Standby*Server*™
for NetWare/IntranetWare

Contents

Welcome

Welcome to Standby*Server* for NetWare/IntranetWare. Standby*Server* is a high availability, transaction-based server-mirroring solution that connects one or more secondary, standby machines to one of your critical (primary) servers. Should the primary server fail due to either hardware or software failure, the standby machine can automatically take over making the mirrored data available in just a few moments. Data is mirrored between the servers using either a dedicated high-speed Vinca link, or the client network, creating a fully redundant system to protect users against both hardware and software failures.

Standby*Server*'s architecture is compatible with most makes and models of Intel x86 based, Novell-certified servers. Using Standby*Server* in conjunction with its Utility Server feature allows an existing server to not only function as a regular server, but also as a fault-tolerant mirror of the primary server. Should the primary server fail, the standby machine can automatically failover to assume the primary role so users always have access to the most up-to-date data.

Figure W.1 Simple Standby*Server* Configuration
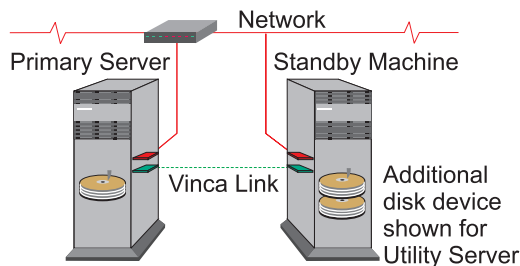
Standby*Server* consists of three main elements; a primary server, a standby machine, and the communications path (Vinca link) that connects them.

The exported disk devices in the standby machine are treated as external disk systems to the primary server. Using NetWare mirroring, all reads and writes are performed on both disk devices in real time.

Standby*Server* does not require the standby machine to be returned to its original role before fault tolerance is restored after a failover. For example, if the primary server fails and the standby machine failed over and assumed the primary role, the primary server can be repaired and then started in the standby role. This enables you to resynchronize the mirrors and return your system to a fault tolerant configuration without having to down and reboot the standby machine to its original role.

You can maintain this reversed role configuration until you want to reestablish each machine in their original role. However when a failover occurs, all mirroring to additional standby machines (vault machines) is disabled. Only after the original configuration is restored will mirroring to the vault machine continue.

How Standby*Server* Works

Standby*Server* constantly monitors the communication between the machines, while mirroring, to ensure the primary server is accessible. If the primary server becomes unavailable and the standby machine can no longer communicate with it, the standby machine fails over and assumes the primary role.

The graphic below shows a typical configuration where the primary server has failed (grayed out), and the standby machine has assumed the primary role. The failover takes only a few moments before users again have full access to the mirrored copy of the data stored on the standby machine. Because all NetWare data has been mirrored, including the bindery NDS, and system volume(s), in most cases users are automatically reconnected (using Microsoft or Novell's 32-bit client software).

Figure W.2 Assuming the Primary Role
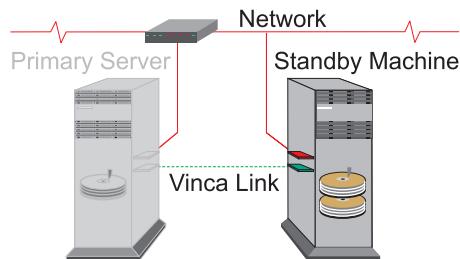
The standby machine's ability to automatically assume the primary role depends on your failover configuration. If you have the AutoSwitch feature enabled, this failover takes place automatically. If you do not, you can use NetWare to alert you of the

primary server's failure and manually failover the standby machine so users can have access to their data.

As shown in the graphic above, the Vinca link is a dedicated direct connection used for mirroring. When you use a Vinca link, you not only move all mirroring traffic from your client network, but you also decrease the chances of a inadvertent failover (when enabled) or user down time.

With the Vinca link, a failure of a component in the primary server, such as a disk controller, does not disable communication or client access to the data. In this case, the information is simply accessed from the mirrored device in the standby machine. The standby machine will only failover when the primary server is dead, or locked up.

Standby*Server* Implementations

Standby*Server* includes the ability to connect additional standby machines (vault machines) to the standard primary server-standby machine configuration. Vault machines are used as additional redundant mirrors of the primary server. The vault machine acts like the standby machine in every way except it does not failover automatically when the primary server fails. For more information on using a vault machine with your configuration, see Appendix F, *Using a Vault Machine*.

Standby*Server* (excluding Entry-Level) includes a feature called Utility Server. With this feature the standby machine can be used for both a fault tolerant mirror of the primary server, and as an independent server running its own processes.

The Utility Server configuration requires that an extra disk device be available in the standby machine to be used as the standby's local SYS: volume. This volume is not mirrored and can be used to run server-based utilities such as Vinca's SnapShot*Server*, which facilitates server backup.

Because NetWare does not allow more than one SYS: volume on the same server at the same time, when the standby machine fails over and assumes the primary role, the standby's SYS: volume is renamed to SYS_UTILITY by the SYSSWAP.DSK.

About this Guide

This guide documents Standby*Server*, Standby*Server* using the Utility Server feature, and Entry-Level Standby*Server*. Entry-Level Standby*Server* is a Standby*Server* implementation with the following limitations:

▼   Primary server's NetWare license cannot be greater than 25 users.

▼   There cannot be more than one 'hop' between the primary server and the standby machine. Routers and hubs cannot be used with a Vinca link.

▼   No Utility Server feature.

Instructions in this guide are given for all implementations. Specific instructions are clearly marked for Entry-Level Standby*Server* and Utility Server implementations.

Conventions

The following conventions are used in this document:

Select   Using the arrow keys to highlight an option.

Choose   Equivalent to selecting an item and pressing Enter.

Type   Enter specified information at the specified prompt.

Keys other than standard command keys (Enter, Esc, Del, Ins, etc.) are given within quotes. For example, "p".

Benefits of Standby*Server*

▼ Complete server fault tolerance
Because data is mirrored to a completely separate computer, all server components are redundant, but not necessarily identical.

▼ Automatic failover to the standby machine
When the primary machine fails, the standby machine can restart as the working server without user intervention.

▼ The machines need not be identical
The primary and standby machines should be similar (Novell-certified servers), but they do not need to be identical. The standby machine must contain enough disk devices with sufficient space to mirror the primary volumes, and enough RAM to mount the mirrored volumes if a failover occurs.

▼ The standby machine can still function as an active server
Using the Utility Server configuration, the standby machine can function as an active NetWare server at the same time that it mirrors the primary server. If the standby machine fails over and assumes the primary role, it cannot function as a Utility Server until each machine is restarted in its original role.

▼ Decreased disk read times
Because data is stored in two identical volumes, NetWare can read from either disk in the mirror set, allowing multiple reads at the same time and improving overall performance.

▼ All NDS structures are mirrored
NDS structures such as replicas, time synchronization, user objects, etc. are automatically mirrored to the standby machine.

Vinca Technical Support

Vinca Technical Support is now available through the following support programs:

- ▼ Premium Support—7x24-hour toll-free telephone support.
- ▼ Priority Support—7:00 a.m.–6:00 p.m. Mon.-Fri. (MST) telephone support.
- ▼ Incident Support*—Per incident charge telephone support.
- ▼ Basic Support—Free fax and e-mail support.
- ▼ Extended Incident Support—Weekend telephone support by appointment.

These programs are discussed in detail in the Technical Support Programs insert included in the product box. Some manuals contain misprinted information about Vinca's support programs and are superseded by this information.

*One free Incident Support is included with each product purchase. An incident is defined as the resolution of one issue, problem or question, regardless of the number of telephone calls required. To use this free incident support, you will need to give the Incident Number located on the back of the Quick Setup Card to the support technician.

For more information about Vinca's support programs contact your nearest Vinca sales representative, Vinca Sales at 800-934-9530, Vinca Technical support, or visit our Web site at www.vinca.com.

Before accessing technical support for any issues, please complete the Pre-Assistance Checklist (next page).

Welcome to Standby*Server*

Pre-Assistance Checklist

Check the following conditions on the system before calling technical support:

- ▼ Verify card settings, including the interrupts, IO ports, slots, and memory settings, etc.
- ▼ Ensure that there are no interrupt or I/O conflicts.
- ▼ Ensure hard drives are well ventilated to avoid overheating.
- ▼ Ensure all cables have a good connection.
- ▼ Check all DOS partitions and NetWare volumes for viruses.

When calling for technical support, please have the following information available; it will be needed to assess your system's problem:

- ▼ Vinca registration number (located on Registration Card).
- ▼ Brand and model of the primary and standby machines.
- ▼ Processor type and speed (e.g., Pentium 200).
- ▼ Type and size of disk devices used.
- ▼ Type of disk controllers used.
- ▼ Network (and Vinca link) card(s) types and settings.
- ▼ Versions of NetWare (3.12, 4.10, 4.11, or IntranetWare) and DOS.
- ▼ Version of any application software.

Services

After completing the Pre-Assistance Checklist, you can contact us using the method that best fits your needs:

Method	Access
Phone support	801-223-3104 Monday – Friday, 7:00 am - 6:00 PM (MST)
Internet	http://www.vinca.com/support
E-mail	support@vinca.com
Fax	801-229-2110
BBS	801-224-1210
Compuserve	74774,1425 (non-priority response only)

Chapter 1
Installing Standby*Server*

Standby*Server*'s installation includes both hardware (if needed) and software procedures. The software is installed from the standby machine using the VINSTALL.NLM utility. This utility enables you to access all disk partitions (DOS and NetWare) in both the primary server and the standby machine.

The installation process includes the following procedures:

1. Review the System Requirements to ensure all requirements are met before starting the hardware installation.
2. Install and/or test the target machines to ensure they contain the necessary components (including NetWare) and any other necessary hardware.
3. Install Standby*Server* software.
4. Validate Standby*Server**.
5. Establish the mirrors between the primary servers and the standby machine's disk devices. See Chapter 2, *Mirroring* to complete this step.
6. Test the failover configuration. See Chapter 3, *System Failures & Recovery* to complete this step.

*After Standby*Server* is installed, you have 30 days to validate it. During this time, Standby*Server* will run normally without validation. After the 30 days, Standby*Server* will report validation warnings on the network.

If you are upgrading from Standby*Server* 2.x, VINSTALL will automatically locate your current Standby*Server* configuration and prompt you to upgrade. See "Updating StandbyServer" on page 32 for instructions on upgrading Standby*Server*.

System Requirements

These hardware and software requirements must be met before Standby*Server* can be successfully installed. Both machines must meet the following requirements unless otherwise noted:

▼ The primary server must be a Novell-certified server running a valid, licensed copy of NetWare 3.12, 4.1x, or IntranetWare.

▼ The standby machine(s) (including any additional standby machines) must be bootable and running a matching NetWare Runtime version, or another valid, licensed copy of NetWare. The Standby*Server* package includes one Runtime NetWare versions for 3.12, 4.10 and 4.11.

▼ 386 or better processor.

▼ Equal number of disk devices (plus one extra in the standby machine if you are going to use the Utility Server feature).

▼ 10 MB free disk space on the DOS partition.

▼ Adequate RAM— both machines should have the same amount of RAM. Use the following formulas to determine NetWare's memory requirements:

▼ NetWare 3.12 required RAM=volume size (in MB)x0.023+2MB (for the OS)

▼ NetWare 4.1x and IntranetWare required RAM=volume size (in MB)x0.008+8 MB (for the OS)+2 MB (for other file systems)+2 MB (for each NLM)+ 1 to 4 MB (cache buffer)

▼ A network connection between the machines using compatible, Novell-certified LAN cards.

Note: If you are using a RAID device with a primary server, make sure you use a disk or RAID device in the standby machine that is large enough to mirror the NetWare partition from the primary server's disk devices. A RAID can be used on the standby machine to mirror all devices from the primary servers. Standby*Server* also works with RAID devices that support multiple concurrent connections, but Vinca has not tested every device. For more information on using RAID devices with Standby*Server*, or RAIDShare™, see Tech Notes on Vinca's Web site at www.vinca.com.

Additional Hardware Requirements for a Dedicated Vinca Link

When using a dedicated Vinca link (highly recommended), an additional high-speed IPX compatible, Novell-certified, LAN card (100 Mbps Ethernet, FDDI, or token ring, etc.) needs to be installed in each machine. These cards should be as fast as possible to decrease any chances of latency during mirroring. The cards need to be connected using a dedicated cable.

Additional Hardware Requirements for Utility Server

The Utility Server feature requires an additional disk device (minimum 100 MB) in the standby machine to hold the local SYS: volume. The actual size of this disk device depends on how much data you intend to store on it.

For example, if you intend on using Vinca's SnapShot*Server*, the NetWare volume(s) on the local partitions must be large enough to hold all the captured snapshots, as well as any additional software stored there. Normally 10 to 20% of the volume's size is adequate for taking snapshots. Additionally, because SnapShot*Server* can mount the SnapShot volumes, enough RAM will be needed to mount these volumes.

Additional Requirements for Entry-Level Standb*yServe*r

The license agreement for Entry-Level Standby*Server* includes the following:

- ▼ The primary server's NetWare license cannot be greater than 25 users.
- ▼ There cannot be more than one 'hop' between the primary server and the standby machine. Routers and hubs cannot be used within the Vinca link connection.
- ▼ No Utility Server feature.

If you are installing an Entry-Level Standby*Server* configuration and these requirements are not met, the installation process will abort when a primary server is selected in Step 3 of the installation instructions.

Hardware Installation

This section discusses disk device usage and installing a dedicated Vinca link.

Reviewing Your Disk Device Usage

The primary server and standby machine should contain the same number of disk devices (unless you are using a Utility Server configuration, which requires an additional disk device in the standby machine to be used as a local SYS: volume). Because only one NetWare partition can exist per disk device, the NetWare partitions used as mirrored sets should be the same size. If the primary server's disk device contains a larger NetWare partition than the standby machine's, the mirror cannot be established. If the standby machine's disk device contains a larger NetWare partition than the primary, any space greater than the primary server's partition is not used. See the NetWare documentation for exact mirroring specifications.

Using a Dedicated Vinca Link

A vinca link is created between the machines when the Vinca IPX driver is loaded on each machine. Through command-line statements. the driver ensures that mirroring traffic is directed to the other machine over the client network or a dedicated Vinca link.

For example, when you install Standby*Server* and select the LAN cards used for a dedicated link, the Vinca IPX load lines contain a "master/slave=" statement to direct the mirroring traffic through the LAN cards dedicated to mirroring. See Appendix B: *Sample Files* for sample statements for dedicated and non-dedicated configurations.

A dedicated Vinca link is like having a second mini-network dedicated to mirroring traffic and also used as a second means of monitoring the primary servers condition. The dedicated link is made up of industry standard LAN cards and a crossover cable. Using a dedicated Vinca link is highly recommended, and gives you two major benefits:

▼   A second path for communicating with the primary server.

▼   Keeps mirrored data off the client network, reducing latency.

If you cannot use a dedicated link, the client network can be used; however, you will not receive the full benefits of Standby*Server*. Because not every configuration will use a dedicated Vinca link, several features have been added to Standby*Server* to lighten the burden of mirroring traffic on your client network:

▼   A Throttle control enables you to control how much mirroring data is placed on the network at a given time.

▼   A Read Blocker can be used to block split disk reads and limit all disk read traffic to the primary server.

Because all mirrored traffic is packaged in standard IPX packets, it is fully routeable whether you are using a dedicated link or not. (Routing is not available in Entry-Lever Standby*Server*.)

To install a dedicated Vinca link

1. Install the LAN cards as per the manufacturer's directions.
2. Install the Vinca link cable, connecting the two LAN cards with a dedicated cable. If the cards are connected point-to-point a crossover cable must be used. Refer to the LAN card manufacturer's documentation to establish a point-to-point connection. Some newer LAN cards require a hub and don't allow a crossover cable.
3. Test the link to ensure both cards and cable are functioning properly.

Software Installation

After the "System Requirements" on page 16 has been reviewed, and the necessary hardware has been installed, the machines are ready for the software installation. The Standby*Server* software installation has four major steps:

1. Start NetWare on both the primary server and standby machine.
2. Load VINSTALL.NLM on the standby machine and follow the instructions on the screen. Because the installation is run from a CD-ROM, you must ensure your CD-ROM is accessible while at a console prompt.
3. (Non-Utility Server only) Remove NDS (4.1x only) and delete the local SYS: volume. If you do not delete the local SYS: volume you will receive unnecessary error messages when establishing the mirror (s).
4. Down and restart each machine in its proper role.

After these steps are completed and the Standby*Server* software has been installed successfully, you will need to:

1. Establish the mirror (see Chapter 2, *Mirroring*).
2. Test the installation, mirroring and failover configuration (see Chapter 3, *System Failures & Recovery*).

The examples in Appendix B are helpful in seeing what the minimum content of each configuration file (*.NCF) should look like when the installation is complete.

Installation Options

During the installation you will need to accept the default paths and options or enter new paths and change the option's state to ensure your Standby*Server* configuration is installed the way you want.

Path/Option	Description
NetWare Directory	Directory from which NetWare is loaded on each machine (C:\NWSERVER for NetWare 4.1x and C:\SERVER.312 for Net-Ware 3.12, by default).
Standby*Server* Directory	Directory from which Standby*Server* runs (C:\STANDBY, by default).
Dedicated link	The LAN card used for the dedicated Vinca link (none, by default) for each machine. Make sure the driver uses the same network number and is set up with the same frame type on each machine.
AutoSwitch	Displays whether the AutoSwitch feature is enabled or disabled (Enabled, by default).
	When enabled, the standby machine automatically fails over and assumes the primary role if the primary server fails. For more information, see Chapter 4, *Using the AutoSwitch Feature.*
Disk Read Blocker	Displays whether the Disk Read Blocker feature is enabled. When enabled (default), disk reads only goes to the disk devices physically located in the primary servers. When disabled, disk reads are serviced by whichever part of the mirror that can respond next. For more information, see.
Utility Server	Displays whether the Utility Server feature is enabled (default). When enabled, the standby machine is automatically configured to function as a Utility Server (excluding the hardware requirements). When disabled, no configuration changes are made.

To install Standby*Server*

1. Start NetWare on both machines.

2. Make sure both machines have their local SYS: volume mounted.

3. At the standby machine's console prompt, type `display servers` and press Enter to make sure the primary server is visible to the standby machine.

Note: If the primary server is not listed, there is a NetWare configuration problem. See the NetWare documentation for assistance in solving this problem before continuing.

On the standby machine

4. Insert the Cluster Pack CD-ROM into the CD-ROM drive.

5. At the console prompt, type `load d:\sbs40\vinstall` and press Enter to load the VINSTALL.NLM., where d: is the CD-ROM drive.

6. Read and accept the License Agreement to continue.

Figure 1.1 VINSTALL Main Screen
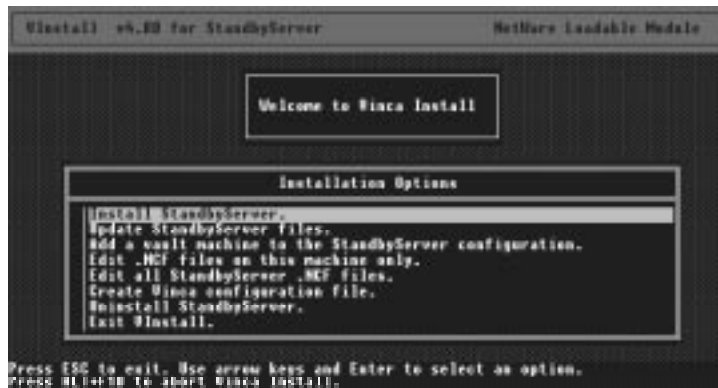
7. Choose "Install Standby*Server.*"

Figure 1.2 Server Selection Screen

8. Choose the primary server.

Figure 1.3 Primary Server Login Screen

9. Enter a login name and password that has full access to the SYS:SYSTEM directory on the primary server and press Enter.

📝 **Note:** If the password fails, you can choose No to retry, or Yes to continue. If you choose to continue, you can follow the instructions on the screen to manually install the communications drivers on the primary server.

When the VincaIPX drivers are loaded on the standby machine, the following message appears on the screen:

Figure 1.4 Waiting for Remote Message

On the primary server

10. Type v.ncf and press Enter.

On the standby machine

11. Set the paths and installation parameters you want in the Standby*Server* Options screen.

Figure 1.5 Standby*Server* Options Screen

Set the values for each machine by using the arrow keys to select the field and pressing Enter to edit it, or toggle the option's state.

12. Press F10 to accept the settings and choose Yes to confirm the settings or No to return and modify them.

When the options are accepted, Standby*Server* copies the files to the machines in the selected directories.

Figure 1.6 File Copy Progress Screen
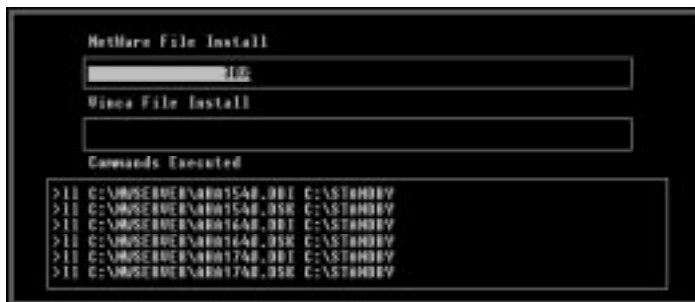
13. When the file copy is completed, you are prompted to edit the new NCF files.

📝 **Note:** Editing the .NCF files helps to ensure that your applications will load correctly.

Figure 1.7 Edit New .NCF Files Prompt

Choose No to continue the installation without editing the files.(go to Step 18).

Choose Yes to open the File Selection screen to select the files you want to edit.

VINSTALL creates all the configuration files needed for Standby*Server* operation. This utility extracts all of the LAN and disk drivers, version information, and other data from the copy of NetWare running on each machine to create the new configuration files.

Looking at each file can help ensure everything loads properly. Make sure to include full paths. See Appendix B for sample .NCF file contents for your configuration.

📝 **Note:** In NetWare 3.12 installations, check the C:*netware*\\AUTOEXEC.NCF file on the standby machine to ensure there are no "MOUNT ALL" commands in the file.

VINSTALL automatically inserts a "VMOUNT SYS" command that can conflict with the "MOUNT ALL" statement.

Use "VMOUNT *volname*" to mount each volume. Remember, this only applies to the AUTOEXEC.NCF in the *netware* directory used during a failover.

Example: `vmount sys vol1 vol2`

Notice that there is no listing for SYS:\SYSTEM\AUTOEXEC.NCF. This file is no longer used; the disk and LAN driver used as the Vinca link must be loaded before Standby*Server* can function, so they are loaded from the local drive. All loads are done from either the C:*netware*\AUTOEXEC.NCF file or the C:\STANDBY\AUTOEXEC.NCF file. The SYS:SYSTEM\AUTOEXEC.NCF can be called at the end of the AUTOEXEC on the DOS partition to load applications that can be run on both the primary server and standby machine.

14. Edit the new NetWare configuration files individually (as needed), by selecting the file and pressing Enter.

Figure 1.8 Edit New .NCF Files Screen
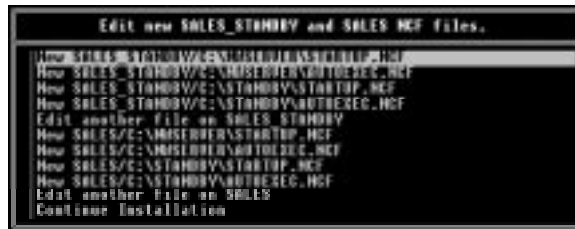
15. Press Esc when finished to return to the File Selection screen.
16. When all files have been edited, choose Continue Installation.
17. Choose Install new *.NCF files.

Figure 1.9 Save .NCF Files Options Screen

The Install new *.NCF file option saves the changes to the new configuration files and renames any existing configuration files with the same name to <filename>.OLD so you can view the previous versions if necessary.

If you defer saving these files now, you will need to copy the .NEW files over the existing .NCF files on both machines in both the NWSERVER and STANDBY directories before running Standby*Server*.

Figure 1.10 Finish Steps Screen

The Finish Steps Screen is a visual reminder to complete the remaining Installation steps after the software is installed. These steps will vary depending on your configuration (e.g., Utility Server, NetWare 4.1x, etc.).

18. Press Enter to clear this screen and exit VINSTALL.

Finish Steps

1. (Non-Utility Server, NetWare 4.1x only) Remove NDS on the standby machine:

    a. From the standby machine's console prompt, type load install and press enter.

    b. Choose Directory options, Remove Directory Services from this server.

    c. Follow the prompts on the screen, confirming that directory services should be removed.

    d. When finished, escape back to the main screen.

2. (Non-Utility Server only) Remove the local SYS: volume on the standby machine:

    a. From the standby machine's console prompt, type install and press enter.

    b. Choose Volume Options.

    c. Select the volume you want to delete and press Delete.

    d. Choose Yes to confirm you want to delete the volume.

> **Note:** If you do not remove the local SYS: volume in a non-Utility Server configuration, you will receive a number of NetWare warning messages when establishing the mirror(s).

3. Down both machines.

On the standby machine

4. Change to the STANDBY directory.

5. From the DOS prompt, type standby and press Enter.

Figure 1.11 Standby*Server* Screen

The flashing red indicator at the bottom of the screen indicates that Standby*Server* cannot currently see the primary server. This indicator turns green when NetWare is started on the primary server and two machines are communicating.

On the primary server

6. From the DOS prompt, type server and press Enter.

   When the server comes up completely, make sure the Standby*Server* screen's indicator turns green.

   If you installed the AutoSwitch feature, you can press Alt+Esc to switch to the AutoSwitch screen.

Figure 1.12 AutoSwitch Screen

The status bar at the bottom of the screen should be green, indicating that AutoSwitch is armed and Standby*Server* is ready to automatically failover if the primary server fails.

The Standby*Server* software is now installed.

7. Establish the mirror (Chapter 2, *Mirroring*).

8. Test the failover configuration (Chapter 3, *System Failures & Recovery*).

For troubleshooting tips see Appendix A, *Troubleshooting*.

After completing the Finish Steps, you should validate Standby*Server*. You have 30 days to validate Standby*Server* after it is installed. After the 30 days, Standby*Server* reports validation warnings on the network.

Validating Standby*Server*

Each of the applications in the Cluster Pack can be run as 30-day evaluation programs. When you decide which program you want to validate, you need to contact Vinca and exchange the Cluster Pack serial number for a Vinca, product-specific serial number. After installing Standby*Server*, it can be used for 30 days during which pop-up warnings are invoked to remind you how many days are left in the evaluation period. After 30 days, an expiration notice is invoked and the application will not function until the validation process is completed.

The validation process requires contacting Vinca to register your Cluster Pack serial number and primary server's NetWare serial numbers.

The NetWare serial number can be obtained by typing "s" from the Standby*Server* screen.

The Cluster Pack serial number is located on the Cluster Pack Registration Card.

Vinca can be contacted by Internet e-mail, phone, or fax at:

E-mail: validation@vinca.com

Phone: 800-274-6042

Fax: 801-223-0199

When you contact Vinca, be sure to provide the following information:

- ▼ Cluster pack serial number.
- ▼ Primary Server's NetWare serial number.
- ▼ Contact person.
- ▼ Company name.
- ▼ Address.
- ▼ Phone.
- ▼ Fax (optional)
- ▼ E-mail (optional)

All of the following steps should be performed on all Standby*Server* machines including the primary server, the standby machine, and any additional standby machines. When validating additional standby machines, the original validation key is used. When validating, you can select the NetWare Serial Number field and press "t" to populate the field with the NetWare serial number of the current machine.

To validate Standby*Server*

1. Obtain the required information (see the bulleted list on the previous page).
2. Contact Vinca and exchange the Cluster Pack serial number and the primary server's NetWare serial number for a Standby*Server* serial number and a validation key.
3. From the console prompt, type `load c:\standby\validate` and press Enter to load VALIDATE.NLM

Figure 1.13 Validation Screen
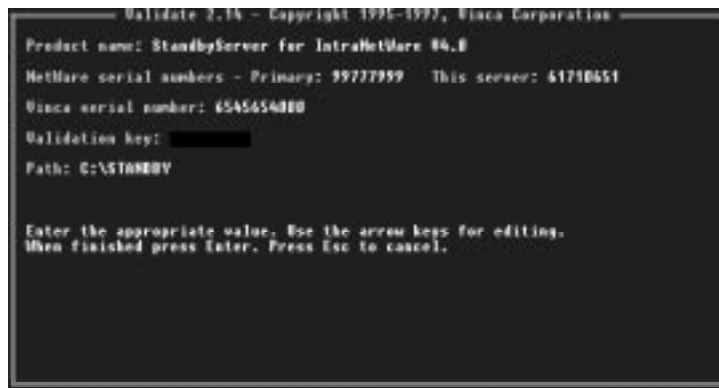
4. Select the product to validate by pressing the space bar.
5. Verify the primary server's NetWare serial number.
6. Enter the Standby*Server* serial number.
7. Enter the Validation Key received from Vinca.
8. Enter the path to the standby directory.
9. Press Enter to validate the information.
10. Choose Yes at the prompt to finish.

Note: Remember, all machines need to be validated; including the primary server and any additional standby machines.

Other VINSTALL options

After the initial installation is complete, the VINSTALL program can be used to create a configuration file, update the Standby*Server* files, or edit the system .NCF files. After an initial installation, VINSTALL can be accessed from the C:\STANDBY directory of all machines running Standby*Server*; however, it is most useful when run from the standby machine(s).

All .NCF file editing should be done using VINSTALL's file editing option to ensure any changes to your files are saved to the appropriate directories to maintain fault tolerance. Do not use the NetWare Install utility for editing .NCF files; changes saved from the NetWare Install utility's file editor are not saved to the Standby*Server* directories.

Creating a Vinca Configuration File

This VINSTALL option is run on the standby machine (or vault machine) to create a configuration file containing the STARTUP.NCF and AUTOEXEC.NCF files from STANDBY, SERVER (NWSERVER or SERVER.312 by default), *netware*, and SYSTEM directories on the primary server and the standby machine from which it is run. You can use this information for comparing your system's configuration before and after you installed Standby*Server*.

Should you have any configuration problems, this file can be created and e-mailed to Vinca's Technical Support to help troubleshoot your situation. Appendix B, *Sample Files* contains information to help you understand the changes VINSTALL makes to the configuration files used to start each machine.

When creating a file, you are prompted to enter the following information:

- ▼ Name
- ▼ Organization
- ▼ Phone
- ▼ Fax
- ▼ E-mail.
- ▼ Output filename

Only the filename is a required field (SYS:\SYSTEM\VCONFIG.TXT, by default).

To create a configuration file

1. From the standby machine, run the VINSTALL utility.
2. Choose the "Create a Vinca configuration file" option.
3. Enter the appropriate information.
4. Change the path and filename as needed and press Enter.
5. Press Enter to return to VINSTALL's Main Menu.

Updating Standby*Server*

If Standby*Server* is already installed on your system, you can update the Standby*Server* files by using the Update Files option. Updating replaces only the Standby*Server* files; it does not change any installation options or the mirroring configuration. The following steps presume that both machines are up and Standby*Server* is working properly.

To update Standby*Server*

1. On the standby machine, insert the Standby*Server* for NetWare Install CD-ROM into the CD-ROM drive.
2. From the console prompt, type `load d:\sbs40v\vinstall` and press Enter to load the VINSTALL.NLM, where d: is the CD-ROM drive.
3. Choose "Update the files of a previous version of Standby*Server*."
4. Choose the Standby*Server* directory.
5. Complete the Finish Steps and retest the failover configuration (Chapter 3, *System Failures & Recovery*).

Editing .NCF Files

Standby*Server* puts all of the NetWare configuration files on the local hard disk and removes any entries in the SYS:\SYSTEM\AUTOEXEC.NCF file, putting those lines in the local AUTOEXEC.NCF files. This is done to ensure the LAN drivers are loaded prior to VINCAIPX being loaded, and all Standby*Server* files are loaded before the SYS: volume is mounted.

When adding new applications to the primary server or the Utility Server (standby machine), many installation utilities will add SET parameters and LOAD statements to SYS:\SYSTEM\AUTOEXEC.NCF. When this happens you should move those lines from the SYS:\SYSTEM\AUTOEXEC.NCF to the appropriate AUTOEXEC.NCF file on the boot partition to ensure all files are loaded properly and Standby*Server* maintains its fault tolerance.

If you choose to add an additional standby machine, remember that it acts like the original standby machine in every way except automatic failover. When you edit the NCF files from a standby machine, you can edit both the standby machine, where you ran VINSTALL, and the primary server. You cannot edit a standby machine's .NCF files from another standby machine.

When editing .NCF files, use the Edit .NCF files on this machine only option to edit the local .NCF files. Use the Edit all Standby*Server* .NCF files option when you want to edit both the standby machine and primary server's .NCF files.

To edit .NCF files with VINSTALL

1. From the standby machine's console prompt, type `load c:\standby\vinstall` and press Enter to load the VINSTALL.NLM.

2. Choose "Edit Standby*Server* .NCF files."

Figure 1.14 Edit .NCF Files Screen

3. Select the file you want to edit and press Enter.

4. When finished editing, press Esc to save the changes and return to the file selection menu (Figure 1.2).

5. When you have edited all of the files you want, choose "Return to main menu" to close VINSTALL and return to the console prompt.

Uninstalling Standby*Server*

Standby*Server* features an uninstall utility that completely removes the Standby*Server* files and directories, and restores both the primary and standby machines to the state they were in before Standby*Server* was installed.

📝 **Note:** This procedure restores each machine to the state it was in before Standby*Server* was installed, except cases where NDS and the SYS: volume were deleted. You will need to manually restore NDS and the local SYS: volume for the standby machine. Any modifications made to .NCF files after Standby*Server* was installed will not be saved; i.e., any changes made by applications installed after Standby*Server*.

Uninstall is a feature of the VINSTALL utility and must be run from the standby machine. Both the primary and the standby machines must be up and running in their proper roles so Standby*Server* can load VCOPY to access the primary server's DOS drives.

If you installed additional standby machines, you must uninstall Standby*Server* from the vault machines before uninstalling from the original server pair.

To uninstall Standby*Server*

1. From the standby machine's console prompt, type `load c:\standby\vinstall` and press Enter to load the VINSTALL.NLM. Screen

2. Choose "Uninstall Standby*Server*."

3. Choose Yes to continue.

Figure 1.15 Waiting for Remote Message

4. On the primary server type `v.ncf` and press Enter.

5. On the standby machine, when the uninstall process is complete, press Enter to clear the screen.

6. Down and restart each machine.

You will have to manually reload NDS and the standby machine's SYS: volume if they were removed during the install process.

Chapter 2

Mirroring

This chapter introduces basic mirroring information and then describes how to establish mirroring between your primary server and standby machine using NetWare's mirroring technology. If you already understand the basics, you can skip to "Establishing Mirrors with NetWare" on page 43.

Mirroring Basics

Disk devices can be divided into up to four sections called partitions. Each partition is a contiguous set of sectors which share common characteristics. For instance, one partition can be set up to support a DOS file system while another partition on the same disk device can be set up for NetWare. Only one partition on each disk device can be a NetWare partition.

Drive Geometries and the Partition Table

Information about each of the partitions is stored in a table at the end (starting at byte 446) of the first sector on the disk device (head 0, cylinder 0, sector 1). This sector is referred to as the Master Boot Record (MBR).

The partition table has room for four entries. Each entry is 16 bytes long. Of the 16 bytes, 14 are used to describe where and how big the partition is. One byte is a boot flag. Only one of the four partitions can have its boot flag set. The NetWare 386 partition should not be made active because the partition does not contain the boot program necessary to start the system. When the system initializes, the partition table is scanned and control is transferred to the boot record on the partition with its boot flag set. Another byte is used to identify the type of system the partition is set up for (e.g. DOS, UNIX, NetWare, etc.).

Figure 2.1 Drive Geometries

The layout of the partition table entry is shown in Figure 2.1. The shaded areas illustrate the starting and ending physical sector addresses of the partition. Some systems have restrictions about where partitions can begin and end. For instance, DOS partitions must begin on a track (head) boundary while NetWare partitions must begin on a cylinder boundary. Note that head and cylinder boundaries are based upon the geometry reported by the disk or disk driver which can be simulated. The starting and ending partition addresses are each encoded into three bytes for a total of 24 bits. There are 8 bits for the head number, 6 bits for the sector number, and 10 bits for the cylinder number.

DOS Partitioning

With DOS, use FDISK to create, examine, and alter the partition tables. Using DOS 5 or higher it is possible to delete non-DOS partitions, but FDISK can only create DOS partitions. It is possible to make primary DOS or non-DOS partitions active with FDISK.

Note: If having problems booting a machine when everything seems correct with the partition table through FDISK and other disk utilities, run FDISK /MBR to rebuild the master boot record before returning the drive to the manufacturer as defective. This solution might work if it is possible to boot from a floppy and get to the hard drive, but the hard drive won't boot after running FORMAT /S.

There can be up to four partitions per device, but only one NetWare partition per device. To boot your machine from the hard drive and then run NetWare, a small DOS partition is needed. The rest of the device can be partitioned for NetWare. The DOS partition must contain enough free space to hold the Standby*Server* program and necessary support NLM files (about 10 MB).

Note: The DOS partition is not mirrored by NetWare.

NetWare Partitioning

NetWare partitioning is done from the primary server because it can see all disk devices in both machines.

NetWare recognizes primary and extended DOS partitions and NetWare partitions. Partitions from other operating systems are displayed as non-NetWare partitions. With NetWare, use INSTALL.NLM to create, examine, and alter the partition tables. It is possible to delete any partition from INSTALL.NLM, but only NetWare partitions can be created from INSTALL. If needed, make a DOS partition to boot from before installing NetWare.

Note: Always remember to reboot the machine after making a DOS partition change from NetWare (using INSTALL.NLM) before continuing any further DOS operations. It is not necessary to reboot if changing the NetWare partition from NetWare.

Using RAID Devices

If using a RAID on the primary server for maximum data protection, make sure there is a disk or RAID of the same size or larger in the standby machine as the other part of the mirrored set, otherwise the data on that RAID cannot be mirrored. A single large RAID system can be used on the standby machine to mirror all disk devices from the primary servers.

Standby*Server* also works with RAID devices that support multiple concurrent connections, but Vinca has not tested every device. For more information on using RAID devices and Standby*Server*, or RAIDShare™, see Tech Notes on Vinca's Web site at www.vinca.com.

Mirroring

Mirroring is the duplication of data from a NetWare partition on one disk device to a NetWare partition on another disk device. Up to 16 disk devices can be mirrored as a set, although commonly only two disk devices are mirrored.

Figure 2.2 Disk Mirroring—One Disk Channel
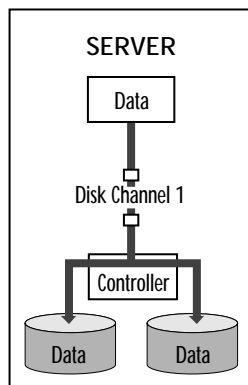
If a disk device fails in a mirrored set, the users on the system are able to keep working without interruption. If mirroring is set up and the controller fails, the volumes will be dismounted and the users have to wait for the system repairs to be made. Duplexing solves this problem.

Duplexing

Duplexing is the duplication of data from a NetWare partition on one disk device to a NetWare partition on another disk device, each on a separate disk channel. Duplexing is really a case of mirroring on separate controllers. Duplexing is not treated as a separate entity from mirroring in this manual or in the NetWare INSTALL.NLM. Therefore, the term mirroring can also refer to duplexing.

If a disk device or controller fails in a duplexed set, data is still accessible through a second channel and the users are able to continue operations. The failed components can then be repaired when it is more convenient for the system to be shut down.

Figure 2.3 Disk Duplexing—Two Disk Channels
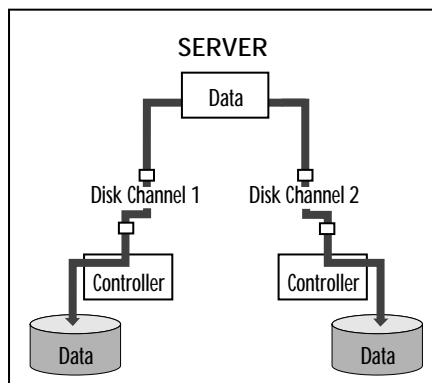
Disk Drivers

Disk drivers establish the communication channel between the disk device and the operating system. They manage the movement of data and even determine the disk device's performance as well as its reliability.

Because mirroring is a part of the operating system, the only thing needed to mirror is for the disk drivers to be loaded. When booting, NetWare examines the mirror tables and if the device sync bits do not match, re-synchronization begins 10 seconds after the console prompt is displayed.

For example, it is possible that if the server boots and loads the disk drivers that are part of the mirrored set and can't mount the SYS: volume, bad data could be mirrored onto a good disk device. However, this mirroring problem only occurs if there has been a system failure. To avoid this kind of situation, make sure only one half of the mirrored set is available when recovering from a server crash.

NetWare Mirroring

Once Standby*Server* is properly installed the mirror can be established, which is to say NetWare writes data to multiple disk devices known as a mirrored set at the same time. In this case, one of those disk devices is in the primary server and the other is in the standby machine.

Standby*Server* mirrors partitions, not volumes or files. This means that the NetWare partition on both disk devices in the mirrored set must be the same size.

A partition is a logical unit into which a disk device can be divided. In NetWare, disk devices can contain both a DOS partition and a NetWare partition, though the only disk device that needs to contain two partitions is the startup drive in each machine; all other disk devices need only contain a NetWare partition. The DOS partition can't be mirrored by NetWare; only NetWare partitions are mirrored from NetWare.

Mirroring

Figure 2.4 What NetWare Mirrors
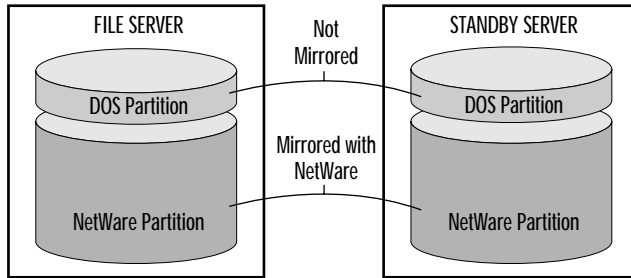
Only one NetWare partition can exist per disk device. That partition can contain more than one volume, or can contain only part of a volume. NetWare allows up to 8 volumes on a single NetWare partition, or a single volume can span up to 32 different disk devices with NetWare partitions. What is important is that Standby*Server* maintains a duplicate copy of that partition on a disk device in another server.

Physically, a NetWare partition consists of a large data area and a small hot fix area containing information about the partition.

Figure 2.5 Disk Device Partitioned for NetWare Use
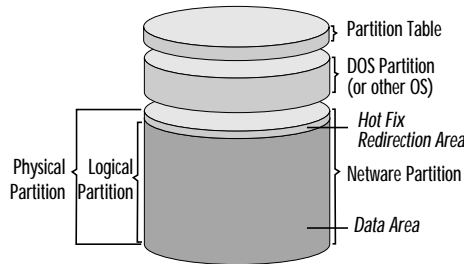
NetWare only mirrors the large data area, or logical partition. This way the hot fix area can be maintained separately for each part of the mirrored set.

Figure 2.6 NetWare Mirrors the Logical Partition Only
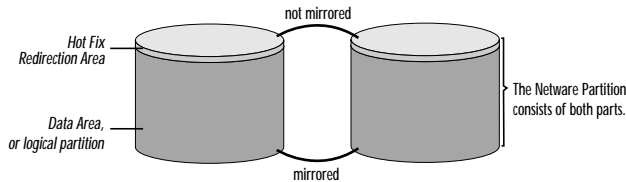
The hot fix area of a NetWare partition contains the mirroring table; this is what NetWare uses to determine how the mirror is established and whether it is synchronized with other parts of the mirrored set.

The mirroring table consists of several key components.

▼ The partition ID is determined at the time the NetWare partition is created, and is based on the system clock. The chance of having two partitions with the same ID is nearly impossible.

▼ The group list is a list of the partition IDs that constitute the mirror.

▼ Mirror status indicates which members of the group list have valid information and which ones need to be synchronized.

▼ The time stamp tells when the mirror table was last updated. For example, dismounting volume(s) on a disk device updates the mirror table. NetWare uses this time stamp to determine which disk device is the most current if the parts of the mirror are not all "in sync." The partition with the most recent time stamp is considered to contain the most current data.

Since the IDs of each partition are unique, NetWare is kept from arbitrarily mirroring to or from any disk device it finds.

Consider the following example. Partition A is mirrored to partition B in System A. Partition C is mirrored to partition D in System B. Partition A has no relationship to either partition C or D.

Figure 2.7 Mirrored Sets
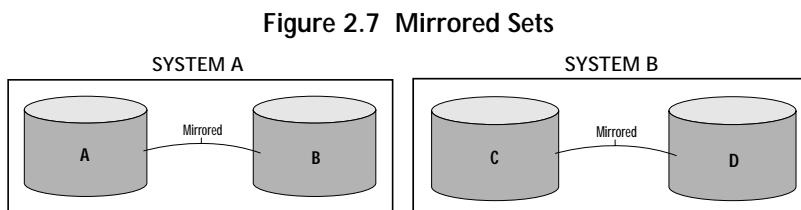
If the disk device containing partition B was replaced with the disk device containing partition C, NetWare would see no relationship between the two and would not mirror them.

A is mirrored only to B and will not mirror to another disk device unless explicitly told to do so.

Figure 2.8 Unmirrored Set

SYSTEM A
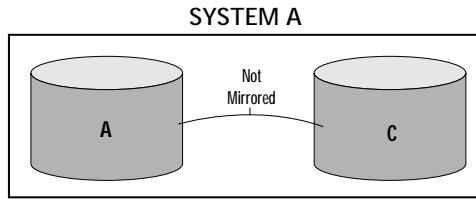
Mirroring is an automatic function of NetWare and is based on the time stamp. If the disk devices in a mirrored set come up and down independently of each other, it's possible for old data with a new time stamp to be mirrored over new data with an older time stamp. The mirror table with the most recent time stamp determines the mirror direction.

Remember that though data is written to volumes, NetWare mirrors partitions, not volumes. A single volume can be spanned onto multiple disk devices using this segmenting, or spanning, capability. Spanning volumes decreases access time but increases chances of failure.

Figure 2.9 A Volume Spanned Over Several Disk Devices

Both disk devices must be mirrored (four disk devices total)
in order to have volume SYS: protected.
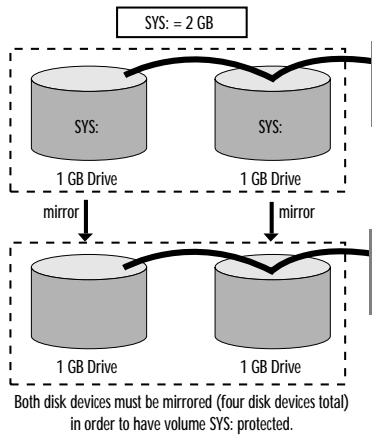
As long as all of the partitions the volume is stored on are mirrored, the volume will be mirrored. It will also mirror any name spaces (Mac, NFS, etc.). Since mirroring is done at the partition level, the mirroring process has no idea what type of files it is mirroring—it just mirrors blocks.

Establishing Mirrors with NetWare

The remainder of this chapter contains steps to mirror using NetWare. See the appropriate section for the NetWare version that you have:

▼   "Mirroring in NetWare 3.12" on page 45

▼   "Mirroring in NetWare 4.1x and IntranetWare" on page 49

When mirroring with NetWare, keep the following in mind.

▼   Always try to make new partitions to be mirrored exactly the same size or slightly larger than the original.

▼   Always establish the mirror from the primary server.

▼   When checking to see if the mirror has completed, type `mirror status` at the console prompt.

▼   Triggering a remirror will mirror the entire partition regardless of how much data is actually stored on the volume. The remirror process is not aware of the data—just that volumes exist on the partition.

▼   When uninstalling mirroring, select the device to be removed and press Del. This makes the rest of the removal process easier to complete.

▼   When uninstalling or changing the current mirroring configuration, you can unload the .DSK for the partition containing the information you want to save to ensure you don't delete or remirror over it.

▼   When uninstalling mirroring (using NetWare Install utility), always remember to press F3 on the "Out Of Sync" partition or the disk device cannot be used later. It can also cause confusion as to which disk device has good data.

▼   After pressing F3 on the "Out Of Sync" partition, always rename or delete the volume segments to eliminate future confusion as to which disk device has good data.

Caution!   Never run the NetWare Install utility on the standby machine in a standard Standby*Server* configuration; mounting mirrored disk devices can give them a newer time stamp than the disk devices on the primary server and cause older data to overwrite newer data when the mirror resynchronizes. Also, other mirror, volume, and disk commands return erroneous information when executed.

You can run Install on the standby machine in a Utility Server configuration as long as the volumes on the mirrored drives are not mounted.

Mirroring

Mirroring Tips

During normal operations, always keep all parts of the mirrored set on-line together—all drivers loaded and disk devices active. This is particularly important when downing and booting the server.

If there is a system failure, always have only part of the mirrored set available to the operating system. Don't load the drivers for all disk devices.

▼   There is a chance that part of the mirrored set will be in better shape than the other part.

▼   There is a bigger chance that an improper procedure will cause the loss of ALL data when trying to recover. Having part of the mirrored set available after a crash guarantees everything can't be lost with one keystroke.

If it is necessary to run VREPAIR or any other disk repair utility, it is a good practice to remove part of the mirrored set in case the utility causes more damage than good. By having the utility only run on part of the mirrored set this gives a second chance to try a different utility or method to gain access to the data.

Calculating Mirroring Times

The time it takes r and/or remirror depends on the speed of the disk components, the disk channel, and the speed of the Vinca link. This time can be estimated using the following formula:

Number of minutes = Disk size / (60 * request size * average requests/second). The request size is 4096 bytes and the average requests/second is displayed in the Standby*Server* screen when you press "m". See page 76 for more information on displaying Standby*Server* screen commands.

The following table uses a 1 GB drive and a variety of requests/second times to calculate the times shown.

Ave. Requests/Second	Time (Minutes)
100	43.7
250	17.5
600	7.3
1000	4.4

For example, 1 GB drive (1073741824) / (4096 * 60 *100) = 44 minutes.

Mirroring

Mirroring in NetWare 3.12

Once the primary and standby machines are properly connected, the Standby*Server* software is loaded and configured, and the servers are started in their roles as primary and standby, the mirror can be established.

This section describes the following:

- ▼ How to create a NetWare partition.
- ▼ How to establish a mirrored set of disk devices.
- ▼ How to remove a disk device from a mirrored set.
- ▼ How to repair a broken mirror.

Creating a NetWare Partition

Before establishing the mirror make sure that both disk devices have NetWare partitions that are the same size. The primary server already has NetWare partitions; this section describes how to create NetWare partitions on the disk devices exported from the standby machine.

All steps are performed on the primary server while both machines are up and running in their proper roles.

To create a NetWare partition

1. From the primary server's console prompt, type `load install` and press Enter to load the NetWare Install utility.

2. Choose Disk Options, Partition Table to open the Available Disk Drives window.

Figure 2.10 Available Disk Drives Window
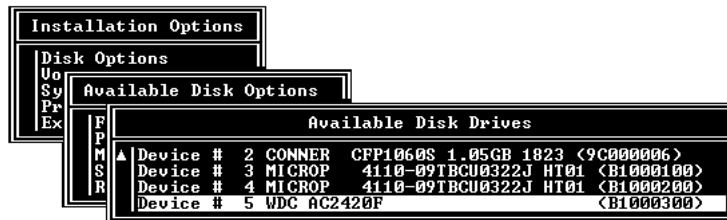

```
 Installation Options
 Disk Options
 Uo
 Sy  Available Disk Options
 Pr
 Ex  F           Available Disk Drives
     P
     M ▲ Device #  2 CONNER   CFP1060S 1.05GB 1823 <9C000006>
     S   Device #  3 MICROP   4110-09TBCU0322J HT01 <B1000100>
     R   Device #  4 MICROP   4110-09TBCU0322J HT01 <B1000200>
         Device #  5 WDC AC2420F                    <B1000300>
```

This window lists all disk devices accessible to NetWare, both from the primary server and from the standby machine (devices that start with a B1). Note the device number; this number is needed to choose which disk device to add to the mirrored set when establishing the mirror in the next section.

3. Choose the disk device, exported from the standby machine that will be part of a mirrored set.

Figure 2.11 Partition Options Menu
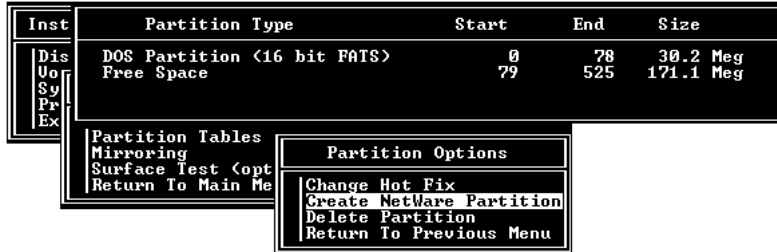
4. Choose Create NetWare Partition.

Figure 2.12 Partition Information Window
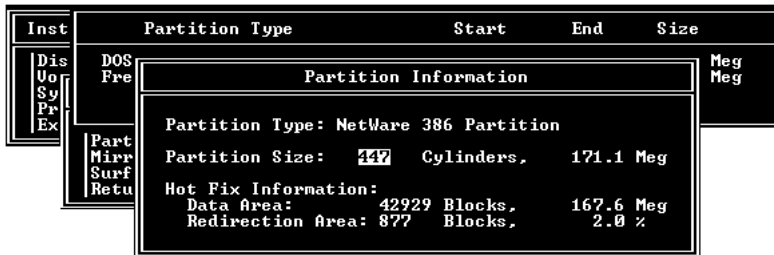
5. Enter the size of the partition to be created.

   Make sure this partition is at least as large as the partition on the corresponding disk device from the primary server. It is best to make this partition a little bit bigger.

   📝 **Note:**   If this partition is not at least as large as the one on the primary server, NetWare will not establish the mirror.

6. Press Esc to save the new partition and choose Yes when prompted to confirm the action.

7. Repeat steps 3-6 for each disk device on the standby machine that will be used to mirror data from the primary server.

When the needed partitions have been created on the standby machine's disk devices, everything is ready to establish mirrored sets.

Establishing a Mirrored Set

Once there are partitions on the disk devices exported from the standby machine that are as big as, or slightly larger than, the partitions on the primary server's disk devices, create mirrored sets. One disk device in each mirrored set is from the primary server; another disk in each set is from the standby machine.

The following steps presume the NetWare Install utility is already running.

To establish a mirrored set

1. Choosing Disk Options, Mirroring.

Figure 2.13 Partition Mirroring Status Screen

2. Choose the partition in the primary server to be mirrored.

   Note: NetWare creates the partition list in no particular order, so make sure the partition selected is an original in the primary server. Determine which partition is from the primary by taking note of the disk device on the Mirrored NetWare Partitions screen, then escaping back to Available Disk Drives and comparing the number to the name of the disk device. Look at the number in parentheses at the end of the line; if the number starts with a "B" it is from the standby machine.

3. Press Ins to insert a disk device in the mirrored set.

4. Choose a disk device exported from standby machine that will be the second half of the mirrored set.

   Exported disk devices are displayed with "B1" in parentheses at the end of the line.

5. Press Esc to create the mirrored set.

   If the selected partition size is larger than the existing partition, choose Yes. If it is not, choose No and see "Creating a NetWare Partition" on page 45 to recreate a partition on the standby machine that is large enough mirror the partition on the primary server.

   Note: If you choose Yes and the existing partition is larger than the selected partition, you will lose the data on your primary server's device.

If you choose Yes, the mirror is now established and will take time to synchronize—
see "Calculating Mirroring Times" on page 44 for information on calculating the time
your system will take to synchronize the mirrors.

When the mirror is synchronized, the message "All mirrored partitions on this system
are synchronized" appears on the screen.

> **Note:** If running NetWare 3.12 and using a vault machine, SYNCFMIX patch
> must be used. This patch fixes errors caused when mirroring to more than
> two disk devices is available from Novell. See "SYNCMFIX.NLM (NetWare
> 3.12)" on page 110 for more information.

Undoing a Mirror

Most problems with NetWare mirroring arise when disk devices are moved between
systems or deleted from the mirrored set. By following these instructions on removing
mirroring, these problems can be avoided. "Unmirroring/Remirroring Scenarios" on
page 84 describes when to perform this task.

The following steps presumes both machines are running and the NetWare Install
utility is running on the primary server.

To undo a mirror

1. Choose Mirror/Unmirror disk partitions.

2. Choose the mirrored set you want to undo.

3. Select the disk device to be removed from the mirrored set and press Del.

   Remember that partitions on disk devices in the standby machine have a number
   that begins with "B1" in parentheses.

   > **Note:** Make sure to choose the right disk device. If the wrong disk
   > device is deleted data can be lost.

4. Press Esc to return to the Partition Mirroring Status window.

5. Select the disk device and press F3 to make the partition available for other use.

   If you don't make the disk device available for other use, the volume(s)
   contained on it are unmountable.

   If error messages appear, press Esc to clear them. If this disk device is to be
   removed from the mirrored set, choose NO when asked whether to salvage the
   volume segment; the volume is permanently lost. If this disk device is to be kept
   as part of the mirrored set, choose YES. If there are several volumes on this
   partition, repeat the procedure for each volume.

Mirroring

Mirroring in NetWare 4.1x and IntranetWare

Once the primary and standby machines are properly connected, the Standby*Server* software is loaded and configured, and the servers are started in their roles as primary and standby, the mirror can be established.

This section describes the following:

▼ How to create a NetWare partition.

▼ How to establish a mirrored set of disk devices.

▼ How to remove a disk device from a mirrored set.

▼ How to repair a broken mirror.

Creating a NetWare Partition

Before establishing the mirror make sure that both disk devices have NetWare partitions that are the same size. The primary server already has NetWare partitions; this section describes how to create NetWare partitions on the disk devices exported from the standby machine.

These steps are performed on the primary server. NetWare should already be running on the primary server, and the standby machine should be up and functioning as a standby.

To create a NetWare partition

1. From the primary server's console prompt, type `load install` and press Enter to load the NetWare Install utility.

2. Choose Disk Options, Modify Disk Partitions, Hot Fix to open the Available Disk Drives window.

Figure 2.14 Available Disk Drives Window

```
╔══════════════════════════════════════════════════════════════╗
║                    Installation Options                      ║
╠══════════════════════════════════════════════════════════════╣
║|Disk Driver Options (Configure/Load/Unload Disk Drivers)     ║
║                                        /Unload LAN Drivers)  ║
║          Available Disk Options        or/Test Disk Partitions)║
║                                        t/Dismount Volumes)   ║
║ |Modify                                                       ║
║ |Mirror/          Available Disk Drives                       ║
║ |Perform ╔══════════════════════════════════════════════════╗║
║ |Return  ║▲|Device #  3 Compaq SMART Slot 6 Dsk 4 NFT (47000300)║
║          ║ |Device #  1 Compaq SMART Slot 6 Dsk 1 NFT (B1000100)║
║ |Other O ║ |Device #  5 Compaq SMART Slot 6 Dsk 2 NFT (B1000200)║
║          ║▼|Device #  6 Compaq SMART Slot 6 Dsk 3 NFT (B1000300)║
╚══════════╚══════════════════════════════════════════════════╝╝
```

This window lists all disk devices accessible to NetWare, both from the primary server and from the standby machine. Note the disk device number; this number is needed to choose which disk to add to the mirrored set when establishing the mirror in the next section.

3. Choose the disk device, exported from the standby machine that will be part of a mirrored set.

4.   Choose Create NetWare Disk Partition

Figure 2.15   Disk Partition Information Window
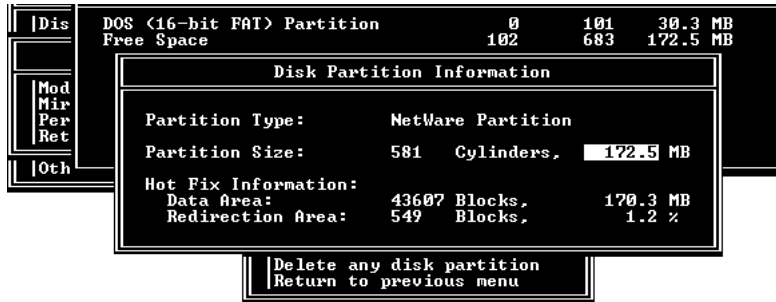
5.   Enter the size of the partition to be created.

Make sure this partition is at least as large as the partition on the corresponding disk device from the primary server.

6.   Press Esc to save the new partition.

Choose Yes when prompted to confirm the action.

7.   Press Esc to return to the Available Disk Options menu.

8.   Repeat steps 3 and 7 for each disk device on the standby machine that will be used to mirror data from the primary server.

When the needed partitions have been created on the standby machine's disk devices, everything is ready to establish mirrored sets.

Establishing a Mirrored Set

Once there are partitions on the disk devices exported from the standby machine that are as big as, or slightly larger than, the partitions on the primary server's disk devices, create mirrored sets. One disk device in each mirrored set is from the primary server; another disk in each set is from the standby machine.

The following steps presume the NetWare Install utility is already running.

To establish a mirrored set

1. Choosing Disk Options, Mirror/Unmirror disk partitions.

Figure 2.16 Disk Partition Mirroring Status Window

2. Choose the partition in the primary server to be mirrored.

   Note: NetWare creates the partition list in no particular order, so make sure the partition selected is an original in the primary server. Determine which partition is from the primary server by taking note of the disk device on the Mirrored Disk Partitions screen, then escaping back to Available Disk Drives and comparing the number to the name of the disk device. Look at the number in parentheses at the end of the line; if the number starts with a "B1" it is from the standby machine.

3. Pressing Ins to insert a disk device in the mirrored set.

4. Choose a disk device exported from standby machine that will be the second half of the mirrored set.

   Exported disk devices are displayed with "B1" in parentheses at the end of the line.

5. Press Esc to create the mirrored set.

   If the selected partition is smaller than the original, NetWare will not establish the mirror. Go back and create a NetWare partition on a disk in the standby machine that is large enough (see "Creating a NetWare Partition" on page 49).

The mirror is now established. It will take time for the mirror to synchronize—see "Calculating Mirroring Times" on page 44 for information on calculating the time your system will take to synchronize the mirrors.

When the mirror is synchronized, the message "All mirrored partitions on this system are synchronized" appears on the screen. The mirror is established; test the installation and become familiar with Standby*Server*.

Undoing a Mirror

Most problems with NetWare mirroring arise when disk devices are moved between systems or deleted from the mirrored set. By following these instructions on removing mirroring, these problems can be avoided. "Unmirroring/Remirroring Scenarios" on page 84 describes when to perform this task.

The following steps presumes both machines are running and the NetWare Install utility is running on the primary server.

To undo a mirror

1. Choose Mirror/Unmirror Disk Partitions.
2. Choose the mirrored set you want to undo.
3. Choose the mirrored set from which you want to remove a partition.
4. Press Esc to return to the Partition Mirroring Status window.

> **Note:** NetWare displays a warning screen. Follow the instructions closely. It is a good practice to delete the device to be removed from the mirrored set by choosing No when asked to salvage volume information. If you choose to salvage the volume enter a new name for the volume.

Mirroring

Repairing a Broken Mirror

These instructions are provided in case the mirroring gets "Out Of Sync." The mirror is not in sync if one of the following messages is displayed on the console after typing mirror status:

"Logical Partition # ? is Out of Synchronization"

"Logical Partition # ? is in an Orphaned State"

Generally if mirroring is started and allowed to run, these mirroring problems will not occur. Most often, these problems only occur during testing or when the server and other disk devices are going down frequently.

If an out of sync mirror is on the production network, Do not panic; be very patient and closely follow the instructions listed here. Mirrored data is lost more often by using improper procedures than for any other reason. This procedure removes the bad disk device from the mirrored set, then reestablishes the mirror as described earlier in this chapter.

The procedure listed below is for two duplexed disk devices that are out of sync. If there are more disk devices, follow the same procedure for each disk device individually. Trying to repair too many disk devices at once becomes very confusing.

Note: If the drives are mirrored off of the same controller, physically remove the disk devices rather than unloading the device driver.

To repair a broken mirror

1. On the primary server, remove part of the mirrored set by unloading the disk driver at the console.
2. Try to mount the volume(s) on the active disk device. It might be necessary to run VREPAIR to get them to mount. If the volumes mount, go to step 4.
3. If the volume(s) won't mount, remove the driver by unloading it at the console. Then load the driver for the other disk device. Go back to step 2.
4. Login and test all the data. If it is good, make a reliable backup.
5. After the backup is completed, remove the driver for the disk device with the good data. This step is vital to a successful recovery.
6. Load the driver for the disk device with the bad data.

   Note: If either disk device's volume(s) were mounted and tested, then assume, for this procedure, that the other disk device's data is bad.

7. Load install, then go to Mirrored NetWare Partitions and undo the mirror by pressing Del on the disk device listed as "unavailable."

8. Press Esc to return to Partition Mirroring Status. If the disk device is listed as "Out Of Sync," press F3. Choose Yes to delete the volume(s).

    CAUTION!   Make sure to delete the volume(s). If this isn't done, NetWare can mirror it to the disk device with good data later in this procedure.

9. Go to Volume Options. Make sure no volumes exist on the disk device with the bad data. If there are any, delete them.

10. Load the driver for the disk device with good data.

11. Go to Partition Mirroring Status and verify that the disk devices are "Not Mirrored." If either one is mirrored, select it and press Enter. Then from Mirrored NetWare Partitions, press Del on the disk device listed as "unavailable."

12. If the disk device with good data becomes listed as "Out Of Sync" in Partition Mirroring Status, press F3.

    CAUTION!   DO NOT DELETE THE VOLUMES ON THIS DISK DEVICE.

13. Both disk devices should now be listed as "Not Mirrored" in Partition Mirroring Status.

14. Reestablish the mirror using the instructions in this chapter appropriate to the version of NetWare.

Mirroring

Mirroring Console Commands

These mirroring/device console commands are only available in NetWare 3.12, 4.1x, and InternetWare. Type the following commands at the primary server's console prompt and press Enter to execute them.

Abort remirror x

where x is the number of the logical partition # to abort.

Stops remirroring of a logical partition. If there is a large partition (3- 5GB) on a heavily used server, consider remirroring during the night or a non-peak load time. Use this command to stop the mirroring process and restart it at a later time when the remirroring process won't affect users.

Remirror partition x

where x is the number of the logical partition # to restart mirroring.

Manually start remirroring after the abort remirror command has been issued.

The partition # for abort and remirror partition # is determined from the mirror status command.

List devices

Displays device information for the server. A device can be a disk driver, tape driver, optical disk driver, or any other storage device driver. This command is used to check if all the disk devices are currently available to the server.

Mirror status

Displays all mirrored logical partitions and the status of each one. This command shows if all partitions are fully synchronized, or if they are still remirroring and what percentage of remirroring is completed.

Scan for new devices

Checks for disk devices that have been added since the NetWare server was booted. NetWare 3.12, 4.1x, and IntranetWare scan for disk devices differently than 3.11. Because of this feature, a device can be added after the server has booted by manually scanning to make it available. When loading a disk device driver, nothing might happen or some of the disk devices might not be seen from NetWare. NetWare can't see the devices until told to go look for them. The scan for new devices command picks up the new drives and allows volumes to be mounted or starts remirroring to the new device. It might be necessary to scan for new devices if a disk device fails during operation and is repaired in order for the operating system to recognize it.

Chapter 3
System Failures & Recovery

This chapter contains two sections; Testing the Failover Configuration, and Understanding the Recovery Process for a standard configuration. If you have installed a vault machine, see Appendix F, *Using a Vault Machine* for vault machine specific instructions on testing, failover, and recovery processes.

The Testing the Failover Configuration section should be used to complete the initial installation, any Standby*Server* updates, and after adding additional applications to either the primary server or the standby machine (when using the Utility Server feature) to ensure the fault tolerant configuration is working properly.

The Understanding the Recovery Process section is used to recover from specific types of failures.

Testing the Failover Configuration

Standby*Server* categorizes system failures in one of the following categories:

Category	Description
Complete system failure	The primary server and standby machine cannot communicate over the Vinca link (when used) or client network.
Component failure	The primary server and standby machine are able to communicate, even though a component has failed.

A complete system failure causes the standby machine to failover (when AutoSwitch is enabled) to assume the primary role. For example, a software ABEND would make the server unavailable and the machines would not be able to communicate.

A component failure does not cause a failover. NetWare can be configured to warn you that a component has failed, but there is no action by Standby*Server*. For example, you can have NetWare alert you if a disk device failed, but because the machines could still communicate, the standby machine would not failover. In this case, mirroring would discontinue and the working disk device from the mirrored set would handle all reads and writes.

Standby*Server* has two tests to simulate these failures; "The AutoSwitch Test" simulates a complete system crash where automatic failover occurs; "Disk Device Failure Test" simulates a disk failure. The recovery procedures for these tests are the same as would be used in the event of an actual failure.

The AutoSwitch Test

The AutoSwitch test walks you through a primary server failure, standby machine failover, and recovery of both machines returning them to their original roles. It is best to do this test with no users logged in to reduce the chance of error while still becoming familiar with Standby*Server*.

After completing the AutoSwitch testing steps, complete the test by returning the machines to their original roles.

To test automatic failover

1. Boot the standby machine first, and then the primary server to ensure the machines start in their original roles.

On the primary server

2. From the console prompt, type `mirror status` and press Enter to check the mirror status.

   If the mirrors are not synchronized, synchronize them before continuing.

On the standby machine

3. Access the Standby*Server* screen and make sure the Status Bar is green indicating the machines are communicating properly. If the Status Bar is red, troubleshoot the problem before continuing.

On the primary server

4. Down and exit the primary server.

   As the primary server is shut down, the status bars in the Standby*Server* and AutoSwitch screens turn red and start flashing to indicate that communication with the primary server has been interrupted.

   The AutoSwitch screen displays the Failover Delay countdown.

System Failures & Recovery

Figure 3.1 AutoSwitch Activated Screen

On the standby machine

5. After the standby machine fully assumes the primary role, add or edit an existing file to test the mirror resynchronization (to take place later in the test).

On the primary server

6. Change to the STANDBY directory.

7. At the primary server's DOS prompt, type `standby` and press Enter to restart the primary server in the standby role.

8. Check the Standby*Server* screen to ensure the machines are communicating again.

9. If the Status Bar is green, let the mirror resynchronize. This should not take long because the server was only down for a moment. When the server is down for a long period of time, the resynchronization time will be longer.

    If the Status Bar is red, there is a problem with the LAN card.

Troubleshooting a LAN card problem

On the standby machine

1. From the console prompt, type `display servers` and press Enter to access the server list. If the primary server is not listed, the LAN drivers are not configured properly.

On both machines

2. From both machine's console prompt, type `config` and press Enter to see if the LAN drivers are loaded.

3. Check the frame type used on both sides and make sure they are the same; i.e., 802.3 to 802.3.

System Failures & Recovery

Returning the machines to their original roles

These steps are a continuation of the AutoSwitch test. In Step 8 of the AutoSwitch test, the mirrors were resynchronized with each machine functioning in the other machine's role. These steps walk you through downing each machine and rebooting them in the proper order to reestablish each machine in its original role. Again, it is best to do this test with no users logged in to reduce the chance of error while still becoming familiar with Standby*Server*.

To return the machines to their original roles

On the primary server (currently in the standby role)

1. Press Alt+Escape to access the AutoSwitch screen.
2. Press "p" to pause AutoSwitch.

On the standby machine (currently in the primary role)

3. Down and exit the standby machine.
4. Wait until the standby machine is completely down and the volumes unmounted (the Status Bar on the Standby*Server* screen turns red).

On the primary server

5. Down and exit the primary server (in the standby role).

On the standby machine

6. Change to the STANDBY directory.
7. Type `standby` and press Enter to load Standby*Server*.

On the primary server

8. Boot the primary server and change to the NetWare directory.
9. From the primary server's DOS prompt, type `server` and press Enter.
10. Let the two machines connect and resynchronize.
11. Check the file that was added or modified earlier to ensure the information was updated correctly.

The AutoSwitch test is now complete. This is the same procedure you would perform in case of primary server failure. In case of real primary server failure, take time to follow proper recovery procedures. Failing to follow proper procedures can result in lost data. If recovery is rushed it is easy to delete all data. If only half of the mirrored pair is available, it is impossible for NetWare to delete all data at once.

Disk Device Failure Test

Once a mirrored set is established, NetWare views both disk devices as though they were the same. If one disk device in a mirrored set fails, NetWare continues to use the other disk device. Because a disk device is still available to the primary server, no failover is initialized.

Unloading Standby*Server* on the standby machine can simulate a disk device failure. When you unload Standby*Server*, you remove the primary server's ability to communicate with the disk device(s) located in the standby machine.

To test a disk device failure

1. Boot the standby machine first, and then the primary server to ensure the machines start in their original roles.

On the standby machine

2. From the console prompt, type `mirror status` and press Enter to check the mirror status. If the mirrors are not synchronized, synchronize them before continuing.

3. Access the Standby*Server* screen and make sure the Status Bar is green indicating the machines are communicating properly. If the Status Bar is red, troubleshoot the problem before continuing.

4. Login users and create activity on the network by performing large file copies to causes NetWare to write data to the disk devices in both the machines.

5. Access the AutoSwitch screen and press Esc to close the program (choose Yes when prompted).

6. Access the Standby*Server* screen and press Escape to exit the program (choose Yes when prompted).

7. Wait for the primary server to deactivate the disk.

8. From the console prompt, type `c:autoexec` and press Enter to execute the AUTOEXEC.NCF file and reload Standby*Server* and AutoSwitch, or C:

9. Notice the momentarily increased disk device activity as NetWare automatically resynchronizes the mirror. The resynchronization time won't be long because the disk was unavailable for only a moment. When the disk is unavailable for a long period of time, the resynchronization time will be longer.

In an actual recovery scenario it would be possible to let the system run with the missing disk device until it is convenient to down the system and repair it.

System Failures & Recovery

Understanding the Recovery Process

The recovery process has three main tasks:

1. Make sure users can still access network services, whether on the primary server (in case of standby machine failure) or on the standby machine (in case of primary server failure).

2. Restart the machine in case of software faults, or repair the hardware fault by fixing or replacing the faulty item.

3. Resynchronize or reestablish the mirrors.

There are a limited number of things to do in case of system failure—trigger a failover, break a mirrored set, establish a mirrored set, and start each machine in either the primary or standby role.

The remainder of this chapter discusses specific scenarios and how to recover from them. Each scenario is presented in checklist form and references other sections in this guide for more detailed information about specific steps.

All scenarios presume that the machines are currently functioning in their original roles.

Recovering From a Complete Primary Server Failure

A complete system failure, when the standby machine cannot communicate with the primary server, will when enabled cause an automatic failover. The most common causes of complete system failure are:

▼ Software ABEND.

▼ Software lockup.

▼ Logic board failure.

▼ Disk controller failure.

▼ Power interruption.

In each case, the primary server should be repaired and started in the standby role to fully resynchronize the mirrors before restoring each machine to its original role. In Utility Server installations the Utility Server functionality is not restored until both machines are returned to their proper roles.

To recover from complete system failure

❒ Let AutoSwitch trigger the standby machine to automatically failover and assume the primary role. The system will automatically run any volume repairs necessary to restore service.

❒ Repair the primary and test it off-line. When repairs are complete and verified, reconnect the primary server to the network.

❒ Start the primary server as a standby.

❒ Let the mirror completely resynchronize. Enter `mirror status` at the console prompt to see the status of the mirror.

❒ When the mirror is complete, pause AutoSwitch. Down first the standby machine (in primary role), then the primary server (in standby role).

❒ Restart each machine in its proper role.

LAN Card Failure (Non-Dedicated Vinca Link)

If the LAN card fails in either machine when there is no dedicated Vinca link, the machines cannot communicate and this scenario is treated as a complete system failure. If AutoSwitch is enabled, the standby machine will failover and assume the primary role. Because the primary server didn't completely fail, you will have two servers up and running, but only one communicating with the network. When you use a dedicated Vinca link (highly recommended), this situation is avoided.

To recover from a LAN card failure

❒ Down the machine with the failed card.

❒ Repair or replace the card.

❒ Restart the machine in standby role.

❒ Allow the mirrors to resynchronize.

If it was the primary server's LAN card that failed, you can use the "To return the machines to their original roles" steps to return the machines to their original roles.

Dedicated Vinca Link Failure

When you are using a dedicated Vinca link and a part of that link fails, mirroring stops.

To recover from a dedicated Vinca link failure

❒ Disable the AutoSwitch if it is enabled to prevent failover.

❒ Test the Vinca link cable.

❒ Test the standby machine's Vinca link LAN card.

If either the cable or the standby machine's Vinca link LAN card failed, replace the failed item and restart the standby machine in standby role as needed.

System Failures & Recovery

If both are working properly, the primary server's Vinca link LAN card has probably failed. The following paths are examples of what can be done to minimize downtime or data loss. Use the path that best suits your time and client demand for the data:

Some down time, no data loss

❒ Disable AutoSwitch.

❒ Shut down both machines and change the mirroring to use the client network.

❒ Reboot both machines (standby first, primary second) and enable AutoSwitch.

❒ Allow the mirrors to resynchronize.

❒ Shut down the primary server and allow the standby machine to failover and assume the primary role.

❒ Replace and test the primary server's Vinca link LAN card.

❒ Change the mirroring to use a dedicated Vinca link.

❒ Follow the steps for recovering from a primary server failure.

Down time, no data loss

❒ Disable AutoSwitch on the standby machine.

❒ Shut down the primary server.

❒ Repair the Vinca link card in the primary server.

❒ Reboot the primary server in the primary role.

❒ Enable AutoSwitch on the standby machine.

No down time, possible data loss

❒ Down the primary server.

❒ Allow the standby machine to failover and assume the primary role.

❒ Repair the Vinca link card in the primary server.

❒ Start the primary server in the standby role.

❒ Let the mirror resynchronize.

❒ Enable AutoSwitch on the primary server, which is currently assuming the standby role.

Because no new data is written to the mirrored disks in the standby machine until it is downed, the time stamps on the disks in the standby machine will cause the mirror to synchronize correctly from the primary to the standby.

Primary Server System Disk Failure

Because NetWare loads drivers, routing, and directory information into RAM, a failure of the primary's system disk (the one containing SYS:) will not necessarily cause the primary to fail. Read and write requests are routed over the Vinca link to the standby machine and serviced by the mirrored disks there. Users will continue to have full access to the data in those cases that don't cause a complete primary failure.

It is *strongly* recommended that you keep a backup of the files on the boot partition so that they can be easily restored after this type of failure. This section assumes that such a backup—including the Standby*Server* files and the NetWare files—has been made and can be used for recovery. If there is no backup of the boot disk files, it is necessary to reinstall NetWare and Standby*Server*. You can also use VCopy to copy DOS files to the mirrored NetWare partition.

This scenario presumes that the mirrored data on the failed disk device is no longer accessible and the mirror must be re-established.

To recover from a system disk failure

❒ Down the primary server and let AutoSwitch trigger a failover on the standby machine.

❒ Repair or replace the failed disk device and restore the boot files from backup. If the disk device is replaced, make sure to copy the correct disk drivers to the boot partition and add appropriate lines to the NetWare configuration files.

❒ On the standby machine (functioning in primary role), break the mirror to the failed disk device. See the guidelines in "Repairing a Broken Mirror" on page 53 for more information.

❒ Start the primary server in standby role.

❒ On the standby machine (functioning in primary role), use the NetWare Install program to create a NetWare partition on the new disk and to establish the mirror as it was before the failure. See Chapter 2, *Mirroring* for more information on how to perform these tasks.

❒ When the mirror is synchronized, on the primary server (in standby role) pause AutoSwitch and down standby machine (in the primary role) first, then the primary server (in the standby role).

❒ Restart each machine in its proper role, standby machine first and primary server second.

System Failures & Recovery

Primary Server Non-System Disk Failure

Because NetWare treats the mirrored disk devices in the standby machine as if they were local devices in the primary, a failure of drives in the primary will not interrupt service to users. Because all network communications continue to function, AutoSwitch does not trigger a failover. All disk requests are routed over the Vinca link and serviced by the disk devices in the standby machine.

This scenario assumes that the mirrored data on the failed disk device is no longer accessible and the mirror must be re-established.

When a primary disk device failure is detected, do the following:

To recover from a non-system disk failure

❒ Down the primary server and let AutoSwitch trigger a failover on the standby machine.

❒ Repair the damaged disk device. If the disk device controller is replaced, make sure to copy the correct disk drivers to the boot partition and add appropriate lines to the NetWare configuration files.

❒ On the standby machine (functioning in primary role), break the mirror to the failed disk device. See the guidelines in "Repairing a Broken Mirror" on page 53 for more information.

❒ Start the primary server in standby role.

❒ On the standby machine (functioning in primary role), use the NetWare Install program to create a NetWare partition on the new disk and to establish the mirror as it was before the failure. See Chapter 2, *Mirroring* for more information on how to perform these tasks.

❒ When the mirror is synchronized, on the primary server (in standby mode) pause AutoSwitch and down standby machine (in the primary role) first, then the primary server (in the standby role).

❒ Restart each machine in its proper role, standby machine first and primary server second.

Standby Machine Complete System Failure

If the standby machine has a complete failure, it will have no direct impact on the primary server; however, mirroring functionality and fault tolerance stop.

To recover from complete system failure

❒ Power off the standby machine. Leave the primary server running.

❒ Repair the standby machine. Take the standby machine off the network to test it.

❒ Start the standby machine (in standby role).

❒ Let the mirror completely resynchronize. From the primary server's console prompt, type `mirror status` to see the status of the mirror.

Because the time stamps on the mirrored data in the primary server are newer than those in the standby machine, data will be mirrored correctly from the primary to the standby without requiring a restart.

Standby Machine Any Disk Device Failure

If the standby machine has a disk device failure, it will have no direct impact on the primary server; however, mirroring functionality and fault tolerance stop.

To recover from disk device failure

❒ Down the standby machine. Leave the primary server running.

❒ On the primary server, use NetWare's Install utility to break the mirror to the failed disk device. See the guidelines in "Repairing a Broken Mirror" on page 53 for more information.

❒ Repair or replace the failed disk device in the standby machine.

❒ On the primary server, use the NetWare Install program to create a NetWare partition on the new disk and to establish the mirror as it was before the failure. See Chapter 2, *Mirroring* for more information on how to perform these tasks.

❒ Let the mirror completely resynchronize. From the primary server's console prompt, type `mirror status` to see the status of the mirror.

System Failures & Recovery

Chapter 4
Using Standby*Server*

Standby*Server* includes several screens to manage and display information. The availability of these screens depends on what features you have loaded. For example, if the AutoSwitch feature is not loaded, the AutoSwitch screen will not be available.

Standby*Server*'s Main Screen

The Standby*Server* program, running on the standby machine, displays the following screen. A table containing screen descriptions is on the next page.

Figure 4.1 Standby*Server* Screen
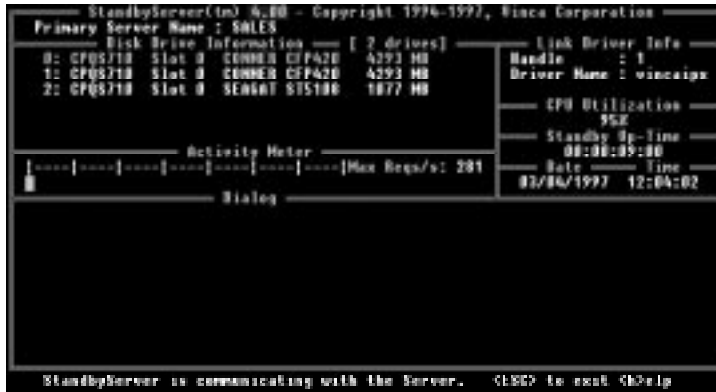
Field	Description
Primary Server Name	Primary server's name.
Disk Drive Information	Local disk devices information. Grayed out devices are those used by Utility Server or another drive that is not exported.
Activity Meter	Amount of disk activity.
Link Driver Info	The driver used for the Vinca link.
CPU Utilization	Percent of local CPU utilized for current tasks.
Standby Up-Time	How long Standby*Server* has been running.
Date and Time	The current system date and time.
Dialog	Information such as disk reads can be displayed here. You can press "h" for help to display a list of available commands. See "Commands" on page 71 for more information on these commands.
Status Bar	When green, Standby*Server* is communicating with the primary server. When red, Standby*Server* is not communicating with the primary server. This indicates primary server is down, the Vinca link is disconnected, or there is a conflict with another card in either system.

Commands

The following commands can be used on the Standby*Server* screen to clear the message window, unload Standby*Server*, or display information:

Key	Description
Space	Clears the message window.
Esc	Unloads Standby*Server*.
A	Resets the Average Requests/Second count.
d	Displays information about the disk devices in the standby machine.
e	Displays any errors that have occurred during the current session.
h	Displays the Help Command Options (the list of commands which are available when working in Standby*Server*).
i	Displays information about Standby*Server* including where to call for technical help.
m	Displays communication information such as the maximum and average requests per second. These statistics can help you calculate the time it will take to synchronize a mirror. See "Calculating Mirroring Times" on page 44 for information on how to calculate the time your system will take to synchronize the mirrors.
s	Scans for new disk devices and displays the primary server's NetWare serial number. If new devices are found, they are registered and made available for mirroring.
v	Toggles verbose mode, and displays read and write commands.

Using StandbyServer

Using the AutoSwitch Feature

If the AutoSwitch feature was loaded during the install (default), the AutoSwitch screen will be available from the Standby*Server* program. If it is not loaded, you can load it at any time after Standby*Server* is installed from the console prompt. AutoSwitch can also be unloaded or paused at anytime.

Loading AutoSwitch

When loading AutoSwitch, you can change the Failover Delay (40 seconds, by default) to be longer or shorter. This delay causes Standby*Server* to countdown the number of entered seconds before the standby machine fails over after a primary server failure is detected. During this delay time, you can abort the failover if needed. If you don't enter a Failover Delay when loading AutoSwitch from the console prompt, 40 seconds will be used.

To load AutoSwitch

- From the machines' console prompt, type
  `load c:\standby\sbsentry <-s delay>`
  where the *delay* is the number of seconds for the Failover Delay.

You can use the following command line options when loading the SBSENTRY.NLM.

Options	Description
-s n	Wait n seconds after detecting a primary failure before starting the AutoSwitch process. The default is 40.
-a	Call AttachToFileServer() to see if the server is still alive, instead of using the SAP table in case the user is doing SAP filtering.
-c net	Finds and connects to the primary server using its IPX internal net number, where *net* is the primary server's IPX internal net number.
-q	Uses NetWare's Query Services API.
-u	Does not use NetWare's DownFileServer API.

Sample

This is a sample command line for this file. Remember that capitalization counts on switches

`load C:\STANDBY\SBSENTRY -s 10`

Loads SBSENTRY with a delay of 10 seconds after server failure before the autoswitch is triggered.

Using Standby*Server*

Unloading AutoSwitch

AutoSwitch can be unloaded to disarm (disable) the automatic failover feature. This can be done at any time, including during the Failover Delay to abort a failover.

To unload AutoSwitch

1. Press Alt+Escape to access the AutoSwitch screen and press Esc.

2. Choose Yes.

   Or

   • From the console prompt, type `unload sbsentry` and press Enter.

Pausing AutoSwitch

Pausing AutoSwitch allows the NLM to be loaded while disabling the automatic failover. When you pause AutoSwitch, no failover will occur until you press any key to continue.

To pause AutoSwitch

   • Access the AutoSwitch screen and press "p".

Using Standby*Server*

How AutoSwitch Works

Standby*Server* monitors the primary server to ensure it is available. If the primary server becomes unavailable, the standby machine fails over and assumes the primary role.

When a Vinca link is used and it becomes unavailable, Standby*Server* pings the primary server over the client network to see if it is the server or link that has failed. If the link has failed, disk reads and writes are handled by the primary server's disk devices and a failover is not initiated. If the server is unavailable, a failover occurs.

Figure 4.2 AutoSwitch Logic Diagram
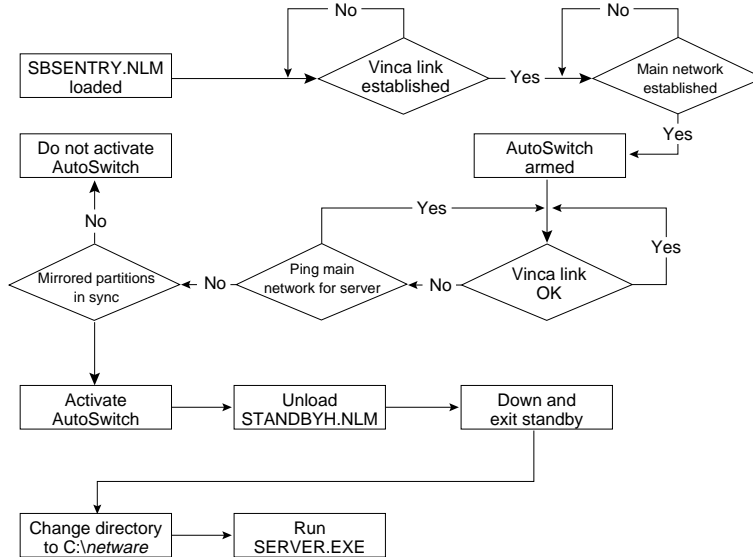
Keep in mind that if you are not using a dedicated Vinca link, the client network is used for the Vinca link connection.

Understanding the AutoSwitch Screen

The AutoSwitch screen displays the following information:

Figure 4.3 AutoSwitch Screen

Field	Description
Primary Server Name	The primary server's name.
Connection Status	CONNECTED when Standby*Server* is communicating with the primary server over the specific path, or NOT CONNECTED when Standby*Server* is unable to communicate over the specific path.
AutoSwitch	ARMED when ready to failover for the primary server, NOT ARMED when not ready due to an IPX connection failure, or ACTIVATED when a server failure has been detected and the Failover Delay has been reached.
Failover Delay	The number of seconds Standby*Server* waits after a server failure is detected before initiating a failover. This time is configured when SBSENTRY is loads.
Dialog	Messages generated while monitoring server connections. The messages include a time and date stamp to help track the activity between the two machines. These messages are erased as they scroll off the top of the screen. You can press "h" for help to display a list of available commands. See "Commands" on page 76 for more information on these commands.
Status Bar	A green Status Bar indicates is servers are communicating. A red Status Bar indicates the servers are not communicating. If the servers are not communicating, the primary server is down, the Vinca link is disconnected, or there is a conflict with another card in either machine.

Using StandbyServer

Commands

The following commands can be used on the AutoSwitch screen to clear the message window, unload AutoSwitch, or display information:

Key	Description
[Space]	Clears the message window on the AutoSwitch screen.
[Esc]	Unloads SBSENTRY.NLM and requires that the user respond by typing 'y' to the prompt to confirm exiting AutoSwitch.
h	Displays the Help messages.
p	Pauses the AutoSwitch operation. It can be resumed by pressing any key.
s	Change the Failover Delay.
i	Standby*Server* information screen.

The Connection Status

When the communication between the machines exists and the connection is running, both lines should display "CONNECTED." This means that both the Vinca link and the IPX connection are functioning.

If either connection is not functioning, one or both of these lines will display "NOT CONNECTED."

Troubleshooting a NOT CONNECTED Status

1. From the standby machine's console prompt, type `display servers` and press Enter to access the server list.

   If the primary server is not listed, the LAN drivers are not configured properly.

1. From both machine's console prompt, type `config` and press Enter to see if the LAN drivers are loaded.

2. Check the frame type used on both sides and make sure they are the same; i.e., 802.3 to 802.3.

Configuring the Throttle Feature

When a dedicated link is not used, the Throttle switches can be used to control the amount of mirroring traffic Standby*Server* sends over the client network. You can enter a maximum data rate in bits per second (bps, kbps, or Kbps) when loading the VINCAIPX.NLM to control the amount of mirroring traffic on the network. The lower the rate, the less mirroring traffic is on the client network at a given time. The affect of changing the maximum data rate can be seen when you run LinkTest.

The maximum data rate is the maximum rate that Standby*Server* sends from the machine where the switch is loaded. The throttle switches should be loaded on both machines using the same rate.

To limit mirroring traffic

1. From the standby machine's console prompt, type `load c:\standby\vincaipx t4=n[k|K]`.

2. From the primary server's console prompt, type `load c:\standby\vincaipx t4=n[k|K]`.

   Where n is the number of bits per second, and k or K act as a multiplier (k=1024 and K=1000) to n. For example, t4=500K or 500,000.

The amount of network traffic and the speed of the Vinca link make it impossible to give recommened values for this setting. You will need to experiment with it to find a setting that meets your needs.

For more details on the use of throttle switches on VINCAIPX.NLM, see "VINCAIPX.NLM" on page 111.

Using Standby Server

Using LinkTest

The LinkTest program sends test packets to the other machine in a Standby*Server* configuration to test link performance. LinkTest simulates maximum Vinca link traffic by sending test data (nothing written to disk), using as much bandwidth as it can.

When using a dedicated link (recommended) this test shows the maximum speed at which data is mirrored. When the client network is used, this test shows the impact of mirroring traffic on the main IPX line, and lets you see the effects of using the Throttle feature.

The LinkTest program must be run on both machines at the same time. You can use the following options to more accurately simulate a re-mirror.

Option	Description
send	Only sends packets, does not receive any.
receive	Only receives packets, does not send any.

To run LinkTest

1. From the standby machine's console prompt, type load c:\standby\linktest receive.
2. From the primary server's console prompt, type load c:\standby\linktest send.

Figure 4.4 LinkTest Screen

Using Standby*Server*
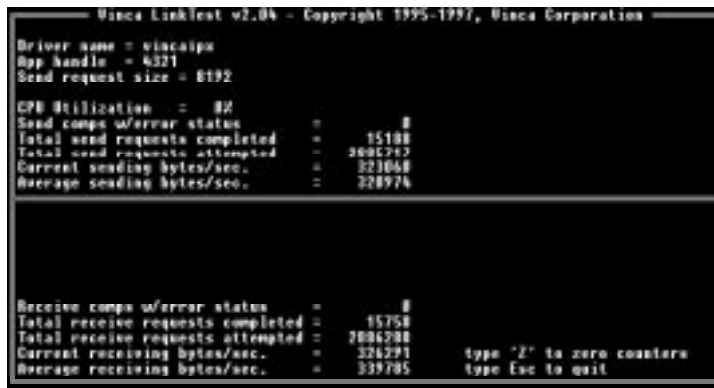
To reset the counters

- Press "z".

To quit LinkTest

- On both machines, press Esc.

Understanding Your Configuration's Performance

Running the LinkTest for a few minutes will return more accurate values. If any errors appear during the test, there is a problem with the Vinca link that needs to be repaired. Adding the Average sending bytes/sec and Average receiving bytes/sec yields the total link performance. This figure should be used to see the effects of changing the VINCAIPX Throttle switches.

Appendix A

Troubleshooting

This section covers a variety of topics from common questions and answers to troubleshooting. Up-to-date information can be obtained from Vinca's Web site at www.vinca.com.

Known NetWare Issues

The following issues can be corrected by updating NLMs.

Remirroring aborts at 99%

▼ If you are using NetWare 4.10 and the REMIRROR BLOCK SIZE is increased from the default value of 1 (4k), NetWare aborts the remirror process at 99%. Novell has two NLMs that fix this problem:

MMREMMFX.NLM
MMMIRRFX.NLM

These NLMs are contained in the file 410PT7.EXE (or newer) available from Novell Support Connection at http://support.novell.com.

Standby Machine Hangs When Using a Vinca Link

▼ If PCI cards are used for the Vinca link in a NetWare 4.10 installation, the standby machine might hang due to a NetWare 4.10 PCI memory problem when loading STANDBYH.NLM. Novell has a patch to SERVER.EXE found in the file 410PT7.EXE (or newer). See the readme file LOADER.TXT (found in 410PT7.EXE) for information on how to apply the patch.

The file 410PT7.EXE (or newer) available from Novell Support Connection at http://support.novell.com.

The Vinca Standby*Server* CD-ROM contains a NOVELL subdirectory with a number of Novell patches that were available when the product was shipped.

Common Questions, Problems, and Considerations

This section is considered a 'live document' that is constantly being updated. The information contained in the printed manual is only the most common issues that we are aware of at the time of printing. For more complete, and up-to-date information, see our Web site at www.vinca.com.

Question: What do I do when I get the following error message while trying to load SBSENTRY.NLM?

Loader cannot find public symbol: SBRestart

Reason: STANDBYH.NLM must be loaded prior to SBSENTRY.NLM.

Solution: Load STANDBYH.NLM. Then load SBSENTRY.NLM.

Question: How do I keep the standby machine from automatically becoming the server during maintenance?

Reason: The AutoSwitch function will failover the standby machine to assume the primary role when it can no longer communicate with the primary server.

Solution: When shutting down the primary, pause AutoSwitch by pressing "p" while in the AutoSwitch screen on the standby machine. This pauses the autoswitch.

Problem: Disk Devices are not Seen by Standby*Server*

If disk devices are loaded after the Standby*Server* application and are not in the Disk Device Information window, press "s" on the keyboard of the standby machine. This command forces NetWare to scan for new disk devices making them available to Standby*Server*.

If the disk devices are still not made available, go to the console prompt and dismount all volumes, then press "s" while in the Standby*Server* screen.

Problem: Drive Repeatedly Disconnects

After loading STANDBY the file server displays "drive disconnect due to drive failure" errors and cycles through these errors over and over.

Reason: There might be a a hardware interrupt conflict.

Solution: Check all interrupts in each machine to assure that they are correct and there are no conflicts.

Consideration: Using IDE Drives with Standby*Server*

Be consistent in the use of disk drivers. Use the same drivers for both primary mode and standby mode. For example, when Standby*Server* is run, the local disk driver used to access the IDE drive is IDE.DSK. When the standby machine is run as the primary, IDE.DSK should be used. Using ISADISK.DSK in one mode and IDE.DSK in the other can cause drive translation differences, meaning the NetWare partition (and data on it) will not be accessible.

Consideration: Using Drives With Different Controllers

If there will be drives that use different controllers—such as a SCSI drive and an IDE drive in the same machine—make sure to load all appropriate card drivers in the startup files for both the primary and the standby roles of the machine. For example, if the standby machine uses both types of drives, makes sure to include the correct drivers in NetWare configuration files in both the C:\STANDBY directory and the C:*netware* directory. This is a common cause of drive problems when the standby switches roles.

Consideration: Mirroring with Different Size Drives

Make sure the NetWare partition data area in the standby machine is at least as big as the partition being mirrored in the primary machine. Make the DOS partition on the standby machine smaller or decrease the size of the hot fix area to increase the NetWare partition area.

Troubleshooting

Unmirroring/Remirroring Scenarios

Sometimes problems occur in mirroring through the use of improper mirroring methods. These scenarios define some typical mistakes that occur during unmirroring and remirroring NetWare disk devices. All three mistakes stem from the same situation. If one of these scenarios arises, use the instructions in "Repairing a Broken Mirror" on page 53.

Note: If the directions outlined in Chapter 2, *Mirroring* were followed, these problems should not arise.

To Avoid Unmirroring/Remirroring Problems

▼   Follow the proper procedure for installing and uninstalling the mirror.

▼   When deleting a mirrored partition, finish the process by pressing F3 from the Partition Mirroring Status menu in the NetWare Install menu. Doing so avoids all problems listed in this section.

▼   When pressing F3 decide whether to retain the volume(s) on the partition being unmirrored. When unsure, salvage the volumes, but rename them. This allows access to the volumes later to determine if they have valid data.

▼   If a drive is not available when it should be, check to see if it is "Out Of Sync" in the Mirrored NetWare Partitions menu.

▼   If caught in one of these scenarios, always remove part of the mirrored set (unload the driver) so good volumes are not accidentally deleted. This is very important because once a volume is deleted the only way to restore it is from a backup.

Scenario Assumptions

Assume there are two duplexed disk devices and one of those disk devices needs to be physically removed from the mirrored set, such as is necessary when upgrading disk devices, adding disk devices, or replacing failed components.

Assume there are only two disk drivers loaded: IDE and SCSI, in that order. The corresponding controllers have only one disk device attached. Each disk device contains a NetWare partition, and volume SYS: which is the only volume defined on the system. The data on volume SYS: is duplicated on each disk device.

Although this example deals with volume SYS:, the discussion also applies to any other volumes that might be mirrored.

The SCSI drive is to be replaced. First, unmirror the drives, go into INSTALL, select Disk Options from Installation Options, and then select Mirroring from Available Disk Options.

From Partition Mirroring Status, press Enter to display Mirrored NetWare Partitions to see the individual physical disk devices. Select the second physical disk device and

press Delete. The disk device entry is then removed from that particular window, while the other disk device is still displayed as being "In Sync."

When coming back out to Partition Mirroring Status, it now lists the "In Sync" disk device as a "Not Mirrored" logical partition. The disk device deleted is listed as an "Out Of Sync" partition.

Figure A.1 Partition Mirroring Status "Out of Sync"
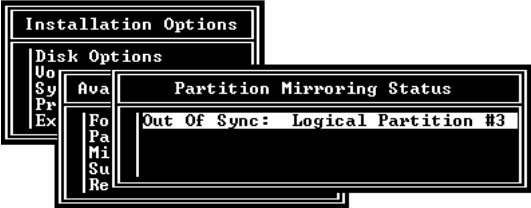
The reason the disk device deleted is considered out of sync is because it was once a member of a mirrored set, and it still contains system fault tolerance (SFT) information. As a precautionary feature, NetWare does not delete the drive's data when it is removed from the mirrored set. Manually tell the operating system to remove the SFT data if the disk device will no longer be used as part of the mirrored set.

When an "Out Of Sync" disk device is present in the system, be careful, especially when remounting the volume.

Scenario 1—Single Disk Device Out of Sync

The following scenario is specific to NetWare 3.12, but the principles are applicable to NetWare 3.12, 4.1x, and IntranetWare as well. Because NetWare 3.12 requires more manual intervention, this example shows more clearly what actually happens under these circumstances, and what is done to recover.

For this scenario, assume that INSTALL is showing the first disk device (SCSI) as "Not Mirrored" and the second disk device (IDE) as "Out Of Sync." Bring down the server, turn it off, and remove the SCSI disk device and controller. So that users can continue working while the replacement disk device is obtained, bring the server back up and load only the IDE driver. What was once the second disk device is now the only disk device in the system.

The problem is that this disk device is still "Out Of Sync" because it hasn't been modified to indicate that it's now the only disk device. Without realizing this, you type the MOUNT SYS command at the console. The console displays the following message:

Figure A.2 "No Accessible Disk Drives" Console Message


```
:mount sys
There are no accessible disk drives with NetWare partitions
Check to see that the needed disk drivers have been loaded, and that
your disk drives are properly connected and powered on.
:_
```

For most people, the first reaction to this message is, "Wait a minute, all I did was unmirror the disk devices. There is still one good disk device in there with a NetWare partition on it." The next impulse might be to go into INSTALL and check under Volume Options to see if volume SYS: is still there. When pressing Enter, the Volumes window appears but no volumes are listed.

To resyncronize a single disk device

1. Go back to INSTALL's Mirroring option, which is under Disk Options in the Installation Options menu. Check for a disk device listed as "Out Of Sync" in the Partition Mirroring Status window (Figure A.3).

Figure A.3 Partition Mirroring Status Window
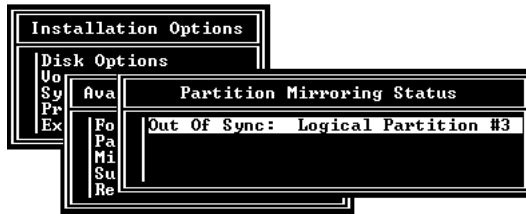
2. Select a partition and press Enter to view/modify the associated mirror set. Press F3 to restore an "Out Of Sync" partition. Press Escape to return to the previous menu.

   The message about no accessible disk drives is only a warning message, but it doesn't indicate what's really happening. Remember that when a disk device's status is "Out Of Sync," the operating system can no longer recognize volume information on that disk device.

   The operating system is trying to say that it checked for a disk device that might have a copy of volume SYS: on it to mount, but couldn't find one.

Figure A.4 Available Disk Drives Window

```
┌─────────────────────────┐
│ Installation Options    │
├─────────────────────────┴──┐
│ Disk Options               │
│ Vo┌───────────────────────────┐
│ Sy│ Available Disk Options    │
│ Pr│                           │
│ Ex│ F┌──────────────────────────────────────────────────────────┐
│   │ P│             Available Disk Drives                         │
│   │ M├──────────────────────────────────────────────────────────┤
│   │ S│▲ Device #  2 CONNER   CFP1060S 1.05GB 1823 <9C000006>     │
│   │ R│  Device #  3 MICROP   4110-09TBCU0322J HT01 <B1000100>    │
│      │  Device #  4 MICROP   4110-09TBCU0322J HT01 <B1000200>    │
│      │  Device #  5 WDC AC2420F                    <B1000300>    │
```
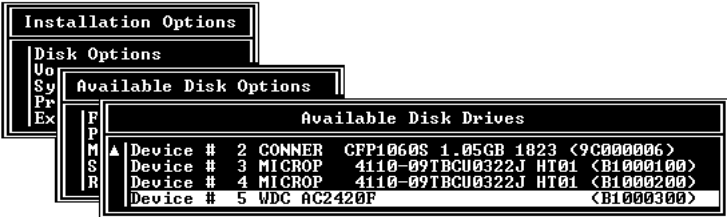
3. The help text at the bottom of the Install screen says to press F3 to restore an "Out Of Sync" partition. With the "Out Of Sync" disk device selected, press F3. Again, the message saying, "There are no accessible disk drives with NetWare partitions" appears. As indicated in the message, press Escape to continue.

4. NetWare asks whether to salvage volume SYS: segment 0.

    If the volume should remain SYS: and retain its data, answer Yes to this prompt. The operating system then modifies the drive's tables to indicate that this is a stand-alone drive; it is no longer part of a mirrored set; and it contains volume SYS: data. The disk device is then listed in the Partition Mirroring Status window as a "Not Mirrored" disk device.

Caution!   An answer of No to this prompt is in essence saying, "No, I don't want this disk device to be a member of a mirrored set. I don't care about the volume and I don't want to salvage its data." The operating system then proceeds to delete the entire volume definition table, leaving a "raw" NetWare partition containing no volume and no data.

Troubleshooting

Scenario 2—Two In Sync Disk Devices with Same Volume Name

The second scenario continues from where Scenario 1 left off. With the SCSI drive still gone, the other disk device is now back into sync with itself. It is now a stand-alone drive containing volume SYS:. In the meantime, it turns out that there was really nothing wrong with the first drive after all—it was a cable problem. Bring the server down again, turn it off, replace the cable, reinstall the SCSI controller and disk device, and power up the server, loading both IDE and SCSI drivers.

Without realizing it, two separate disk devices that both have the same volume name but have different table information have been introduced.

Going into INSTALL and selecting Mirroring shows two disk devices that are "Not Mirrored." Everything seems fine there, so the MOUNT SYS command is entered at the system console to get the server back up in a hurry. The console now displays a series of warning messages:

Figure A.5 Volume Segment Has Multiple Definitions Message
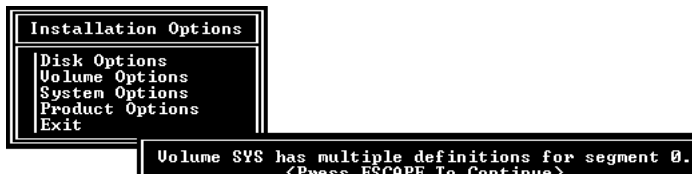
The numbers in the second message could be different depending on the size of the volume. The third message is a warning message; even though it says the definition has been removed, it hasn't yet. These messages are saying that there are two disk devices that have the same volume name, and the operating system can't determine which one contains the valid volume segment.

Again, the first impulse for most people is to go back into INSTALL and check the volume options because SYS: was there before the server was downed. At that point, these same messages start displaying one by one in the middle of the screen. This time, press Escape after each one.
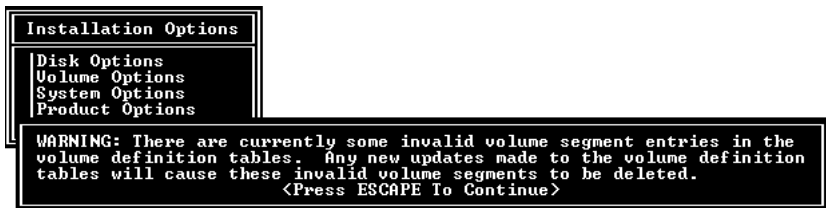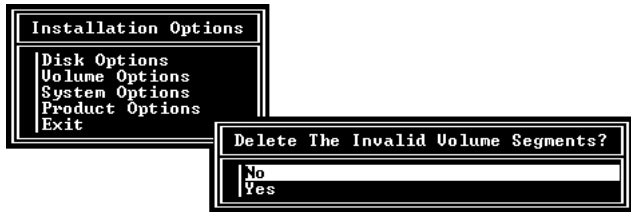
Figure A.6 NetWare Install Utility Error Messages

```
┌─────────────────────┐
│ Installation Options │
├─────────────────────┤
│ Disk Options        │
│ Volume Options      │
│ System Options      │
│ Product Options     │
│ Exit                │
└─────────────────────┘
        ┌──────────────────────────────────────────────────────┐
        │ Volume SYS has multiple definitions for segment 0.   │
        │              <Press ESCAPE To Continue>              │
        └──────────────────────────────────────────────────────┘
```

```
┌─────────────────────┐
│ Installation Options │
├─────────────────────┤
│ Disk Options        │
│ Volume Options      │
│ System Options      │
│ Product Options     │
│ Exit                │
└─────────────────────┘
┌────────────────────────────────────────────────────────────────────┐
│ Volume SYS segment 0 ends at block 6999, and segment 0 starts at block 0. │
│                    <Press ESCAPE To Continue>                      │
└────────────────────────────────────────────────────────────────────┘
```

```
┌─────────────────────┐
│ Installation Options │
├─────────────────────┤
│ Disk Options        │
│ Volume Options      │
│ System Options      │
│ Product Options     │
│ Exit                │
└─────────────────────┘
        ┌──────────────────────────────────────────────┐
        │ Definition for sync 0 of volume SYS removed. │
        │          <Press ESCAPE To Continue>          │
        └──────────────────────────────────────────────┘
```

```
┌─────────────────────┐
│ Installation Options │
├─────────────────────┤
│ Disk Options        │
│ Volume Options      │
│ System Options      │
│ Product Options     │
│ Exit                │
└─────────────────────┘
        ┌──────────────────────────────────────────┐
        │ Definition for volume SYS is invalid.    │
        │        <Press ESCAPE To Continue>        │
        └──────────────────────────────────────────┘
```

After going through this string of error messages, a box appears that says:

Figure A.7 Invalid Volume Segment Entries Error Message

```
┌─────────────────────┐
│ Installation Options │
├─────────────────────┤
│ Disk Options        │
│ Volume Options      │
│ System Options      │
│ Product Options     │
├──────────────────────────────────────────────────────────────────────┤
│ WARNING: There are currently some invalid volume segment entries in the │
│ volume definition tables.  Any new updates made to the volume definition │
│ tables will cause these invalid volume segments to be deleted.          │
│                    <Press ESCAPE To Continue>                          │
└──────────────────────────────────────────────────────────────────────┘
```

Press Escape; the following prompt appears (Figure A.8):

Troubleshooting

Figure A.8 Delete Invalid Volume Segment Prompt


```
┌──────────────────────┐
║ Installation Options ║
╠══════════════════════╣
║ Disk Options         ║
║ Volume Options       ║
║ System Options       ║
║ Product Options      ║┌─────────────────────────────────┐
║ Exit                 ║║ Delete The Invalid Volume Segments? ║
└──────────────────────┘╠═════════════════════════════════╣
                         ║ No                              ║
                         ║ Yes                             ║
                         └─────────────────────────────────┘
```

Caution!   If Yes is chosen, the operating system deletes the invalid volume segments. But since it can't determine which of the disk devices had the correct (valid) volume segment, it deletes all of the volume definition tables on every disk device associated with the error. The volume must be rebuilt from scratch pulling all data from a backup. Because this deletes all the volume segments from all drives, when these messages appear, go to the console prompt and unload the disk drivers from all but one part of the mirrored set. Taking this precaution will ensure a volume segment is not accidentally deleted from the wrong disk device (which is very easy to do in this situation).

To rename one of the disk devices

1. Answer No to the above mentioned prompt.

    Caution!   Pressing Escape instead of selecting No and pressing Enter deletes all the volume segments on all associated disk devices. This means the loss of all data stored on every disk device associated with the mirror.

2. Everything up to this point has been a series of warning messages. When answering No, nothing is deleted. Determine which disk device has the most current data on it. If necessary, switch to the console prompt, unload both disk drivers, and load them one at a time to try to decipher which disk device contains the most recent volume SYS: data.

3. Unload the most current device driver, load the other driver, delete the volume, and reload the driver. Then start the remirror process as described in "Mirroring in NetWare 3.12" on page 45 or "Mirroring in NetWare 4.1x and IntranetWare" on page 49.

    Note: Make sure to mount the volumes separately to determine which one is the most current. Delete the volume that has old data to ensure that old data is not accidentally mirrored over the top of newer data. For more information, see "Repairing a Broken Mirror" on page 53.

Scenario 3—One Disk Device In Sync and One Out of Sync

Return to the original unmirroring situation. There are two disk devices: one listed as "Not Mirrored" and the other listed as "Out Of Sync." At this point no device drivers have been unloaded. Both IDE and SCSI drivers and associated hardware are present.

To get an "Out Of Sync" disk device back in sync with itself, just select it in the Partition Mirroring Status window and press F3 (as explained in Scenario 1). When there are multiple disk devices the tables are modified, NetWare does not modify the tables on disk devices that contain the same volume.

When F3 is pressed on the out of sync disk device, a message similar to the following is displayed:

Figure A.9 Volume Already Defined Warning Message
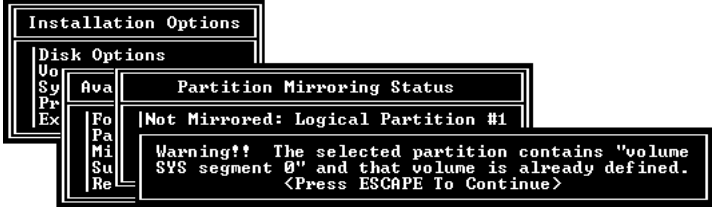
When Escape is pressed, a prompt appears that asks whether to rename the volume segment.

To resyncronize the disk device

1. To keep the volume's data intact, choose Yes and rename the volume segment. If No is chosen, there will be two volume segments with the same name, but different disk device information. The only way to recover from this problem is to restore volume SYS: from a backup.

2. After renaming the volume segment, another prompt appears:

Figure A.10 Salvage Volume Segment Prompt
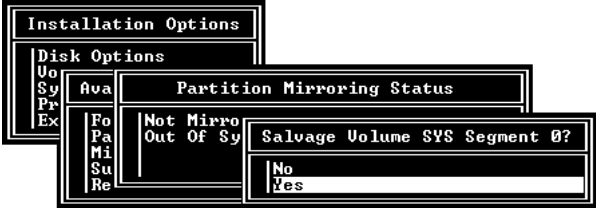
3. Choose Yes to salvage the volume.

4. Now there should be two separate disk devices with the same data but with different volume names. Determine which volume is the most current, delete the other volume, and remirror the disk devices.

Or

1. Choose No to both prompts. Before doing so, make sure that one of the disk devices is still in sync and contains the needed data.

2. Install updates the Partition Mirroring Status window so that the disk device is displayed as "Not Mirrored."

   The operating system has deleted the volume definition table. This is because choosing No above says, in essence, not to rename the volume and not to keep the data. It is now possible to remirror the partitions.

   Note: Vinca recommends renaming the volume segment unless absolutely sure there is a good volume segment on another disk device. We also recommend going to the console prompt and unloading the disk driver for the disk device with the good volume segment, just to make sure it isn't accidentally deleted.

Appendix B
Sample Files

This appendix contains sample file listings for the C:\STANDBY and C:*netware* directories for both the primary server and the standby machine. In all cases, if you are using Entry-Level, the "standbyh" is replaced by "standbye".

For purposes of these samples, C:*netware* is used as the NetWare directory where the the NetWare files are located. This directory is typically called C:\SERVER.312 for NetWare 3.12 installations, and C:\NWSERVER for NetWare 4.1x installations.

C:\STANDBY is the directory where the Standby*Server* files and the standby version of NetWare are stored. While this directory can be called anything, use this name for the Standby*Server* directory regardless of the version of NetWare or any other factors.

You will need to substitute the actual path to load the files such as LAN or disk drivers that can be stored anywhere on the DOS partition. There is no need to copy these types of files to the C:*netware* or C:\STANDBY directories if they already exist somewhere on the disk.

With the additional functionality of multiple standby machines, there are additional lines added by the VINSTALL utility to the standard configuration (one primary server and one standby machine). Because you can install multiple standby machines, an App number is assigned to each standby machine in the order they are installed. For example, the first standby machine is assigned the App number 1 (app=1). Additional standby machines are assigned App number 2, 3, and so on. You will notice in the following pages that the app=1 tag is on the standbyh and sbsh load lines.

The load lines added when a second standby machine is added to your configuration is documented at the end of this appendix on page 104.

Installation Notes

▼   Make sure the *.LAN and *.DSK drivers for the LAN card and the disk devices are properly installed on the DOS partition and accessible to Standby*Server*. Verify that the drivers are intended for the appropriate version of NetWare.

▼   Use the most recent versions of Streams and CLIB for the version of NetWare you are using. The most recent versions are available from Novell.

▼   (NetWare 3.12 only) Check the AUTOEXEC.NCF files in the C:\ *netware* directory on the standby machine(s) to ensure there are no "MOUNT volname" commands in the file. VINSTALL automatically inserts a "VMOUNT" command that can conflict with the "MOUNT volname" statement. Use "VMOUNT volname" to mount each volume.

▼   (Utility Server only) Only the standby machines can function as a Utility Server. This feature is available as long as the standby machines are in the standby role. Although you can start the primary server in the standby role, it cannot function as a Utility Server. Additionally, if you have more than one standby machine, all mirroring to the vault machine(s) is disabled when the primary server is not acting in the primary role. For these reasons, if you are using the Utility Server feature on any standby machine, you should return the primary server to the primary role as soon as you can to completely reestablish the full functionality of your configuration.

▼   (Utility Server only) When establishing the mirror make sure not to mirror to the additional disk device installed in the standby machine; this disk is reserved for utility server use and should not be part of a mirrored set.

Note: Make sure to use SnapShot*Server* 1.21 or newer with this version of Standby*Server*. Earlier versions of SnapShot*Server* will not function correctly.

NetWare 3.12 (Non-dedicated Vinca Link, Non-Utility Server)

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry

STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx
  load c:\standby\sbsh app=1
  mount all
  load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry

STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312 (Failover Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load vmount sys vol1
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx
  load c:\standby\sbsh app=1
  unload retyes
  load apps used after failover here
```

NetWare 3.12 Dedicated Vinca Link (non-Utility Server)

Dedicated Vinca link related entries are bolded.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123,vlink
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry

STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
  load c:\standby\vincaipx
  load c:\standby\sbsh app=1
  mount all
  load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123,vlink
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry

STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312 (Failover Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load vmount sys vol1
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
  load c:\standby\vincaipx
  load c:\standby\sbsh app=1
  unload retyes
  load apps used after failover here
```

NetWare 3.12 Dedicated Vinca Link and Utility Server

Dedicated Vinca link related entries are bolded. Utility Server related entries are bolded and italicized.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123,vlink
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry




STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
  load c:\standby\sbsh app=1
  mount all
  load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name STANDBY
  IPX Internal Net abc
  search add c:\server.312
  load ide port=1f0 int=e
  load c:\standby\sysswap standby util_sys
  mount SYS
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123,vlink
  load c:\standby\standbyh utility app=1
  load c:\standby\sbsentry

STANDBY.BAT
  autosbs -s C:\SERVER.312
```

C:\SERVER.312 (Failover Directory)

```
STARTUP.NCF
  Set Enable Disk Read After Write
Verify=OFF
  Set Concurrent Remirror Requests=30
  load c:\standby\pm312
  load c:\standby\elevfix
  load c:\standby\mmhandfx.312

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  load ide port=1f0 int=e
  load c:\standby\sysswap primary
  load vmount sys vol1
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
  load c:\standby\vincaipx
  load c:\standby\sbsh app=1
  unload retyes
  load apps used after failover here
```

NetWare 4.10 (Non-dedicated Vinca Link, Non-Utility Server)

Primary Server

C:\STANDBY (Recovery Directory)

STARTUP.NCF
```
  Set Automatically Repair Bad Volumes=ON
  Set AutoTTS Backout Flag=ON
  Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF
```
  File Server Name STANDBY
  IPX Internal Net abc
  Search Add c:\nwserver
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry
```

STANDBY.BAT
```
  autosbs -s C:\NWSERVER
```

C:\NWSERVER

STARTUP.NCF
```
  Set Automatically Repair Bad Volumes=ON
  Set AutoTTS Backout Flag=ON
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm410
  load c:\standby\mmhandfx.410
```

AUTOEXEC.NCF
```
  File Server Name SALES
  IPX Internal Net 123
  Set Concurrent Remirror Requests=30
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vincacom
  load c:\standby\vincaipx
  load c:\standby\vncdown
  load c:\standby\sbsh app=1
  mount all
  load apps here
```

Standby Machine

C:\STANDBY

STARTUP.NCF
```
  Set Automatically Repair Bad Volumes=ON
  Set AutoTTS Backout Flag=ON
  Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF
```
  File Server Name STANDBY
  IPX Internal Net abc
  Search Add c:\nwserver
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123
  load c:\standby\standbyh app=1
  load c:\standby\sbsentry
```

STANDBY.BAT
```
  autosbs -s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

STARTUP.NCF
```
  Set Automatically Repair Bad Volumes=ON
  Set AutoTTS Backout Flag=ON
  Set Enable Disk Read After Write
Verify=OFF
  load c:\standby\pm410
  load c:\standby\mmhandfx.410
```

AUTOEXEC.NCF
```
  File Server Name SALES
  IPX Internal Net 123
  Set Concurrent Remirror Requests=30
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  mount all
  load c:\standby\vincacom
  load c:\standby\vincaipx
  load c:\standby\vncdown
  load c:\standby\sbsh app=1
  unload retyesfordreamed
  load apps used after failover here
```

NetWare 4.10 Dedicated Vinca Link (non-Utility Server)

Dedicated Vinca link related entries are bolded.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs –s C:\NWSERVER
```

C:\NWSERVER

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
   load c:\standby\pm410
   load c:\standby\mmhandfx.410

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\vncdown
   load c:\standby\sbsh app=1
   mount all
   load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs –s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
   load c:\standby\pm410
   load c:\standby\mmhandfx.410

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   mount all
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abcvlink
   load c:\standby\vncdown
   load c:\standby\sbsh app=1
   unload retyes
   load apps used after failover here
```

NetWare 4.10 Dedicated Vinca Link and Utility Server

Dedicated Vinca link related entries are bolded. Utility Server related entries are bolded and italicized.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
   load c:\standby\pm410
   load c:\standby\mmhandfx.410

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\vncdown
   load c:\standby\sbsh
   mount all
   load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load c:\standby\sysswap util_sys
   mount SYS
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh utility app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

```
STARTUP.NCF
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
   load c:\standby\pm410
   load c:\standby\mmhandfx.410

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load c:\standby\sysswap primary
   mount sys
   mount other volumes here
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abd,vlink
   load c:\standby\vncdown
   load c:\standby\sbsh app=1
   unload retyes
   load apps used after failover here
```

NetWare 4.11 and IntranetWare (Non-dedicated Vinca Link, Non-Utility Server)

Primary Server

C:\STANDBY

STARTUP.NCF

```
   Set AutoRestart After Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF

```
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry
```

STANDBY.BAT

```
   autosbs -s C:\NWSERVER
```

C:\NWSERVER

STARTUP.NCF

```
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF

```
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load c:\standby\vincacom
   load c:\standby\vincaipx
   load c:\standby\vncdown
   load c:\standby\sbsh app=1
   mount all
   load apps here
```

Standby Machine

C:\STANDBY

STARTUP.NCF

```
   Set AutoRestart After Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF

```
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry
```

STANDBY.BAT

```
   autosbs -s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

STARTUP.NCF

```
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF
```

AUTOEXEC.NCF

```
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load c:\standby\vncdown
   load c:\standby\vincacom
   load c:\standby\vincaipx
   load c:\standby\sbsh app=1
   unload retyes
   load apps used after failover here
```

NetWare 4.11 and IntranetWare Dedicated Vinca link (non-Utility Server)

Dedicated Vinca link related entries are bolded.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vncdown
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\sbsh app=1
   mount all
   load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry

STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   mount all
   load c:\standby\vncdown
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\sbsh app=1
   unload retyes
   load apps used after failover here
```

NetWare 4.11 and IntranetWare Dedicated Vinca Link and Utility Server

Dedicated Vinca link related entries are bolded. Utility Server related entries are bolded and italicized.

Primary Server

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh app=1
   load c:\standby\sbsentry


STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vncdown
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\sbsh app=1
   mount all
   load apps here
```

Standby Machine

C:\STANDBY

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name STANDBY
   IPX Internal Net abc
   Search Add c:\nwserver
   load ide port=1f0 int=e
   load c:\standby\sysswap util_sys
   mount SYS
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vincacom
   load c:\standby\vincaipx master=123,vlink
   load c:\standby\standbyh utility app=1
   load c:\standby\sbsentry


STANDBY.BAT
   autosbs -s C:\NWSERVER
```

C:\NWSERVER (Failover Directory)

```
STARTUP.NCF
   Set AutoRestart after Abend=0
   Set Enable IO Handicap Attribute=ON
   Set Automatically Repair Bad Volumes=ON
   Set AutoTTS Backout Flag=ON
   Set Enable Disk Read After Write
Verify=OFF

AUTOEXEC.NCF
   File Server Name SALES
   IPX Internal Net 123
   Set Concurrent Remirror Requests=30
   load ide port=1f0 int=e
   load c:\standby\sysswap primary
   mount sys
   mount other volumes here
   load 3c509 port=300 int=3
   bind ipx to 3c509 net=ace
   load e100b slot=10 name=vlink
   bind ipx to vlink net=face
   load c:\standby\vncdown
   load c:\standby\vincacom
   load c:\standby\vincaipx slave=abc,vlink
   load c:\standby\sbsh app=1
   unload retyes
```

Multiple Standby Machines

This page contains the additional load lines contained in the .NCF files added by the VINSTALL program when an additional standby machine is added. If you added a third standby machine to your configuration, these same lines would be added using "app=3" for the App number.

Notice in the C:\STANDBY\AUTOEXEC.NCF file on the standby machine there is no sbsentry load line. This is because additional standby machines do not automatically failover and assume the primary role.

The following load lines were taken from the NetWare 4.11 Dedicated Vinca Link and Utility Server example from the previous page. The lines added/changed for the vault machine, are indicated with an asterisk.

Primary Server

Vault Machine

C:\STANDBY (Recovery Directory)

```
STARTUP.NCF SAME


AUTOEXEC.NCF SAME
```

C:\STANDBY

```
STARTUP.NCF SAME

AUTOEXEC.NCF
* File Server Name VAULT
* IPX Internal Net def
  Search Add c:\nwserver
  load ide port=1f0 int=e
  load c:\standby\sysswap util_sys
  mount SYS
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
  load c:\standby\vincacom
  load c:\standby\vincaipx master=123,vlink

* load c:\standby\standbyh utility app=2
```

```
STANDBY.BAT SAME
```

C:\NWSERVER

```
STARTUP.NCF SAME

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  Set Concurrent Remirror Requests=30
  load ide port=1f0 int=e
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
* load and bind the 2nd dedicated link here
  if using an additional LAN card
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
* load c:\standby\vincaipx slave=def,vlink
  load c:\standby\sbsh app=1
* load c:\standby\sbsh app=2 block
  mount all
  load apps here
```

```
STANDBY.BAT
  autosbs -s C:\NWSERVER
```

C:*netware* (Failover Directory)

```
STARTUP.NCF SAME

AUTOEXEC.NCF
  File Server Name SALES
  IPX Internal Net 123
  Set Concurrent Remirror Requests=30
  load ide port=1f0 int=e
  load c:\standby\sysswap primary
  mount sys
  mount other volumes here
  load 3c509 port=300 int=3
  bind ipx to 3c509 net=ace
  load e100b slot=10 name=vlink
  bind ipx to vlink net=face
* load and bind the dedicated link here
  load c:\standby\vncdown
  load c:\standby\vincacom
  load c:\standby\vincaipx slave=abc,vlink
* load c:\standby\sbsh app=2
  unload retyes
  load apps used after failover here
```

Appendix C
File Reference

Standby*Server*'s main files are listed below with a brief description, and discussed individually with their command line options or switches later in the chapter. For more information about the contents of NetWare configuration files see Appendix B, *Sample Files* of this guide or your NetWare documentation.

File	Description
STANDBYH.NLM	NLM that runs on the standby machine to exports the local disk devices to a primary server running the SBSH driver. STANDBYH.NLM is a slave to SBSH.DSK.
SBSH.DSK	NLM that runs on the primary server allowing it to control drives exported from the standby machine.
VINCACOM.NLM	NLM that runs on both machines to facilitate communication between the various components of the Standby*Server* system.
VINCAIPX.NLM	NLM that runs on both machines to control mirroring traffic over a standard IPX network and LAN cards.
VNCDOWN.NLM	NLM that runs on the primary to ensure all volumes are dismounted before IPX gets unloaded during a server downing.
MMHANDFX.312, MMHANDFX.410	NLM that runs on both machines to permit read blocking over the Vinca link on NetWare 3.12 and 4.10 versions. This patch is not required on newer versions of NetWare.
AUTOSBS.EXE	DOS executable that determines whether to initiate a failover.
LINKTEST.NLM	NLM that tests the Vinca link's performance and displays the test results to the screen. See "Using LinkTest" on page 78 for more information.

File (cont.)	Description (cont.)
STANDBY.BAT	DOS batch file used to recover failed primary server.
SBSENTRY.NLM	NLM that runs on the standby machine to monitor the primary server and initiate the failover process. See "Using the AutoSwitch Feature" on page 72 for more information.
SBWARN.DSK	NLM that auto-loaded by AUTOSBS.EXE to display a message on the server's console, and broadcast a message to connected workstations alerting users of a failover.
STANDBY.BAT	DOS batch file that starts the Runtime NetWare with the proper startup files to initiate Standby*Server*.
PM312.NLM	Patch manager for NetWare 3.12.
RETYES.NLM	NLM that allows NetWare 3.12 or later to boot without user intervention after a primary server crash.
README.TXT	Important information about Standby*Server* that might not have made it into this guide.
VMOUNT.NLM	NLM that automatically repairs NetWare 3.x volumes. See README.TXT for more information on this file.
VCOPY.NLM	NLM that gives NetWare servers access to the DOS drives on each server. Used to facilitate installation. See Appendix D, *Using VCopy* for more information.
VINSTALL.NLM	NLM that installs and uninstalls Standby*Server* and allows users to edit NetWare configuration files.
VALIDATE.NLM	NLM used to validate Standby*Server*.

AUTOSBS.EXE

AUTOSBS.EXE determines if the AutoSwitch process is to be initiated. If so, it will change to the server directory and run SERVER.EXE. This file is started from STANDBY.BAT.

The following options are case sensitive:

Options	Description
–?	Display help menu.
–B	Runs a DOS batch file "AS.BAT" during an autoswitch, before running SERVER.EXE.
–f	Check DOS file for AutoSwitch flag if problems occur using the default CMOS on the motherboard.
–h	Display help menu.
–n	For servers that have removed DOS—checks AutoSwitch flag and switch of set when program is first run, such as after a reboot.
–s dir	(Required) Directory where the primary SERVER.EXE is located.
–w file	Warning file to be displayed on server console screen in case of a failover. Use the file AUTOSW.TXT as the default text file.

Sample

This is a sample command line for this file. Remember that command line switches are case sensitive.

```
autosbs –s c:\server.312 –w autosw.txt
```

This changes to C:\SERVER.312 when the flag is set to true to run SERVER.EXE, and displays the contents of the file AUTOSW.TXT on the NetWare 3.12 server console after a failover.

File Referance

SBSH.DSK

SBSH.DSK allows the primary server to control drives exported from the standby machine using STANDBYH.NLM in a Standby*Server* installation. This driver is loaded from AUTOEXEC.NCF in the directory from which the primary version of NetWare runs. The number in the file name refers to the version of NetWare running on the primary server. The following options are case sensitive:.

Options	Description
app=n	Specifies application handle to be used. The same application handle must also be specified on the instance of STANDBYH that connects to this primary.
block	Enables the read blocker for disk devices in the standby machine.
buffers=n	Specifies the number of buffers (concurrent requests) allowed on the Vinca link. n is a value between 1 and 30. Use higher values when the Vinca link is serviced by a dedicated network (30, by default).
debug	Enables debug mode.
name=x	Specifies the name of the link driver to use.
nodelete	Ensures disk devices are not deleted when the IPX link fails. If the IPX link fails, the disk devices are simply deactivated.
retry=n	Sets the number of retries on each request before the request fails. Recommended values for n are between 0 and 3 (3, by default).
timeout=n	Specifies the number seconds before requests time out. Default=15.
verbose	Displays extra information to the server console when SBSH is run. Used to aid troubleshooting.
syncclocks	Synchronizes the standby machine's clock with the primary server's clock. This option should not be used in a NetWare 4.1x Utility Server configuration. In these configurations, the clocks are already synchronized via NDS.
waitforsync=n	Where n is the number of seconds to wait for IPX synchronization before mounting volumes.

Sample

This is a sample command line for this file.

```
load c:\standby\sbsh.dsk block buffers=4
```

This loads the Vinca disk driver and specifies that reads to the standby should be blocked and that the maximum number of buffers used for the link is 4.

STANDBYH.NLM

STANDBYH.NLM exports the disk devices from the standby machine so the primary server can mirror data to them over the Vinca link using the SBSH disk driver. This file is started from the AUTOEXEC.NCF file used to start the standby machine.

Options	Description
app=n	Specifies the application handle to be used. The same application handle must also be specified on the SBSH.DSK that connects to this primary server.
debug	Enables debug mode.
name=x	Specifies the name of the link driver to use if more than one is available.
net=n	Input IPX Internal Net number of the primary server if it doesn't connect automatically.
query	Uses NetWare's Query Services instead of Vinca's.
timeout=n	Sets the number of seconds without any I/O from SBSH.DSK before STANDBYH.NLM initiates a failover (40, by default). **Note:** The timeout value must be increased to at least the number of seconds it takes to mount the largest volume on the primary server if SNAPSHOT.NLM is in use
verbose	Displays extra information to the server console when STANDBYH is run. Used to aid troubleshooting.

Sample

The following sample loads the Standby*Server* application and enables the AutoSwitch feature for the PS410 (app 2) primary server.

```
LOAD C:\STANDBY\STANDBYH app=2 autoswitch switchdir=C:\PS410
```

SYNCMFIX.NLM (NetWare 3.12)

SYNCMFIX.NLM not included on the Vinca disks, but is commonly used.

One drive off of one HBA is mirrored to two drives, both of which are on the other HBA (a total of three drives mirroring the same data). The single drive off of the first HBA is in sync with the other two drives off of the second HBA are mirrored to the first drive. The server is downed while the two secondary mirrored drives are still out of sync (the Install NLM shows them still to be in the mirroring process).

When SERVER.EXE is invoked, INSTALL.NLM shows the primary drive as In Sync, one of the secondary drives as In Sync, and the other secondary drive as Out of Sync. The two secondary drives are the only ones showing disk activity as if they are mirroring each other and ignoring the actual In Sync primary drive.

This file is started from STARTUP.NCF on systems running NetWare 3.12; this bug was fixed for NetWare 4.x.

VINCAIPX.NLM

VINCAIPX works with VINCACOM.NLM to facilitate mirroring over a standard IPX network. This file is started from the AUTOEXEC.NCF file on both machines from the STANDYBY directory.

Options	Description
checksum	Enables a checksum of the data in each packet. Used to trouble-shoot problem links. Normally disabled.
master=net[,l]	Used on the standby machine, this option targets the Vinca link communications to a specific machine. net is the internal net number of the primary server. l is the name (or logical name assigned when loaded) of the LAN driver when used with a dedicated Vinca link
maxwin=n	Sets the maximum number of packets in each burst, where n is a number less than or equal to 128.
minwin=n	Sets the minimum number of packets in a burst, where n is greater than or equal to 1 and less than the maximum value.
name=x	Specifies the name to register the link driver (vincaipx, by default)
nounbind	Disables the automatic unbinding of IPX from a failed, dedicated Vinca link.
packetsize=n	Sets the size (in bytes) of data in each packet. The value of n depends on the type of LAN card used to service the link. The minimum is 512. Normally the size will be automatically negotiated when the link is established.
slave=net,l	Used on the primary server, this option targets the Vinca link communications to a specific machine. Where net is the internal net number of the standby machine and l is the name (or logical name assigned when loaded) of the LAN driver when used with a dedicated Vinca link
rle	Enables run length compression.
sync=n	Sets how many sync packets can be missed before the link is considered out of sync (20, by default).

File Referance

Options (cont.)	Description (cont.)
syncdelay=n	Sets the time in milliseconds between sync packets. Default=1000
t0=n	Delay ThreadSwitch() *n* times between sending packets.
t1=n	Delay ThreadSwitchWithDelay() n times between sending packets. Takes precedence over any t0=*n* setting.
t2=n	Delays 25 ms between sending packets every nth packet. Takes precedence over any t0=*n* or t1=*n* settings.
t3=n	Delays n ms between sending each packet. Takes precedence over any other t0=*n*, t1=*n*, t2=*n* settings.
t4=n[k | K]	Uses a maximum of *n* bits of bandwidth of the Vinca link; k indicates *n* x 1024 bits; K indicates *n* x 1000 bits.
xor	Enables packet compression using XOR.

Sample

The following loads VINCAIPX on the standby machine with a shared Vinca link and targets communications to the primary server with an internal net number of 456.

```
load c:\standby\vincaipx master=456
```

Appendix D
Using VCopy

VCopy is a NetWare utility program that enables you to access both DOS and NetWare files on multiple servers from a single server. VCopy was created to facilitate the Standby*Server* installation, but can be used as a separate application.

With VCopy you can:

▼ Copy files between the local DOS drives and the local NetWare volumes on a server.

▼ Copy files between the DOS drives and/or NetWare volumes on two different servers.

▼ Perform standard file operations on all accessible files, including creating directories, setting file attributes, copying and/or deleting files, and getting directory listings.

▼ Create DOS-type batch files containing VCopy commands that execute immediately.

▼ Set a password on VCopy to provide limited access to the above features.

Using VCopy's ability to access DOS and NetWare files across servers enables you to:

▼ Archive critical files.

▼ Perform file updates across multiple servers. For example, drivers or patches.

▼ Backup local boot environments to a NetWare directory for recovery.

▼ Search directories for NLMs that need to be loaded.

How VCopy Works

VCopy functions in both a master and slave role. The master provides a user interface and controls remote slave and local file operations. The slave role allows a remote master to access its DOS and NetWare directories. Any server where Standby*Server* has been installed is already configured to run VCopy.

VCopy uses the established Vinca links, the same links that Standby*Server* uses to communicate and mirror between the standby machine the each primary server. Once a Vinca link is operational, VCopy can be run on each side of the link to gain access to the other side's DOS and NetWare directories. Standby*Server* indicates the Vinca link is operational when the Status Bar for the primary server's screen is green. Another indication is when VincaIPX displays a "VincaIPX:*date time* net (IPX internal net number of the remote machine) in sync, size (*n*)".

The default installation of Standby*Server* establishes a Vinca link from the standby machine to each primary server. In the default configuration, the standby machine has access to all of the primary servers' DOS and NetWare directories. There is no link established between any two primary servers.

The standby machine has the same app number of each of the primary servers. Each Vinca link matches the application numbers on each side of the link allowing the programs (Standby*Server*, or VCopy) loaded with those application numbers as parameters to communicate.

Loading VCopy

Because VCopy is installed with Standby*Server*, you can run VCopy from the STANDBY directory on any of the machines in your Many-to-One configuration. If you want to run VCopy on another machine, or between two primary servers, you will need to manually load it using the appropriate command line options. See "Manually Loading VCopy" on page 118.

To load VCopy

- From each machine's console prompt, type "v" and press Enter.

You can also load VCopy from the prompt by typing, load c:\standby\vcopy. However, if you load VCopy one a primary server using "v" and on another one using the load line, you run the risk of the having two servers use the default VCopy assigned app number (100). When two primary servers have the same VCopy app number, the standby machine will not be able to communicate with all of the primary servers.

How To Use the VCopy Screen

The VCopy screen displays a VCopy prompt, which acts like a DOS prompt, and a REMOTE CWD field displaying the remote directory where you are currently working. Remote commands control the directory and file manipulation on the remote machine. Typing help displays VCopy's commands as shown in Figure D.1.

If you are working on a single machine, the REMOTE CWD field displays, "VCopy not using communication link." If this message is received when you are working with two machines, the Vinca link was not established.

Figure D.1 VCopy Screen

VCopy Commands

The following VCopy commands are available to provide simple DOS-type file access, directory manipulation, and file copying. Type help followed by the command name for help on a specific command.

Local Commands	Remote Commands
drive:	*rdrive:*
vol:	*rvol:*
ren	rren
dir [/p /s]	rdir [/p]
type [/p]	rtype [/p]
attrib [/p /s]	rattrib [/p /s]
cd	rcd
md	rmd
rd	rrd
del	rdel
deltree	rdeltree
volumes (or vol)	rvolumes (or vol)

Using VCopy

Copying Commands

Because VCopy is designed to connect two servers, copying commands need to specify the source and direction of the file copy. VCopy supports both COPY and XCOPY commands with a two-letter prefix indicating the source and destination of the copy. Use "l" for local, and "r" for remote.

For example, to copy a file from a local NetWare volume to a remote DOS drive, you would use the following syntax:

```
lrcopy sys:\system\autoexec.ncf c:\nwserver\autoexec.ncf
```

The "lr" prefix for the COPY command indicates that the first path is local, and the second path is the remote. Wildcards can be used to copy multiple files or directories. For example, the following command line copies the entire contents of a local DOS drive to an archive directory on a remote server:

```
lrxcopy c:\*.* vol1:\archive
```

VCopy supports relative paths, as well. If the current local directory is C:\ and the CWD for the remote is VOL1:\ARCHIVE, the sample above could be entered as follows:

```
lrxcopy *.*
```

Here is a review of the COPY commands supported by VCopy used in a sample command line:

```
llcopy sys:\system\autoexec.ncf c:\nwserver\autoexec.ncf
```
      (or `ll`) to copy from one local directory to another local directory

```
lrcopy sys:\system\autoexec.ncf c:\nwserver\autoexec.ncf
```
      (or `lr`) to copy from a local directory to a remote directory

```
rlcopy sys:\system\autoexec.ncf c:\nwserver\autoexec.ncf
```
      (or `rl`) to copy from a remote directory to a local directory

```
rrcopy sys:\system\autoexec.ncf c:\nwserver\autoexec.ncf
```
      (or `rr`) to copy from one remote directory to another remote directory

Here is a review of the XCOPY commands supported by VCopy:

```
llxcopy c:\*.* vol1:\archive
```
      (or `llx`) to xcopy from a local directory to another local directory

```
lrxcopy c:\*.* vol1:\archive
```
      (or `lrx`) to xcopy from a local directory to a remote directory

```
rlxcopy c:\*.* vol1:\archive
```
      (or `rlx`) to xcopy from a remote directory to a local directory

```
rrxcopy c:\*.* vol1:\archive
```
      (or `rrx`) to xcopy from one remote directory to another remote directory

General Commands

These are the application commands that control how VCopy functions.

Command	Description
app n	Connects VCopy to the machine with the application number *n*.
app n add	Registers Vinca application number *n* to be accessible to VCopy. This is exactly the same as including the app=*n* switch on the command line. Use "app *n*" to connect to this application.
app n del	Unregisters Vinca application number *n* to be accessible to VCopy. VCopy will no longer recognize this application when the "app *n*" command is used.
edit filename	edit text file.
batch filename	Executes the specified batch file immediately. The file listed should contain only VCopy commands. The VCopy commands in the text file are executed in order, and the results are written to the log file.
lock	Locks the keyboard. When entered, you are prompted for a password; enter a password of up to eight digits. The keyboard will be locked until the password is entered to unlock it.
log filename	Chooses a new log *filename*, including its full path.
quit	Exits VCopy and tells the current remote VCopy to quit, as well. Press Esc and confirm to exit from the local VCopy only.
set dosdelay=n	Sets one of two types of delay used after each DOS interrupt. Use values between 0 and 1,000,000 to set a ThreadSwitchWithDelay. Use values between -1 and -500 to set a delay of *n* milliseconds.
set log=on,off	Determines whether VCopy writes results to the log file SYS:\SYSTEM\VCOPY\V$COPY.LOG. The directory must exists or this log file cannot be written. This file is created automatically when Standby*Server* is installed. The log file can be changed using the "log" command.
set timeout=n	Sets the timout value for VCopy commands. Acceptable values are from 100–1000 hundredths of a second. Default is 300.
set updateonly =on,off	Sets the copy on update only flag on or off. When set to on, copy operations only happen with files that have changed since they were last copied.

Using VCopy

Manually Loading VCopy

You can load VCopy from the Standby*Server* Installation CD-ROM, or from a local directory where you have copied the required files. VCopy requires:

File	Description
VINCACOM.NLM	Needed to establish the Vinca link (required for multiple server usage only).
VINCAIPX.NLM	Needed to establish the Vinca link (required for multiple server usage only).
VCOPY.NLM	VCopy application.

Manually Loading VCopy on a Single Server

When you run Vcopy on a single server, you don't need to establish a Vinca link so only the VCOPY.NLM is required.

To load VCopy on a single server

• From the server's console prompt, type `load path\vcopy` and press Enter.

Manually Loading VCopy On Multiple Servers

To run VCopy on multiple servers, you must load both VincaCOM and VincaIPX to establish the Vinca link before loading VCopy. As discussed in the "How VCopy Works" on page 114, loading VCopy on multiple servers requires command line parameters to be entered when loading VincaIPX and VCopy to manage the master/ slave relationship. The master of the Vinca link uses more processor cycles to establish the Vinca link than the remote slave. For this reason it is best to use the least critical machine as the master.

Loading VCopy on multiple servers where Standby*Server* has not been installed, or to run VCopy in a mixed environment where some machines run Standby*Server* and others don't, is simply a matter of loading the NLMs with the correct parameters.

The parameters used depend on the whether the Vinca link is a dedicated link, or if the client network is used. In cases where there is a dedicated link, the dedicated link's LAN card name must be entered on the VincaIPX line.

In the table below, the bold text represents the additional information that must be

Machine 1 n=abc	Machine 2 n=123
load vincacom	load vincacom
load vincaipx master=abc,**vl**	load vincaipx **slave=123,vl**
load vcopy	load vcopy

entered when using a dedicated Vinca link. Vl1 was used as the cardname on machine 1 and vl2 was used as the cardname on machine 2.

To manually load VCopy on two servers with a non-dedicated link

1. From the master's console prompt, type `load path\vincacom` and press Enter to load VincaCOM.
2. Type `load path\vincaipx master=x` and press Enter (where x is the internal net number of the target slave) to load VincaIPX.
3. Type `load path\vcopy` and press Enter to load VCopy.
4. From the slave's console prompt, type `load path\vincacom` and press Enter to load VincaCOM.
5. Type `load path\vincaipx` and press Enter to load VincaIPX.
6. Type `load path\vcopy` and press Enter to load VCopy.

To manually load VCopy on two servers with a dedicated link

Follow the steps outlined above for a non-dedicated link and add the additional parameters as shown in bold in the table above.

To manually load VCopy on three or more servers with a non-dedicated link

Follow the steps above for a non-dedicated link and add the additional parameters as shown in bold in the table below:

Machine 1 n=abc	Machine 2 n=123	Machine 3 n=456
load vincacom	load vincacom	load vincacom
load vincaipx **master=123 master=456**	load vincaipx	load vincaipx
load vcopy **app=100 app=102**	load vcopy **app=100**	load vcopy **app=102**

Although you can load VCopy on up to 20 servers at one time, communication and file copy only works between the master and one slave at a time. When multiple servers have VCopy running, changing communications to a different slave is done with the app=n command.

Command Line Options

You can use the following commands when loading VCopy.

Command	Description
master=off	Disables the machines ability to issue VCopy commands, although the machine can still function in the slave role.
slave=off	Disables the machines ability to fulfill VCopy commands from another machine functioning in the master role.
p=password	Enables password protection for this machine. The VCopy slave only fulfills commands from a VCopy master loaded with this same password.
app=n	Assigns and registers an application number (n) for the machine with VCopy. n must be an even integer between 100 and 198. The master is loaded with all app numbers for existing slaves. For example, on the master machine the vcopy load line would include app=n1 app=n2 app=n3... This can also be done by using the "app add n" command.

Disabling the Master/Slave Relationship

VCopy lets you disable the master or slave part on a server. For example, you could disable the slave functionality on one server so that no other server running VCopy could access its DOS drives. This feature was added to provide additional security.

Because the relationships are saved to the V.CFG file when Standby*Server* is installed, you must add/remove the appropriate line in the V.CFG file for the appropriate machine, or include/exclude the appropriate parameters when loading manually.

To disable the master or slave relationship

When loading VCopy, add the command line parameter "master=off" or "slave=off" depending on which part of VCopy you want to disable.

To disable the slave relationship when manually loading VCopy on machines where Standby*Server* is not installed

• Don't load VincaIPX before loading VCopy.

Using VCopy

Appendix E
Forms

This section includes installation forms and a problem resolution worksheet. The installation forms are designed to help gather information needed to successfully install Standby*Server*. Photocopy the forms as needed to document your machine's configurations before starting the installation to ensure proper:

- ▼ paths and file names
- ▼ disk and LAN drivers
- ▼ proper version numbers
- ▼ directory names

The problem resolution worksheet is designed to ease support in case you need to contact Vinca for assistance. Complete a problem descriptions and obtain the contents of the listed files before contacting Vinca to make sure you have all the information needed to troubleshoot the problem. This can reduce problem resolution time significantly.

VINSTALL also includes the option to create a Standby*Server* configuration file that contains your systems configuration files. See "Creating a Vinca Configuration File" on page 31 for more information on creating this file.

Primary Server Installation Form

Use the following table to keep track of primary server information.

Server Name: Internal IPX Net Number:

Hardware

Machine Hardware: Bus types:

Brand: Model:

Processor type: Processor speed:

Disk Devices

Brand: Model:

Size: Type:

Disk Device 2

Brand: Model:

Size: Type:

Disk Interface(s)

Brand: Model:

Bus Type: Drive Interface:

Interface settings: Port & IRQ:

Network Interface

Brand: Model:

Bus Type: Protocols used:

Interface settings: Port & IRQ:

Vinca Link (if a dedicated link is used)

Brand: Model:

Bus Type: Protocols used:

Interface settings: Port & IRQ:

Software   Standby*Server* version:

DOS version: NetWare version:

Disk Driver (.DSK) name(s) and date:

Standby*Server* File Dates

STANDBYH.NLM: SBSH.DSK:

VINCACOM.NLM: VINCAIPX.NLM:

Forms

Standby Machine Installation Form

Use the following table to keep track of standby machine information.

Server Name: Internal IPX Net Number:

Hardware

Machine Hardware: Bus types:

Brand: Model:

Processor type: Processor speed:

Disk Devices

Brand: Model:

Size: Type:

Disk Device 2

Brand: Model:

Size: Type:

Disk Interface(s)

Brand: Model:

Bus Type: Drive Interface:

Interface settings: Port & IRQ:

Network Interface

Brand: Model:

Bus Type: Protocols used:

Interface settings: Port & IRQ:

Vinca Link (if a dedicated link is used)

Brand: Model:

Bus Type: Protocols used:

Interface settings: Port & IRQ:

Software   Standby*Server* version:

DOS version: NetWare version:

Disk Driver (.DSK) name(s) and date:

Standby*Server* File Dates

STANDBYH.NLM: SBSH.DSK:

VINCACOM.NLM: VINCAIPX.NLM:

Froms

Problem Resolution Worksheet

Please list the exact steps followed on each machine to recreate the problem. The order of events is very important, as well as which machine they occurred on. If there are any errors during operation on any of the machines please supply the exact working of the errors as well as the time they occur in relation to the steps listed in the problem description. If the problem has to be recreated using a specific program or batch file, the program will need to be sent to Vinca to allow our engineers to recreate the problem. The more information you can supply here the faster we will be able to respond with a solution.

Sample Problem Description

The primary and standby are communicating and are fully mirrored. The workstation is running a program called TEST.EXE. The following steps cause a problem:

Primary Server	Standby Machine
1. Power is turned off.	2. Escape out of Standby*Server*.
	3. Change to the netware directory and run server.exe.
	4. Volumes do not mount.
	5. VREPAIR is run and is not able to re-pair volumes.

The error "Mirrored copies of the FAT don't match" displayed when VREPAIR is run.

Use the VINSTALL utility on the standby machine to create a configuration file. If you have added additional standby machines to your configuration, use the VINSTALL utility to create a configuration file for each vault machine as well. See "Creating a Vinca Configuration File" on page 31 for details on creating this file.

Appendix F
Using a Vault Machine

Standby*Server* now includes the ability to add additional standby machines to a primary server-standby machine configuration. This information has been included in an appendix for those advanced users who want to add an additional standby machine to their current configuration to act in a data vaulting role. Before adding an additional standby machine, or vault machine, to the current Standby*Server* configuration, the current configuration should be running and fully tested.

If you have not tested you current configuration, see Chapter 3, *Testing the Failover Configuration* and make sure your system is setup and working properly before adding a vault machine to your configuration.

What is a Vault Machine

A vault machine is an additional standby machine that by default functions in a data vaulting role. The vault machine contains a disk device(s) that is exported to the primary server and used as part of the mirrored set that is being mirrored between the primary server and the standby machine. In the vault role, the additional standby machine does not automatically failover and assume the primary role if the primary fails. However, in cases where neither the primary server nor standby machine are able to assume the primary role, the vault machine can be manually started in the primary role giving users access to the mirrored data.

Depending on your configuration, the vault machine can continue to mirror with the standby machine when it has failed over and assumed the primary role. This ability is discussed in more detail in the "StandbyServer Hardware Configurations Using a Vault Machine" on page 126. If the mirroring option is not enabled, the vault machine will discontinue mirroring when the primary server fails.

Like the standby machine, the vault machine also can use the Utility Server feature that enables it to function both as a fault-tolerant mirror for the primary server and a regular server. Because the vault machine generally doesn't assume the primary role, clients attached to, or services run using the Utility Server feature are generally not disrupted. You can also run Vinca's SnapShot*Server* to facilitate server backups on either or both the standby and vault machines when the Utility Server feature is enabled.

Standby*Server* Hardware Configurations Using a Vault Machine

The configuration diagrams in this section show three drives in both the standby and vault machines. Two of the disk devices are used to mirror the two devices in the primary server. The third disk device is an extra disk devices used when you want to employ the Utility Server feature. If you do not use the Utility Server feature in either machine, you do not need the additional disk device as shown.

When you use direct dedicated links to the vault machine, the client network link is optional and would only be used if you were to manually failover the vault machine. The following two graphics illustrate two direct connections; one with direct card to card connections to each standby machine, and the other using one card and a hub for both standby machines.

Figure F.1 Direct Dedicated Links

In this scenario, the primary server has three LAN cards.

The network connection to the vault machine is optional.

Adding an optional router on the dedicated link between the primary server and the vault machine enables you add space between the machines.
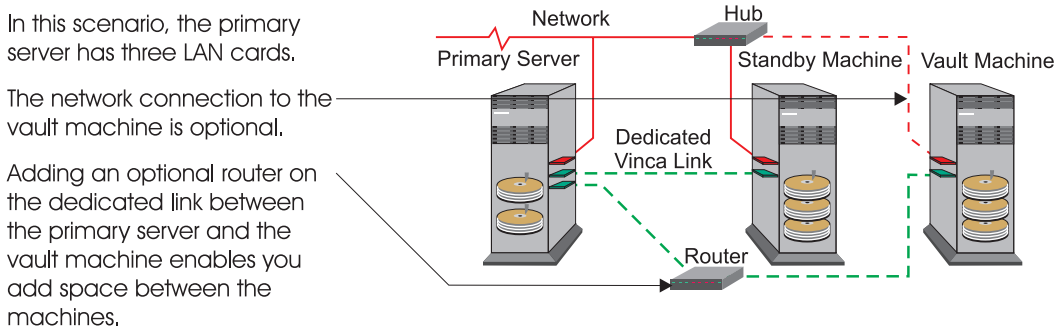
In Figure F.1, the Vinca link can be a dedicated link without a router, or a non-dedicated link with a router. Using a router enables you to add space between the primary server and the vault machine.

If you wanted to have the mirroring continue after a primary server failure, you would have to have the optional client network connection so there was a link between the standby and vault machines. If you enabled the vault machine to continue mirroring, all mirroring traffic would travel on the client network.

To enable mirroring after a primary server failure and maintain a connection other than the client network, a hub would need to placed in the secondary link connection so that all machines were connected to the hub (see Figure F.2).

Figure F.2 Using a Hub on the Dedicated Link

In this scenario, the primary server has two LAN cards and the connections (both the client network and dedicated links) are run through a hub.
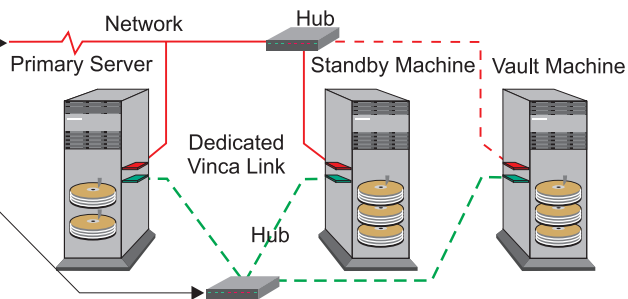
In this configuration where there is no client network connection, all mirroring takes place on the secondary link. For this reason, this configuration is better if you are going to enable mirroring after a primary server failover.

The advantages and disadvantages of these configurations are the number of cards used in the primary server versus the cost of a fast hub and the link speed needed to continue mirroring to the vault machine after a primary server failure. In Figure F.1, mirroring goes over the client network and will slow down both the network and the mirroring after a primary server failure.

Using A WAN Link

A WAN link enables you to locate your vault machine away from your primary server. Having a copy of your data away gives you extra security for disasters that might make both the primary server and standby machine unavailable. To implement a WAN environment, long distance T1 or ATM lines are necessary to ensure the mirrored data reaches the vault machine in a timely manner.

Figure F.3 Using A Dedicated WAN Link

In this scenario, the primary server has three LAN cards.

The vault machine's link uses a T3 connection across the WAN.
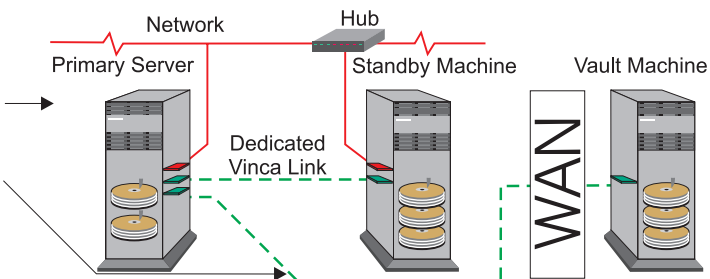
This configuration (Figure F.3) would be best if you don't have the client-network bandwidth and wanted to keep your mirroring to the dedicated link.

If you wanted to enable mirroring to the vault machine after a primary server failure, you would have to add a hub like in Figure F.2) to ensure there was a connection between the standby and vault machines when the primary server was down.

If your client network has enough bandwidth to support both normal traffic and mirroring before and after a primary server failure, you could use it to connect to the vault machine through a WAN with a hub (Figure F.4).

Figure F.4   Using A Non-dedicated WAN Link

In this scenario, the primary server has two LAN cards.

The vault machine's link uses routers and a T3 connection across the WAN.
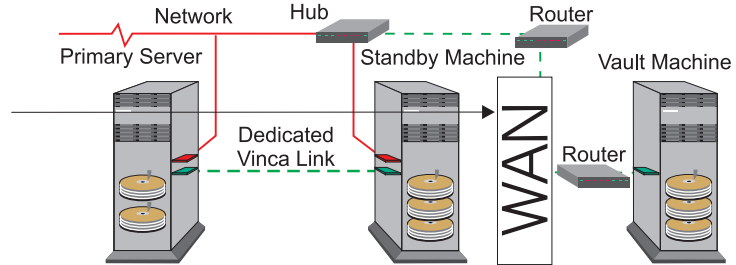
The advantages and disadvantages of these configurations are the number of cards used in the primary server versus the burden of mirroring traffic across you client network. In both cases, the WAN enables you to put the vault machine far from the primary server.

Whether or not you enable the vault machine to continue mirroring after the primary server fails, the recovery process is the same as when the primary server fails and the standby machine assumes the primary role. If you enable the vault machine mirroring, the mirror will be up to date when you restore the primary server to its proper role. If you do not enable the vault machine mirroring, the vault machine's disk device(s) becomes an orphan and will be resynchronized when you return the primary server to its proper role. Make sure you follow the recovery procedures to ensure the more recent data is mirrored back to the primary server.

Installing a Vault Machine

The vault machine is installed using the VINSTALL program following as outlined in "Software Installation" on page 19 The system requirements for the vault machine are the same requirements as the standby machine as outlined in the "System Requirements" on page 16.

The only difference in the installations is that the AutoSwitch feature is disabled by default to ensure that both standby machines don't failover and assume the primary role if the primary server fails, and the Read Blocker is enabled by default to increase the vault machine's performance. If you plan to use the Utility Server feature on the vault machine, make sure you follow the necessary steps during the install to properly configure the vault machine for the feature.

See also "Multiple Standby Machines" on page 104 for installation notes and sample load lines when using an additional standby machine.

Enabling Mirroring After a Primary Server Failure

To enable mirroring to the vault machine after a primary server failure, you must add a second SBSH load line to the standby machine's AUTOEXEC.NCF file in the *netware* directory. This load line enables the standby machine to see the vault machine when the standby machine is assuming the primary role.

To enable vault machine mirroring after a primary server failure

1. Add the following load line after the first sbsh load line to the standby machine's AUTOEXEC.NCF file in the *netware* directory:

2. load c:\standby\sbsh app=2

Additionally, if you are using a dedicated Vinca link between the standby machine and the vault machine, you must add a statement to the VINCAIPX load line to the same file, AUTOEXEC.NCF in the *netware* directory on the standby machine.

To enable a dedicated standby-vault machine Vinca link

• Add slave=*vault's internal net number*,vlink to the VINCAIPX load line.

For example:

load c:\standby\vincaipx **slave=def,vlink**

Where def is the vault machine's internal net number, and vlink is the name of the dedicated link card in the standby machine. Keep in mind that there might be a slave statement already in the vincaipx load line to establish the vinca link between the standby machine and the primary server.

For more information on dedicated Vinca links, see "Using a Dedicated Vinca Link" on page 18 and Appendix B, *Sample Files* for examples of the required additions to the AUTOEXEC.NCF file.

Using a Vault Machine

Mirroring

Like the standby machine, the unmounted disk devices are automatically exported for use to the primary server. The only difference between the way the standby machines and vault machine's disk devices are displayed is the machines App number follows the "B1" in the device number. For example, the standby machine's devices would start with B101 and the vault machine's devices would start with B102. This is important to remember when you have to resynchronize the mirrors.

Use the appropriate mirroring steps as outlined in Chapter 2, *Mirroring* to add the disk device(s) located in the vault machine to the mirrored set (s) currently shared by the primary server and standby machine.

Testing the Failover Configuration

Like the standby machine, the vault machine needs to be tested to ensure it can assume the primary role if needed. Because the vault machine does not use the AutoSwitch feature, both the failover and recovery processes are completely manual. The following test presumes that all machines are running in their proper roles.

Because this is only a test to ensure the vault machine can failover if necessary, you should disconnect the vault machine's link(s) to the network. Disconnecting the link(s) ensures that the current Standby*Server* configuration is undisturbed during the test. Do not down either the primary server or standby machine for this test. You can disconnect the vault machine from the network by physically disconnecting the cable(s).

The following steps should only be followed for testing the vault machine's ability to assume the primary role. The actual failover and recover processes are different than the test steps.

To test the vault machine's failover capabilities

1. Disconnect any links between the vault machine and the primary server's network.

On the vault machine

2. Down and exit NetWare.
3. Change to the *netware* directory.
4. Type `server` and press enter to start the vault machine in the primary role.
5. Ensure that the server starts and runs as the primary server.
6. Down and exit NetWare.
7. Change to the STANDBY directory.
8. Type `standby` and press enter.
9. Ensure the machine starts and runs in the vault role.
10. Reconnect the link(s) between the vault machine and the primary server.

On the primary server

Note: The vault machine's disk devices will be "orphaned" or "out -of-sync".

11. Run Install.
12. Delete the vault machine's orphaned disk device(s) from the mirrored set(s).
13. Reinsert the orphan devices into the mirrored set.
14. Reestablish the mirror between the primary server and the vault machine.

Using a Vault Machine

Manually Failing Over the Vault Machine

The vault machine should only be failed over to assume the primary role in three cases. The first case would be if both the primary server and standby machine are unable to assume the primary role because some kind of disaster caused them to fail simultaneously.

The second case is when the standby machine failed and then the primary server failed. In this case, the standby machine would no longer be acting as a fault tolerant mirror of the primary machine and mirroring between the primary server and the vault machine would still be active.

The third case is when the primary server is down and the standby machine is assuming the primary role and then it fails. In this case, if you had enabled the mirroring to continue after the primary server failed, the most recent data would by on the vault machine and you might want to start it in the primary role. If you didn't enable the mirroring to continue, the most recent data would be on the failed standby machine and you would risk loosing information if you started the vault machine in the primary role.

Cases where you would not want to fail over vault machine would be if the primary server failed, and the standby machine assumed the primary role. If you failed over the vault machine when the standby machine was acting in the primary role, you risk loosing all data written to the standby machine's disk devices.

When you failover the vault machine and make the mirrored data available to users, the vault machine will most likely contain the most recent data. Make sure you carefully follow the vault machine recovery process below to ensure you don't lose any data when restoring your Standby*Server* configuration.

To failover the vault machine

1. On the vault machine, down and exit NetWare.
2. Change to the *netware* directory.
3. Type server and press enter to start the vault machine in the primary role.

The Standby Machine's Role During a Vault Machine Failover

When the vault machine is assuming the primary role, the standby machine should not be restarted in the standby role. The standby machine can only failover for the primary server. Also, to properly recover from a vault machine failover the primary server must be started in recovery mode. For this reason, the standby machine should only be restarted in its standby role after the vault machine has been fully recovered.

Recovering From a Vault Machine Failover

Depending on the length of time the vault machine was in the primary role, you could have a large amount of data that is only located on the disk device in the vault machine. It is extremely important to follow the steps below to ensure you don't lose that data.

The following steps presume that the vault machine is currently assuming the primary role and the primary server and standby machine have been repaired and are ready to be returned to their proper roles.

To return the vault machine to its original role

On the primary server

1. Start the primary server and change to the STANDBY directory.
2. Type standby and press Enter to start the primary server in recovery mode.
3. Allow the mirrors to resynchronize.

On the vault machine

4. Down and exit NetWare.

On the primary server

5. Down and exit NetWare.

On the vault machine

6. Change to the STANDBY directory.
7. Type standby and press Enter to start the vault machine its proper role.

On the standby machine

8. Start the standby machine and change to the STANDBY directory.
9. Type standby and press Enter to start the standby machine its proper role.

On the primary server

10. Change to the netware directory.
11. Type server and press Enter to start the primary server in the primary role.

Using a Vault Machine

Appendix G
Technical Notes

Creating an Ethernet Crossover Cable

You can create an Ethernet (category 5 unshielded twisted-pair (UTP)) crossover cable by crossing-over the send and receive pairs on each RJ-45 connector as follows:

Figure 4.1 Crossover Cable

RJ-45 Connector 1   RJ-45 Connector 2

Green
White/Green
White/Orange
Orange

White/Green
Green
Orange
White/Orange

Connectors shown metal up, clip down.
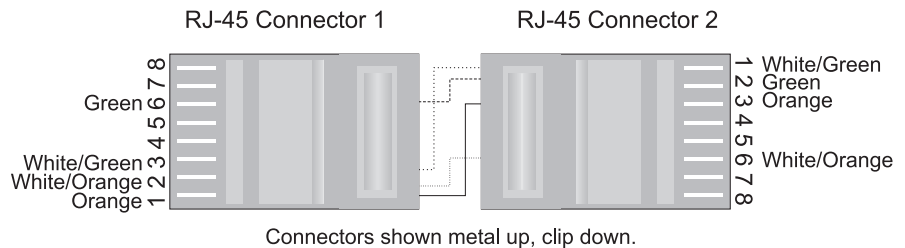
Note: Some newer model LAN cards require four pairs of category 5 cable and therefore require a hub to complete the connection. Consult your LAN card manufacturer, or the card's documentation for information on configuring a point-to-point connection.

Upgrading to a Dedicated Vinca Link

If Standby*Server* has already been installed without a dedicated link, you can complete the following steps to update to a dedicated link. When converting the system to a dedicated link, you need to specify both the target server and LAN card that will be used on both machines in both NetWare and Standby directories. This requires editing the VINCAIPX load line and specify "master=123,vlink" on the standby machine side, and "slave=abc" on the primary server side, where '123' is the primary server's IPX internal network number and 'abc' is the standby machine's IPX internal network number, and vlink is the name of the link driver instance. Notice in the examples below (Step 9) where the Vinca IPX load line follows the load and bind statements for the LAN driver.

To update to a dedicated Vinca link

1. Down the primary server.
2. Down the standby machine.
3. Install the dedicated Vinca link LAN cards.
4. Copy the LAN card's drivers into the NetWare directories on each machine.
5. Connect the dedicated Vinca link LAN cards with a point-to-point crossover cable, or whatever is required to connect the LAN card.
6. Test the cards to ensure that they are functioning properly.
7. Edit the AUTOEXEC.NCF files in both the C:\SERVER (NWSERVER for 4.1x) and C:\STANDBY directories on both machines to load the NetWare driver for the dedicated Vinca link LAN card and bind it to IPX.
8. Edit the AUTOEXEC.NCF files in both the C:\SERVER (NWSERVER for 4.1x) and C:\STANDBY directories on both machines to reflect the bold text below:
9. C:\STANDBY directory:

    `load <LAN driver> port=340 int=2 name=vlink`

    `bind ipx to vlink net=face`

    `load c:\standby\vincaipx master=<primary servers internal`
    `net>,`**`vlink`**

    C:\SERVER (NWSERVER for 4.1x) directory:

    `load <LAN driver> port=340 int=2 name=vlink`

    `bind ipx to vlink net=face`

    `load c:\standby\vincaipx `**`slave=<standby machine's internal`**
    `net>,vlink`

    Review the bold references in the examples located in Appendix B, *Sample Files* for more information on the changes.

10. Restart the standby machine.
11. Restart the primary server.

Technical Notes

Index

StandbyServer for NetWare User's Guide