

Quick Tour

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
Technical Support.....	3
Chapter 2. Introducing LANtegrity	4
Overview.....	4
Features.....	5
Hardware and Software Requirements.....	6
Chapter 3. Installing and Setting Up LANtegrity	8
Installation Checklist	9
Installing LANtegrity Server Software	10
Installing Protected Server Software	12
Setting Up a LANtegrity Server.....	14
Setting Up a Protected Server	16
Setting Up the LANtegrity Administrator	18
Chapter 4. Configuring LANtegrity	19
Overview	19
Logging In to the LANtegrity Server.....	20
Dispatching Alerts to the Administrator.....	23
Configuring and Protecting a Server.....	24
Verifying a Protected Server.....	26
Standing In.....	27

Restoring Files	32
Conclusion	35

Welcome

The *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.

Then follow the steps to install, set up, and configure LANtegrity, and to exercise its major features. The instructions give you the basics to complete the Tour. If you want more comprehensive information, refer to the *Set-up Guide*, the *Administrator's Guide*, or to online Help.

Other documentation

The *Quick Tour* is part of a 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.
- ***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.
- ***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.

Technical Support

We're always looking for ways to improve our products and documentation, and make them easier to use. 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.

Overview

The *Quick Tour* is designed to help you “test drive” the major features of LANtegrity. It assumes that you are an experienced NetWare administrator and familiar with Windows applications. With easy-to-follow steps, the *Quick Tour* guides you through the following basic procedures:

- Checking the hardware and software requirements, and installing NetWare 4.1 on the designated LANtegrity Server.
- You also need to refer to Chapter 2, “*Configuration and Installation Notes*” of your *LANtegrity for NetWare Set-up Guide* for the latest information about requirements and common installation pitfalls.
- Installing LANtegrity on the LANtegrity Server and one protected server.
- Protecting a single server.
- The failure of the protected server, automatic stand-in and exiting stand-in.
- Providing traditional file recovery services.

Features

LANtegrity enables a single Novell NetWare 4.1 server to provide **Instant Recovery** and data protection for NetWare 3.x and 4.1 servers.

LANtegrity provides an **Intelligent Data Vault**, a secure, automatically managed repository for all current and historical files on the protected servers. The data vault uses disk cache storage for all recently active files and online tape storage for all current files. It can also maintain a complete archive history of deleted and modified files. With its default configuration, the LANtegrity Server transfers a copy of a protected server's file within 15 minutes after you create or change a file. This **continuous protection** can be applied to all files or a subset of files on a protected server. You can place files that are not suitable for continuous protection (such as large data base files) on protection schedules (e.g., once a night at 1:00 AM). Temporary files that do not need to be protected can also be identified to reduce unnecessary overhead.

The data vault provides **Instant Recovery** stand-in service for all the protected servers. When a protected server goes down (either for scheduled maintenance or an unexpected failure) the LANtegrity Server can provide the file and print services of the down server within 15 seconds. Stand-in service is completely transparent to DOS and Windows IPX network users. They see the same server name, volume mappings and directory structures that they see when the protected server is up and running. Furthermore, the LANtegrity Server continues to protect the other protected servers.

When the down server is ready to come back on-line, the LANtegrity Server completely automates the process of **synchronizing** (updating) the file system of the protected server with the stand-in file system on the LANtegrity Server. This ensures that **all** changes made by users of the stand-in service are moved back to the original protected server before it comes back on-line.

Hardware and Software Requirements


The Chapter 2, “*Configuration and Installation Notes*,” of your *LANtegrity for NetWare Set-up Guide* has the most up-to-date information about requirements. However, for the *Quick Tour*, you do not have to fulfill all of the requirements. This section describes the minimum configuration and points see “*Configuration and Installation Notes*” for further details.

LANtegrity server

For the most part, the server must meet the requirements listed in the “*Configuration and Installation Notes*.” However, note the following:

- **Memory.** You can take the *Quick Tour* with a LANtegrity Server that has the minimum amount of memory required: 48MB.
- **Disk space.** The disk capacity can be less than the minimum requirement: 250 MB larger than the server you want to protect.
- **Tape autoloader.** Highly recommended. You can take the *Quick Tour* without an autoloader but many key LANtegrity features are not available. Call Technical Support for information about running LANtegrity without an autoloader.
- **SCSI Host Adapter.** The *Quick Tour* assumes you are using an Adaptec 1542C SCSI host adapter that is dedicated to the autoloader. If possible, use DMA 5, IRQ 11, and port address 330, which are the default parameters, and set the BIOS OFF.

If you use the same Adaptec 1542C for both the autoloader and disks, call Technical Support for additional information.

 *Make sure that the settings on the Host Adapter do not conflict with other boards in the server. Such conflicts are one of the most common installation problems.*

Protected server

You can use an existing NetWare server running NetWare 3.11, 3.12 or 4.1 as the protected server. It must meet most of the requirements described in Chapter 2, “*Configuration and Installation Notes*” of your *Lantegrity for NetWare Set-up Guide*. However, to minimize the time needed for the *Quick Tour*, select a server that uses

- 1 GB or less of its disk capacity.
- A minimally-sized SYS volume (reduces reboot time during stand-in).

Workstation for the LANtegrity administrator

For the LANtegrity Administrator application, you can use a workstation running 386 enhanced mode Microsoft Windows, version 3.1 or later.

Installing NetWare 4.1

Before you install LANtegrity Server software, you need to install NetWare 4.1. Use the standard NetWare 4.1 installation instructions with the options listed in the Configuration and Installation Notes. However, also note:

- The *Quick Tour* assumes that the LANtegrity Server uses a dedicated test NetWare Directory Services (NDS) tree.

If the LANtegrity Server is the only NetWare 4.1 server on the network, the NDS installation asks you to create a new NDS tree. For the Tour, we suggest the name “Lantegrity_Tree.”

- If one or more NDS trees exist on the network, create a new tree by pressing the <INS> key at the **Install into** screen.
- In the new NDS tree, set the “Company or Organization” to INTEGRITY and leave all three (Sub-) Organizational Unit’s blank.
- Set the Administrator Name to **Admin** with a password of **admin**.

After you install NetWare 4.1 and test communication (that is, you see the protected server when you type `DISPLAY SERVERS`), install LANtegrity.

3

Installing and Setting Up LANtegrity

When your systems are configured correctly, installing and setting up LANtegrity is a simple process. You'll need to have the information in the installation checklist handy (see below). 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. If you want more information about a step, you can refer to the *LANtegrity for NetWare Set-up Guide*.

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


Installation 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 username and password below. However, if you are familiar with NDS, you can substitute other values.

You will be asked to supply...	Enter...
Username/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.
Username 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.

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.

 *If you are installing LANtegrity from a NetWare 3.1 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:
`LOAD NICD:INSTALL.`

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 `Username`

 *It may also prompt for a password.*
5. Type a valid username (for example, **.ADMIN.INTEGRITY**). The username 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:
`SYS:\LANTEG`

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 <code>Username</code></p> <p> It may also prompt for a password.</p>
4.	<p>Type a valid user name. The username 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: <code>SYS:\LANTEG</code></p>
5.	<p>Accept the default <code>SYS:\LANTEG</code> 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 <code>SYS:ETC\RPCNET.CFG</code> or <code>SYS:NETWARE\SERVERICES.CFG</code>. 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: `LOAD SYS:LANTEG\SETUP`.

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.

 *You may be prompted for the 'Port address of Host Adapter', enter the correct port address.*

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.

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

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

If an AUTOEXEC.NCF file exists on both the DOS partition and the SYS: volume, the FILE SERVER NAME and the IPX INTERNAL NET ADDRESS commands can appear only in the AUTOEXEC.NCF file in the DOS partition. These commands cannot appear, even as comments, in the SYS: volume. In addition, the AUTOEXEC.NCF file in the DOS partition must mount the SYS: volume. Follow the procedure below to set up a protected server.

- | Step | Action |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <p>At the LANtegrity Server's system console or RCONSOLE, type:</p> <pre>LOAD SYS:LANTEG\SETUP.</pre> <p>Response: Displays a list of all the servers visible to the protected server.</p> |
| 2. | <p>Select the LANtegrity Server that will protect this server.</p> <p>Response: Where is the local SERVER.EXE program loaded from?</p> |
| 3. | <p>Press ENTER to accept the default or enter the correct path.</p> <p>Response: Displays a message about the alternate IPX Net address and the original IPX Net address followed by: <code>Enter alternate internal IPX address</code></p> |
| 4. | <p>Type the unique alternate IPX address for the protected server.</p> <p>See the Checklist for more information.</p> <p> <i>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.</i></p> <p>Response: [PATH]AUTOEXEC.NCF requires modifications.</p> |
| 5. | <p>Choose Save changes. If desired, choose view changes to display a list of changes, then choose Save changes to continue with the procedure.</p> |


 *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.

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.*

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

Follow the procedure below to set up a 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 drive:setup.exe, where drive is the drive mapped to the LANtegrity product directory. Click OK.

Response: 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. |
| 5. | Click Continue.

Response: A dialog box appears. It asks you where on the workstation to install the software. The default is C:\LANTEG. |
| 6. | Follow the instructions on the screen to create the Program Manager Group and complete the installation. |

4

Configuring LANtegrity

Overview

To initiate protection, you'll do the following:

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

For the Quick Tour, you'll accept most of the default configuration values.

Logging In to the LANtegrity Server

At the workstation set up to run the LANtegrity Administrator.

- | Step | Action |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Make sure that the LANtegrity Server and protected server are displaying a LANtegrity Status screen that tells you that LANtegrity is operating. |
| 2. | Double-click the LANtegrity Administrator icon in the Program Manager window. |

Response: The Login to LANtegrity Server dialog appears.

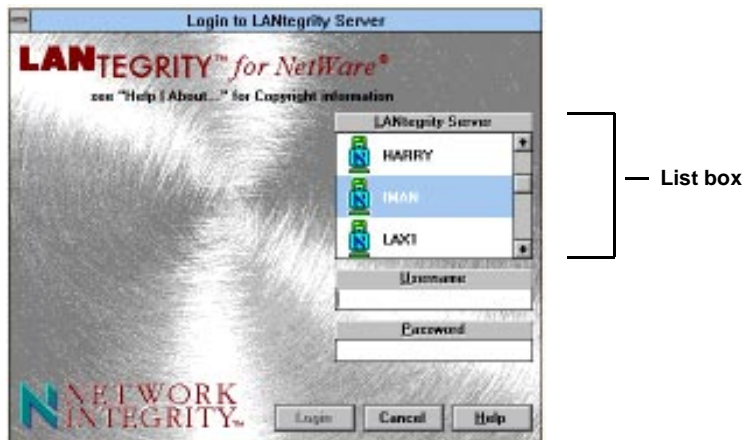



Figure 4-1. Logging into a LANtegrity NetWare Server

3. In the list box, select the LANtegrity Server you want to log into.
4. Type the user name and password specified when you installed NetWare on the LANtegrity Server.

 *If you are using the examples in the Quick Tour, enter the user name .Admin.INTEGRITY and the password admin.*

5. Click Login.

Response: LANtegrity displays a message box similar to Figure 4-2.



Figure 4-2. LANtegrity Administrator message box

6. Click OK.

Response: LANtegrity opens the LANtegrity Administrator desktop and the Configure LANtegrity Server panel.

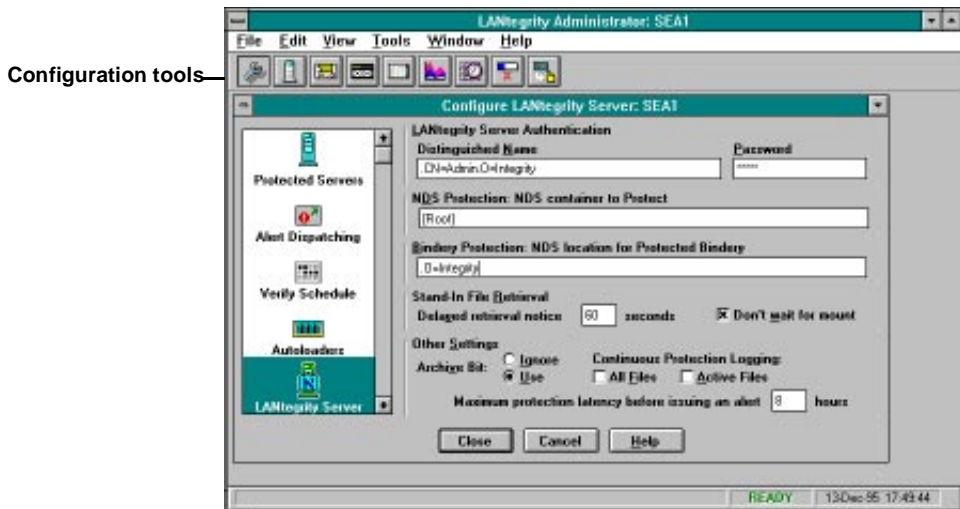


Figure 4-3. Configuring the LANtegrity Server

7. Fill in the fields as follows:

Field	Your Action
Distinguished Name/Password	Type .Admin.INTEGRITY/admin This is the user name and password specified when you installed NetWare.

Field	Your Action
NDS Protection: NDS container to protect	Accept the default, ROOT.
Bindery Protection: NDS location for Protected Bindery	Accept the default. This is the name of the new NDS tree you created.
Stand-in File Retrieval and Other Settings	Accept the defaults.

8. With the Configure LANtegrity Server panel open, continue to the next section.

Dispatching Alerts to the Administrator

By default, LANtegrity posts alerts to the Alert Status window. You can also route alerts to other destinations. For the Quick Tour, you'll post all alerts to any user logged in to the LANtegrity Server as the administrator.

Step

Action



1. In the list box (on left) of the Configure LANtegrity Server screen, pick the Alert Dispatching icon.

Response: LANtegrity saves the changes to the Configure LANtegrity Server panel and displays the Alert Dispatching panel.

2. Select all of the alerts; then select Send Message (bottom left).
3. Click on the Send To button.

Response: LANtegrity displays the Configure Send window.

4. In the Username box, type a valid NetWare user name (such as **Admin**), and click Add.
5. In the Hold message for box, type the number of hours that LANtegrity should hold messages if the user is not logged-in.

✍ By default, LANtegrity holds messages for 72 hours.

6. With the Alert Dispatching panel open, go to the next section.

Configuring and Protecting a Server

LANtegrity uses NetWare's Storage Management Services (SMS) to move files between the protected server and the LANtegrity Server. To support this communication, you first supply a user name and password that has supervisor-equivalent privileges on the protected server.

Step

Action



1. In the list box on the left, select Protected Servers.

Response: LANtegrity displays the Configure Protected Servers panel. It lists the NetWare servers that you set up as protected servers.

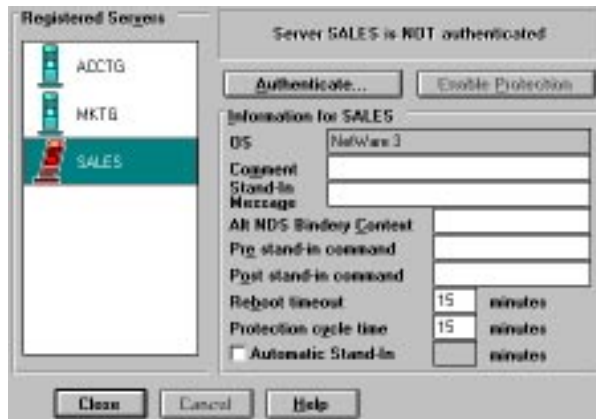


Figure 4-4. Configuring and Protecting a server

The server icon selected in Figure 4-4 indicates that the protected server agent is loaded and the server is authenticated, but not under protection.

2. Follow the table below when entering data in the dialog displayed in Figure 4-4.

Button/Field	Your Action
Authenticate The server icon changes to indicate that the server is authenticated but that protection has not yet started.	Click Authenticate to display the Authenticate window. Type a valid user name and password that is a Supervisor or Supervisor-equivalent for the protected server and click OK. <i>If NetWare 4 server: user must have supervisor rights to NDS object on Protected Server. Enter typed or typeless distinguished name.</i>
Stand-in Message A broadcast message that users see when they log into a protected server during Stand-in.	Type message. For example: LANtegrity Server standing in for <Server>; where <server> is the name of the protected server. Enter up to 58 characters, including punctuation marks and spaces.
Alt NDS Bindery Context/ Server Bindery Context	Accept default.
Reboot timeout The default is 15 minutes.	Check the value and increase if necessary. It should be about twice the time it takes to reboot your protected server. (As LANtegrity exists stand-in, it reboots the protected server.)
Enable Protection The server icon changes to indicate that protection has started but LANtegrity does not have enough data to stand-in for it.	Click to start continuous protection, which uses the archive bit to pick up new or changed files. The initial verify job, which by default runs at 7PM, transfers copies of all the files, regardless of the archive bit. To accelerate the Quick Tour, you'll run the verify job now (next section).
Close	LANtegrity saves changes to the Protected Server Configuration panel.
Automatic Stand-in	Select it and accept the default(s).

Verifying a Protected Server

Follow the procedure below to verify a protected server.

Step

Action



1. Click Protected Servers. LANtegrity to display the Protected Servers window.
2. In the list box on the left, select the server you want to verify.
3. Click Verify Now.

Response: LANtegrity starts a verify job on the selected server. Depending on the size of the server's disk space, the verify job can take some time.



4. If you want to check on the status of the Verify job, click Current Jobs. The Current Jobs window displays an entry for the Verify Now job.

When the verify job is complete, the protected server is fully protected. The verify job disappears from the Current Jobs window. In addition:

- The LANtegrity Server and the protected server operate normally: the LANtegrity Server provides continuous protection for the protected server; the protected server provides file services to its users.
- The LANtegrity Server's disk cache has mostly recently protected files, which only now, may not be the most recently active files.
- The red X is removed from the server icon.
- The LANtegrity Server can stand-in for the protected server at any time.



Standing In

For the Quick Tour, users should create, modify, and save files before you simulate a server failure. Run some standard applications (for example, word processing or spreadsheets) to allow the cache to normalize with the user community's file activity.

Only files that have actually been saved to the protected server are picked up by continuous protection. If users edit a document for several hours without periodically saving it, they lose their changes just as they would when any server or workstation disconnects. Also, only saves that are older than the protection cycle time (default 15 minutes) are guaranteed protection. Files that have been saved more recently may or may not be protected the time of server failure. A 15 minute protection cycle implies that the file was saved about 7.5 minutes ago.

If you want more information about a step, you can refer to the *LANtegrity for NetWare Administrator's Guide* or to online Help.

Initiating stand-in

Follow the procedure below to initiate stand-in.

Step

Action

1. With "users" connected to the protected server, down the protected server.

Response: If Automatic Stand-In is selected, the stand-in timer starts. After the delay that you specified, the LANtegrity Server automatically stands in for the down server.



2. If Automatic stand-in is not selected or if you want to start stand-in immediately, click on the Protected Servers button. LANtegrity displays the Protected Servers window.

Response: LANtegrity displays the Protected Servers window.

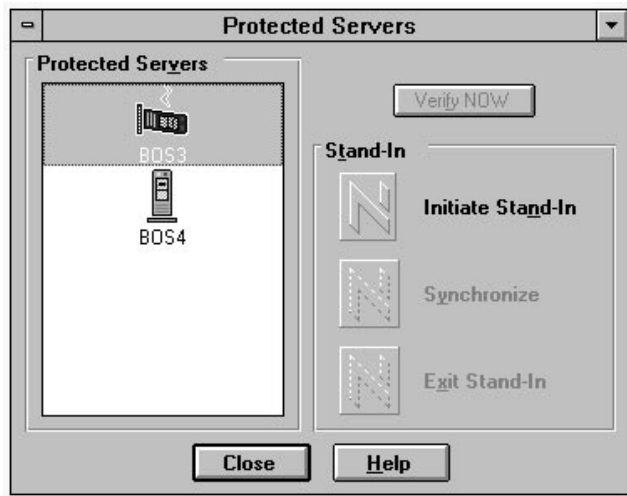


Figure 4-5. Protected Servers screen

3. Select the down server and click Initiate Stand-in.



Response: The protected server icon changes to the LANtegrity Server icon.

What to do during in stand-in

After the LANtegrity Server is in stand-in, have users do the following:

- Log in to the server as usual, with the same ID and password.

Upon connecting, users receive the stand-in message that you created earlier. They also see the same volumes and directory structures before the protected server went down.
- Resume work on the documents they were working on before the server went down, make changes, and save two or more updates at least an hour apart. You need to allow time for two complete protection cycles so that all updates get to tape.

Typically, users find their most recently saved file(s) unless they saved the file within the last few minutes. In this case, they have the previously saved version.

LANtegrity provides much more recent file versions than can typically be provided with conventional backup. It eliminates the risk, inherent in mirroring systems, that the failure that causes the server crash damages the mirror. If you need earlier versions of files, you can restore them from the LANtegrity Server to its stand-in file system for the down server.

Synchronizing files

As users continue to modify and save files during stand-in, the files on the LANtegrity Server are newer than the files on the protected server. To get these newer files back to the protected server, you direct the LANtegrity Server to synchronize the files on the protected server. This is a fully automated process that ensures that all the changes made during stand-in are transferred back to the original server.

You can synchronize files in one or two steps:

- **(Optional) *Synchronize files during stand-in***

During this synchronization, users can continue to access their files on the LANtegrity Server. You might use this option if there was a large amount of data to transfer (e.g., the failed server lost an entire disk drive).

- **(Required) *Exit stand-in with synchronization***

During this synchronization, users cannot access their files on the LANtegrity Server or the protected server. This allows LANtegrity to take a final, stable snapshot of any changes to the file system. Ordinarily, you'd run this synchronization during off-hours.

For the Quick Tour, there's not a large amount of data to transfer. You only have to transfer the changes made during stand-in. So you can disregard the synchronization during stand-in and synchronize as you exit stand-in.

Exiting stand-in with synchronization

To synchronize the files, you bring the protected server back online during stand-in. Since the LANtegrity Server is using the protected server's name, you need to boot the protected server with the alternate name and IPX address created during setup. LANtegrity automates this process by booting the server with LSSTART. What's more, this ensures that the protected server is never brought up under its normal name while the LANtegrity Server is standing in for it.

Step

Action

1. To perform an exit with synchronization, reboot the server.

Be sure to reboot the protected server with LSSTART. If the server boots from AUTOEXEC.BAT, it automatically uses LSSTART. If your server doesn't boot automatically from AUTOEXEC.BAT, change to the subdirectory that contains SERVER.EXE and type LSSTART. This starts an automatic reboot sequence that brings the server up correctly with its alternate name and IPX address.

Response: LANtegrity Server displays a message prompt similar to Figure 4-6.



Figure 4-6. LANtegrity server message prompt

2. Select 'Standing-In for this server'.

Response: LANtegrity reboots the protected server under its alternate name and IPX address and establishes communications with the LANtegrity Server. Then it displays a status box similar to Figure 4-7.



Figure 4-7. LANtegrity status box

Action: You can now exit stand-in with synchronization.



3. Click Protected Servers on the toolbar.



4. From the Protected Servers window, select the protected server that the LANtegrity Server is standing in for.

Response: When the protected server is connected to the LANtegrity Server under its alternate name, both Synchronize and Exit Stand-In are enabled.

5. Click Exit Stand-In.

Response: LANtegrity displays a dialog similar to Figure 4-8.



Figure 4-8. LANtegrity Administrator dialog

6. Ensure that 'Sync filesystem' is selected and click OK.



7. If you want to check on the status of the synchronization job, open the Current Jobs window.

Response: When the synchronization is complete, the job disappears from the Current Jobs window. LANtegrity then reboots the protected server under its normal name and IPX address. When the protected server resumes operation, the server icon indicates that it is online and fully protected. Users can again log in.

Restoring Files

LANtegrity eliminates the need for conventional server backup. It provides full file history and disaster protection for a protected server. You can restore deleted or modified files from the LANtegrity Server using the LANtegrity Administrator. Because the autoloader contains a large amount of recent file history, you can usually restore files without loading and unloading any tapes.

Restoring recently deleted files

Follow the procedure below to restore recently deleted files.

Step

Action

1. Delete a file from the protected server.
2. Open the LANtegrity Administrator and click Restore on the toolbar.
3. In the Restore window, select the protected server and click Restore Files.



Response: The Restore Files window displays the most recently protected volumes on the protected server.

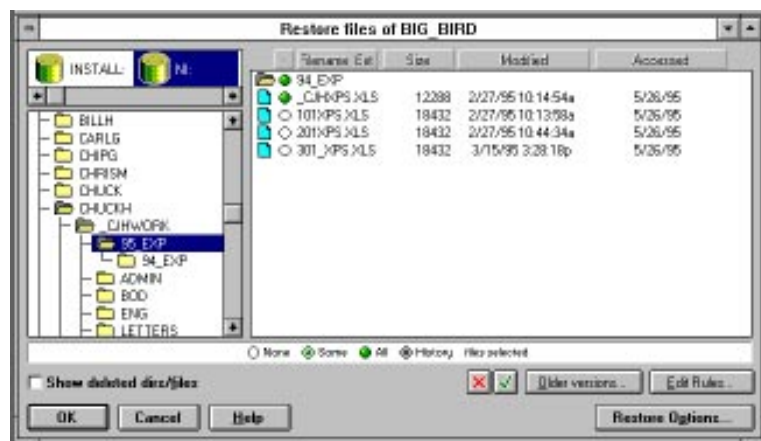



Figure 4-9. Restoring deleted files

4. In the volume list box, click the volume that contained the deleted file.

Response: The directories on that volume appear in the directory list box below.

5. Navigate through the directories until the deleted file appears in the file list box on the right.

 *Because you are doing this procedure immediately after deleting the file, you do not have to click Show deleted dirs/files. Files are not listed as deleted until a verify job runs.*

6. Click once on the empty restore circle to the left of the name of the file you want to restore.

Response: The circle fills and turns green.

7. Click OK.

Restoring older versions of files

To restore older versions of a file, the LANtegrity Server needs to protect the file long enough to have saved different versions of the same file to tape. Different versions may be saved to tape many times in a single day. But the frequency depends upon the data change rate and other factors.

Step	Action
1.	Change a file and save it on one day. Repeat the process on another day.
2.	Follow Steps 1-5 in the previous section.
3.	Select the name of the file you want to restore (not the restore circle), and then click Older Versions.
	Response: The file history window displays, showing all versions of the file.
4.	Select the version you want to restore and click OK.

5. Click Restore Options.

Response: LANtegrity opens the Restore Options window.

6. Select Overwrite Option or Restore to Different Location.

If you select Overwrite Option, select Auto-rename if existing file. In this case, if the DOS file name exists, LANtegrity replaces the last character of the file extension with a number. For example, if the file name was february.xls, it renames the restored file to february.xl1.

Conclusion

This completes a brief exploration of the stand-in and restore features. You can explore LANtegrity's many other features with the Administrator's Guide and online Help. For example, you could check the monitoring tools or protection statistics, autoloader and media library management, scheduled protection, print services during stand-in, or disaster recovery.