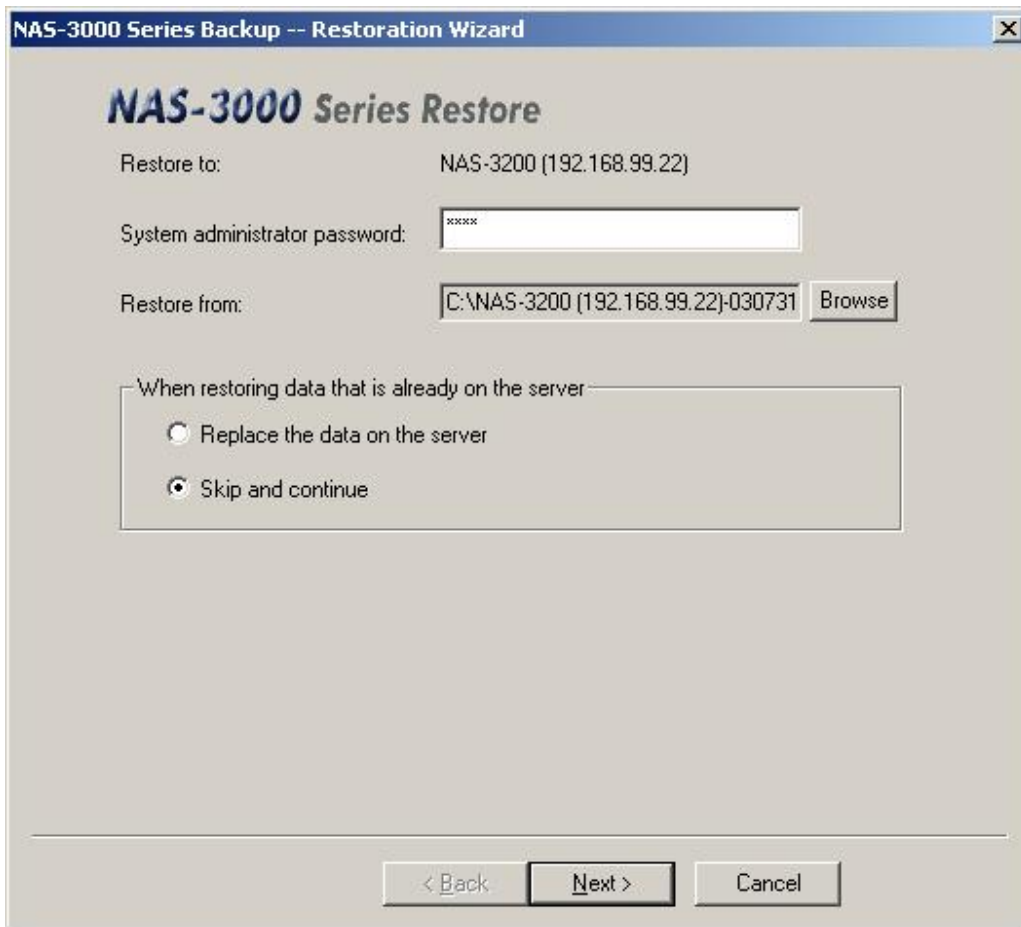
3. Enter the "System administrator (root) password".

4. Browse for the backup file to restore form the "Restore from" item. If previously only changed data was backed up, restoring each ".bkp" file chronologically is necessary in order to restore the NAS server to a designated date.

5. Choose to "Replace the data on the server" or "Skip and continue" when restoring data that is already on the server.

With "Replace" mode, "shared folder" is the comparison basis. For the share folders with the same name, the system will replace all data in the folders automatically.

With "Skip and continue" mode, "file" is the comparison basis. When a shared folder on the NAS server has the same name with that in the ".bkp" file that is to be restored, the system will not skip this folder; instead, it merges the data of both folders and skips the files with the same name. The only exception is: for user's home folder, if some home folder on the NAS server and that in the ".bkp" file do not belong to the same user, this folder will then be skipped for security reasons and will not be merged by the system.

6. Click "Next" to proceed.

7. Select the items to restore and click "Next" to start to restore data.
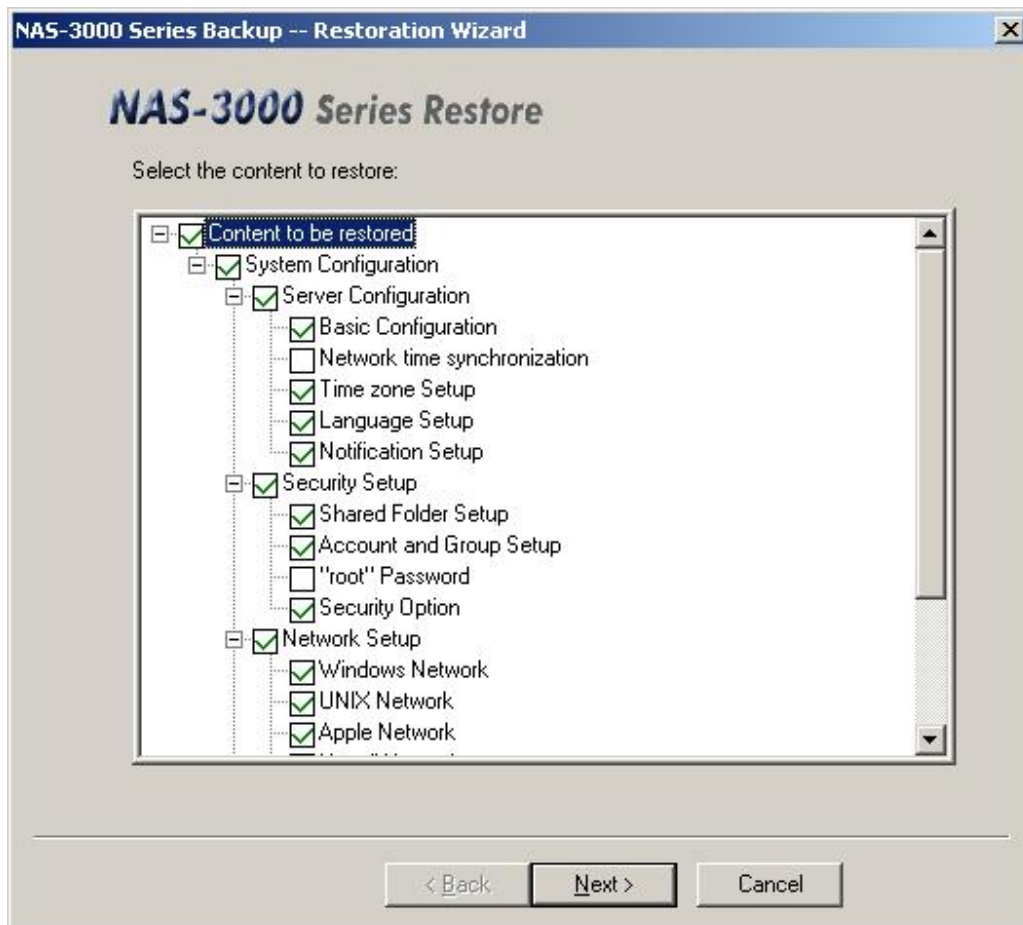
8. If the backup file contains data of shared folders, you can further specify the path to restore these shared folders.
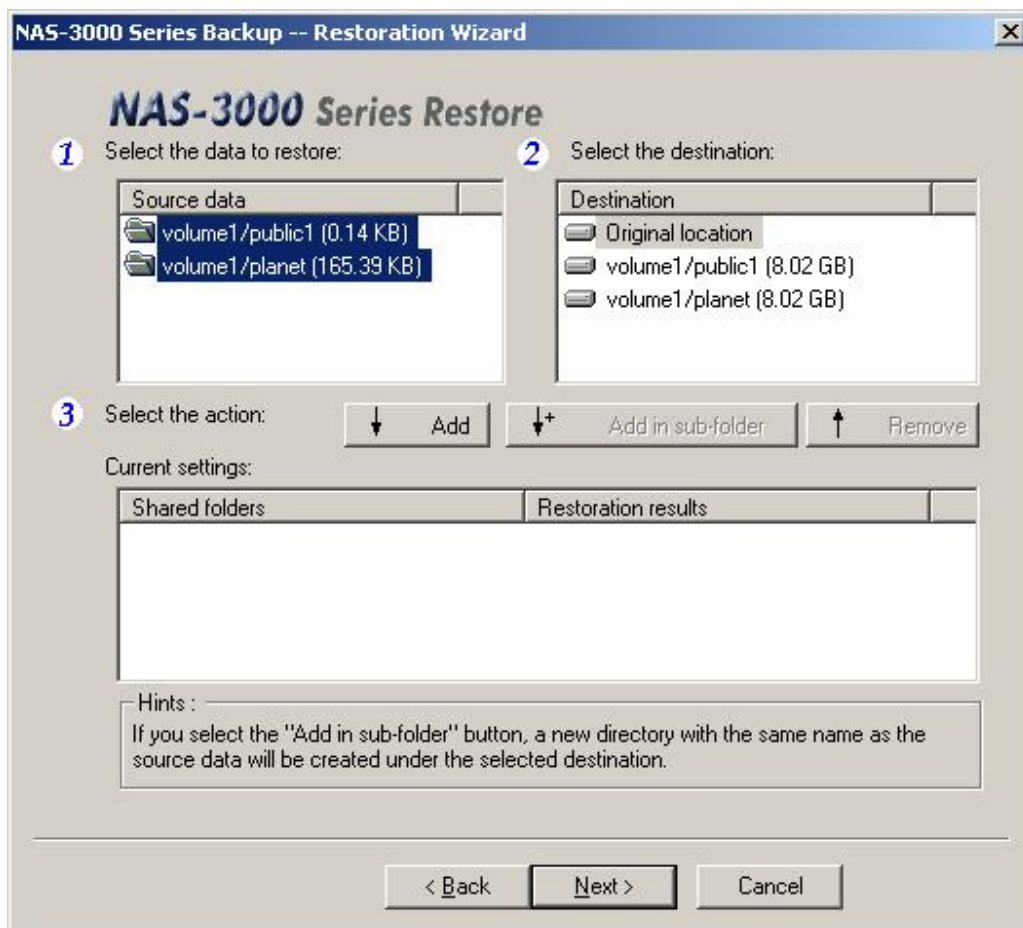
By default the program will select all source data in the "Select the data to restore:" column and "Original location" in the "Select the destination:" column, however, you can change the setting as your need. After the change is made, click the "Add" or "Add in sub-folder" button to add the setting to the list below, then click "Next" to start the restoration.

Please note that for the users' home folders, a sub-folder will be created in the destination location either "Add" or "Add in sub-folder" is chosen.

9. Restoration finishes.
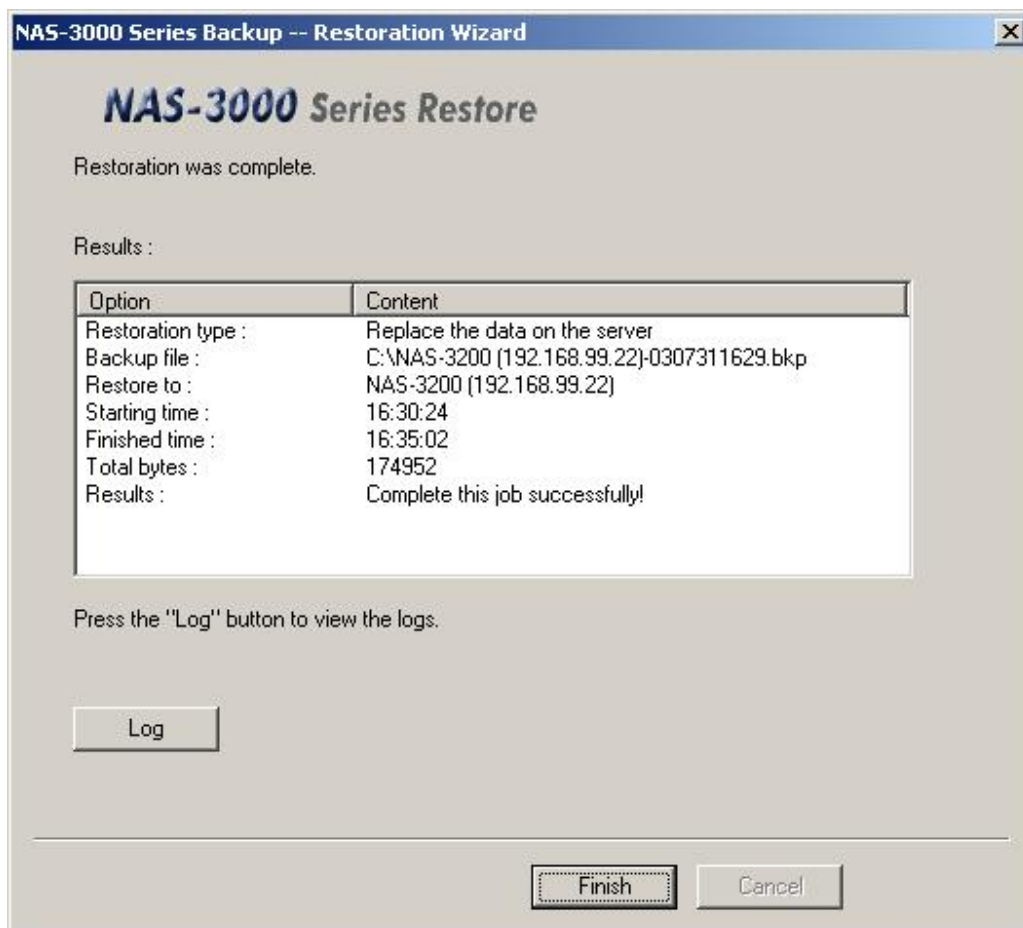
Note:

1. When restoring data back onto the NAS server, please verify there is enough storage space on the server for data restoring; otherwise the restoring process will fail.

2. When backing up/restoring data, many temporary files will be generated in the first volume of the system, therefore the backing up/restoring cannot be performed if the free storage space in the first volume is less than 100MB.

3. When the system fails to backup/restore data on the NAS server, the system administrator will receive e-mail with an error code notifying the data backup/restore failure. The administrator can also go to "system log" tab and search for the error code in the log file.

5.4 Third party backup support

NAS server supports various third party backup tools to backup data from the server. Please see Appendix "Third party backup support" for detail.

Chapter 6

Using Data Replicator

Backup is necessary for ensuring data completeness. But people are always too busy to backup regularly. In order to make users backup more efficiently and on a timely basis, PLANET NAS-3000 series Replicator can fully automate the backup process from Windows client to the NAS server. It features:

1. Monitor file folders of Windows clients and perform immediate backup of selected folders to the NAS server;
2. Password-protect files to make them more secured;
3. Compress backup files in order to save storage space on the NAS server;
4. Provide version management function and save up to 20 file versions in the NAS server;
5. Provide tag management function, tag the most representative version, save up to 20 tags;
6. Restore files from the NAS server to client computer when needed in the future, making file backup, management and protection easy.

6.1 Before you begin

6.1.1 Set up the NAS server

Before you begin using PLANET NAS-3000 series Replicator, network administrator must set up the NAS server on the LAN, and create accounts for all users of Data Replicator on the NAS server.

1. Network Setup
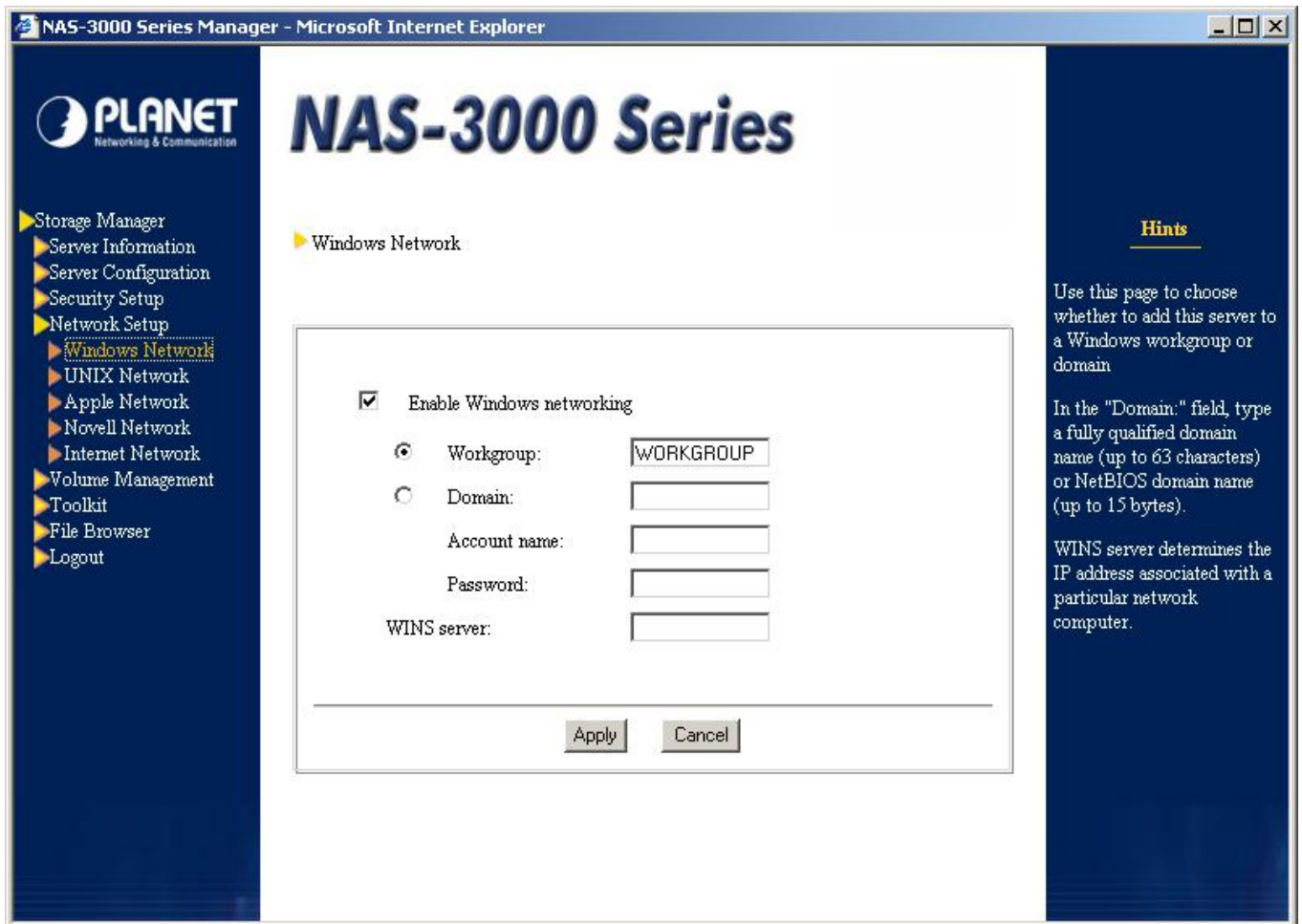
Please Enable Windows networking in Network Setupà Windows Domain of **NAS-3000 Series Manager**.

2. Account Setup
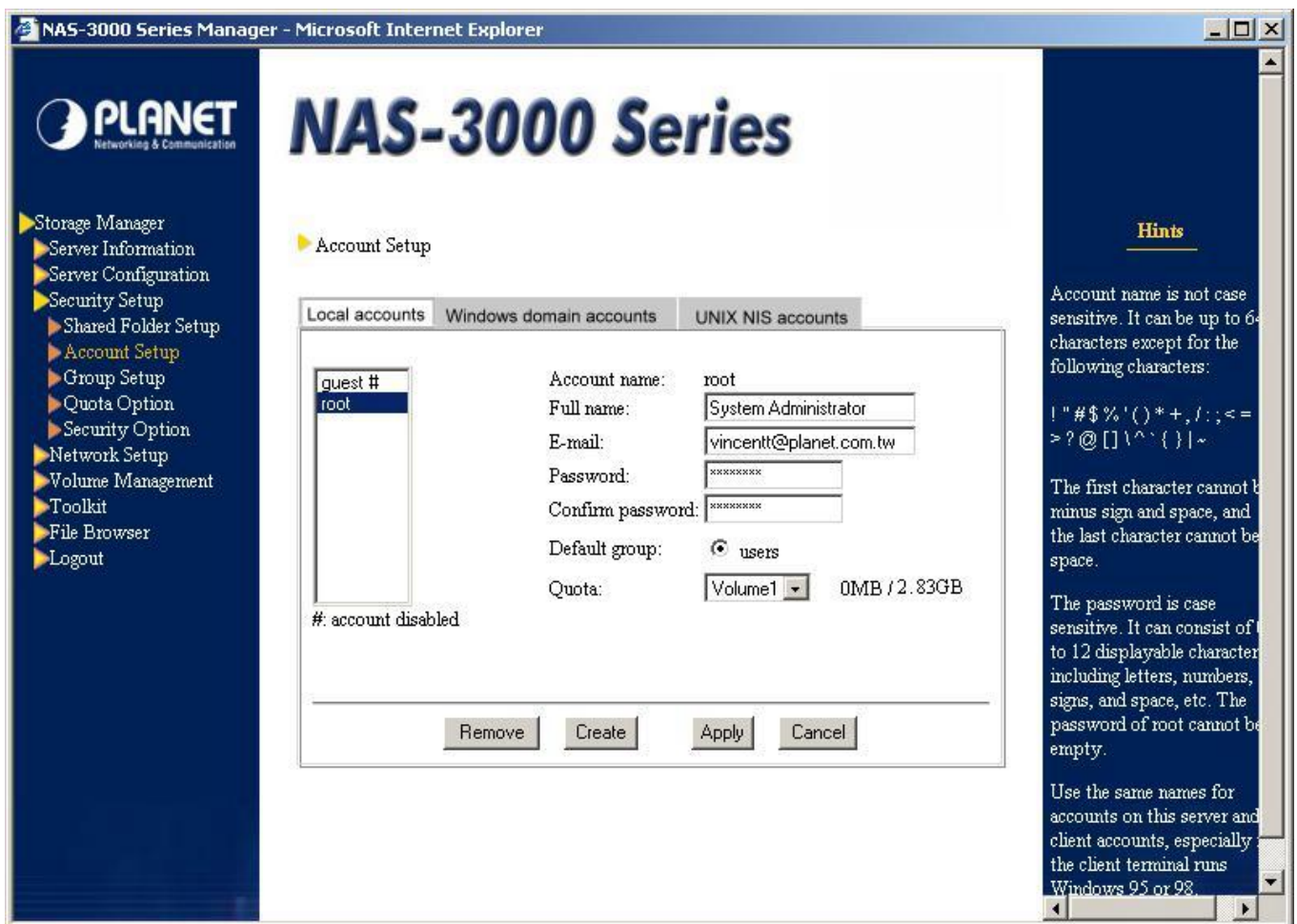
PLANET NAS-3000 series Replicator allows user to backup files to any shared folder with full access right in the NAS server. But due to security consideration, we urge user to backup files to his/her own home folder in the NAS server to prevent other users from unintentional deletion, modification, and use of these files. Thus, in addition to creating account for PLANET NAS-3000 series Replicator users in the NAS server, we suggest system administrator to assign these users to the "users" group so that each user can have his/her home folders only he/she can access.

In addition, when a Windows NT/2000 user desires to save file to the NAS server, Windows operating system (OS) will ask him/her to key in account number and password in the NAS server to authenticate his/her identity. But when a Windows 98/ME user accesses the NAS server, Windows OS will capture directly the account the user used to login to Windows and will only ask user to key in his/her password. If the account the user used to login to Windows client station does not match the account in the NAS server, the user cannot use the NAS server because of mismatched identification. Therefore, in order to make management easy, system administrator must keep the account in the NAS server and Windows client consistent.

3. Language Setup.
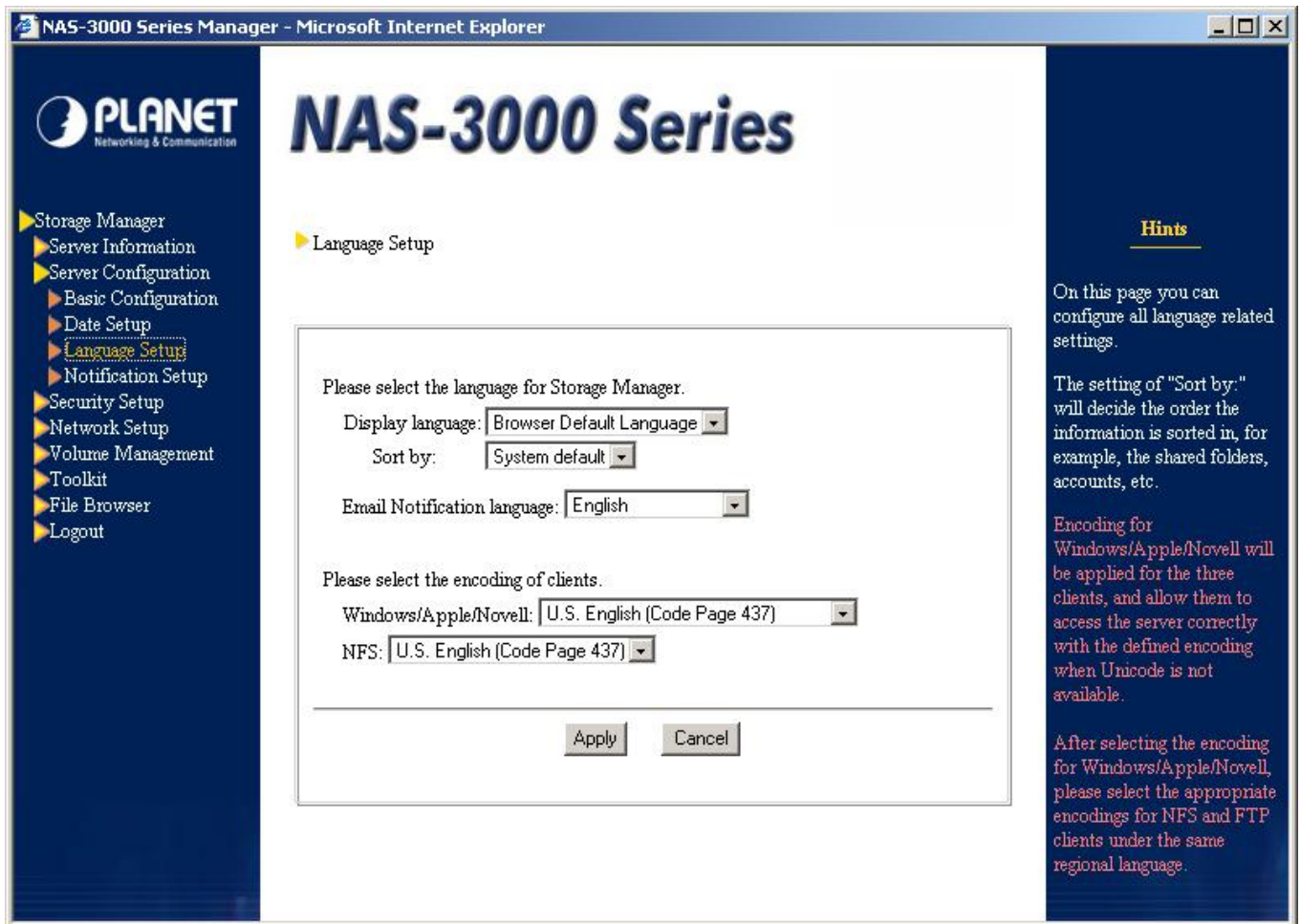
Please make sure the NAS server and the Windows client running PLANET NAS-3000 series Replicator use the same encoding. A wrong setting may result in problems when accessing data

6.1.2 PLANET NAS-3000 series Replicator Basic Requirements

1. 5MB Hard Disk Space

2. Operating System: Windows 98/ME/NT/2000/XP

3. Optimal Screen Resolution: 1024*768 or above

4. The Windows client running PLANET NAS-3000 series Replicator has to support Microsoft Networking over TCP/IP protocol, and can be connected to the NAS server through physical network medium (e.g. hub, switch, etc.).

6.2 Install PLANET NAS-3000 series Replicator

Insert the bundled CD in the CD-ROM drive to initiate the autorun program. Once completed a menu screen will appear as follows.

Please click on the hyper link of "NAS-3000 series Replicator" to enter the file folder. Double click on the file "setup.exe" and install PLANET NAS-3000 series Replicator to your hard disk according to the instruction given on the screen.

6.3 Start Using PLANET NAS-3000 series Replicator

6.3.1 Backup Windows client data to the NAS server

First-Time Use & Run Complete Backup

When running PLANET NAS-3000 series Replicator the first time, user must first backup all the files in this machine's file folders to the NAS server before modified/new versions can be monitored.

1. Start the Backup tab.

2. In the "Server" field, select the destination to store backup files. Click the "Browse" button to display the search page and select the NAS server and shared folder where you wish to store your backup files. After the selection is complete, click "OK" to return to the previous page.

The column at the top of the search page will list all shared folders a user have read/write access to. But due to security consideration, we urge user to backup files to his/her own home folder in the NAS server to prevent other users from unintentional deletion, modification, and use of these files.
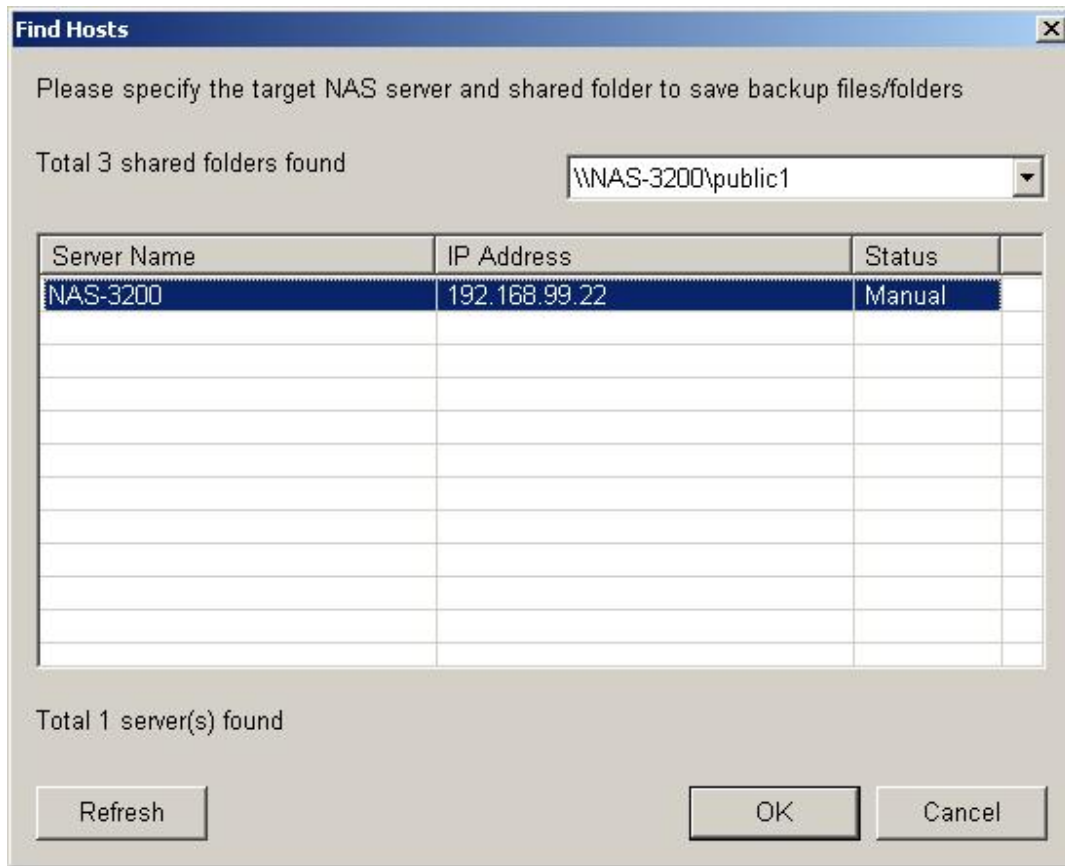
3. Select those file folders of this computer you wish to backup/monitor in the tree structure below.

4. Click the *Upload* button on the right side to display the dialogue window below:
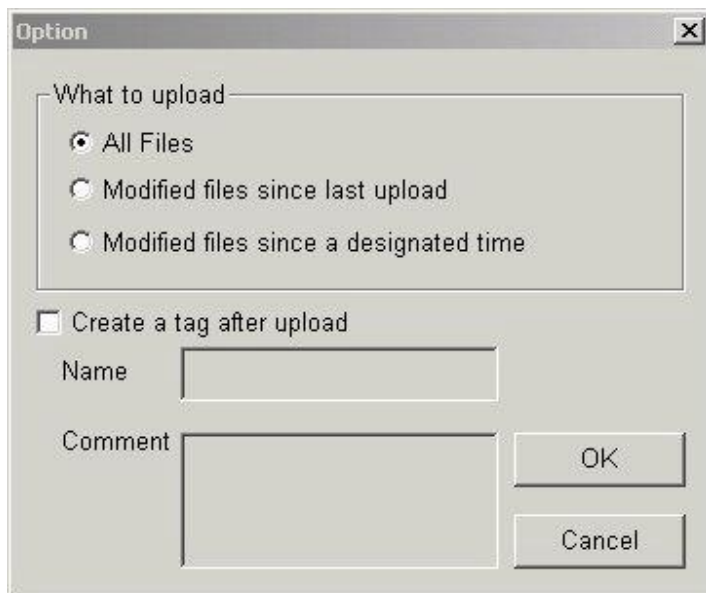
Because this is the first time you use PLANET NAS-3000 series Replicator for backup, please select "All Files" from the "What to upload" column.

If this version has a special representative meaning, user may select the option "Create a tag after upload" so that after the upload is complete, this version can be created with a tag to allow for easy restoration in the future.

PLANET NAS-3000 series Replicator allows the user to create up to 20 tags. The purpose of tag is to help user record version of a specific time. For example, if a software engineer has already completed program version 1.0 and is prepared to start coding version 2.0. For this engineer, version 1.0 is the version with special representative meaning. While completing all version 1.0 program files, he/she can create a tag for these files at the specific time. In case any problem is encountered while modifying version 2.0, the engineer can easily restore all 1.0 program files to his machine for further modification.

5. After you have completed the selection, click "OK" button. PLANET NAS-3000 series Replicator will backup all the files in the selected file folders to the NAS server designated.

Note:

1. PLANET NAS-3000 series Replicator only targets its monitoring on file folders and sub file folders in the local hard disk. The monitoring does not include network disk drives or other external storage devices.

2. PLANET NAS-3000 series Replicator does not support monitoring of files under the root directory in this machine.

Monitor File Folders in Your Own Computer

After first-time backup, PLANET NAS-3000 series Replicator can help its user to continue monitoring file folders in his/her computer. Any changes made to files in the file folders will be saved to the NAS server.

To monitor the file folders of your own computer, please select file folders of your machine and the NAS server to save backups, and then and click the "Monitor" button. PLANET NAS-3000 series Replicator will be minimized to the system tray to perform monitoring.

Backup changed data only

When files at the client are large and changed frequently, if every time any change made to these files are updated automatically to the backup in the NAS server, this may cause heavy network traffic. Due to consideration of performance efficiency, after running the complete backup in the first instance user may choose not to run automatic monitoring, instead the user should manually upload the changed files to the NAS server.

To backup any changed files, please select the file folders on your machine and the NAS server to save backups, click "Upload" button on the right, select "Modified files since last upload" to backup any changes made since last update or "Modified files since a designated time" to backup any changes since a specific time.
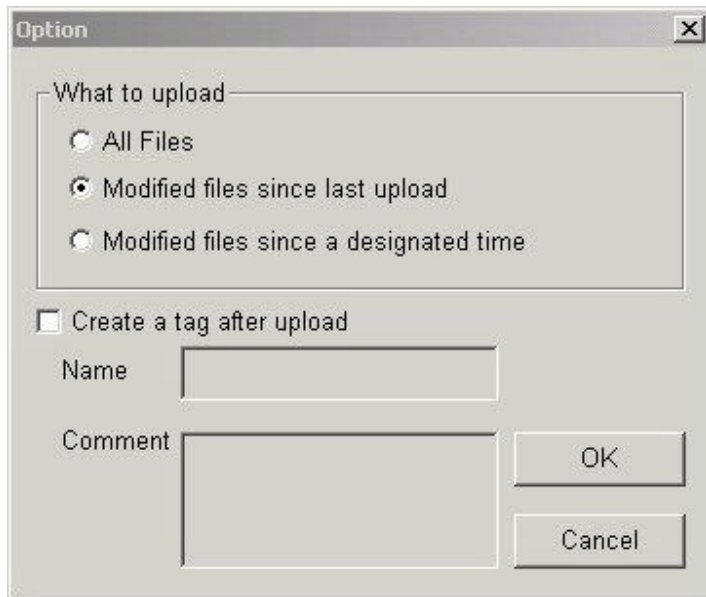
Files Filtering

User may choose not to backup non-essential files (e.g. .tmp or temporary files created by Windows client)

To setup not to backup by file type, click "Filter" on the right and add "extension" or "prefix" to avoid backing up of files with the extension/prefix.
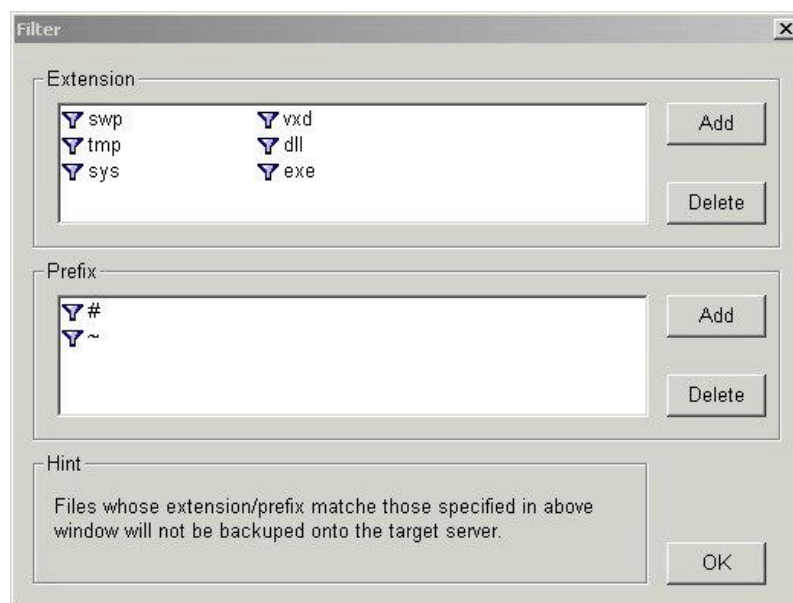
6.3.2 Recover files from the NAS server to Windows client

1. Select the "Restore" tab. In the right column is the display of backup file directory in the NAS Server. PLANET NAS-3000 series Replicator by default uploads Windows client files to the

---

directory on the NAS server: *\DR BACKUP-client computer name\the disk of the client computer*. The column on the right displays all subdirectories/files in each directory.
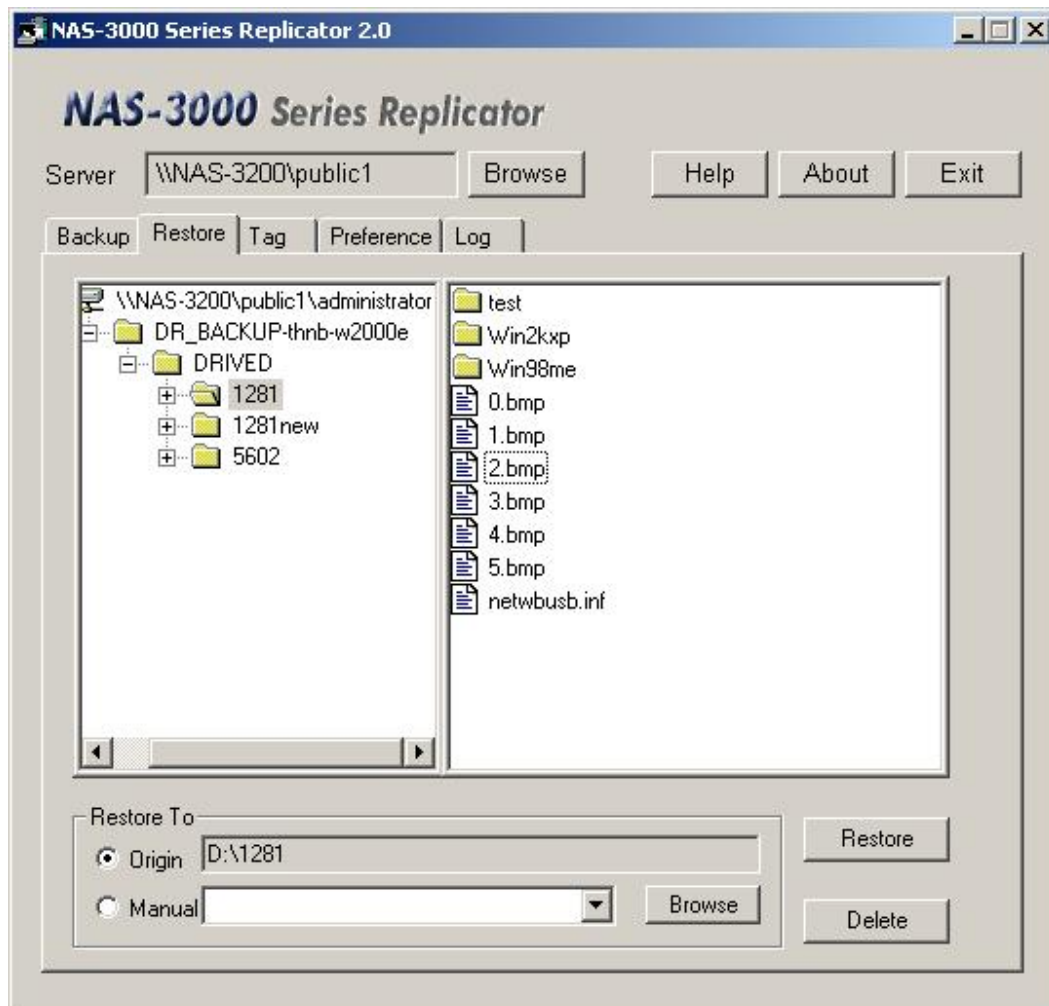
2. Select at the bottom of the page the destination of the restored files. (Path of your own machine)

3. Select files or file folders from the right-hand column, click the right mouse button, click "Restore" in the browse function. Or click the "Restore" button at the bottom of the window.

   When restoring an individual file, you can only choose to restore by specific version, and when restoring more than one file or file folder, because of different versions for each file, you can only choose to restore the "Current Version" or tag.

6.3.3 Tag Management

PLANET NAS-3000 series Replicator allows the user to create up to 20 tags. The purpose of the tag is to help user record version of a specific time.

Once the number of tags has reached 20, and the user wants to add more tags, it is required to

manually delete unwanted tags from the previously created tags. PLANET NAS-3000 series Replicator will not delete the oldest tags automatically when the user creates more than 20 tags.

The tag name is using the date and time of the tag is created by default. For example, "0111072228" means the tag is created on November 7, 2001 at 10:28 pm. User may change the tag name according to his/her preference.

There are two ways a user can create a tag:

1. Add new tag after files upload.
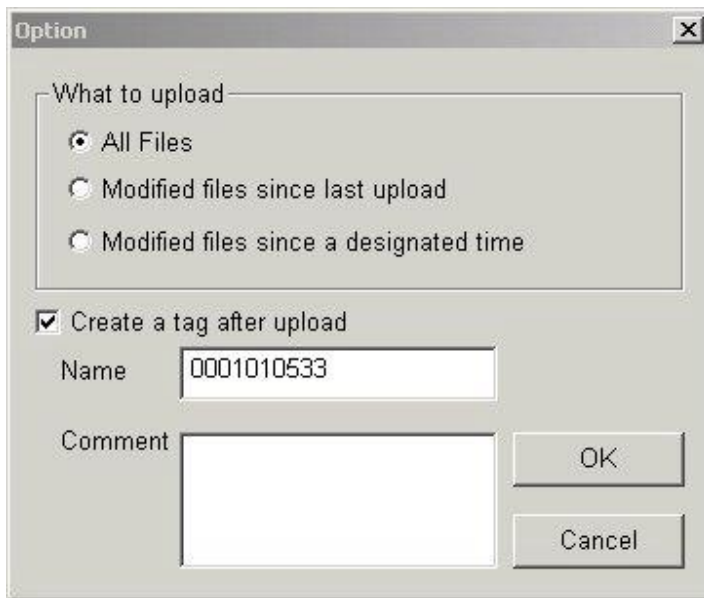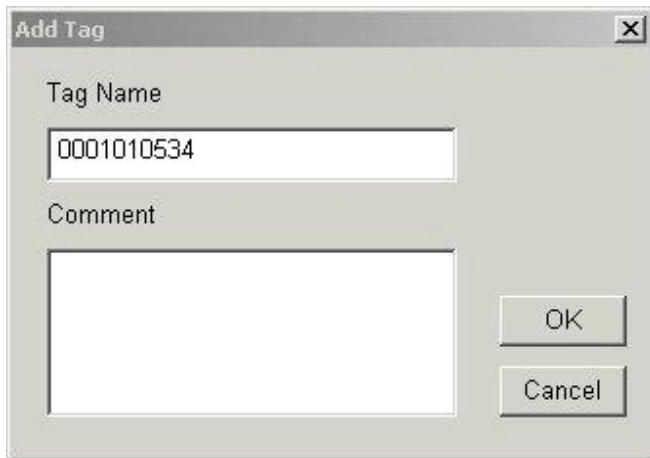
User can create new tag to uploaded files when uploading files in the "Backup" tab.

Please note, when creating tag the most updated versions of files in backup directories in the NAS server will be saved. The two examples will illustrate this point:

 i. During uploading of "All Files", if you click "OK" after selecting "Create a tag after upload", PLANET NAS-3000 series Replicator will create a tag for all files uploaded to the NAS server after upload.

 ii. When uploading "Modified files since last upload" or "Modified files since a designated time", you can select "Create a tag after upload" and click "OK". Accordingly, PLANET NAS-3000 series Replicator will create a tag for all files uploaded (the most updated version) and the latest version of files not uploaded (due to no change) but already existed in the NAS server.

2. Create a new tag in the "Tag" tab.

Select "Tag" tab, click "Create" button, and then click "OK" after key in "Tag Name" and "Comment". PLANET NAS-3000 series Replicator will create a tag for the latest version of every file in the NAS server backup directory. If user enables "Upload files before adding new tag" in the "Preference" tab before new tag is created, PLANET NAS-3000 series Replicator will upload changed files from client to the NAS server and then create tag after the upload. This is to ensure that all tags created represent the latest version at the client station, especially before user starts to run the monitoring function.

6.3.4 User Preferences

Upload

1. Upload before monitoring.

   When this option is selected, each time "Monitor" is executed, the system will check to see if there are files that have not been backed up. If yes, it will automatically upload these files. This is to prevent client computer to change certain files when there is network disconnect or if user did not run monitor immediately after running the complete backup in the first instance.

2. Upload before creating tag.

   If user enables this option, PLANET NAS-3000 series Replicator will upload changed files from client to the NAS server and then create tag after the upload. This is to ensure that all tags created represent the latest version at the client station, especially before user starts to run the monitoring function.

File Copying

1. Copy with compression

   In order to save storage space, when this option is enabled, PLANET NAS-3000 series Replicator will compress all backup files stored in the NAS server.

2. Copy with encryption

   In order to ensure data security and prevent others from data interception, user can choose this option to have password protection for files in the NAS server.

Initialization Setup

1. Auto start when login.

   User can choose to run PLANET NAS-3000 series Replicator in client station after it is powered on.

2. Start with monitoring.

   User can choose to run "Monitoring" after starting PLANET NAS-3000 series Replicator. Of course, if you also enable "Upload before monitoring", once a user is logged in, the system will first upload all the files that have not been uploaded before running the monitor function.

Version Setup

PLANET NAS-3000 series Replicator can support up to 20 versions. User can choose to select the number of versions for files to be backed up.

Assume a user chooses to backup 20 versions, each backup file will be given an extension that

indicates its version number, that is, the first version of the backup file will be given the file extension "v00", the second "v01", and so on. This number will increase each time a new version of file is backed up. When all twenty versions are used up, you will see a file extension of "v20" and the file with the extension "v00" will be deleted. Following this numbering scheme, the file extension will increment and accumulate until "v99" and then reinitialized to "v00" to begin a new cycle.

Trouble Shooting

Q: First-time Network Setup with PLANET NAS-3000 series Assistant fails.

A: Please check the followings:

1. Make sure you have selected the correct server.

2. Make sure the server is connected to the LAN. Check the LAN LED on the server panel to see if the connection is normal.

3. Make sure the power source is connected to NAS server and power is on.

4. Make sure the LAN still has free IP addresses.

5. Make sure the manually entered network settings are correct.

6. Make sure the client terminal you are using has correctly installed/set up the TCP/IP protocols, and is running Microsoft Internet Explorer 5.0 or higher.

7. Make sure the NAS server and the client computer that runs PLANET NAS-3000 series Assistant can be connected through physical network medium (e.g. hub, switch, etc.).

8. The firewall function of some firewall or anti-virus software will cause failure for the PLANET NAS-3000 series Assistant to find NAS servers. Please disable the firewall or anti-virus software and try again.

Q: Cannot use Internet Explorer to connect to NAS server.

A: Please check the followings:
 	
   1. Check if the network settings of the NAS server are correct and make sure that the IP of the NAS server does not conflict with those of other servers on the LAN.
 	
   2. Make sure the Windows client has correctly installed/set up TCP/IP.
 	
   3. Make sure the NAS server and the client computer that runs Microsoft IE can be connected through physical network medium (e.g. hub, switch, etc.) and in the same subnet.
 	
   4. Make sure that the browser is IE 5.0 or above and it can connect to other servers in the network.
 	
   5. Try typing the server name of the NAS server in the address field of IE.
 	
   6. Try typing the IP address of the NAS server in the address field of IE.
 	
   7. Try restoring the IE settings to defaults and try again.
 	
   8. Try restarting the server.

Q: Buttons missing on Date/Time page in Quick Configuration.
A: Certain web trap modules of anti-virus software cause a situation where certain buttons on the Date/Time Page of the Quick Configuration module cannot be displayed. Disable the web trap and try again, or use a different terminal for the setup.
Q: System boot failure.

A: There are two possibilities that could cause a system reboot failure.
 	
   1. If the system administrator has ever added the NAS server into a NIS domain before, he/she will not be able to reboot the NAS server in case the NIS server is not available. Please make sure the NIS server is available first and then restart the NAS server.
 	
   2. At least one hard disk has to be installed before booting up the server.

Q: It takes a long time to start the server and it seems to be a boot failure.

A: If the NAS server is improperly shut down when it is operating, the system will automatically check the file system when the server is restarted. The more data are saved on the server, the longer the system check will take. It probably takes from several minutes to several hours, and sometimes users tend to regard it as a boot failure.

If clients cannot access the NAS server after turning on the computer, check the LED on the server. If the lights under the hard disks keep blinking, it means that the system is still checking the file system and the booting has not completed yet. Wait until it finishes instead of improperly shutting down the server again, or removing the hard disk drive. The booting is completed when the LED on the front panel of the server is back to normal.

Q: The server shuts down right after being booted.

A: You need at least one hard disk to boot the server.   When such a problem occurs, check if there is a hard disk installed on the server. If not, install the hard disk onto the server and then reboot it.

Q: Hard disk failure.

A: When any hard disk in the system fails, it will be reported on the NAS-3000 Series Manager's Server Informationà Status page. A notification will be sent to the system administrator, who will only need to shut down the server, replace the failed hard disk with a new one, and reboot. The system will automatically configure the new hard disk.

A Non-RAID or RAID 0 volume has no inherent safety measures so that if any hard disk fails, all data on that volume will be lost. However, for a RAID 1 volume, after a new hard disk is replaced, the system will automatically rebuild the disk and all the data on the volume.

Note:

1. The replacement disk should be a new and empty disk. In the interest of smooth system operation and better performance, try to use the same brand and disk model for all disks.

2. Before inserting the new disk, make sure its jumpers are correctly set.

Q: Hard disk rebuild failure.

A: The following reasons can cause a hard disk rebuilding operation to fail:

1. The hard disk used to rebuild is damaged. Try using a brand-new hard disk.

2. The hard disk used to rebuild is too small to rebuild the original volume on it.

3. The jumpers of the hard disks are set incorrectly. Since jumper settings depend on the model, refer to the instructions that came with your hard disk.

4. The hard disk used to rebuild is of a different type. E.g., if the original is an ATA 100 model, and you try to use an ATA 66, or a similar model from a different manufacturer, the data rebuild may fail. Always use models from the same vendor with similar specifications.

Q: After inserting the hard disk and turning on the computer, Removed is displayed on the Server Information > Status page of the NAS-3000 Series Manager.

A: Please check the followins:

1. Please check if the connection between the hard disk and the cable is correct.

2. The NAS server only supports hard disks with jumpers configured on Master mode. Please make sure the hard disks are not configured as Slave or Cable Select.

Q: Cannot browse files/folders on the page of "File Browser".

A: Update the web browser to IE 5.5 or above.

Q: Failed to download files to Windows clients from the "File Browser".

A: When downloading a file to Windows clients from the "File Browser", Windows will first copy the file to a system temporary directory and the file will only be redirected to the user-defined location after the copying finishes, thus the Windows client should keep available space at least twice the file size when downloading files.

Q: Cannot find the NAS server in "Network Neighborhood".

A: Please check the followings:

1. Make sure that the NAS server has been turned on and connected on the LAN.

2. Make sure the system administrator has enabled Windows Networking on the NAS server.

3. Make sure the Windows client has correctly installed a TCP/IP server.

4. Enter "My Computer" or "Windows Explorer" and input "\\Server_Name" in the field of http address.

5. Start "Findà Computer" on the Start Menu, input the name of the NAS server and search for it.

6. Click on "Toolsà Map Network Drive" in "My Computer" or "Windows Explorer". Enter "\\ Server_Name\public1" in the field of "Path." Press OK to open and connect with the public1 folder on the server.

Q: Cannot access the file(s) in a certain shared folder on the NAS server via Windows clients.

A: Please check the followings:

1. Check if there is such a shared folder on the NAS server. In some cases, a shared folder on the NAS server deleted by the system administrator may still be shown in "Network Neighborhood" in the Windows client's terminal. This is due to Windows limitation that it cannot real-time update "Network Neighborhood".

2. Make sure the system administrator has enabled Windows Networking on the NAS server.

3. Make sure this account has authorized access to the shared folder.

4. Check if the account used for logging into the Windows 98/ME client also has a same-name account on the NAS server or Windows domain, and check if the password is correct.

5. Make sure that the system administrator does not set a password for the guest account when users log in as guest.

6. If users have added the NAS server into a Windows domain, please check that the Windows domain controller is operating normally. The system administrator can try to re-join the NAS server to the Windows domain in NAS-3000 Series Manager. In addition, please check the client failed to access the NAS server has correctly logged onto the same Window domain.

7. Check to see if there are any hosts on the network using the same IP or server name as the NAS server. If there are, correct the situation as soon as possible.

8. When a Windows 2000 client cannot access privileged files unexpectedly, it could be the client has been logged in as a guest because the wrong account name was entered when logging on to the NAS server. Please log out of the server and log in again.

9. If all the above settings are correct, please reboot the NAS server.

Q: After the Windows XP Professional client successfully logs in the NAS server, the NAS server does not require user authentication when the client logins again after the client PC is rebooted.

A: This is a new feature "manage my network password " of Windows XP Professional. When logging in a NAS server for the first time, if user checks the box "Remember My Password" at the bottom of the account/password prompt, the user does not need to input the account and password the next time he/she logs in again even after rebooting or logging out the client PC.

If the client wants to disable this option, go to "Control Panel/User Account" to select the account to be changed. Click "Related Tasks/Manage my network password" and delete the password to be removed.

Q: Novell clients cannot use the root account to access the NAS server.

A: For the system administrator "root" to access the server from Novell clients, please use the "supervisor" account and the root password of the NAS server to log in (there's no need to create this account on the NAS), or create another admins group account on the server.

Q: Novell clients will not be able to save any single file larger than 2GB onto the NAS server.

A: This is due to the limitation of the system.

Q: Cannot access/create folders with small-letter English names on the NAS server via the Novell client's terminal.

A: The Windows Client service for Netware will automatically change small letters into capitals in the background, which can cause errors with some double byte characters, but this problem will not happen with Novell client 4.8 for Windows NT/2000, or client 3.3 for Windows 98.

Q: Cannot access files in a certain shared folder on the NAS server via the Novell clients.

A: Please check the followings:

1. Check if there is such a shared folder on the NAS server.

2. Make sure that the system administrator has enabled Windows Networking on the NAS server.

3. Make sure that this account has authorized access to the shared folder.

4. Check if the account used for logging into the Novell client also has a same-name account on the NAS server, and check if the password is correct.

5. Make sure that the system administrator does not set a password for the guest account when users log in as guest.

6. Check to see if there are any hosts on the network using the same IP or server name as the NAS server. If there are, correct the situation as soon as possible.

7. If all the above settings are correct, please reboot the NAS server.

Q: How to compose a system login script on the NAS server to automatically map it as a network drive in Novell clients.

A: Apart from setting individual network drives on the Novell clients' terminals on a one-by-one basis, the system administrator may compose a "system login script" on the NAS server to automatically map the NAS server as a network drive for all Novell clients. Please take the following steps:

1. Log into the NAS server via a Novell client with the ID "SUPERVISOR."

2. In the Novell client's terminal, use any word program, e.g. Wordpad, to edit the login script containing the following content and save it as "net$log.dat".

    map p:=\\NAS-3200_nw\public1

    write login_name

    if login_name<>"SUPERVISOR" and login_name<>"SUPERVIS" and login_name<>"GUEST" then

    map h:=\\NAS-3200_nw\home

    end

    As shown in the example, the login script will map the public1 folder on NAS-3200 as "p" drive and map users' home folders on NAS-3200 as "h" drive for all Novell clients on the LAN.

3. Save the "net$log.dat" file to the \SYS\PUBLIC folder on the NAS server.

Q: Cannot find the NAS server via Chooser or Network Browser from Mac clients.

A: Please check the followings:

1. Make sure the NAS server has been turned on and connected on the LAN.

2. Check if the Mac client is able to connect with other AppleTalk servers. If not, the network settings of this Mac client are incorrect.

3. Make sure the system administrator has enabled Apple networking connections over AppleTalk or TCP/IP protocol, and make sure the network adapter that belongs to the sub-net where AppleTalk service is provided is working properly.

Q: PLANET NAS-3000 series Assistant for Mac OS cannot find the NAS server with "Unknown" status.

A: If the network of Mac client was set to "DHCP:

1. Please change to "Fixed IP" or

2. Change to "Fixed IP" first, and then change back to "DHCP"

If the network of Mac client was set to "Fixed IP":

1. Please change to "DHCP" or

2. Change to "DHCP" first, and then change back to "Fixed IP".

Q: Mac clients will not be able to save any single file larger than 2GB onto the NAS server.

A: This is due to the limitation of the system.

Q: Cannot access files in a certain shared folder on the NAS server via Mac clients.

A: Please check the followings:

1. Check if there is such a shared folder on the NAS server.

2. Make sure the system administrator has enabled Apple networking connections over AppleTalk or TCP/IP protocol.

3. Make sure this account has authorized access to the shared folder.

4. Check if the account used for logging into the Mac client also has a same-name account on the NAS server, and check if the password is correct.

5. Make sure that the system administrator does not set a password for the guest account when users log in as guest.

6. Check to see if there are any hosts on the network using the same IP or server name as the NAS server. If there are, correct the situation as soon as possible.

7. If all the above settings are correct, please reboot the NAS server.

Q: Cross marks appear when a Mac client is browsing an English web site.

A: When an Mac client, for example a Mac OS 9.0.2 client, is trying to browse an English web site and sees many "cross" marks appear, please close Smartview from the Control Panel.

Q: HDD space is not released after an Mac client deletes a file on the NAS server

A: When an Mac client deletes a file on the NAS server, the file is not actually deleted so the available HDD space shown on the Server Information/Status page is not enlarged. To release the space, use "Empty Trash" on the Mac client's terminal.

Q: Windows clients cannot delete files saved by Mac clients to the NAS server.

A: The Mac system allows the last digit of the file name to be a space while the Windows system does not accept such a format. Thus when the Mac client saves a file of this format to the NAS server, the Windows client cannot delete the file for it is unrecognizable. It is suggested that Mac users avoid creating files with a space at the end of the file name if they have to share files on the NAS server with Windows clients.

Q: Mac clients failed to set ACL to files and folders.

A: Please note:

1. Mac OS 9 clients cannot set ACL to files and folders on the NAS server, but existing ACL setting of files and folders is still valid to Mac OS 9 clients.

2. Due to the limitation of Mac OS 10, the Mac OS X clients can only set ACL to folders on the NAS server, but not to files. However, files created under a folder will inherit the ACL setting of the folder. Moreover, when setting folder ACL, applying the "Apply to all enclosed folders" setting will make all files and folders inherit the ACL setting of that folder.

3. On Mac OS X, access right of a folder cannot be set to "Read & Write" after it has been set to "Write only."

Q: NAS server lost connection to client terminal.

A: If due to heavy network traffic NAS server fails to respond or freezes while running setup, try clicking on another section, then on the original section again. If this doesn't work, close the browser window and re-open NAS-3000 Series Manager.

Q: Cannot connect to NAS after modifying network configuration

A: After modifying the network configuration (including server addresses, domain, DNS entries, etc.), re-confirm the network settings and change them as necessary. Try closing the browser and reconnecting to NAS-3000 Series Manager.

Q: Local users cannot access NAS-3000 Series Manager.

A: Possible reasons a user's account on the local machine cannot connect to the NAS-3000 Series Manager may include:

1. The account was originally a Windows domain account. The system administrator did not setup a password when adding it to the local accounts.

2. If the client platform is using a language different from the one used on NAS-3000 Series Manager, then the client might be reading random codes when using the system. The system administrator has to re-set the languages on NAS-3000 Series Manager so that they are readable by the client.

3. The user may not be able to launch NAS-3000 Series Manager via PLANET NAS-3000 series Assistant if he has installed a browser other than IE (e.g. Netscape) and uninstalled it.   We suggest that you use a computer without other browsers installed and uninstalled.

Q: E-mail notifications not received.

A: If you don't receive e-mail notifications from the server, go to NAS-3000 Series Manager, "Server Informationà System Log", and check the messages in the log. The following error messages refer to undelivered mail notifications:

1. Cannot resolve the host address: xxxxxx, errcode: xxx.

   This message indicates that the DNS server could not verify the SMTP server name you provided. This may be due to one of the following reasons:

         i.   DNS entry error

         ii.   DNS server powered down

         iii.   Incorrect domain name

         iv.   Incorrect SMTP server

   Verify these options and try again.

2. Cannot connect to host: xxxxxx (xxx.xxx.xxx.xxx).

This message indicates that the system could not connect to the SMTP server. This may be due to one of the following reasons:

    i.   Network connection broken. Check the network connection and try again.

    ii.   SMTP server unavailable. Confirm that the server is working properly.

    iii.   SMTP server rejected the message. Verify that the SMTP server does not filter out junk messages. Contact the system administrator or try using a different SMTP server.

3. Mail server connection failed.

This message indicates that the SMTP server has timed out and not responded within 30 seconds. Verify that the SMTP server is working properly.

4. Send email error: xxx.

This message indicates an unknown mail error. Note the error code and contact the system manufacturer's representative.

5. Cannot create socket resource.

This message indicates that the system has insufficient resources to execute the mail send operation. Reboot the server to correct the problem.

Q: Cannot add multiple user IDs to a workgroup at a time.

A: Update the web browser to IE 5.5 or above.

Q: Time synchronization failed to work.

A: If time synchronization failed to work after the time synchronization setting is configured, please check:

1. If a hostname is entered in the "Network time server:" column, if yes, try to enter the IP of the time server instead of the hostname, or check if the DNS and gateway of the network adapter is properly entered.

2. If the configured network time server still exists.

3. If the configured network time server still works properly.

4. If the configured server still supports Network Time Protocol.

Q: Failed to add the NAS server to the Windows domain.

A: If the NAS server cannot be added into the native mode Windows 2000 domain, please check if the DNS setting of the domain controller is correct. The following hyperlink on the Microsoft web site is a reference for the DNS setting:

http://support.microsoft.com/default.aspx?scid=kb;en-us;260371.

Q: UPS configuration becomes invalid after the IP of the NAS server is changed.

A: If the UPS is configured as controlled by SNMP, the administrator should update related UPS privilege on the UPS management page provided by the UPS manufacturer whenever the IP of the NAS server is changed so that the UPS will allow the NAS server to query the UPS status with the new IP.

Q: Cannot back up/restore the data on the NAS server.

A: When the system fails to backup/restore data on the NAS server, the system administrator will receive e-mail with an error code notifying the data backup/restore failure. The administrator can also go to system log tab of NAS-3000 Series Manager and search for the error code in the log file.

Q: Not sure if PLANET NAS-3000 series Backup has finished the restoration.

A: The restoration consists of "data transmission" and "restoration process". If both actions are finished within the system predetermined time, the NAS-3000 Series Manager will show a message indicating that the restoration is successful; if by the end of the system predetermined time the data transmission is complete, but not the restoration process, the NAS-3000 Series Manager will show a message asking the administrator to check the system log or e-mails for the result. In this case, please check the system log or e-mails, which will depend on the data size to be processed.

Q: Cannot find the NAS server after pressing "Browse" in PLANET NAS-3000 series Replicator.

A: Please check:

1. If the network adapter is connected properly to the Windows client.

2. If the NAS server can be found by browsing the "Network Neighborhood" or "My Network Places". If not, please solve this problem first, and then try PLANET NAS-3000 series Replicator again.

Q: PLANET NAS-3000 series Replicator cannot back up data in Outlook.

A: Outlook saves data to a file named "mailbox.pst" in a directory "Ourlook". The file is locked when you launch Outlook so PLANET NAS-3000 series Replicator cannot back up the data. To solve the problem, shut down Outlook before making backups.

Q: PLANET NAS-3000 series Replicator uploads empty folders to the NAS server or the uploaded data files are incomplete.

A: Here are the possible causes of this problem:

1. The folders on the Windows client are empty.

2. The user has set filter items for files with certain extensions or prefixes in "Files Filtering". The files with these extensions or prefixes will not be uploaded. Please reset filter in "Files Filtering".

3. Incomplete data uploading before doing monitoring will cause inconsistency between data saved on the NAS server and that on Windows client. Go to "Backup"à"Upload" and select "All Files" in upload settings. Click "Apply" to upload all files first.

Q: How to deal with lost passwords.

A: If a user has forgotten his/her password, he/she can turn to the system administrator to reset the personal settings. If the system administrator forgets the password, the server must be returned to the dealer. All the data on the server will be lost.

Appendix 1
What Is RAID

The acronym RAID stands for Redundant Array of Independent Drives, a method to combine a number of small, inexpensive drives into an array which offers more functionality than a single large disk with comparable capacity, while simultaneously taking advantage of the individual disks to increase the efficiency of the system. In other words, during the writing process, data is split into segments and stored on multiple disks; likewise, during the reading process, data is retrieved simultaneously from multiple disks in order to increase the access speed of the array.

RAID can also be configured to use part of the disk capacity for mirroring or redundant data, thus preserving the integrity of the system in case one of the disks in the array fails.

NAS-3200 supports the RAID 0 and RAID 1 volumes, and NAS-3400 supports RAID 0, RAID 1, RAID 5, and RAID 5 with Spare, described below:

RAID level	Functionality
RAID 0	Offers Striping, a process where multiple disks are combined to form one virtual large disk, but without safety measures.
RAID 1	Half of the disks are used for backup purposes; the content of disk A is mirrored to disk B to assure data integrity. The available storage space is only one half of total physical disk capacity.
RAID 5	This configuration includes a backup option. It treats multiple disks as one virtual disk to increase access speed. It uses parity mode to store redundant data on a space equal to the size of one disk for later data recovery. The actual available storage space in a system with n disks is thus n-1 hard disks.
RAID 5 with Spare	RAID 5 with Spare adds one spare disk to the RAID 5 array, allocating one for redundancy and the second one as a spare. The actual available storage space in a system with n disks is thus n-2 hard disks.

Each of the RAID configurations offers a different disk capacity and level of safety. When making your choice, consider the following:

1. The bigger the available space, the fewer safeguards the system has.

2. For any RAID array, the capacity of the array is determined by the smallest hard disk. E.g., for a RAID 1 array created with one 20 GB and one 30 GB hard disks, the total available capacity is defined based on the 20 GB hard disk. Therefore you should always choose to use hard disks with identical size to create a RAID array.

A1.1 RAID 0 (striping)

In a RAID 0 array, data is split and stored in different locations, but without fault tolerance. The server treats the array as one big disk, with a size of almost all individual disks combined. The parallel access to multiple disks allows for faster read and write, making the array faster than individual disks. Because of that, this configuration is ideal for applications where large amounts of streaming data have to be efficiently transferred while assuring good quality, e.g. in a recording.

RAID 0 offers no mirroring or redundancy options. If one disk in the array fails, the entire array is inoperable. RAID 0 is not fault-tolerant.

A1.2 RAID 1 (mirroring)

A RAID 1 array consists of at least two disks that duplicate the storage of data; data is always written to all disks. This system is rather fault-tolerance and is often used in environments with multiple users where safety is of great importance, but more expensive than other solutions, since the actual storage capacity is only 1 disk. RAID 1 is often used in environments with multiple users where safety is of great importance.

A1.3 RAID 5

RAID 5 is the same as RAID 0, i.e. using multiple disks to emulate one large virtual disk, but using parity data format to store redundant information. While the user is writing data, RAID 5 scans the data and stores redundancy information on a separate disk in the array. Parity information is split and stored on different disks together with the actual data. If one disk in the array fails, parity data on the safeguard disk can still be used to rebuild the entire information.

In other words, in a RAID 5 array, you use one disk for redundancy data, leaving you with n-1 disks available for actual data storage.

A1.4 RAID 5 with Spare

RAID 5 with Spare is a RAID 5 configuration with one additional spare disk. Should any disk in the array break down, the spare disk will automatically go online and rebuild damaged data. In other words, you are providing two disks for safety, leaving you with n-2 disks storage capacity in an array of n disks.

Note: Even though RAID greatly increases the level of safety in your system, you should still make it a habit to back up data periodically. If you accidentally erase data, even a RAID array cannot restore it. RAID can only compensate for the failure of one disk, that is, if two disks fail simultaneously, data loss is inevitable.

Appendix 2

Windows Access to NAS Server

After installing the NAS server (we shall assume the default server name NAS-3200), the server NAS-3200 will appear in Windows Network Neighborhood. Users who are members of the users group (see Security Setup section above) can access a folder named after their account and other folders to which they have access privileges.

To access storage space on the NAS server from a Windows client, access the drive through Network Neighborhood, or create a permanent link (map network drive) to the drive on NAS-3200 in the client's file manager.

Windows NT 4.0/2000 users accessing the NAS server will be prompted for their account and password when accessing the NAS server.

When Windows 98 clients try to access the server, the Windows operating system will read the login name of the client and prompt the user to enter only the correct password. If the account information on the NAS server does not match the client's login name, access will be denied. Therefore, if the client terminal runs Windows 98, please use the same names for accounts on this server and the clients.

UNIX Access to NAS Server

One of the purposes for the NFS protocol is to have similar management methods of the remote file system and local file system. Therefore, they can both use the "mount" command to mount.

    mount   /dev/dsk/c0t0d0s5   /home (local filesystem, Solaris)

    mount   /dev/hda5   /home (local file system, Linux)

The UNIX administrator will usually set the above-mentioned scripts in /etc/vfstab (Solaris) or /etc/fstab (Linux, FreeBSD). These settings will automatically execute once the system starts. The following example shows the contents of a /etc/vfstab (NAS3200 is a NAS/NFS server name).

# Filesystem	Mountpoint	Type
/dev/dsk/c0t0d0s0	/	ufs
/proc	/proc	proc
NAS3200:/volume1/programs	/usr/local	nfs
NAS3200:/volume1/homes	/home	nfs

When there are a lot of UNIX clients in the network, writing NFS file systems into client /etc/vfstab or /etc/fstab files becomes a complicated task. When the path of one NFS file system changes, or a new NFS file system is added, the administrator has to change the settings for each UNIX client one by one.

Using NIS (Network Information Service) is one solution because NIS saves all mount information in the NIS server. Once NFS clients join the NIS domain, they will be able to use the shared directories on NFS servers through the function of "automount" instead of modifying /etc/vfstab or /etc/fstab individually. Most UNIX systems (Solaris, Linux, FreeBSD etc.) can be configured as an NIS server.

The following description is based on the settings on a Solaris NIS server.

Master map is the database of the mount information on the NIS server. Before building this database, administrators must edit the pure text file /etc/auto_master as follows.

Master map: /etc/auto_master

#Directory   Map   Mount options

/net	-hosts	-rw
/home	auto_home	-nosuid
/-	auto_direct	

The first column in the file is the path to automount, which means that when users at clients try to access this directory, the link will be enabled automatically. In the second column, the parameters are the paths for databases, which record the mount information about the directory in the first column except for "-hosts". The example above has a special line " /-auto_direct." "/-" is not a directory. The directories to be mounted are in the database "auto_direct." Its format is:

/etc/auto_direct

#Mount point	Mount options	File system
/usr/local	-ro,nosuid	NAS3200:/volume1/programs
/public	-rw	datakey:/volume1/public1

The first column is the mount point and the second column represents the mounting parameters. The third column shows the NFS file system in use. For example, if users of UNIX clients want to access the files in /usr/local, /usr/local will automatically link to NAS3200:/volume1/programs based on auto_direct.

The other database "auto_home" can have different links according to different user names. Its format is:

#User name	File system
sysadmin	NAS3200:/volume1/homes/sysadmin
justind	NAS3200:/volume1/homes/justind
anneli	datakey:/volume1/users/anneli
jiem	datakey:/volume1/users/&

Assume that /etc/passwd (the file holding the user accounts) on the NIS server has the following content:

sysadmin:x:1000:500:System Administrator:/home/sysadmin:/bin/tcsh

justind:x:1001:500:Justin Deng:/home/justind:/bin/tcsh

anneli:x:1002:500:Anne Li:/home/anneli:/bin/tcsh

jiem:x:1003:500:Jiem Deng:/home/jiem:/bin/csh

When the user "sysadmin" logs in to the UNIX clients, he will enter his default home directory /home/sysadmin according to "/etc/passwd". Due to the auto_home database, /home/sysadmin will be automatically mounted to NAS3200:/volume1/homes/sysadmin. With auto_home, the administrator can easily allocate hard disk space to users. When the NAS server named "NAS3200" is out of space, the newly added or some original users (such as anneli and jiem) could be moved to the NAS server named "datakey".

Appendix 4
Mac Access to NAS Server

This system software supports the two access protocols AppleTalk and TCP/IP. The system administrator only has to configure the desired protocol in NAS-3000 Series Manager, "Network Setup"à"Apple network".

Suppose you are running a NAS server called "NAS3200". To allow access from a Mac client via AppleTalk, select "AppleShare" and select "NAS3200" in the "Select File Server" option. When logging in, provide the name and password of the client account, or log in as "guest". All the data for which access privileges exist will be visible. Users who are part of the users group will find their own home folders. Select the desired data: once its icon appears on the desktop, a proper connecting has been established.

If the Mac client supports TCP/IP, you may also choose TCP/IP as an access protocol. Under "Server IP Address", enter the IP address of NAS3200, then log in with your name and password, or as "guest".

If a Zone exists on the LAN, the server will automatically login the zone of the client.

Note:

1. Mac clients are not able to save single files larger than 2GB onto the NAS server.

2. When there is more than one network card in the NAS server and the server is set up as having multiple subnets, this system only supports Mac client in one single subnet to read/write from the server through AppleTalk or TCP/IP protocol. Mac clients in other subnet(s) can only read/write through TCP/IP protocol. Due to this limitation, this system can only support the Zone in a single subnet

Appendix 5

Novell Access to NAS Server

A Windows client terminal must have "Client Service for Netware" or "Novell Client for Windows" installed before access to the NAS server's Novell service (this server only offers Bindery Service, and no NDS).

Suppose you wish to access the server named NAS3200 from a client with "Client Service for Netware" installed. In the Windows Network Neighborhood, you will find an entry "Netware or compatible networks" with the entry NAS3200_NW inside. Enter your name and password, or log in as "guest". All the data for which access privileges exist will be visible. Users who are part of the users group will find their own home folders.

From a terminal running "Novell Client for Windows", you can log in with the Bindery Service. In Windows NT/2000 clients, select Network Neighborhoodà Entire Networkà Netware Servicesà Netware Servers. Here you will find the entry NAS3200. The remainder of the login procedure is the same as for Client Service for Netware.

To access storage space on the NAS3200 from a Windows client, access the drive through Network Neighborhood, or create a permanent link to the drive on NAS3200 in the client's file manager.

Note:

1. Novell clients cannot access the NAS server with the root account. If the system administrator "root" wants to access the server from a Novell client, please use the "supervisor" account and the root password on the NAS server to log in (there's no need to create this account on the NAS), or create another admins group account in the server host.

2. Novell clients are not able to save single files larger than 2GB onto the NAS server.

The Windows Client service for Netware will turn small letters into capitals, which will cause wrong interpretation of some double byte character, but this is not the case with Novell client 4.8 for Windows NT/2000, and client 3.3 for Windows 98.

Third Party Backup Support

A6.1 CA BrightStor Enterprise Backup v10.0

Backup-able/Restore-able items

All share/home folders.

Authentication

"root" can log in from CA BrightStor, browse all users' home folders, and perform fully backup/restore.

Normal user who logs into the Windows client running CA BrightStor with the same account/password in NAS server can backup data in his/her home folder and other share folders he/she has permission to access. Because CA BrightStor uses "user mode" authentication, which is similar to Windows neighborhood, the user has to re-login Windows if he/she wants to switch to different identification/user name.

Important Note

1. When backing up data with CA BrightStor, a directory named "registry" will be automatically generated by CA. To ensure the backup runs correctly, do not choose this directory since it actually doesn't exist on the NAS server.

2. If the user, excluding the accounts "root" and "guest", wants to change to "root" permission after connecting to the NAS server through CAEB, he/she should right-click the NAS server to enter "root" authentication data before unrolling the tree view in CAEB. Moreover, the user, as described above, should log out Windows first and log in again if he/she wants to change as another user after connecting to the NAS server through CAEB.

3. As long as the user logs in CA BrightStor as the root permission of the NAS server, he/she could not switch to any other user by right clicking the mouse to change the security information.

Agent Support

The NAS server can be backed up without an agent installed.

NAS server as backup destination

When using CA BrightStor Enterprise Backup (CAEB) v10.0 to backup data to the NAS server, please note that:

1. The user name and password required during installing CA BrightStor Enterprise Backup (CAEB) v10.0 should be identical with the pair used to map the shared folder on the NAS server.
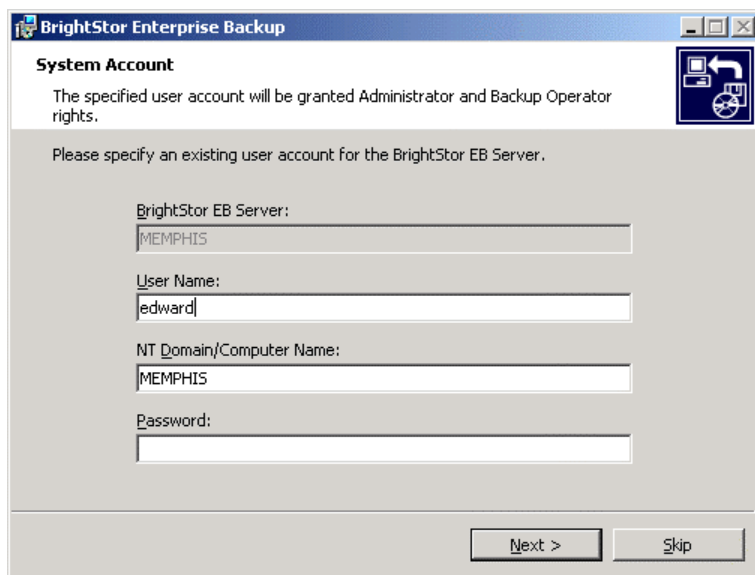
2. The Windows client should belong to the administrators group in order to install CA BrightStor Enterprise Backup (CAEB) v10.0.

A6.2 CA BrightStor ARCserve Backup v9 for Windows

The same as CA BrightStor Enterprise Backup (CAEB) v10.0.

A6.3 Veritas BackupExec v8.6

Backup-able/Restore-able items

All share/home folders.

Authentication

"root" can log in from Veritas BackupExec, browse all users' home folders, and perform fully backup/restore.

Normal users can backup data in his/her home folder and other shared folders he/she has permission to access. Because Veritas BackupExec uses "share mode" authentication, the user does not have to re-login Windows if he/she wants to switch the identification.

Agent Support

The NAS server can be backed up without an agent installed.

NAS server as backup destination

When using Veritas BackupExec v8.6 to backup data to the NAS server, please note that:

1. The user name and password required during installing Veritas BackupExec v8.6 should be identical with the pair used to map the shared folder on the NAS server.
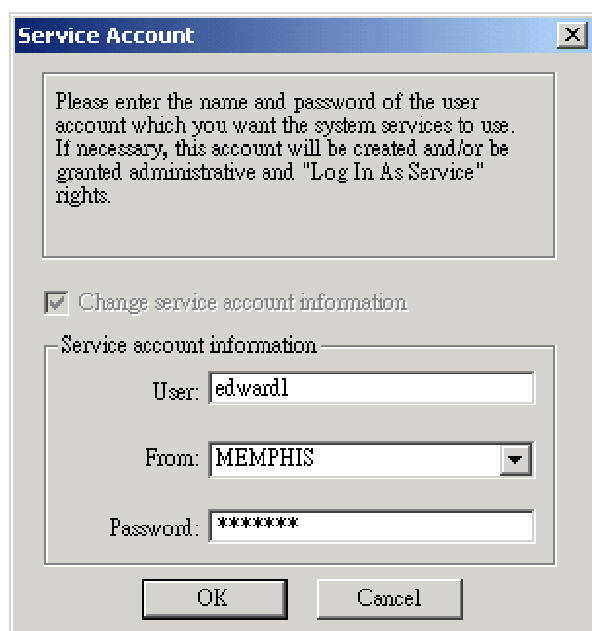
2. The Windows client should belong to the administrators group in order to install Veritas BackupExec v8.6.

A6.4 Dantz Retrospect Backup v5.6

Backup-able/Restore-able items

All share/home folders.

Agent Support

The NAS server can be backed up without an agent installed.

Appendix 7

Using PLANET NAS Assistant on Mac

A7.1 Using PLANET Filer Assistant on Mac OS 9

Before You Start

1. Connect the NAS server to the LAN and turn on the server.

2. Set the resolution of the client terminal screen to 1024*768 or higher.

3. Make sure Mac OS Runtime for Java 2.2.5 (MRJ 2.2.5) is installed on the client. (you can download it from:
   http://kbase.info.apple.com/cgi-bin/WebObjects/kbase.woa/117/wa/query?searchMode=Expert&type=id&val=KC.75097)

4. Make sure the IE version is 5.0 or above and its Java security options is configured as "Unrestricted Access". (Edit-> Preferences-> Web Browser-> Java-> Network access-> Unrestricted Access)

Setup

1. Double click "NAS3000SeriesAssistant.sit" to extract the file.

2. Enter the extracted folder and activate "NAS3000SeriesAssistant".

3. Except the following functions, PLANET NAS-3000 series Assistant for Mac OS 9 functions the same as that for Windows.

   i. PLANET NAS-3000 series Assistant for Mac OS 9 does not provide the "Map Drive" function.

   ii. When you set up the NAS server with "Unknown" status, PLANET NAS-3000 series Assistant for Windows will open a new dialog box for setup, while PLANET NAS-3000 series Assistant for Mac OS 9 will show related data on the top of the same dialog box for the system administrator to set up.

   iii. When setting up a NAS server with "Unknown" status, if you select "Use manual configuration", PLANET NAS-3000 series Assistant for Windows will provide "Suggest" options, but PLANET NAS-3000 series Assistant for Mac OS 9 does not provide the option. The system administrator should manually enter related data.

A7.2 Using PLANET Filer Assistant on Mac OS 10

1. Copy the file "NAS3000SeriesAssist.dmg.gz" to the Mac OS 10 client.

2. Double-click the file "NAS3000SeriesAssist.dmg.gz" to extract the file to "NAS3000SeriesAssist.dmg".

3. Double-click the file "NAS3000SeriesAssist.dmg" to extract the file to the folder "NAS3000SeriesAssist".

4. Enter the folder and double-click the program in it.

5. Except the following functions, PLANET NAS-3000 series Assistant for Mac OS X provide the same functions as that for Windows.

   i. PLANET NAS-3000 series Assistant for Mac OS X does not provide the "Map Drive" function."

   ii. When setting up a NAS server with "Unknown" status, if you select "Use manual configuration", PLANET NAS-3000 series Assistant for Windows will provide "Suggest" options, but PLANET NAS-3000 series Assistant for Mac OS X does not provide the option. The system administrator should manually enter related data.

Specification

Model	NAS-3200	NAS-3400
Form Factor	Tower	
Processor	VIA C3 800MHz	
Memory	256MB	
Hard Disk Tray	Two	Four
	ATA 66/100 IDE interface	
Scalability	Up to 500GB	Up to 1TB
RAID Level	0, 1 with on-line rebuild	0, 1, 5, 5+Hot Spare with on-line rebuild
LED	SYS: System/alarm 100, GbE: Network status	
LAN Port	10/100Mbps RJ-45 port x 1 10/100/1000Mbps RJ-45 port x 1	
COM Port	1, for UPS	
Network Protocol Supported	TCP/IP, IPX, AppleTalk	
Network Clients Supported	Microsoft Windows, Red Hat Linux, Solaris, FreeBSD, Novell Netware, Macintosh	
Power Supply	Single ATX 180W power supply	
Dimension	120mm(W) x 180mm(H) x 265mm(D)	162mm(W) x 210mm(H) x 271mm(D)
Weight	Approximate 4kg with power supply, no hard disk	Approximate 5kg with power supply, no hard disk
Operating Environment	Temperature: 10~40 degree C Humidity: 10~95 %	
Storage Environment	Temperature: -20~65 degree C Humidity: 10~95 %	
Safety Approvals	CE, FCC Class A	