

Chapter 2 Server Setup and TSAs

Overview

This chapter explains how to:

- update servers with the most recent NetWare modules
- load TSAs on servers and workstations
- create the auto login user (if necessary)
- tune your servers to ensure optimal performance

Contents

Preparing Your Server(s)

Workstation/Server Requirements

Determine Where To Install Backup Director

Running SETUP.NLM

Down the Server

Loading PALSTART.NCF

Installing Target Service Agents

What is a Target Service Agent?

Installing the Target Service Agents

To Protect Servers

To Protect Workstations

Copying TSAs

Protecting DOS and Windows Workstations

Installing the DOS/Windows Workstation TSA

Protecting OS/2 Workstations

Loading TSAOS2.EXE Automatically

Create the TSAOS2.CFG file

Place the TSAOS2 icon in the "Startup" folder

Creating the Auto Login User

Rights

Protecting 3.x Servers

Protecting 4.x Servers

Protecting Servers in Different NDS Trees
Tuning Your Servers

PALCHECK.NLM

Packet Receive Buffers

SPX Settings

Directory Cache Buffers

Cache Buffers

Short Term Memory Allocation

Checking Loaded Modules

Current CLIB Versions

Current LAN Drivers

Preparing Your Server(s)

Prior to installing Backup Director, perform the following steps during off hours or when there is little activity on your server(s).

The following steps are described in detail below.

Determine where to install Backup Director—Determine the server on which you want to install Backup Director

Update Servers—Run SETUP.NLM to install the latest TSAs and NetWare modules on each of your servers.

Load TSAs—On each server you are protecting, load the appropriate TSAs.

Create the auto login user—Backup Director uses the auto login user to access remote servers and the Backup Director job queue.

During installation, the default auto login user is the person installing the software. If you want to use a different user as the auto login user, you should create the user prior to installing the software if the user doesn't already exist.

Install Workstation TSAs—If you want to protect workstations, install the appropriate TSAs on each workstation.

Optimize Server Settings—Check your server environment for proper settings or continue to Chapter 3 to install Backup Director.

Workstation/Server Requirements

- Workstations (at a minimum) must be able to run Windows 3.1 or 3.11

in enhanced mode (at least a 386sx or greater with 4MB RAM). Palindrome recommends a 486-based PC with 8MB or RAM.

- Color monitor is recommended but not required with Super VGA resolution or better.
- The latest versions of NetWare's IPX (or IPXODI) and NETX or NetWare DOS Requestor (VLM). VLMs are required to access Backup Director installations on NetWare 4.x servers.
- At least 8MB of disk space for the Windows executables and DLLs and 3MB disk space on your SYS: volume for NLMs.
- Server memory should be at least 16MB.

Determine Where To Install Backup Director

You can install Backup Director on a NetWare 3.1x, 4.02, or 4.1 server (NetWare 4.01 is not a supported version). When you install Backup Director a job queue is created that stores all backup and restore requests.

When you install Backup Director on a NetWare 4.x server, an NDS connection is required by NetWare if you want to submit jobs to the job queue. Therefore, to access Backup Director installations on NetWare 4.x servers, you must log into the tree with an NDS connection.

This may be especially important for end users that use Palindrome's File Manager (PALFILER.EXE). Users must be logged in with NDS connections to submit jobs to the Backup Director queue on 4.x servers.

Upgrades

Prior to running SETUP.NLM, be sure to unload any currently loaded Palindrome NLMs such as PNASM, PALSDRV, PALALDRV, etc. If you are using Palindrome's File Manager, be sure there are no jobs in the queue before you unload the queue server (PALQSRVR.NLM).

During installation of the client software, all files from previous Palindrome installations are deleted.

Running SETUP.NLM

SETUP.NLM automatically copies Palindrome NCF files, updated TSAs, and NetWare modules to each server you are protecting. You should run SETUP.NLM on all servers that you want to protect prior to installing Backup Director software.

Because you may have to down your server after files are updated on your server, Palindrome recommends running SETUP.NLM during off hours.

To run SETUP.NLM

1. Insert server preparation diskette #1 into the floppy drive of your server.
2. At the server console prompt, type:

```
LOAD A:SETUP
```

(where A: is the floppy drive your diskette is in).

3. The setup program asks if the server you are running SETUP.NLM on is your

installation server. Answer "YES" if this is the server where you will install Backup Director or currently have it installed.

The program then checks what modules you have loaded and copies Novell recommended versions of the following modules to your server (if necessary):

A3112.NLM SPXLISFX.NLM
AFTER311.NLM SPXMSFIX.NLM
CLIB.NLM SPXNSFIX.NLM
IPXS.NLM SPXS.NLM
MATHLIB.NLM STREAMS.NLM
MATHLIBC.NLM TLI.NLM
SMDR.NLM TSA311.NLM
SPXDDFIX.NLM TSADOS.NLM
SPXFIX2.NLM TSAPROXY.NLM
SPXFSFIX.NLM WSMAN.NLM
XMDFIX.NLM

A list of files that were updated displays after the files have been copied. Files that are updated are renamed with a file extension of "PAL".

Down the Server

After the install program has finished copying the necessary files, you may want to down your server to ensure any modules (such as CLIB.NLM) that were updated are loaded on your server.

Loading PALSTART.NCF

If you don't down your server(s), you should run PALSTART.NCF from the server console prompt to load the necessary Palindrome modules.

PALSTART.NCF contains statements to automatically load required files such as your device driver, Palindrome NLMs, and Target Service Agents. SETUP.NLM copies PALSTART.NCF to the SYS:\SYSTEM directory of each server that you run SETUP.NLM on.

By adding the PALSTART.NCF statement to your AUTOEXEC.NCF file on each server, you can be sure required NLMs and TSAs load whenever you reboot your server.

Before loading the file, review the file and edit it as necessary for your particular environment. Note that both the Job Server and PALMEDIA are autoloading during installation of the software.

PALSTART.NCF Example

Below is an overview of the statements contained in PALSTART.NCF. Note that on remote servers, PALSTART.NCF only loads TSAs. All other statements apply only to the installation server.

LOAD AHA1740.DSK port=330

Sample statement for loading host adapter device driver. You must load the device driver for your host adapter. Edit the statement to include your device driver's syntax.

LOAD PALLOADR

PALLOADR.NLM is used by the Windows install program to automatically load NLMs on your installation server during installation of the client software. This statement is remarked out from the PALSTART.NCF file after installing the client software.

LOAD PALJSRVR

PALJSRVR.NLM (the job server) services the Backup Director job queue and must be loaded to process any submitted jobs.

LOAD PALMEDIA

PALMEDIA.NLM scans the SCSI bus and keeps track of currently configured devices and what media is loaded in each device.

LOAD PALSDRV ABOVE16MEG

If you have a server with more than 16MB of memory (and you are using a SCSI adapter that uses on-line DMA or AT Bus Mastering and therefore cannot access memory above 16MB [for example an Adaptec 1540]), you must use Palindrome's SCSI Driver (PALSDRV.NLM) with the ABOVE16MEG switch.

NOTE: PALSDRV ABOVE16MEG is not a substitute for the ABOVE16 option that you may use when loading your host adapter's device driver.

LOAD TSAXXX

This statement loads the appropriate TSAs for your server (for example, if your server is NetWare 4.1 this statement reads:

LOAD TSA410

Installing Target Service Agents

What is a Target Service Agent?

Target Service Agents (TSAs) provide Backup Director access to servers and workstations within Novell's SMS architecture. TSAs handle requests by Backup Director to backup and restore client data.

You must install TSAs on every server and workstation you want to protect. Most workstations also require a TSA module on a server.

The TSA on the server manages communication between the server and the workstation and keeps configuration information about each workstation connected to it. Once loaded, the servers and workstations become the target services for Backup Director.

NOTE: Workstations must be turned on and the proper TSAs must be loaded for Backup Director to access them but workstations do not have to be logged in to the network.

Installing the Target Service Agents

Server TSAs are automatically copied to each server when you run SETUP.NLM from the server preparation diskette and are loaded when you run PALSTART.NCF.

Before loading TSAs manually on your servers and workstations, be sure to unload any previous versions. Also, use only TSAs provided by Palindrome either on the diskette or via the Palindrome BBS.

The procedures below assume you have copied the appropriate TSAs (and SMDR.NLM file) to each server using the SETUP.NLM program or you have manually copied them from the server preparation diskette.

To Protect Servers

Load the following TSAs according to what type of server you want Backup Director to protect.

To Protect...		Type at the server console:
NetWare 4.1	LOAD TSANDS**	LOAD TSA410
NetWare 4.02	LOAD TSA400 LOAD TSANDS**	
NetWare 3.12	LOAD TSA312	
NetWare 3.11	LOAD TSA311	

Note that SMDR.NLM file is autoloaded when you load the TSA on a server.

Protecting NetWare Directory Services**

If protecting NetWare Directory Services, you only need to load the NDS TSA (TSANDS.NLM) once per tree. In other words, if you have multiple servers in the same tree, you only need to load the TSA on a single server in that tree for NDS to be protected.

If you have multiple servers, Palindrome strongly recommends that you use NetWare's Directory Services Replication feature for increased protection of NDS.

To Protect Workstations

To protect DOS/Windows and OS/2 workstations you must load a TSA on the server and on the workstation.

To Protect...
Type at the server console...
Type at the workstation...

DOS/Windows Workstations
LOAD TSADOS (autoloads SMDR.NLM and WSMAN.NLM)

TSASMS.COM*
OS/2 Workstations
LOAD TSAPROXY (autoloads SMDR.NLM)
TSAOS2 .EXE*

*Prior to loading TSAs on the workstation you must create the appropriate configuration file. See the procedures below to create the NET.CFG file at the DOS/Windows workstation and the TSAOS2.CFG file on OS2 workstations.

Copying TSAs

Workstation TSAs are located on server preparation diskette #2 in the \DOS and \OS2 directories. Copy all files from the directories on the diskette to your workstation. You may want to copy the files to your network so you can access them from each workstation prior to loading them.

After configuring the TSAs and installing the client software, you can add your workstations to the Protected Resource List (in Resource Manager) so that they can be backed up.

Protecting DOS and Windows Workstations

TSASMS.COM (loaded on the workstation) and TSADOS.NLM (loaded on the server) allows Backup Director to protect hard disks on DOS and Windows-based workstations.

NOTE: The DOS TSA (TSADOS.NLM) loaded on the server manages a maximum of 100 clients. If you have more than 100 DOS/Windows clients, load TSADOS.NLM on multiple servers. When installing the workstation TSA, specify the appropriate server.

Removing Older Versions

If you are not upgrading your TSAs, skip to Installing the DOS/Windows Workstation TSA below.

In previous versions of the DOS TSA, the workstation name was stored in the Bindery or NDS. New versions of the DOS TSA store the workstation name in WSMAN.NLM.

Prior to removing your TSAs from your workstations, you should remove the workstation name from the Bindery or NDS. To remove the workstation name, type:

TSASMS /U

at each workstation.

If you previously removed the TSA from the workstation without removing it from the Bindery or NDS, a Novell utility SMSDBOBJ.NLM allows you to delete multiple workstation names. You can obtain SMSDBOBJ.NLM from the Palindrome BBS or from NetWire on CompuServe.

Installing the DOS/Windows Workstation TSA

TSASMS.COM (located in the \DOS directory on server preparation diskette #2) must be loaded on each DOS or Windows workstation you want to protect. Prior to loading TSASMS, be sure to load TSADOS.NLM on the server.

When loading TSASMS.COM, you must first create a NET.CFG file (or use command line parameters) to specify:

- the name of the server you want the workstation to register to
- the drives to protect on the workstation
- the name of the workstation
- the security option.

NOTE: When backing up workstations, Palindrome recommends disabling broadcast messages (using NetWare's CASTOFF ALL command) since broadcast messages can interrupt backup operations.

NET.CFG

TSASMS.COM uses the NET.CFG file to load parameters such as the workstation name, the server to register to, etc. NET.CFG is also used by Novell's DOS requestor (VLM.EXE).

To modify the NET.CFG file

1. Create (or edit an existing) NET.CFG file using a DOS editor to add the required parameters as described below. The NET.CFG file must be located in the root directory on your workstation or in the same directory as TSASMS.COM.

NOTE: Verify that SHELL.CFG does not exist in the same directory as your NET.CFG file. TSASMS.COM will use SHELL.CFG instead of NET.CFG if it finds it and will fail.

2. For each workstation, enter parameters similar to the following:

NetWare DOS TSA

```
TSA Server Name = <Myserver>
Workstation Name = <Myworkstation>
Password = (See below)
Disk Buffers = 30
Stack Size = 2048
Drives = C
```

Sample NET.CFG File

Link Driver 3C5X9

Port 300

Int 10

Frame Ethernet_ji

NetWare DOS Requester

NetWare Protocol = NDS BIND

Preferred Server = SERVER1

Search Mode = 0

Show Dots = ON

NetWare DOS TSA

TSA Server Name = SERVER1

Workstation Name = JSMITHS_PC

Password =

Disk Buffers = 30

Stack Size = 2048

Drives = C

To load the DOS TSA

1. After adding the appropriate parameters to the NET.CFG file, from the DOS prompt type:

TSASMS

to load the TSA.

2. Add TSASMS to the AUTOEXEC.BAT or STARTNET.BAT files, so that the TSA is automatically loaded whenever the workstation boots.

For more information on TSASMS parameters, see Appendix A.

NOTE: When adding or renaming any workstations, be sure that these workstations are logged on to the network when you modify the Protected Resource List.

Assigning Passwords To Workstations

Backup Director allows you to configure a separate password for each target service (workstation or server) you are protecting or use Trust mode (no password is required). Adding a password is not required by Backup Director but you may find it useful for security purposes.

Trust Mode

You can enable Trust mode by leaving the Password field blank. This automatically allows the auto login user (defined during installation of Backup Director) to back up the workstation's local drives.

When using Trust mode on 4.x servers and adding the workstation to the Protected Resource List, you will be prompted to type in the auto login user name and password to attach to the DOS/Windows workstation.

Configuring Passwords

If you configure a password when loading the TSA on the workstation, you will be prompted for each workstation's password when adding the workstation to the Protected Resource List. Once you identify the password, Backup Director will not prompt for it again unless you change it at the workstation.

Protecting OS/2 Workstations

TSAOS2.EXE (loaded on the workstation) and TSAPROXY.NLM (loaded on the server) allows Backup Director to protect hard disks on OS/2-based workstations.

TSAOS2.EXE is automatically copied to the workstation's hard disk when you install the Novell OS/2 Requestor, and an icon for the TSA is placed in the Novell group on your desktop. Use TSAOS2.EXE (with TSARC.DLL and TSAOS2.HLP) on server preparation diskette #2, however, to ensure you have the correct version to use with Backup Director.

If the TSA icon does not appear on your desktop, create it using the Template Folder specifying the correct path to TSAOS2.EXE.

NOTE: Palindrome recommends using version 2.01 (or greater) of the Novell OS/2 Requestor.

TSAOS2.EXE allows you to specify:

- the name of the server you want the workstation to register to
- the drives to protect on the workstation
- the name of the workstation
- the security option.

TSAOS2.EXE can be loaded automatically or manually. Palindrome recommends starting the program automatically (using the "Startup" folder) so that it loads each time a user boots the workstation.

Loading TSAOS2.EXE Automatically

To configure the TSAOS2.EXE program to start up automatically each time the workstation is booted, you must:

- Set up the TSAOS2.CFG file.
- Place the TSAOS2 icon in the "Startup" folder.

NOTE: Before continuing, be sure that the TSAPROXY.NLM is loaded on the primary server (using the MODULES command at the server) and the NetWare Requestor for OS/2 (version 2.01 or higher) is installed on the OS/2 workstation(s) you plan to protect. (OS/2 workstations should be running OS/2

2.0 or higher.)

Create the TSAOS2.CFG file

You can create a text file called TSAOS2.CFG to store settings for the TSAOS2.EXE program. These settings are automatically read by the TSAOS2.EXE program each time it starts up.

If you load TSAOS2.EXE without creating the TSAOS2.CFG first, a pop-up window displays where you can define the parameters that the TSA uses when loading.

After creating this file, save it to the directory where TSAOS2.EXE is located (usually \NETWARE). Below is an example of what your TSAOS2.CFG may look like and an explanation of each option. Note that the TSAOS2.CFG file is not case-sensitive.

TSAOS2.CFG Example

```
WSName  
JOHN_OS2  
ServerName  
FS1  
UserName  
JSMITH [PASSWORD]  
AutoRegister  
ON  
TempFilesDir  
c:\temp
```

Backup Director requires unique workstation names. When adding workstation resources, no two workstation names can be identical (even if the workstations are protected by different TSAs).

For more information on TSAOS2 parameters, see Appendix A.

Place the TSAOS2 icon in the “Startup” folder

Complete the following steps to place the TSAOS2 icon in the “Startup” folder.

1. Open the “OS/2 System” folder on the desktop. The “OS/2 System” window appears.
2. Open the “Startup” folder from the “OS/2 System” window. The “Startup” window appears.
3. Without closing the “Startup” window, open the “Novell” group on your desktop. The “Novell” window appears.
4. Create a Shadow, or Copy the NetWare TSA icon from the “Novell” window into the “Startup” folder.

Whenever the machine is rebooted, the TSAOS2 program will start automatically when your TSAOS2.CFG file is properly configured.

Creating the Auto Login User

To access servers and the Backup Director job queue, Backup Director relies on an auto login user. Using a single auto login user to attach to remote servers provides maximum security for backup and restore operations.

NOTE: If you have a valid user already defined that can be used as the auto login user, review *Tuning Your Servers* in Chapter 2 or go to Chapter 3 to begin installing the software.

During installation of the software, you will be prompted to specify a single auto login user (either as a Bindery user or as an NDS user) that is stored in the Backup Director System Control Database. When you add resources to protect, if the auto login user doesn't exist on those servers (or in the NDS tree), you will be prompted to specify a user and password to access those resources.

By default, the user installing the software displays as the auto login user name. You can use this user or any other existing user that has supervisor-equivalent rights to each server you want to protect.

Rights

In NetWare 3.x environments, the auto login user must exist on every server and have supervisor-equivalent rights.

In NetWare 4.x environments, the user only needs to exist once in the tree and should have supervisor object rights to the **each server** object you want to protect and to **the container** that the installation server is in.

WARNING: Do not limit concurrent connections for the auto login user.

Protecting 3.x Servers

On each 3.x server you want to protect

- > Create the auto login user using NetWare's Name Service NETCON or SYSCON utility.
- > At each remote server, grant the user supervisor-equivalent rights and give the user a password to keep your network secure.

Protecting 4.x Servers

To protect 4.x servers in the same tree

- > Create the auto login user using NWADMIN.
- > Give the user supervisor-object rights to all servers you want to protect, supervisor object rights to the container the installation server is in, and write rights to the root object.

Protecting Servers in Different NDS Trees

NOTE: If you are not backing up servers in multiple trees, review *Tuning Your Servers* in Chapter 2 or go to Chapter 3 to begin installing the software.

Logging into NDS trees outside of the installation server's tree requires Bindery emulation. (Bindery emulation allows applications that relied on the Bindery in 3.x versions of NetWare to work with NetWare 4.x but is also required for attaching to multiple trees.)

When you install a NetWare 4.x server into the NDS tree, a NetWare server object is created in the specified container object. By default, Bindery emulation is activated and the server's Bindery context is set for that container object. When protecting servers that are not in your installation server's NDS tree, you should create the auto login user in the container object where Bindery emulation is set for each server.

To add the auto login user to the remote NDS tree

Determine the default Bindery context for the remote server. From the server console prompt, type:

SET BINDERY CONTEXT

the server displays:

Bindery Context: O=(Container Name of current Bindery context)

- > If the Bindery context does not show the container object that the server resides in, change it using the "Set Bindery Context =" command at the server console prompt and add the command to your AUTOEXEC.NCF file.
- > Use NWADMIN to create the auto login user in the same container object where your server is located in the NDS tree.
- > Give the user supervisor-object rights to all servers you want to protect.

Bindery Emulation User Example

Assume you have a server named **SERVER1** in an NDS tree part of an Organizational Unit (Container Object) named **SALES** that you want to protect with Backup Director installed on a server in a different NDS tree.

The Organizational Unit **SALES** exists under an Organization named **ACME**. The auto login user should be created in **OU=SALES.O=ACME**.

Therefore, when viewing the Bindery context for SERVER1 it should read: BINDERY CONTEXT: OU=SALES.O=ACME

To set the Bindery context, use the following command:

SET BINDERY CONTEXT =OU=SALES.O=ACME

If the Bindery context cannot be set, ensure that a read-write or master replica of the partition that contains OU=SALES.O=ACME is located on server SERVER1. If it does not, use Partition Manager to place a copy of the partition on the server.

Tuning Your Servers

This section provides instructions on using PALCHECK.NLM and how to modify settings on your server to enhance server performance. These settings include:

- Packet Receive Buffers
- SPX parameters
- Directory Cache Buffers
- Reserving Buffers Below 16MB
- Cache Buffers
- Short Term Memory Allocation

PALCHECK.NLM

PALCHECK.NLM is a Palindrome utility that examines your environment and makes recommendations based on:

- server memory
- loaded modules
- server settings

PALCHECK can be used as a troubleshooting tool or as a preventive maintenance utility to ensure your servers are properly configured.

To run PALCHECK

- > At the server console prompt of each server you are protecting, type:

LOAD PALCHECK

PALCHECK displays recommendations about modules and system settings it finds on your servers.

NOTE: You do not need to manually load PALCHECK.NLM on your installation server. It automatically runs during installation of the client software.

Packet Receive Buffers

Packet Receive Buffers are areas in the server's memory that temporarily hold data packets arriving from network stations. Palindrome recommends setting the "Minimum Packet Receive Buffer" to a minimum of 100 and the "Maximum Packet Receive Buffer" to 500. Use a command similar to the following at the server prompt:

SET MINIMUM PACKET RECEIVE BUFFERS=100

SET MAXIMUM PACKET RECEIVE BUFFERS=500

Add the "Minimum Packet Receive Buffer" statement to your STARTUP.NCF file and the "Maximum Packet Receive Buffer" to your AUTOEXEC.NCF file. When setting this, ensure available cache buffers does not fall below 20-30% of total cache buffers.

SPX Settings

SPX is a communications protocol that monitors network transmissions.

To avoid communications problems, such as an NATV-11 dropped connection error,

Palindrome recommends that you set appropriate SPX settings for your version of NetWare.

To set SPX settings on NetWare 3.x Servers

Palindrome recommends using the following timeout values on your server if SPX is used: Abort=5000, Verify=100, Wait=3000, Retry=255, Quiet=1.

To configure these settings, use a command similar to the following at the server prompt:

LOAD SPXCONFIG A=5000 V=110 W=3000 R=255 Q=1

To set SPX settings on NetWare 4.x Servers

1. Load SERVMAN on your NetWare 4.x server.
2. From the Available Options menu, select IPX/SPX Configuration.
3. From the IPX/SPX Configuration menu, select SPX Parameters.
4. Set the fields with the following values:

SPX Parameter Recommended Setting

SPX wathchdog abort timeout
5000
SPX watchdog verify timeout
110
SPX ack wait timeout
3000
SPX default retry count
255
Maximum concurrent SPX sessions
1000

Directory Cache Buffers

A directory cache buffer is a portion of server memory that holds entries from the directory table. Be sure your cache buffers are set high enough to handle directories with large numbers of files. Generally, you can calculate how many cache buffers a server should have by doing the following:

1. Multiply the number of files (or the potential number of files) in the largest directory by the number of name spaces on the volume (use the VOLUMES command at the server console to view the number of name spaces).

For example, if your largest directory has 5,000 files in it and you have two name spaces loaded (DOS and AFP for example) on that volume, multiply 5,000 X 2 = 10,000

2. Multiply that number (from step 1) by the size of a directory entry, 128 bytes. 128 X 10,000 = 1,280,000
3. Divide this number by the size of the cache buffers (default size is 4K).
1,280,000/4,096 = 320

- Using the number from Step 3 as a minimum baseline, enter the following command at the server console prompt:

SET MINIMUM DIRECTORY CACHE BUFFERS=320

Remember that the Maximum Directory Cache Buffers must be greater than the minimum number.

Cache Buffers

The Total Cache Buffer pool must be greater than 25% of total server memory (according to NetWare documentation, 40-60% of total memory). If Total Cache Buffers are less than 30% of total memory, consider adding more memory to the server.

Palindrome's NLMs require 1.5MB of memory which is taken from the Cache Buffer Pool. After the NLM is loaded there must be 20% still available at a minimum.

Short Term Memory Allocation

On 3.x servers with a large amount of communications activity (many users), the default (2MB) of Allocated Short Term Memory is often not enough.

Depending on the number of users connected, the Allocated Short Term Memory should generally be somewhere between 3 and 9MB. Use the command syntax similar to the following at the server console prompt:

SET MAXIMUM ALLOC SHORT TERM MEMORY = 6000000

You should add this statement to your AUTOEXEC.NCF file.

Checking Loaded Modules

PALSDUMP (located on the last installation diskette in the \TOOLS directory) generates a report of all loaded modules and other valuable information such as what namespaces are loaded, contents of NCF files, and all current SET parameters and is useful for troubleshooting purposes.

Contact Novell (or use NetWare) or Palindrome for a list of the latest versions of NetWare modules. Replace any old versions of NetWare modules that you find.

Current CLIB Versions

Be sure you are using a current version of CLIB. Compare the date of the CLIB loaded on your server(s) to the dates listed below. If you are not using the current CLIB version, update each server you want to protect.

Server

Minimum CLIB version Obtain from

NetWare 3.11

3.11D 12-16-92

Palindrome BBS (CLIB311D.ZIP)

NetWare 3.12
3.12G 5-19-94
Palindrome BBS or NetWire (part of LIBUP3.EXE)

NetWare 4.1
4.10 11-3-94
NetWire

Current LAN Drivers

Be sure you are using the most current LAN driver version available for your specific network card and NetWare version. If you need to verify the current version of your LAN driver, contact the vendor from whom you purchased the driver.

Novell provides updates to the latest Novell-certified server drivers for NExxx.* boards, TOKEN, TRXNET, and PCN2L. These updates are located on NETWIRE in the file LANDR3.EXE.

LANDR3.EXE also contains updates to the NetWare 3.x and 4.x media support module (MSM and MSM31X) and the Ethernet topology support module (ETHERTSM).
