

LANtegrity for NetWare Set-up Guide

LANtegrity

McAfee, Inc.

2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 am - 5:00 pm

FAX: (408) 970-9727
BBS: (408) 988-4004

(For international contact information, see the following page.)

COPYRIGHT

Copyright © 1995 by McAfee, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc.

TRADEMARK NOTICES

McAfee is a registered trademark of McAfee, Inc. SiteMeter, SiteExpress, ServerStor, and NetRemote are trademarks of McAfee, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to Saber Software Corporation, a wholly owned subsidiary of McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

A Reader's Comment Form is provided in the back of this publication. McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. If the form has been removed, please address your comments to: McAfee, Inc., Documentation, P.O. Box 9088, Dallas, Texas 75209.

SUPPORT

For fast and accurate help, please have the following ready when you contact McAfee:

- Program name and version number
- Type and brand of your computer, hard drive, and any peripherals
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem.

INTERNATIONAL CONTACT INFORMATION

McAfee Canada

178 Main Street
Unionville, Ontario
Canada L3R 2G9
Voice: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.

Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Voice: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee (UK) Ltd.

Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Voice: 44 1344 304730
Fax: 44 1344 306902

McAfee France S.A.

50 rue de Londres
75008 Paris
France
Voice: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH

Weltenburger Strasse 70
81677 Munich
Germany
Voice: 49 89 92404214
Fax: 49 89 92404211

Table of Contents

Chapter 1. About This Guide	1
Welcome	1
How to Use This Guide	3
Technical Support	4
Chapter 2. Configuration and Installation Notes	5
Requirements for a LANtegrity Server	6
Requirements for a Protected Server	13
Workstation for the LANtegrity Administrator	15
Installing and Setting Up LANtegrity	16
Chapter 3. Installing and Setting Up LANtegrity	18
Overview	18
Checklist	20
Installing LANtegrity Server Software	21
Installing Protected Server Software	23
Setting Up a LANtegrity Server	25
Setting Up a Protected Server	27
Setting Up the LANtegrity Administrator	29
Removing LANtegrity	30
Chapter 4. Getting Started	31
Initial Login to New LANtegrity Server	32
Configuring the LANtegrity Server	35

Configuring a Protected Server	38
What Next?	42

Appendix A. Stand-In Printing Services 43

For a NetWare 3.x Protected Server	44
For a NetWare 4.1 Protected Server	51

Appendix B. Disaster Recovery 59

Recovering from Online Tapes	60
Recovering from Offsite Tapes	63

Welcome

The *LANtegrity for NetWare Set-up Guide* explains how to install, set up, and configure a complete LANtegrity system, set up stand-in printing, and recover from a disaster. It is part of the LANtegrity for NetWare documentation set that includes:

- **Read Me** is a list of information not available when the *Administrator's Guide* went to press plus additional technical information.
- **Quick Tour** is a guide to installing and setting up a minimum LANtegrity configuration, using stand-in services, and restoring a file. Use this Tour if you are an experienced NetWare Administrator who wants to evaluate LANtegrity or try out its major features.
- **LANtegrity for NetWare Administrator's Guide** contains detailed information about configuring, using, and managing LANtegrity.
- **Help** includes much of the material from the *Administrator's Guide*, organized and formatted for online use.
- Copy of **LANtegrity for NetWare Administrator's and Set-up** guides on CD-ROM, in the DOC directory (included as Adobe Acrobat Portable Document Files LSADMIN.PDF and LSSETUP.PDF) along with the Acrobat Reader 2.0 (ACROREAD.EXE). Install on any Windows workstation. Acrobat Reader requires about 2MB of disk storage on the workstation. Registration is not required.

Other sources of documentation are:

- **Hardware documentation for your LANtegrity system.** Although Network Integrity does not supply the hardware components of your LANtegrity system, we do refer to them in this guide. If you need information about the components, refer to vendor's documentation.
- **NetWare documentation.** References to NetWare Loadable Modules (NLMs) and commands are to standard NetWare products, provided in Novell's normal distribution package and described in its documentation
- **Windows documentation.** You may want to keep the latest Windows documentation available to your operators for reference purposes.

Audience

This guide is intended for experienced NetWare system administrators who intend to install and manage LANtegrity for NetWare. It assumes that you are familiar with NetWare technology and terminology and with Windows application conventions.

How to Use This Guide

First, ensure that your system meets the hardware and software requirements listed in the *Configuration and Installation Notes*. Then follow the procedures in this guide to install, set up, and configure LANtegrity. Provided that your systems are configured correctly, the procedures are quite simple.

The guide is divided into these sections:

Chapter 1. *About this Guide*. Provides details on the information you will find in this document.

Chapter 2. *Configuration and Installation Notes*. Provides checklists of hardware and software requirements. Read before you install LANtegrity.

Chapter 3. *Installing and Setting Up LANtegrity*. Follow the steps to install and set up a LANtegrity Server, the protected servers, and LANtegrity Administrator application. If you followed the *Quick Tour* to set up a minimum LANtegrity configuration, refer to Chapter 1 to set up additional protected servers.

Chapter 4. *Getting Started*. Use to configure and initiate the default protection for your servers.

Appendix A. *Stand-in Printing Services*. Use to set up stand-in printing services.

Appendix B. *Disaster Recovery*. Follow these instructions to recover if the LANtegrity Server's disk fails.

Technical Support

Report all problems to Technical Support, Network Integrity, Inc.

When contacting us by...	Use...
Telephone	You can reach us at 508-460-6670, option 2
Email	Or you can send email to support@netint.com
Fax	Or you can send a fax to 508-460-6771. Mark the cover sheet to the attention of Technical Support.

The key to a quick and easy installation of LANtegrity is to make sure that your systems are configured correctly. Sometimes users overlook just one item. Most often, it's related to hardware!

To help you avoid the usual pitfalls, we've prepared a checklist of hardware and software requirements, which includes details about the most common problems our users have experienced and notes about installing LANtegrity.

You'll find information about:

- LANtegrity Server, with subsections about the SCSI host adapter, SCSI devices, and autoloaders
- Installing NetWare 4.1 on the server designated as the LANtegrity Server
- Protected server
- Workstation for the LANtegrity Administrator
- Notes about Installing LANtegrity.

When you've completed the checklist and are ready to install LANtegrity, turn to the *Read Me First* and the *LANtegrity Set-up Guide*.

These notes assume that you know how to install NetWare 3.1 or higher. And that you also know how to install, configure, and troubleshoot boards in a computer.

If you have any questions or suggestions for improving the checklist, contact us by:

Telephone	508-460-6670, option 2
Email	support@netint.com
Fax	508-460-6771

Requirements for a LANtegrity Server

The bullets below display the checklist items and their details for installing and configuring a LANtegrity server.

- **CPU**
An Intel 486/66 or faster.
- **Memory**
16 MB more memory than on the largest Protected server (Min 48 MB).
- **Disk Space**
A volume for storing data that is 1 GB larger than the disk space on the largest Protected server.
- **NetWare**
Novell NetWare 4.1. See [“Installing NetWare 4.1 on a LANtegrity server.”](#)
- **License**
A NetWare 4.1 license with a license count equal to the number for the largest Protected server. Use the runtime license purchased from Network Integrity[®] or obtain a license from your reseller.
- **CD ROM**
To install NetWare 4.1, you need an installed CD-ROM reader. For configuration information, see [“General guidelines for SCSI devices.”](#)
- **Anti-Virus Programs**
Currently LANtegrity is compatible with the following programs:
 - ❑ Cheyenne's Inoculation 3.0
 - ❑ Intel LANdesk Anti-Virus 2.13
 - ❑ McAfee Anti-Virus 2.1.1
 - ❑ Norton Anti-Virus 1.00E
 - ❑ Thompson's Doctor 95.09.

If your Anti-Virus program is not listed, check with Technical Support before running LANtegrity on this server. When the Anti-Virus and LANtegrity are not compatible, you risk locking up the server on which they are running.

SCSI host adapter

The bullets display the checklist items and their details for installing and configuring a SCSI host adapter.

- ***NWPA-compliment host adapter***

When using an autoloader, the LANtegrity Server needs a host adapter board that is compatible with NetWare 4.1 NetWare Peripheral Architecture (NWPA), and its driver (a Host Adapter Module (HAM)).

Currently, the only NWPA host adapter available is the Adaptec 1542C or 1542CF ISA-to-SCSI adapter. The HAM (SCSI154X.HAM) ships with NetWare 4.1. Other HAMs will be available soon. Contact Technical Support for more information.

If possible, use the Adaptec host adapter with DMA 5, IRQ 11, and port address 330, which are the default parameters, and set the BIOS to OFF.

If you are using an Adaptec 1542C in a server which uses a PCI bus (e.g., Compaq ProLiant), you must use PCI Setup to allocate an IRQ line to the Adaptec 1542C before it's recognized by the LANtegrity Server.

- ***IRQ, DMA, and port address***

Each board in a machine needs a unique IRQ, DMA, and port address setting. Conflicts between settings are one of the most common installation problems. If there is a conflict, the machine will not function or you get unexpected results. For information about changing the settings, see the installation manual for the adapter.

Port addresses have a range. So even if the port address on the host adapter is unique, there may be a conflict because the port address range overlaps the address of another board.

Example: Some 3COM Network boards ship with IRQ 11 and port address 300, with a range of addresses up to 332. Both settings conflict with the defaults on an Adaptec 1542C host adapter, which are IRQ 11 and port address 330.

- **BIOS**

Decide if you want to enable or disable the BIOS.

Example: By default, the BIOS on an Adaptec 1542C host adapter is enabled. However, if you follow our recommendation, you'd put the auto-loader alone on an adapter and disable the BIOS. On the other hand, if you put the autoloader on the adapter along with a hard disk that you want to boot from, you'd enable the BIOS.

- **Termination**

Make sure that the SCSI bus is terminated at both ends of the bus (and that it is only terminated at both ends. All other SCSI devices, including the adapter, that are not at the ends of the bus must have terminators removed/disabled. For information about termination, see the installation manual for the device.

Example: If you connect an external autoloader to an Adaptec 1542C Host Adapter and it is the only device on the adapter, install a terminator on the autoloader and enable termination on the host adapter.

On the other hand, if the external autoloader is not the last device on the bus, do NOT terminate the autoloader. Instead, remove the terminator from the autoloader and terminate the last device on the bus.

General guidelines for SCSI devices

The following applies to any SCSI device (e.g., CD-ROM, autoloader) attached to the host adapter.

- **Type of Connector**

Depending on the type of device, you connect it to a host adapter either internally or externally. Make sure that your cable has the right type of connector for the attachment you need to make.

Example: The cable attaching an internal autoloader to an Adaptec 1542C needs a standard 50-pin internal connector. But the cable for an external autoloader needs a 50-pin Centronics-style external connector.

- ***Length of Cable***

For an external device, use a SCSI cable that is less than 3 feet or very well shielded if it is longer. Longer SCSI cables may create noise on the line and cause the device or the host adapter to report errors.

- ***Termination***

Typically, only two devices on a SCSI bus must be terminated: the first and last device. See “Termination” in section “[SCSI host adapter.](#)”

- ***SCSI ID***

Make sure that the SCSI devices connected to a host adapter have a unique SCSI ID. Use SCSI ID 0 (zero) for a hard disk only.

Autoloader

- ***Type of autoloader***

Currently, LANtegrity supports the following autoloaders:

- Digital Storage Works TZ875N DLT and TZ877N DLT
- Emerald Auto 48-9040 DDS-2
- Hewlett Packard C1553A DDS-2 (the SureStore 12000e)
- Quantum DLT 2500 and 2700.

We recommend that you install the autoloader and disk(s) on separate host adapters. The autoloader must be on a SCSI host adapter; a disk can be on any type of adapter. For information about configuring the autoloader, see “[General guidelines for SCSI devices.](#)”

Custom Device Modules (CDM) for these autoloaders are shipped with LANtegrity. If you want to use another type of autoloader, contact Technical Support to see if it is compatible.

- ***Cleaning tape, if required***

If your autoloader requires regular cleanings, keep a cleaning tape in the highest numbered slot. (LANtegrity assumes the cleaning tape is in this slot and manages the cleaning cycles.) Unless these autoloaders are cleaned in a timely manner, they develop problems such as read/write errors.

Examples: The HP and Emerald autoloaders require a cleaning after a certain amount of usage; the Digital and Quantums do not.

- ***Blank tapes***

When first installing LANtegrity, place blank tapes in the slots of the autoloaders. (If your autoloader requires regular cleaning, you need to reserve one slot for a cleaning tape. See “Cleaning tape, if required” above.)

- ***Other items***

Check the connector, cable, termination, and SCSI ID using information in the previous section [“General guidelines for SCSI devices.”](#)

Installing NetWare 4.1 on a LANtegrity server

The bullets below display the checklist items and their details for installing NetWare 4.1 on the designated LANtegrity server.

- ***CD ROM reader***

On the server or network, mounted as a NetWare volume or DOS device.

- ***HIMEM.SYS***

In CONFIG.SYS, remove the line that installs HIMEM.SYS. If the line is not removed, you cannot install NetWare 4.1 correctly. This step is frequently overlooked by users trying to install NetWare 4.1.

- ***Filename format***

When using Novell's Installation Utility, select the Custom Installation option. When you are prompted for a filename format, select the NetWare file format, not the default, DOS.

- **Volumes**

We recommend that you create two volumes: 1) a small SYS: volume to minimize the time required to reboot; 2) a large second volume (e.g., CACHE) that uses the rest of the disk(s) for data storage. We recommend that you do not use the SYS: volume to store data. To ensure that you have adequate disk space for the second volume, see [“Requirements for a LANtegrity Server.”](#)

- **Name spaces**

If name spaces other than DOS (e.g., MAC, NFS*, or OS/2) exist on a Protected server, add them to the LANtegrity Server's data storage volume (e.g., CACHE). This allows LANtegrity to protect the non-DOS files.

To protect files in the NFS name space, use NFS version 2.0 or greater.

- **NCP Packet Signatures**

Make sure that the NCP Packet Signature option is OFF (the default) so that users can log in to stand-in services.

- **NetWare User Name and Password**

Make sure that there is a user account on the system with ADMIN privileges: unrestricted NDS privileges, access to all of the volumes, and no login restrictions. You need this account for the LANtegrity Server administrator.

- **LANtegrity in NDS tree**

When prompted for NetWare Directory Services (NDS) information, create an Organization container (O) for LANtegrity in the NDS tree.

If the LANtegrity Server is the first NetWare 4.1 server at your site:

Create an Organization container (O). Give it, for example, the name of your company (e.g., O=ACME). Within that container, create an Organizational Unit (OU) for LANtegrity (e.g., OU=LANtegrity) and install the LANtegrity Server (e.g., LS_ONE) within the OU.

For example: .CN=LS_ONE.OU=LANtegrity.O=ACME

If the LANtegrity Server is added to an existing NetWare 4.1 site: Create an OU for LANtegrity (e.g., OU = LANtegrity) and install the LANtegrity Server (e.g., LS_ONE) within the OU.

For example: .CN = LS_ONE. OU=LANtegrity. OU=MKTG. O=ACME

Novell recommends that you do not install a NetWare 4.1 server in an NDS tree that contains a 4.02 server.

- ***Stand-in Services for Bindery Logins***

If you want to support Bindery logins on a 4.x Protected server during stand-in, create a read-write replica of each NDS partition listed when you type `SET BINDERY CONTEXT` on the 4.x Protected server.

- ***Communication with Protected server***

After installing NetWare 4.1, you should see the Protected server when you type `DISPLAY SERVERS` from the system console. If you cannot see the server, there is a communication problem. Make sure that the proper drivers for the network cards are running on both servers.

Requirements for a Protected Server

The bullets below display the checklist items and their details for installing and configuring a protected server.

- **Memory**
2 MB of available memory.
- **Disk Space**
5 MB of hard disk space available for the LANtegrity Agent software.
- **Anti-Virus**
See “[Requirements for a LANtegrity Server](#)” for a list of compatible Anti-Virus programs.
- **NetWare**
NetWare 3.11, 3.12, or 4.1.
- **Names of Bindery objects**

On a 3.x Protected server, make sure that:

- the names of a Bindery objects do not include a period (.). NetWare cannot convert such Bindery objects into NDS objects
- no duplicate names exist in the Bindery
- no bindery objects have same name as Protected server.

Otherwise, LANtegrity cannot protect the data.

- **NetWare User Name and Password**
Make sure that there is a user account on the server with SUPERVISOR or ADMIN privileges to the entire system: no login restrictions or restrictions to accessing any files. You need this account to authenticate the Protected server.

- ***AUTOEXEC.NCF***

If an AUTOEXEC.NCF file exists in both the DOS partition and the SYS: volume, the FILE SERVER NAME and IPX INTERNAL NET ADDRESS must only appear in the AUTOEXEC.NCF file in the DOS partition. These commands cannot appear, even as comments, in the SYS: volume. Also, AUTOEXEC.NCF in the DOS partition must mount the SYS: volume with MOUNT SYS or MOUNT ALL.

- ***Network File System (NFS)***

To protect files in the NFS name space, use NFS version 2.0 or greater.

- ***Communication with LANtegrity Server***

You should see the LANtegrity Server when you type `DISPLAY SERVERS` from the system console. If you can't see the server, there's a communication problem. Verify that the proper drivers for the network cards are running on both servers.

Workstation for the LANtegrity Administrator

The bullets below display the checklist items and their details for installing and configuring a workstation for the LANtegrity Administrator.

- **Windows**
386 Enhanced mode Window or Windows for Workgroups, 3.1 or higher.
- **Client software**
NetWare client software such as NETX or VLM
- **Communication**
Ensure that the workstation can access the LANtegrity Server.
- **Windows for Workgroups**
If the workstation is running Windows for Workgroups:
 - In the [386ENH] section of the SYSTEM.INI file, add VNETWARE.386 and VIPX.386 to the NETWORK line.
 - In the [BOOT] section of the SYSTEM.INI file, make sure that the NETWORK.DRV=NETWARE.DRV statement is before any other NETWORK.DRV statement.
- **User Name and password**
To log into the LANtegrity Server as an administrator, you need ADMIN privileges to the entire server or be a member of the NDS group LANtegrity Administrators for LServer (LServer is the name of the LANtegrity Server).

Network

The bullets below display the checklist items and their details for installing and setting up LANtegrity on your network.

- **Routers**
You can have routers in your network. There are no special considerations for running LANtegrity in these systems. Just make sure that all users on each Protected server can **see** the LANtegrity Server so that they can log in during stand-in.

Installing and Setting Up LANtegrity

LANtegrity server and protected server

The bullets below display the checklist items and their details for installing and setting up a LANtegrity server and protected server.

- ***Same tree***

To authenticate a Protected server and protect it, the server must be in the same tree as the LANtegrity Server (a NetWare login restriction).

- ***Name of User and Install Volume***

When using the LANtegrity INSTALL program, the administrator's user name cannot contain any of the following characters: ! @ # % ^ & * () +

If the user name contains any of these characters, create a temporary user name for the installation and delete it after you finish.

Also, the name of volume where you are going to install LANtegrity Server or Agent software cannot include any of the characters above.

- ***Overwriting NLMs***

The LANtegrity INSTALL program may ask to overwrite/update NLMs. Unless the version on your server is later than the version on our CD, allow the overwrite or else LANtegrity may not work correctly. You may also want to record the names of the original NLMs. Call Technical Support if you have any questions.

Protected server only

The bullets below display the checklist items and their details for installing and setting up a protected server.

- ***NDS vs. Bindery Login***

When using LANtegrity INSTALL, decide if you need to log in as an NDS or Bindery user. Log in as:

Nds User if you are installing from a NetWare 4.1 server to a 4.1 Protected server in the same tree (e.g., .ADMIN.ACME)

Bindery User (e.g., SUPERVISOR) if you are installing from a:

- ❑ NetWare 4.1 server to a 3.x Protected server.
- ❑ NetWare 4.1 server to a 4.1 Protected server in a different tree. The bindery context must be set on the target 4.1 server so you can log in and complete the installation.
- ❑ NetWare 3.x server. If the target Protected server is a 4.1 server, the bindery context must be set for the installation to succeed.

■ ***If NetWare 3.11***

After you install LANtegrity on a NetWare 3.11 Protected server, you must reboot the server before you can run LANtegrity SETUP.

■ ***Pathname to Server.exe***

If the pathname to `Server.exe` contains any of the following characters, you will have to move it to another location: `! @ # % ^ & * () +`

■ ***Starting the serve***

Instead of starting the Protected server with `SERVER.EXE`, use `LSSTART.BAT`, which LANtegrity adds to the DOS NetWare directory and to `AUTOEXEC.BAT`. See *Read Me First* for more information.

3

Installing and Setting Up LANtegrity

Overview

Once you've made sure that your system meets the requirements described in the *Configuration and Installation Notes*, you can install and set up LANtegrity. When your systems are configured correctly, installing and setting up LANtegrity is a simple process.


LANtegrity consists of three software components:

- The LANtegrity Server NLM, `LSSERVER.NLM`, for a dedicated NetWare 4 server, called the LANtegrity Server.
- The LANtegrity agent NLMs, `LSAGENT.NLM` and `LSSTART.NLM`, for each of the NetWare 3 and NetWare 4 servers you want to protect. Each server is called a protected server.
- The LANtegrity Administrator application, for one or more Windows workstations. You can use this application to monitor and control LANtegrity operations.

You install and setup these components using the LANtegrity `INSTALL` and `SETUP` NLMs. Take a few minutes to gather the information in the installation checklist. Then:

- Use `INSTALL` to copy the LANtegrity software to the designated LANtegrity Server and each server it will protect.
- LANtegrity comes with the latest Novell NetWare updates. If the `INSTALL` program detects an out-of-date NLM, it prompts you to install the newer one. Accept the updates to ensure consistent operation.

- Use LANtegrity SETUP on the LANtegrity Server and protected server.
- SETUP also makes changes to your startup files. You have the option to accept all changes at once or to be prompted to confirm each one. In a few instances, you may have to make the changes manually.
- Set up the LANtegrity Administrator application.
- Most prompts in INSTALL and SETUP offer default values. Either press ENTER to accept the default or type a new value.

 *Depending on what needs to change, you may not see all of the screens described.*


Checklist

Have the following information handy as you install, set up, and configure LANtegrity. If you are not familiar with NetWare Directory Services (NDS), you can use the user name and password below. However, if you are familiar with NDS, you can substitute other values.

You will be asked to supply...	Enter...
User name/password for authenticating the LANtegrity Server This is the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity Server.	Admin.INTEGRITY/admin
Port address of the host adapter for the auto-loader on the LANtegrity Server.	Your LAN-specific information.
User name and password for authenticating each protected server. For NetWare 4 servers this is the distinguished name and password you entered above. For NetWare 3 servers this is the name and password of a supervisor-equivalent.	Your LAN-specific information.
For each protected server, a unique alternate IPX address. The IPX address is a hexadecimal number (base 16, using the numbers 0-9 and the letters A-F), from 1-8 digits. We suggest adopting a naming convention (for example, prefix the original address with a fixed code such as FF).	Your LAN-specific information.
The distinguished name of the NDS container used to hold the Lantegrity server object.	
Do other applications running on the protected servers set and clear the archive bit?	
A Server Bindery Context if protecting a NetWare 4 server that supports Bindery logins.	
The time needed to reboot each protected server.	

Installing LANtegrity Server Software

To install LANtegrity on a NetWare 4 server, you need a CD-ROM drive on the server or network, mounted as a DOS device or a volume. Follow the procedure below to install LANtegrity server software.


 *If you are installing LANtegrity from a NetWare 3.11 server, make sure that it has Novell's latest NWSNUT.NLM.*

- | Step | Action |
|------|--|
| 1. | Insert the LANtegrity CD-ROM into the CD-ROM drive. |
| 2. | At the console for the CD-ROM server, load the LANtegrity INSTALL NLM. For example, if you mounted the CD-ROM as a volume, type:
<code>LOAD NICD:INSTALL.</code>

Response: Displays the Main Menu. |
| 3. | Choose 'Install LANtegrity Server'.

Response: Lists the accessible servers. |
| 4. | Select the NetWare 4.10 server that you'll use as the LANtegrity Server. If installing over a network:

Response: Enter name of user <code>Username</code> .


 <i>It may also prompt for a password.</i> |
| 5. | Type a valid user name (for example, .ADMIN.INTEGRITY). The user name must be a supervisor-equivalent, able to write to the destination path (below), and to create/modify files in SYS:SYSTEM and SYS:ETC.

Response: Specify path for the LANtegrity Server software:
<code>SYS:\LANTEG</code> |
| 6. | Accept the default SYS:\LANTEG or enter another destination path. |

Response:

- If INSTALL needs to overwrite system files, it displays the 'Select handling of overwrites' menu.
- If TIRPC is detected, INSTALL displays a message that it needs to overwrite SYS:ETC\RPCNET.CFG or SYS:NETWARE\SERVICES.CFG. The original files are saved.

7. Accept the overwrites and record the names of the files in case you want to remove LANtegrity.

 *We recommend that you accept the overwrites to ensure consistent operation.*

Response: Displays an Installation Status message stating that the installation is complete.



8. Press ENTER to continue.

Response: Displays the Main Menu.

9. To install the protected server software, continue to Step 2 in the next section.

Installing Protected Server Software

Follow the procedure below to install protected server software.

Step	Action
1.	<p>If the LANtegrity INSTALL NLM is not loaded, load it from the CD-ROM.</p> <p> See Steps 1-2 in the previous section for details.</p> <p>Response: Displays Main Menu.</p>
2.	<p>Choose 'Install Protected Server'.</p> <p>Response: Lists all of the accessible servers.</p>
3.	<p>Select the server that you want to protect.</p> <p>Response: Enter name of user.</p> <p> It may also prompt for a password.</p>
4.	<p>Type a valid user name. The user name must be a supervisor-equivalent, able to write to the destination path (below), and to create/modify files in SYS:SYSTEM and SYS:ETC.</p> <p>Response: Specify path for the Protected Server software: SYS:\LANTEG</p>
5.	<p>Accept the default SYS:\LANTEG or enter another destination path.</p> <p>Response:</p> <ul style="list-style-type: none">■ If INSTALL needs to overwrite system files, it displays the Select handling of overwrites menu.■ If TIRPC is detected, INSTALL displays message that it needs to overwrite SYS:ETC\RPCNET.CFG or SYS:NETWARE\SERVERICES.CFG. The original files are saved.

6. Accept the overwrites and record the names of the files in case you wish to remove LANtegrity.



We recommend that you accept the overwrites to ensure consistent operation.

Response: Displays an Installation Status message stating that the installation is complete.

7. Press ENTER to continue.



Response: Displays the Main Menu.

8. Do one of the following:

- If you want to install the protected server software on another server, repeat Steps 2-7.
- If you want to set up the LANtegrity Server, choose Exit and continue to the next section.

Setting Up a LANtegrity Server

Follow the procedure below to set up a LANtegrity server.

Step	Action
1.	At the LANtegrity Server's system console or RCONSOLE, load SETUP from the LANtegrity product directory. For example, if you selected the default directory, type: <code>LOAD SYS:LANTEG\SETUP</code> .
	Response: Choose the volume for the data storage.
2.	Choose the volume that you set up for data storage, for example, CACHE . Do not use SYS for data storage.
	Response: Where is the local SERVER.EXE program loaded from?
3.	Press ENTER to accept the default or enter the correct path.
	Response: Displays the Host adapter menu.
4.	Choose the host adapter configuration for the autoloader on the LANtegrity Server. If the Host adapter for your autoloader is not listed, choose 'No predefined host adapter'. SETUP adds a comment line to AUTOEXEC.NCF that indicates where you have to add information about the autoloader.
	 <i>You may be prompted for the 'Port address of Host Adapter', enter the correct port address.</i>
	Response: Displays the Tape Device menu.
5.	Choose the tape device on the LANtegrity Server. If your tape device is not listed, choose No predefined tape device.
	 <i>Messages may display periodically throughout the remainder of this procedure informing you of any system changes and updates. Press enter to continue.</i>
	Response: [PATH] AUTOEXEC.NCF requires modifications.

6. Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.

Response: `[PATH] STARTUP.NCF` requires modifications.

7. Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.

Response: Displays the Setup Status message stating that the setup is complete.

8. Press ENTER to continue.

Response: Displays the Main Menu.

9. Choose Exit.

Response: Displays a LANtegrity Setup message that tells you to cold boot the server.

10. Press ENTER to return to the console prompt.

11. Cold boot the server. Type `down` and then exit. At the DOS prompt, press Reset.

Response: Displays a LANtegrity Status message: LANtegrity Server operating.

12. Add blank tapes to the autoloader. If your autoloader requires a cleaning tape, insert a new one into the last slot.

Setting Up a Protected Server

Follow the procedure below to set up a protected server.

Step

Action

1. At the LANtegrity Server's system console or RCONSOLE, type:
`LOAD SYS:LANTEG\SETUP.`

Response: Displays a list of all the servers visible to the protected server.

2. Select the LANtegrity Server that will protect this server.


Response: Where is the local SERVER.EXE program loaded from?

3. Press ENTER to accept the default or enter the correct path.

Response: Displays a message about the alternate IPX Net address and the original IPX Net address followed by: `Enter alternate internal IPX address`


4. Type the unique alternate IPX address for the protected server.

See the Checklist for more information.

 *The protected server uses the alternate IPX address when it reboots during stand-in. It also needs an alternate name, which SETUP creates by prefixing the original name with _PS_. The alternates are stored in AUTOEXEC.NCF.*

Response: `[PATH]AUTOEXEC.NCF` requires modifications.

5. Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.


 *Messages may display periodically throughout the remainder of this procedure informing you of any system changes and updates. Press enter to continue.*

Response: *[PATH]STARTUP.NCF* requires modifications.

6. Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.

Response: *[PATH]AUTOEXEC.BAT* requires modifications.

7. Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.

 *SETUP adds LSSTART.BAT. It automates the reboot and ensures that the server is not brought up under its normal name during stand in. If you manually boot the server, type LSSTART, not SERVER.*

Response: Displays the Setup Status message showing that the setup is complete.

8. Press ENTER to continue.

Response: Displays the Main Menu.


9. Choose Exit.

Response: Displays a LANtegrity Setup message that tells you to cold boot the server.

10. Press ENTER to return to the console prompt.

11. Cold boot the server. At the console prompt, type `down` and then exit. At the DOS prompt, press Reset.

Response: Displays the LANtegrity Status message 'LANtegrity Agent connected and operating'.

 *Make sure that you can start NetWare with LSSTART.BAT, located in the same place as SERVER.EXE.*

Setting Up the LANtegrity Administrator

Use the following procedure to set up the LANtegrity Administrator.

Step	Action
1.	Using a NetWare client workstation, start Windows and connect to the LANtegrity Server.
2.	Map a drive to the LANtegrity product directory SYS:\LANTEG.
3.	Go to the Windows Program Manager and choose File/Run .
4.	In the Run dialog box, type <i>drive</i> :setup.exe, where <i>drive</i> is the drive mapped to the LANtegrity product directory and click OK.
5.	The LANtegrity Administrator Setup dialog box appears and prompts you to enter the location of the LANtegrity Administrator source files. If you have not moved SETUP.EXE, accept the default.
6.	Click Continue. Response: A dialog box appears. It asks you where on the workstation to install the software. The default is C:\LANTEG.
7.	Follow the instructions on the screen to create the Program Manager Group and complete the installation.

Removing LANtegrity

If you need to remove LANtegrity, perform the following steps:

- | Step | Action |
|------|---|
| 1. | At the LANtegrity Server, unload the LANtegrity Server NLM, LSSERVER.NLM. |
| 2. | At a protected server, unload the protected server NLM, LSAGENT.NLM. |
| 3. | On the LANtegrity Server, load the LANtegrity Setup NLM, SETUP.NLM. |

It is located where you loaded the LANtegrity software.



Figure 3-1. LANtegrity Main Menu

- From the Main Menu, choose **Remove LANtegrity Server**.
- On a protected server, load SETUP.NLM. It is located where you loaded the LANtegrity software.



Figure 3-2. Removing protected server

- From the Main Menu, choose **Remove Protected Server**.

You can quickly place your servers under LANtegrity protection if you retain most of the defaults. LANtegrity's continuous protection is designed to provide maximum protection coverage for your servers with no changes required on your part. To initiate protection using the following steps:

- Log into the LANtegrity Server from the LANtegrity Administrator.
- Configure the LANtegrity Server.
- Authenticate each protected server and initiate protection.

This chapter describes how to get started using the default values. For information about how to change the defaults, see the *Administrator's Guide*.

Initial Login to New LANtegrity Server

A single LANtegrity Administrator interface can monitor and control the operations of any LANtegrity Server on your network.

Follow the procedure below to log into a LANtegrity Server.



Step

Action


1. Double click the LANtegrity Administrator icon in the Program Manager window.

Response: The Login to LANtegrity Server dialog appears.



Figure 4-1. Logging into a LANtegrity Server

2. In the list box, select the LANtegrity Server you want to log into.
3. Type the user name and password.

 *To log in as the administrator for the first time, use the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity Server.*

4. Click Login.

Response: The first time you log into a newly installed LANtegrity server a message box is displayed.



Figure 4-2. LANtegrity Administrator message box

5. Click OK.

Response: LANtegrity opens the LANtegrity Administrator desktop and the Configure LANtegrity Server panel where you enter this information about a LANtegrity Server.

The following figure illustrates the LANtegrity Administrator desktop and the Configure LANtegrity Server panel.



Figure 4-3. LANtegrity Administrator on server: BOS5

The next section describes how to fill in the required fields.

If for any reason you close the Configure LANtegrity Server panel before filling in all the information, you can open the panel as follows:



1. Click the General Configuration button or select **Tools/General Configuration**. LANtegrity displays the General Configuration window.



2. In the list box on the left, select LANtegrity Server. LANtegrity displays the Configure LANtegrity Server panel.

Configuring the LANtegrity Server

Minimally, you need to supply the information for the following fields on the Configure Protected Server window:

- LANtegrity Server's NetWare user name and password.
- NDS container that contains the LANtegrity Server object. This is used as the NDS location for Protected Bindery information.
- The protection method used by LANtegrity, i.e., whether or not the archive bit is used to detect changes.

You can accept the default values for **Stand-in File Retrieval** and **Continuous Protection Logging** until you have a chance to evaluate them. See the *Administrator's Guide* for information.

Entering the server's name and password

LANtegrity uses the name you enter to access NDS data, access the LANtegrity Server's file system, and protect files during stand-in. Follow the procedure below to enter the LANtegrity Server's user name/password.

Step	Action
1.	<p>On the Configure LANtegrity Server panel, type the user name in the Distinguished Name input box.</p> <p>The user name should be the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity Server.</p>
2.	<p>Type the password for the user name in the 'Password' input box.</p> <p>If you make a typing error, delete the contents of the input box and start again.</p>

Protecting a NetWare 3 Bindery

You can identify the NDS container in which to store protected NetWare 3 Bindery objects. To do this, specify the distinguished name of the NDS container the holds the LANtegrity Server objects.

LANtegrity then does the following:

- Creates two OU's for each NetWare 3x protected server in the NDS container, naming them LANtegrity Bindery A for protected server name and LANtegrity Bindery B for protected server name.
- Converts the NetWare 3 Bindery objects to NetWare 4 NDS objects.
- Protects the files that contain Bindery information to tape.

Follow the procedure below to identify the Bindery Protection Context.

Step

Action



1. Click the General Configuration button or select **Tools/General Configuration**.

Response: LANtegrity displays the General Configuration window.



2. In the list box on the left, select 'LANtegrity Server'.

Response: LANtegrity displays the Configure LANtegrity Server panel.

3. Type the distinguished name of the NDS container that holds the LANtegrity Server object in the 'NDS location for Protected Bindery' input box.

Specifying the protection method

By default, LANtegrity uses a file's archive bit to detect if the file has been modified on a protected server and, if so, to copy it to the LANtegrity Server. LANtegrity clears the attribute of each file that it copies. If your protected servers load other NLMS that set or clear the archive bit, you will need to indicate to the LANtegrity Server that it should ignore the archive bit and instead use an alternate method of detecting change.

Follow the procedure below to change the protection method.

Step**Action**

1. Click the General Configuration button or select **Tools/General Configuration**.

Response: LANtegrity displays the General Configuration window.



2. In the list box on the left, select 'LANtegrity Server'.

Response: LANtegrity displays the Configure LANtegrity Server panel.

3. Select 'Ignore' to select the Archive Bit method.

Closing the Configure LANtegrity panel

When you complete all changes to this panel, click Close or click on another selection in the list box on the left. LANtegrity verifies and saves changes to the configuration panel. You do not have to have the changed panel displayed when you click Close. Next, you configure each protected server.

Configuring a Protected Server

To support communications between the LANtegrity Server and its protected servers, you authenticate the protected servers by supplying the user name and password for each server.

Authenticating a server and enabling protection

Follow the procedure below to authenticate a Protected Server and enable protection.

Step

Action



1. Click the General Configuration button or select **Tools/General Configuration**.

Response: LANtegrity displays the General Configuration window.



2. In the list box on the left, select 'Protected Servers'.

Response: LANtegrity displays the Configure Protected Servers panel. It shows a list of the NetWare file servers that were setup as protected servers of the LANtegrity Server.

You will not see the protected server unless it is connected to the LANtegrity Server on the network and the protected server's LANtegrity agent screen is displaying the screen in Figure 4-4.



Figure 4-4. LANtegrity Status

Action: You can identify the status of the servers by checking the icons next to their names.

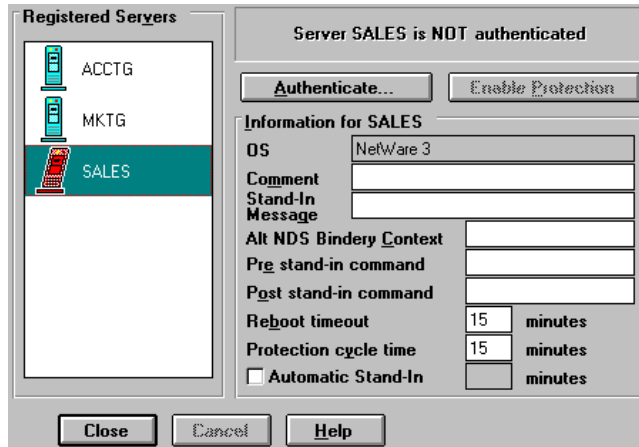







Figure 4-5. Absent from Word File


 *Automatic stand-in is not configured as a default.*

The following table describes the icons.

This icon...	Indicates that the server is...
	Online and fully protected.
	Authenticated and protection enabled but not yet verified; therefore, the server is not ready for stand-in service.
	Agent loaded but not authenticated; therefore, the server is not ready for stand-in service.
	LANtegrity agent is loaded but server is not authenticated.

3. Select the protected server you want to authenticate and click Authenticate.
4. Do one of the following:
 - For a NetWare 3 server, type the name of a supervisor-equivalent and enter the appropriate password.
 - For a NetWare 4 server, type the distinguished name of the administrator you specified when you installed NetWare on your LANtegrity Server and enter the appropriate password.
5. Click OK to register the user name and password with the LANtegrity Server and return to the Configure Protected Servers panel.
6. Click Enable Protection to start protecting the selected server.

Response: The icon for the server displays a red X until an initial verify job completes successfully. Depending on the amount of data on the server, the X could remain on the icon for several hours or for several days.

 *Until the initial verify job for the protected server completes successfully, the LANtegrity Server cannot stand-in for it. By default, a verify job runs nightly at 7PM.*

7. Do one of the following:
 - For a NetWare 3 server you must enter an Alternate NDS Bindery Context to enable protection of the server's Bindery. Type the distinguished name of the NDS container that holds the LANtegrity Server object.
 - For a NetWare 4 server enter a Server Bindery Context to enable Bindery logins to that server while LANtegrity stands in for it. Enter the first distinguished name that appears in a SET BINDERY CONTEXT command on the protected server.
8. Check the value for **Reboot timeout** and increase it if necessary.

The reboot timeout is the amount of time that the LANtegrity Server waits after synchronization for the selected protected server to reboot before it returns to stand-in.



The amount of time must be approximately twice the time it takes to reboot the selected server; otherwise the LANtegrity Server will not be able to exit stand-in reliably.

Closing the Configure Protected Server panel

When you complete all changes to this panel, click Close or click on another selection in the list box on the left. LANtegrity verifies and saves changes to the configuration panel. You do not have to have the changed panel displayed when you click Close.

What Next?

Refer to the *LANtegrity Administrator's Guide* Chapter 2 on *Protecting Server Data* in particular to understand your protection options and to decide if you need to customize LANtegrity for your environment.

A

Stand-In Printing Services

This appendix describes how to set up a LANtegrity Server to provide stand-in printing services for NetWare 3.x and NetWare 4.x protected servers.

To use the instructions, you'll need:

- A working knowledge of NDS, the HP JetDirect Administration utility (JETADMIN), and the LANtegrity Organizational Unit (OU) in the NDS tree.
- For information about the LANtegrity OU, see [Chapter 4, "Getting Started."](#)
- The LANtegrity software installed and functioning correctly on a properly configured LANtegrity Server.
- VLMs that are provided with NetWare 4.1 installed on the administrator's workstation.
- NWADMIN 4.10.2 or later and PCONSOLE 4.1.

For a NetWare 3.x Protected Server

You can set up stand-in printing services on a LANtegrity Server for a NetWare 3.x protected server if the printer is:

- Attached directly to a workstation and configured as remote.
- Any printer directly attached to a protected server is not available when the server is down.
- An HP JetDirect printer in Queue Server or Remote Printer mode.

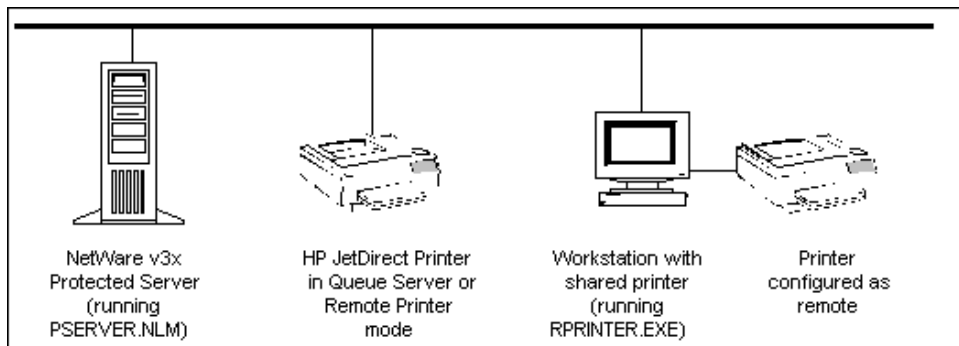


Figure A-1. NetWare 3.x printer configurations you can support during stand-in

The procedures include:

1. Set up an **alternate Bindery context** for each 3.x protected server with user and queue objects.

The alternate Bindery context is the Organizational Unit (OU) for stand-in printing that you create in the NDS tree on the LANtegrity Server and then configure in LANtegrity.

2. Create, if necessary, print server objects in the alternate Bindery context.


You set up print server objects for shared printers attached to a workstation and HP JetDirect printers in Remote Printer mode (not Queue Server mode).

3. Create pre- and post-stand-in commands to handle print NLMs.
4. Configure LANtegrity with the distinguished name of the alternate Bindery context and the pre- and post-stand-in commands.

Creating an alternate bindery context

Create an alternate Bindery context for each NetWare 3.x Protected Server that requires stand-in printing services.

Follow the procedure below to create an alternate Bindery context.

Step	Action
1.	Within the LANtegrity OU, create an OU for stand-in printing for each protected server. For example, if you want the LANtegrity Server to provide printing services for the NetWare 3.x server SALES during stand-in, create an OU in the LANtegrity OU called <i>Stand-In Printing for SALES</i> .
	 <i>Later, you enter the name of this OU on the Configure Protected Servers panel. See “Configuring LANtegrity” in this section.</i>
2.	Within the stand-in printing OU, create an identically named 4.1 print queue for each print queue used on the protected server.
3.	Specify the users and the volume for print spooling as follows: <ul style="list-style-type: none">■ Users. Add the names of both LANtegrity Bindery OUs for the server. For example, for the server SALES, add <i>LANtegrity Bindery A</i> and <i>LANtegrity Bindery B for SALES</i> as print queue users.■ Volume. Specify the SYS: volume of the LANtegrity Server.
4.	If you have an HP Jet Direct printer in Queue Server mode, continue to the next section.

For all other printing devices, refer to “[Creating alternate print server objects.](#)”

Completing HP JetDirect set-up

Use the procedures in this section to:


- Make the 4.1 print queue that you just created (see previous section) visible to Bindery-based printers.
- Add the 4.1 print queue to the queue list of the HP print server.
- Configure LANtegrity with the name of the alternate bindery context.

Follow the procedure to complete set-up for HP JetDirect in Queue Server Mode.

Step

Action

1. At the server console, note the current Bindery context of the server by typing: Set Bindery Context.

 *You'll need the information at the end of this procedure so that you can reset the context to its current setting.*


2. Change the Bindery context to the alternate Bindery context (OU), which you created in the previous section. For example, to set the context to the OU called *Stand-In Printing for SALES* in the Organization *ACME*, type:

```
Set Bindery Context =.OU=Stand-In Printing for  
SALES.OU=Lantegrity.O=ACME
```

Response: The queue should now be visible to the HP print server.

3. Use JETADMIN to view the queue and add it to the queue list of the HP print server.

Response: This step also adds the print server object and the Everyone user group to the stand-in printing OU.

 *If you cannot view the queue from JETADMIN, the queue is set up incorrectly. Repeat Steps 1-3.*

4. Exit JETADMIN and reset the Bindery context to its original setting, which you noted in Step 1.

5. Configure LANtegrity with the name of the alternate Bindery context as follows:

- Open the LANtegrity Administrator and click on the General Configuration tool.
- Open the Configure Protected Servers panel and select the NetWare 3.x protected server.
- Type the distinguished name of the alternate Bindery context in Alt NDS Bindery Context.

For example, to enter the distinguished name of the sample alternate Bindery context on page 45, type:


```
.stand_in_printing_for_SALES.lantegrity.acme
```

Response: The LANtegrity Server can now provide stand-in services for an HP JetDirect printer in Queue Server mode.

Creating alternate print server objects

Use these procedures if the NetWare 3.x protected server uses a print server to manage print services with the following devices:

- HP JetDirect printers in Remote Printer mode

 *Unlike the HP JetDirect printer in Queue Server mode, a JetDirect printer in Remote Printer mode requires a separate print server.*


- Printers attached to a workstation on the network.

Follow the procedure below to create an alternate printer server.

Step

Action

1. If you are using RPRINTER.EXE on a workstation to connect its printer to a print server on the NetWare 3.x server, we recommend that you replace it with NPRINTER.EXE.

 *RPRINTER does not work reliably with NetWare 4.x, which runs on the LANtegrity Server. On the other hand, NPRINTER.EXE is compatible with both NetWare 3.x and 4.x.*

- Replace all references to RPRINTER.EXE in batch files with NPRINTER.EXE. Then, copy the following files to the workstation:
 - IBM_AIO.OVL
 - IBM_RUN.OVL
 - NPRINTER.EXE
 - NPRINTER.HLP
 - NPRINTER.MSG
 - TEXTUTIL.HEP
 - TEXTUTIL.IDX
 - TEXTUTIL.MSG

2. In the alternate Bindery context on the LANtegrity Server, create a print server object for each print server used on a NetWare 3.x protected server. Use the same name for the alternate printer server and its counterpart on the protected server.

For example, if the print server on the protected server SALES is named SALES_PSERV, create an alternate print server named SALES_PSERV in *Stand-In Printing for SALES*.

3. For each print server you created, assign the appropriate print queue to its service list.
4. Create and define each printer object as remote.
5. Ensure that a remote printer can connect to the PSERVER.NLM when it is running on the LANtegrity Server.

Creating pre- and post-stand-in commands

You can configure the LANtegrity Server to automatically load and unload PSERVER.NLM and NPRINTER.NLM during stand-in with pre- and post-stand-in command files. PSERVER loads the print management software; NPRINTER loads the parallel port driver for the remote printer.

Use this procedure if you created an alternate print server (see previous section) for the LANtegrity Server.

Step

Action

1. Using any text editor, create a pre-stand-in NCF batch file to load the appropriate NLMs for each protected server.

If the printer is...	Load...
An HP JetDirect in Remote Printer mode	PSERVER.NLM and NPRINTER.NLM
connected to workstation running NPRINTER.EXE	PSERVER.NLM

For example, to create an NCF file called SALES.LD.NCF that loads the print server SALES_PSERV and NPRINTER for the HP JetDirect printer number 5 in Queue Server mode, type:

```
LOAD PSERVER .cn= SALES_PSERV
.ou=Stand_In_Printing_for_SALES .ou=Lanteg-
rity.o=ACME
```

```
LOAD NPRINTER .cn=SALES_PSERV.ou=
Stand_In_Printing_for_SALES .ou=Lantegrity.o=ACME 5
```

2. Create a post-stand-in NCF file for the protected server, which unloads PSERVER.NLM and NPRINTER when the LANtegrity Server exits stand-in. For example, create a file that contains the command:
UNLOAD PSERVER.

 *Unloading PSERVER also unloads NPRINTER.*

3. Save the pre- and post-stand-in NCF files to SYS: SYSTEM of the LANtegrity server.
4. Configure the protected server in LANtegrity with the pre- and post-stand-in commands (see the next section).

Configuring LANtegrity

To complete the set up of stand-in printing, configure LANtegrity with the name of the alternate Bindery context and, if you created them, the pre- and post-stand-in commands (see previous section).

Use this procedure for each NetWare 3.x protected server that requires stand-in services.

Step	Action
1.	Open the LANtegrity Administrator and click on the General Configuration tool.
2.	Open the Configure Protected Servers panel and select the NetWare 3.x protected server.
3.	Type the distinguished name of the alternate Bindery context in Alt NDS Bindery Context.

For example, to enter the distinguished name of the sample alternate Bindery context on page 45, type:

```
.stand_in_printing_for_SALES.lantegrity.acme
```

4. If you created pre- and post-stand-in commands to load NLMs, type the names of the commands in the appropriate fields.

For a NetWare 4.1 Protected Server

A NetWare 4.x protected server may provide printing services for NDS as well as Bindery-based printing. You can set up stand-in services on the LANtegrity Server for both types of printing.


This section is divided into two parts:

- Setting Up Stand-in Services for NDS printing.

Use these steps if you have an HP JetDirect in Remote Printer mode or if the printer is attached to a workstation or file server.

- Setting Up Stand-in Services for Bindery-based printing.

Use these steps if you have an HP JetDirect in Queue Server mode.

 *The instructions assume that users capture to a printer rather than to a print queue. When capturing to a printer, users do not have to change their print set ups.*

Setting up stand-in services for NDS printing

The LANtegrity Server can provide stand-in printing services for a NetWare 4.x protected server if a print queue, which spools to a volume on the protected server, is assigned to:

- A printer directly attached to a workstation or another file server. You must specify the printer as remotely attached.

Any printer directly attached to a protected server is not available when the server is down.

- An HP JetDirect printer configured in Remote Printer mode.

If the HP JetDirect printer is configured in Queue Server mode, refer to “[Setting up stand-in services for HP JetDirect in queue mode.](#)”

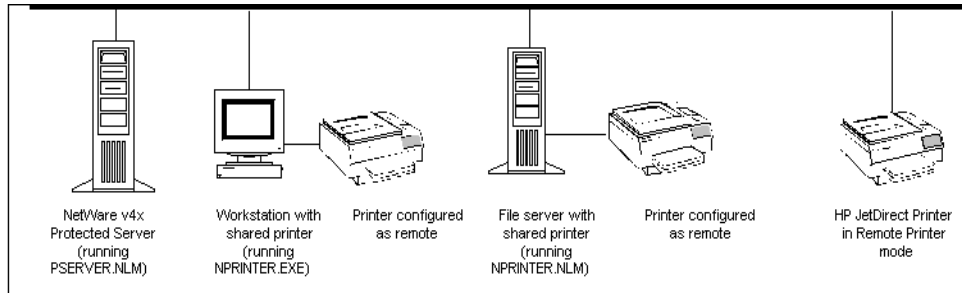



Figure A-2. NDS printer configurations you can support during stand-in

The procedures include:

- Creating alternate print queue and print server objects.
- Creating pre- and post-stand-in commands to handle print NLMs and configuring them in LANtegrity.
- If you have an HP JetDirect printer in Remote Printer mode, using JETADMIN to add the alternate print queue to the printer's service list.

Creating alternate print queue and print server objects

Follow the procedure below to create alternate print queue and print server objects.

- | Step | Action |
|------|--|
| 1. | Make note of the names of any NPRINT print queues and their associated print servers (PSERVER.NLM) that are running on the protected servers. |
| |  <i>You'll need this information to associate objects correctly and to ensure that their names are not duplicated in NDS.</i> |
| 2. | Log in to the LANtegrity Server and start the NetWare Administrator. |
| 3. | Select an NDS context that is accessible to NDS users. |

4. Create an alternate print queue and print server object for each queue and print server used on the protected server.

When you create the print objects, use these guidelines:

- Give each queue and print server a unique name.
- To make the name easy to recognize, we suggest that you name the alternate object like its counterpart on the protected server. For example, if you have a queue called MKT_Q, name the alternate queue ALTMKT_Q.
- Define the SYS: volume on the LANtegrity Server for print spooling.
- Add the alternate print queue(s) to the Queue service list of the existing printer object.

5. Repeat this procedure as necessary to assign all of the alternate queues to printers.

Creating pre- and post-stand-in commands

You can configure the LANtegrity Server to automatically load and unload PSERVER.NLM and NPRINTER.NLM during stand-in with pre- and post-stand-in command files. PSERVER loads the print management software; NPRINTER loads the parallel port driver for the remote printer.

Step

Action

1. Using any text editor, create a pre-stand-in NCF file to load PSERVER.NLM and NPRINTER.NLM for each NetWare 4.1 protected server.

For example, create an NCF file for SALES that loads the print server SALES_PSERV and associates it with printer number 5:

```
LOAD PSERVER .cn=SALES_PSERV.ou=Bindery Printing for
SALES.o=ACME
```

```
LOAD NPRINT .cn=SALES_PSERV.ou=Bindery Printing
for SALES.o=ACME 5
```

2. Create a post-stand-in NCF file for the protected server, which unloads PSERVER.NLM and NPRINT.NLM when the LANtegrity Server exits stand-in. For example, create a file that contains the command
UNLOAD PSERVER.

 *Unloading PSERVER automatically unloads NPRINT.*

3. Save the pre- and post-stand-in NCF files to the SYSTEM directory on the SYS: volume of the LANtegrity Server.

Configuring LANtegrity

To complete the set up of stand-in printing, configure LANtegrity with the name of the pre- and post-stand-in commands. Use this procedure for each NetWare 4.x protected server that requires stand-in services.

Step	Action
1.	Open the LANtegrity Administrator and click on the General Configuration tool.
2.	Open the Configure Protected Servers panel and select the NetWare 4.x protected server.
3.	Type the names of the pre- and post-stand-in commands that you created (see previous section) in the appropriate fields.

Additional steps for HP JetDirect in remote mode

If you have an HP JetDirect printer in Remote Printer mode, you also need to do these steps.

1. Start the HP JetAdmin utility program from a workstation running Windows.
2. Select the print server and select the Configuration icon.
3. Attach to the LANtegrity Server.

4. In the Configuration window, select the printer as a remote printer and add the names of the alternate print queues.

Setting up stand-in services for HP JetDirect in queue mode

In an NDS environment, you may have bindery-based printers, such as the HP JetDirect printer in Queue Server mode, that access a queue on a NetWare 4.x protected server.

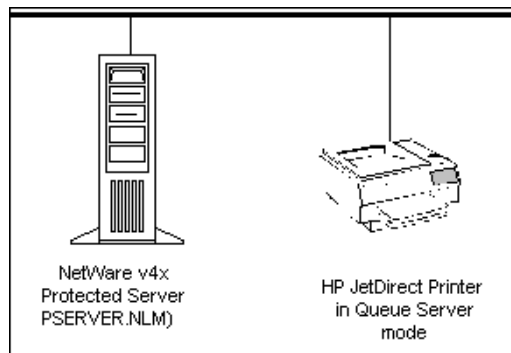



Figure A-3. HP JetDirect printer in Queue Server mode

The procedures for setting up stand-in printing services for the HP JetDirect printer in Queue Server mode include:

- Set up an **alternate Bindery context** for each protected server that supports an HP JetDirect printer in Queue Server mode.

The alternate Bindery context is an Organizational Unit (OU) for stand-in printing that you create in the NDS replica and then configure in LANtegrity.

- Use HP JETADMIN to add the alternate print queue to the printer's service list.
- Create pre- and post-stand-in commands to handle print NLMs and configuring them in LANtegrity.

 *Make sure that the LANtegrity Server has a read/write replica of the NDS partition for the context you want to set.*

For information about providing stand-in services for a 4.x Protected Server that supports NDS printing, see [“Setting up stand-in services for NDS printing.”](#)


Step

Action

1. Start the NetWare Administrator and log into the LANtegrity Server.
2. Within the LANtegrity OU, create an OU for stand-in printing for the NetWare 4.x Protected Server that supports bindery-based printing services.

For example, if you want the LANtegrity Server to provide stand-in printing services for the NetWare 4.x server SALES, create an OU called *Bindery Printing for SALES* in the LANtegrity OU.

3. Within the Bindery printing OU, create an identically named print queue for each print queue used on the 4.x protected server.

 *Specify the SYS: volume on the LANtegrity Server for print spooling.*

4. Create additional queues if necessary to duplicate the printing services provided by the protected server.


Setting the bindery context on the LANtegrity server

To make the alternate print queues that you just created visible to Bindery users, perform this procedure. For information about creating an alternate print queue, see the previous section.

Step

Action

1. At the server console, note the current Bindery context of the server by typing: Set Bindery Context.

 *You'll need the information at the end of this procedure so that you can reset the context to its current setting.*

2. Change the Bindery context to the alternate Bindery context (OU), which you created in the previous section.


For example, to set the context to the OU called *Stand-In Printing for SALES* in the Organization *ACME*, type:

```
Set Bindery Context =.OU=Bindery Printing for
SALES.OU=LANtegrity.O=ACME
```

Response: The queue should now be visible to the HP print server.

3. Use JETADMIN to view the queue and add it to the queue list of the HP print server.

Response: This step also adds the print server object and the Every-one user group to the stand-in printing OU.

 *If you cannot view the queue from JETADMIN, the queue is set up incorrectly. Repeat Steps 1-3.*

4. Exit JETADMIN and reset the Bindery context to its original setting, which you noted in Step 1.

Creating pre- and post-stand-in commands

When the LANtegrity Server stands in for a NetWare 4.x server that provides bindery-based printing services, you need to set the bindery context to the alternate bindery context. In addition, set the bindery context that currently exists on the protected server. You can do this in LANtegrity with a pre-stand-in command.

Step

Action

1. Using any text editor, create a pre-stand-in NCF batch file to set the Bindery context and load the appropriate NLMs for each protected server.

For example, create an NCF file for the protected server *SALES* that loads a print server called *SALES_PSERV*:

```
Set Bindery Context=.OU=Bindery Printing for  
SALES.OU=LANtegrity.O=ACME; .OU=SALES.O=ACME
```

where .OU=SALES.O=ACME is the protected server's bindery context. This ensures that bindery users can connect to stand-in services.

You do not have to reset the alternate Bindery context. When the LANtegrity Server exits stand-in, it resets the alternate Bindery context.

2. Save the pre-stand-in NCF files to SYS:SYSTEM directory on the LANtegrity Server.

Configuring LANtegrity

To complete the set-up of stand-in printing for Bindery-based printing, configure LANtegrity with the name of the pre-stand-in commands.

Step	Action
1.	Open the LANtegrity Administrator and click on the General Configuration tool.
2.	Open the Configure Protected Servers panel and select the NetWare 4.x protected server.
3.	Type the names of the pre-stand-in commands that you created (see previous section) in the appropriate fields.
4.	Use this procedure for each NetWare 4.x protected server that requires stand-in services.

When the LANtegrity server enters stand-in

When the LANtegrity Server enters stand-in, change the default queue to the stand-in queue for that printer object.

B

Disaster Recovery

In the event of an unrecoverable failure of the LANtegrity Server, use LANtegrity's Disaster Recovery option to restore the LANtegrity Server's catalog and internal data sets from tape.

You can also use the Disaster Recovery option to recover the LANtegrity Server fully from the existing Online tapes in the autoloader if the LANtegrity Server's disk fails and data is lost.

If you lose the Online tapes in a disaster, you can use the Disaster Recovery option to recover the LANtegrity Server from a set of Offsite tapes. Also, older versions of the data on the LANtegrity Server may be created by recovering from old tape sets.

When you select Disaster Recovery, LANtegrity scans all of the tapes in the autoloader for LANtegrity datasets that contain catalog data. LANtegrity then allows you to choose which dataset represents the latest valid date that you wish to recover.

Finally, LANtegrity restores all of the datasets spanning a complete set of tapes. This restored LANtegrity Server will have all of the current, deleted, and older versions of files plus the media catalog valid at that time.

Recovering from Online Tapes

Use this procedure to recover the LANtegrity Server if the Online tapes are available in the autoloader. Before you begin:

- If necessary, repair the LANtegrity Server to a properly configured system.
- Then install and setup a LANtegrity Server as described in this manual.
- Unload LSSERVER and make sure the latest Online tapes are in the autoloader.

You do not need any Offsite or Legacy tapes. If the LANtegrity Server only experienced a disk crash, the correct tapes will already be in the autoloader, and you may fully recover from them. You can identify unlabeled tapes by performing an inventory while the LANtegrity Server is running **and authenticated** before beginning this procedure.

1. Load the LANtegrity SETUP NLM. Type: `LOAD SYS:LANTEG\SETUP.`



Figure B-1. The Main Menu

2. Choose **Disaster Recovery**.

Response: You will see two warnings because the current catalog data on the disk will be lost and a screen similar to Figure B-2 appears.

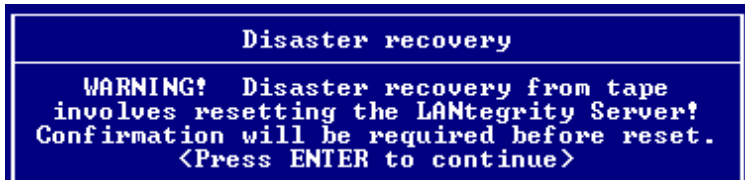


Figure B-2. Disaster Recovery screen

3. Press ENTER when you are ready to proceed, or ESC to quit.

Response: A screen similar to Figure B-3 appears.



Figure B-3. LANtegrity message prompt

4. Select Yes.


Response: LANtegrity resets the LANtegrity Server and asks for a user name and password.

5. Enter a fully distinguished NetWare user name and password.

Response: LANtegrity now scans all of the tapes in the autoloader looking for the most recent datasets.



Figure B-4. LANtegrity Status

 *This may take a substantial amount of time.*

Response: When the process is complete, LANtegrity displays the time and date of the most recent datasets that it found.

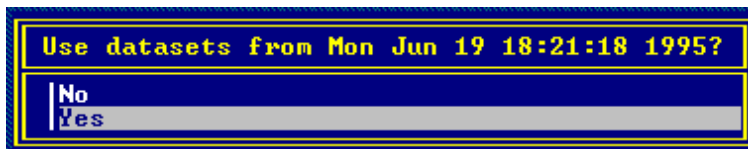


Figure B-5. LANtegrity message prompt

6. Choose Yes to select this latest dataset.

Response: If you select No, LANtegrity brings up the next latest dataset which represent an older state of the LANtegrity Server.

LANtegrity Status
Recovering datasets from Tue Jun 13 14:44:25 1995

Figure B-6. LANtegrity Status screen

Response: LANtegrity requests a series of Offsite tapes.

- Click No for each request. LANtegrity then restores the catalog data from the Online tapes. This process may take considerable amount of time LANtegrity displays screen reporting its status.

LANtegrity Status
Recovering catalog data from tape 51. 31 % Complete

Figure B-7. LANtegrity Status screen

Response: LANtegrity requests another series of Offsite tapes.

- You can press Esc at this time to exit.

Recovering from Offsite Tapes

Before following the steps below, perform these procedures:

- If the LANtegrity Server is beyond repair, choose another properly configured system.
- Then install and setup a LANtegrity Server as described in this manual.
- Unload LSSERVER and load the latest tapes into the autoloader.
- From your vault, get the latest Offsite tape set.
- The latest tape's label identifies the earliest tape ID and the number of tapes in the set. Unlabeled tapes may be identified by performing an inventory with the LANtegrity Server running **and authenticated** before beginning this Disaster Recovery.
- Put the latest Offsite in the autoloader and then sequentially as many others in the set that you can fit into the autoloader.

Follow the procedure below to perform LANtegrity Disaster Recovery from Offsite tapes.

Step	Action
1.	Load the LANtegrity SETUP NLM. Type: <code>LOAD SYS:LANTEG\SETUP.</code>



Figure B-8. The Main menu

2. Choose **Disaster Recovery**.

Response: You will see two warnings because the current catalog data on the disk will be lost and a screen similar to Figure B-9 appears.

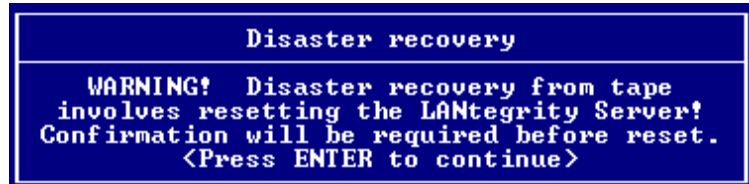


Figure B-9. The Disaster Recovery screen

3. Press ENTER when you are ready to proceed, or ESC to quit.



Figure B-10. LANtegrity message prompt

4. Select Yes.

Response: LANtegrity resets the LANtegrity Server and asks for a user name and password.

5. Enter a fully distinguished NetWare user name and password.

Response: LANtegrity now scans all of the tapes in the autoloader looking for the most recent datasets.



Figure B-11. LANtegrity Status

 *This may take a substantial amount of time.*

Response: When the process is complete, LANtegrity displays the time and date of the most recent datasets that it found.



Figure B-12. LANtegrity message prompt

6. Choose Yes to select this latest dataset.

Response: If you select No, LANtegrity brings up the next latest dataset which represent an older state of the LANtegrity Server.

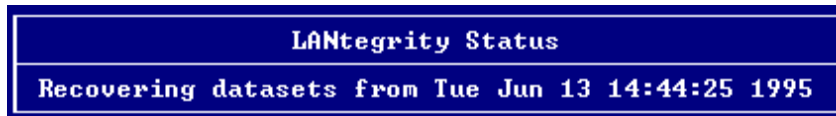


Figure B-13. LANtegrity Status screen

Response: LANtegrity then restores the catalog data that was valid at the time. This process may take considerable amount of time. If all of the Offsite set are not in the autoloader, you will see requests for more tapes such as in Figure B-14.



Figure B-14. LANtegrity request screen

7. Install the requested tape before clicking Yes.

When LANtegrity begins to ask for Online tapes, you may type ESC to exit.