LANtegrity for NetWare Administrators 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

Issued February 1996

Table of Contents

Chapter 1. About This Document 1

Welcome 1

How to Use This Guide 3

Technical Support 4

Chapter 2. Introducing LANtegrity 5

Overview 5

LANtegrity Components 6

Instant Server Recovery 7

Intelligent Data Vault 10

The Tasks of an Administrator 14

Using Customized Workspaces 19

Chapter 3. Protecting Server Data 22

Overview 22

Continuous Protection 23

Managing Continuous Protection 26

Chapter 4. Monitoring LANtegrity Operations 37

Overview 37

Monitoring the Job Log 38

Monitoring Alerts 42

Monitoring the System Log 47

Dispatching Alerts 49

Managing Current Jobs 53
Checking Protection Statistics 57

Chapter 5. Managing the Autoloader and Media Library 60

Overview 60
LANtegrity Tapes 61
Configuring an Autoloader 67
Managing the Autoloader 71
Configuring Media Rotation 86
Reviewing the Media Inventory 89

Chapter 6. Operating Stand-in Service 93

Introduction 93
Preparing for Stand-in Service 95
Initiating Stand-in 101
What Happens During Stand-in Service 104
Exiting Stand-in Service 110

Chapter 7. Restoring Files 120

Overview 120
Restoring File Copies 122
Using Rules to Select Files 130
Selecting Restore Options 134
Restoring the Bindery 140
Restoring NDS 141

Chapter 8. Customizing File Protection 142

Overview 142
Using Master Exclusions 144
Using the Never Protect Sheet 150
Using Scheduled Protection 156

Using Rules to Select Files 165

Chapter 9. Managing the Servers 171

Placing a Server Under Protection 171

Changing Settings of the LANtegrity Server 178

1 About This Document

Welcome

The *LANtegrity for NetWare Administrator's Guide* contains detailed information about configuring, using, and managing LANtegrity. 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 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.
- **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 system administrators who manage LANtegrity for NetWare. It assumes that you are familiar with NetWare technology and terminology, and are familiar with Windows application conventions.

How to Use This Guide

This guide is designed as both a quick reference and a long term planning and operational guide for LANtegrity administrators.

Chapter 1. ***Introduction.*** Introduces the features and functions of LANtegrity for NetWare and explains the desktop features in the interface.

Chapter 2. ***Protecting Server Data.*** Describes the default protection method, continuous protection, and how to change the settings.

Chapter 3. ***Monitoring LANtegrity Operations.*** Provides information and procedures for reviewing the Job Log, the Alert Status Log, the System Log, the current jobs, and protection statistics.

Chapter 4. ***Managing the Autoloader and Media Library.*** Provides procedures for inserting and removing tapes. Also includes information on the types of tape, and media rotation policy.

Chapter 5. ***Operating Stand In Service.*** Describes LANtegrity's stand-in service features and the procedures used to initiate and exit from stand-in services.

Chapter 6. ***Restoring Files.*** Contains procedures for locating files to restore and for directing the files to the desired location.

Chapter 7. ***Customizing File Protection.*** Describes how to remove files from continuous protection by placing them on a schedule or excluding them from protection.

Chapter 8. ***Managing the Servers.*** Provides instructions for adding protected servers and changing settings on a LANtegrity Server.

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.

2 Introducing LANtegrity

Overview

LANtegrity for NetWare is a comprehensive solution to the problems of data protection and server recovery in networks. It enables you to protect NetWare 3 and NetWare 4 file servers under the administration of a single LANtegrity Server. It provides:

- A stand-in service for instant server recovery.
- An Intelligent Data Vault for data protection.
- A mechanism for file restoration and disaster recovery.

LANtegrity Components

LANtegrity for NetWare consists of:

- The LANtegrity Server NLM, **LSSERVER.NLM**, which runs on a dedicated NetWare 4 server and manages the stand-in, data vault, and file restoration capabilities
- The protected server agent NLMs, **LSAGENT.NLM** and **LSSTART.NLM**, which run on each protected NetWare server
- The LANtegrity Administrator interface, which is a Microsoft Windows application. The LANtegrity Administrator runs on a workstation that communicates with one or more LANtegrity Servers.

Instant Server Recovery

LANtegrity supports instant server recovery by providing a **stand-in service** within 15 seconds for a protected server that is down. LANtegrity's **Intelligent Data Vault**, containing copies of all current and historical files, is the foundation for the stand-in service. When a protected server goes down, LANtegrity continues to make the server's files available by accessing the copies saved in the data vault.

The LANtegrity Server assumes the network identity of the server and advertises itself as providing the server's file and print services. Thereafter, the LANtegrity Server responds to any login requests directed to the down server.

The following figure illustrates how the LANtegrity Server stands in for a protected server that is down.

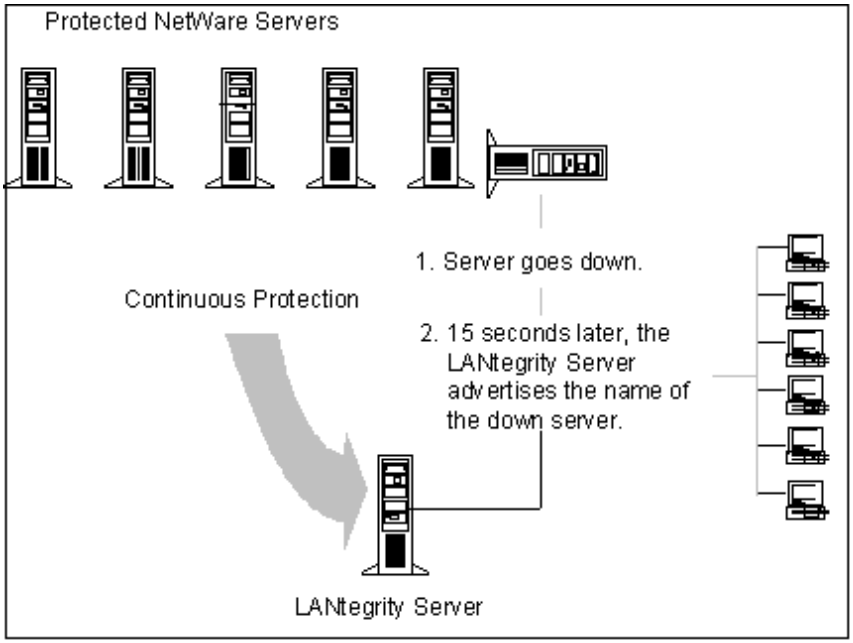


Figure 2-1. LANtegrity Server Stand-in Process

What do users see during stand-in?

Since the LANtegrity Server has assumed the network identity of the down server, the users actually log in to the LANtegrity Server using their customary login sequences.

LANtegrity's Intelligent Data Vault allows access to all protected data. Files are current (usually the most recent saved version) to within a few minutes before their server went down. Files that have been used in the past few days are immediately available because they are in the LANtegrity Server's disk cache. Files that have not been accessed recently are automatically brought into the disk cache from the tape sets in the autoloader and delivered to the user.

The following figure shows the availability of user files during stand-in.

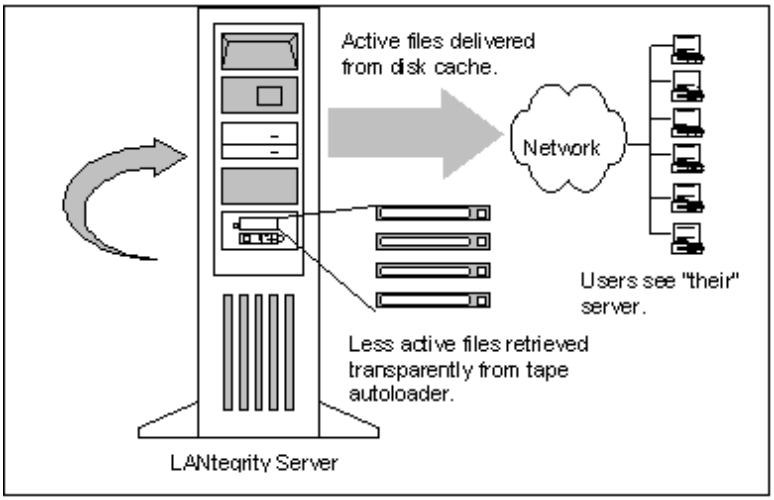


Figure 2-2. File Availability for Users during Stand-in

Are there any limitations to stand-in?

Yes. The LANtegrity Server can stand-in for only one down server at a time. Services that depend on a physical device connected to the down server are not automatically available. Printers must be on the network rather than connected locally to automatically establish service for them.

Stand-in services are available only for MS-DOS and Windows users accessing files over IPX and NCP. These are the normal Novell protocols for DOS and Windows clients. OS/2 clients and clients connecting via Appletalk or NFS cannot use the LANtegrity Server as a stand-in server. Note that while stand-in is limited to DOS and Windows clients, all data in all name spaces is fully protected.

Volume or directory renaming on the stand-in server is not supported, nor is file renaming based on the use of DOS wildcards.

What happens when LANtegrity exits from stand-in?

After the down server has been repaired, LANtegrity restores the latest copies of files to the protected server. This includes all the files that were created or changed during stand-in, as well as any files that were lost when the protected server went down. This process is called **synchronization**.

The following figure shows how LANtegrity performs automatic synchronization for a recovering server.

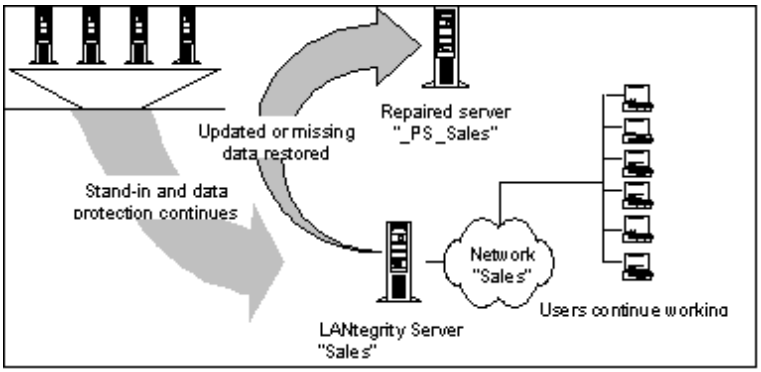


Figure 2-3. Automatic Data Synchronization for Recovering Server

Intelligent Data Vault

LANtegrity's **Intelligent Data Vault** is a secure, automatically managed, repository for all current and historical files used on the protected servers.

What makes the data vault intelligent?

LANtegrity's data vault is "intelligent" because it uses:

- Active processes (on the LANtegrity Server and the protected servers) to continually scan for changed and recently accessed files. When it detects such files, LANtegrity automatically copies them to the LANtegrity Server's disk cache. LANtegrity copies only changed files, which eliminates the need for repeated copying of the unchanged files over the network. This process is called **continuous protection**.

- A hierarchical storage method keeps the most active files immediately available for high performance access during instant server recovery. This activity is called **Hierarchical Storage Management (HSM)**.

How does LANtegrity know when a file needs to be saved?

When a NetWare server is first placed under LANtegrity's protection, LANtegrity protects all of its files. From then on, LANtegrity identifies changed files by checking either the archive bit or the date/time stamp.

LANtegrity copies only changed files. An unchanged file is never copied twice over the network. By saving only changed files, LANtegrity provides an efficient replacement for the conventional cycle of repeated "full and incremental" backups.

The following figure shows how changed files are copied from a protected server to LANtegrity's Intelligent Data Vault.

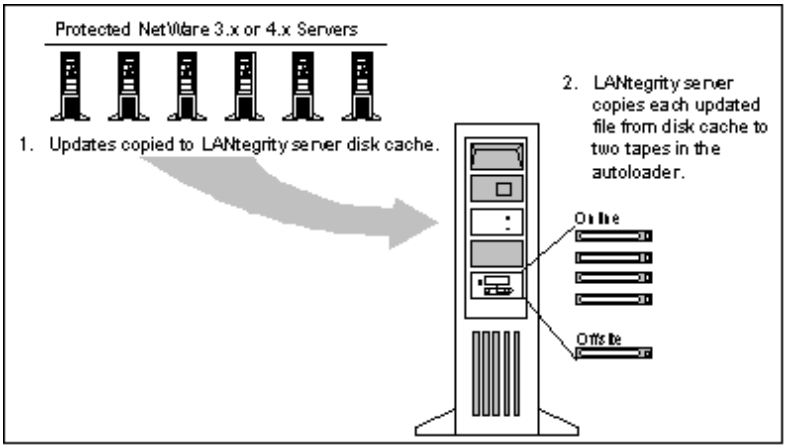


Figure 2-4. Protection of Changed Files

Can LANtegrity protect my NetWare directory?

LANtegrity makes daily copies of the NetWare Directory Services (NDS) and the NetWare 3 Bindery.

Where does LANtegrity keep protected files?

LANtegrity's Intelligent Data Vault contains all of the protected files from all of the protected servers. It also contains all the earlier versions of the current files and deleted files, within the bounds of the media rotation schedule.

LANtegrity manages the saved files by using Hierarchical Storage Management (HSM), which provides the foundation for LANtegrity's instant server recovery. This storage hierarchy consists of the following components:

- **Disk cache storage**, which contains the most recent files. When LANtegrity detects a changed file, it saves a copy of the file in the LANtegrity Server's disk cache. LANtegrity maintains the latest versions of the most actively used network files in the disk cache. This ensures that the most recently changed files will be immediately available to users if a protected server goes down.

- **Online tape storage,** which contains copies of all network files. For protection, LANtegrity immediately queues saved files to the Online tape set, which is always in the autoloader. LANtegrity manages the Online tape set so that it always contains all the current files on all the protected servers. The current files are used to support instant server recovery, restore user's files, and synchronize a server.
- **Offsite tape storage,** which is a redundant copy of all file history. The Offsite tape is a single tape that is intended for periodic removal to a vault or other secure location. It provides archival storage and the ability to recover the LANtegrity Server in the event of a disaster.

Why use hierarchical storage?

LANtegrity's Intelligent Data Vault is a form of Hierarchical Storage Management (HSM). The purpose of HSM is to organize storage to accommodate user access frequencies. First, LANtegrity stores the most recently accessed network files in the LANtegrity Server's disk cache. Secondly, it maintains all current files on Online tapes where they can be accessed directly from the autoloader without manual intervention. Finally, it maintains older versions of files and deleted files on Offsite tapes for restoration or recovery when necessary.

The following figure shows how LANtegrity manages tapes in terms of the Online tape set and the Offsite tape.

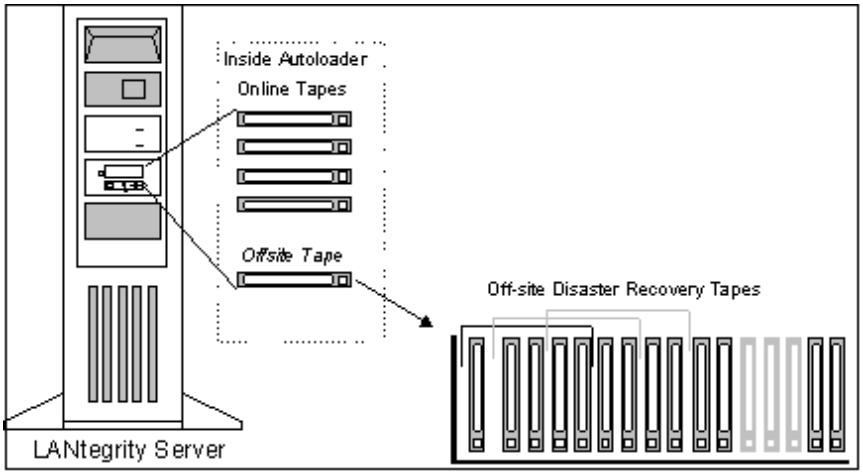


Figure 2-5. LANtegrity Management of Tapes: Onsite and Offsite

What about restoring files to the protected servers?

LANtegrity makes file restoration both easy and convenient since all current files and many older files are usually available in the disk cache or in the autoloader. You can also use the LANtegrity Administrator to browse through a list of files you can restore.

Can a LANtegrity server recover itself from a disaster?

Yes. The LANtegrity Server provides for its own recovery from failure conditions by keeping a **catalog** or record of all the files it protects and continuously copying these files to tape. In the event of disk damage, the LANtegrity Server can fully recover its disk contents from the Online tapes in the autoloader. If the Online tapes also happen to be damaged, the LANtegrity Server can completely recover from any of the tape sets in the Offsite tapes.

The Tasks of an Administrator

To help you perform administrative tasks, LANtegrity provides the LANtegrity Administrator interface application. As administrator, you are responsible for:

- **Protecting Server data.** By default, LANtegrity protects all files with its continuous protection method except for certain files on the **master exclusions** list. From time to time, you may want to review or change some of the optional settings for continuous protection. Chapter 3, “Protecting Server Data,” discusses how to change LANtegrity’s file protection options.

- **Monitoring LANtegrity operations**. This is largely a matter of checking the alert, system, and job logs. Log entries provide a historical record of LANtegrity’s operations. Alerts inform you of conditions that may require your attention. You can create a wider distribution for alerts by specifying additional destinations for them. You can also check on the status of current **jobs**. Jobs are requests initiated by a user either manually or on a schedule. You can cancel any job. Chapter 4, “Monitoring LANtegrity Operations,” describes how to monitor LANtegrity’s operations.

- **Managing autoloader operations**. This is primarily a matter of inserting and removing tapes, as required. Chapter 5, “Managing the Autoloader and Media Library,” describes LANtegrity tapes and how to perform autoloader operations.

- **Operating the stand-in service**. You prepare for LANtegrity’s stand-in service by ensuring that the LANtegrity Server has enough processing power and disk storage, all required files are being protected, and the protected server’s users can access the LANtegrity Server. You can also define a message to be delivered to users as they log in to the stand-in service and test the stand-in service apart from an emergency situation. When stand-in ends, you can synchronize the LANtegrity Server’s file system with that of the recovered server. Chapter 6, “Operating Stand-in Service,” describes how to operate LANtegrity’s stand-in service.

- **Restoring files**. LANtegrity allows you to restore current, deleted, or older versions of files. Current files are typically restored from the disk cache or from the Online tape set.

- **Customizing file protection**. You can place specific files on a protection schedule, exclude some files completely, and set the continuous protection frequency. Chapter 8, "Customizing File Protection," discusses how to use LANtegrity's file protection options.

- **Managing the servers**. Managing the servers involves placing additional servers under LANtegrity protection and changing various parameters to control the operation of the LANtegrity Server. Chapter 9, "Managing the Servers," describes how to manage the LANtegrity environment.

Where can I work?

You can work from any location on your network that allows you to connect to the LANtegrity Server. You can install the LANtegrity Administrator on any Windows workstation that has access to the LANtegrity Server. Only the action of inserting and removing tapes from the autoloader requires you to be physically located at the LANtegrity Server.

Can I assign someone else to manage tape activities?

Yes. You can provide someone else (for example, a computer room operator) with access to the LANtegrity Administrator and allow them to insert and remove tapes as requested by the system. LANtegrity automatically prompts for every action required — insert tape, remove tape, and so on. Your operator can simply follow the system prompts and perform the actions.

How do I manage the Administrators group?

When it is initially loaded, LANtegrity creates an NDS group called **LANtegrity Administrators for *LServer***, where *LServer* is the name of the LANtegrity Server. You can designate users other than the NDS administrators to be LANtegrity administrators by making them members of this group. Thereafter, they will be able to login to the LANtegrity Administrator user interface. They will also have sufficient NDS authorization to add and delete other users for the LANtegrity Administrators group.

How do I access LANtegrity?

When you activate the LANtegrity Administrator, you choose a LANtegrity Server and log in. The LANtegrity Administrator is a client application used to monitor and control the operation of the LANtegrity Server to which it is currently connected.

A single instance of the LANtegrity Administrator can monitor and control the operations of any LANtegrity Server on your network. All you need to specify is a distinguished NDS name with LANtegrity administrator rights and a password. The Administrator application establishes a connection to the server based on the information you provide.

Follow the procedure below to access the LANtegrity Administrator.

Step	Action
1.	Double-click on the LANtegrity Administrator icon on your Windows desktop. **Response**: LANtegrity displays the Login to LANtegrity Server dialog box.

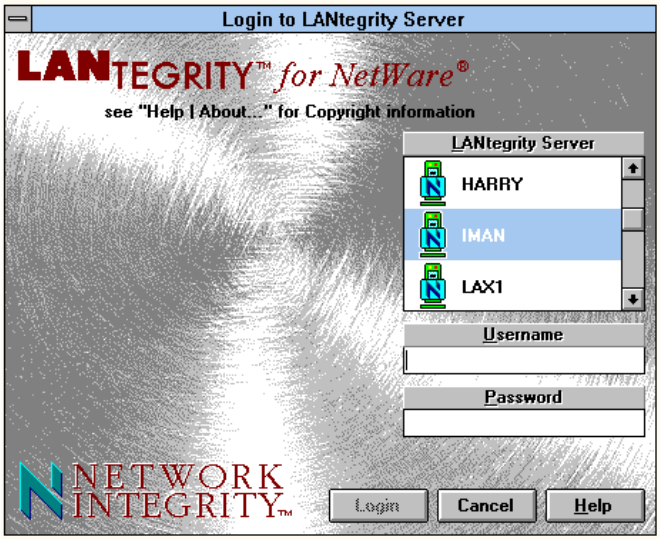


Figure 2-6. Login to LANtegrity Server

2. In the list box, click on the LANtegrity Server you want to access.

3. Type the username and password. The username cannot be abbreviated. It must the name of a user registered in NDS.

   ✍ *To log in as an administrator, you must have privileges equivalent to ADMIN. Alternatively, you must be a member of the NDS LANtegrity group created by the LANtegrity Server. The group is called* ***LANtegrity Administrators for*** **LServer**, *where LServer is the name of the LANtegrity Server.*

4. Click Login.

   Response: LANtegrity connects you to the LANtegrity Server and displays the LANtegrity Administrator desktop.

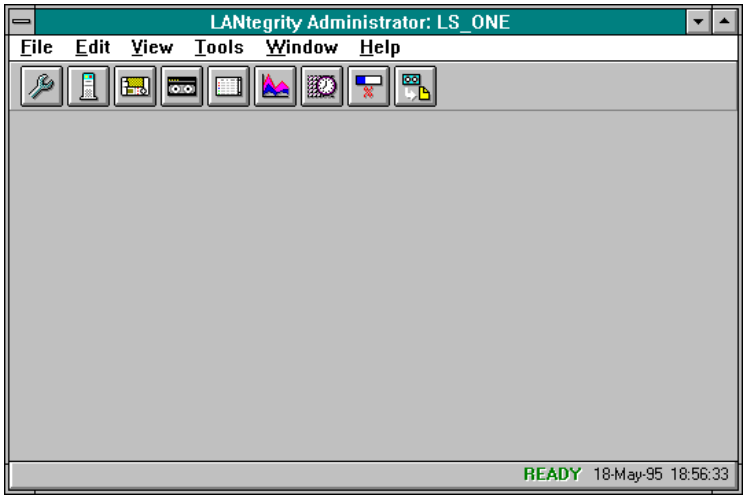


Figure 2-7. The LANtegrity desktop

✍ *When you log in for the first time, LANtegrity displays the Configure LANtegrity Server panel so that you can supply the NetWare distinguished name and password for the LANtegrity Server. For information on how to use this panel, refer to* *"Changing Settings of the LANtegrity Server" on page 178*.

Using online help

LANtegrity's online Help provides much of the information from this guide. To access the online Help system, select **Help/Contents** or **Help/Search** for **Help On**.

While you are working within LANtegrity, you can also obtain context-sensitive help for any dialog box or menu by pressing the F1 key.

Understanding the status bar

The status bar contains (from left to right):

- A "hot" information field, containing either important events or quick help text for the icons in the toolbar
- A state field that identifies which of three possible modes the LANtegrity Server is in:
  - **READY** (Protection mode). The LANtegrity Server is currently protecting the servers in its domain, as specified by its protection policy.
  - **STAND-IN** (Stand-in mode). The LANtegrity Server is currently taking the place of a protected server and managing workstation user requests for files.
  - **SYNC** (Synchronization mode). The LANtegrity Server is currently updating the file system of a recovering protected server.
- The current date and time. Your workstation manages this display. It is not synchronized with the LANtegrity Server.

Using Customized Workspaces

You can customize your LANtegrity Administrator desktop workspace for each Windows workstation. LANtegrity stores each workspace layout locally, where it is available to any administrator who logs into that workstation. For example, if you set up a particular workspace layout for use with a given server, you can save it under a name you assign and then recall it each time you connect to that server. This section describes how to customize a workspace, save it and recall it.

Customizing your workspace

Depending on the size and resolution of your monitor, some LANtegrity windows may not display all of the available data. In these cases, you can change the affected windows to show all of the data. When you change a window's layout, LANtegrity retains the new layout until you change it again.

To customize your workspace, you can:

- Change the location of the button and status bars.
- Adjust the display area, by changing the size of a window, list box, or display column.

To change the location of the button or status bars

You can reposition or hide both the button and the status bars. By default, the button bar appears at the top of the window and the status bar appears at the bottom.

Step	Action
1.	From the **View** menu, select **Show ButtonBar** or **Show StatusBar**. **Response**: A submenu appears, containing three possible settings: **At Bottom**, **At Top**, or **Hide**.
2.	Select the new setting for the bar. ✍ *Do not hide both the button bar and the status bar.*

To maximize and resize a window

To maximize a window's display area, click the maximize button in the upper right corner of the window.

To resize a window, drag its borders to the desired dimensions. Note that not all LANtegrity windows can be resized. In these cases, you can use other techniques to view the contents of text fields or list boxes.

To adjust column width

If a window presents information in tabular format, you can adjust the width of a column by clicking and dragging in the space that separates each column heading from the adjacent column heading. When you click in this space, the cursor changes to a double-sided arrow and you can drag left or right.

To resize a list box

A number of LANtegrity windows use list boxes to present information. For example, the **Restore files** window uses a side-by-side list format with directories shown on the left and files on the right.

You can widen a list box to display more of its contents by clicking and dragging in the adjoining space. When you click in this space, the cursor changes to a double-sided arrow and you can drag left or right.

To scroll a window or field

To scroll a window's contents, use the standard Windows scroll bars. The vertical bar, scrolls the window vertically. The horizontal bar scrolls the window horizontally.

In an input field, you can use the **Right-Arrow** and **Left-Arrow** to scroll within the field. Also, the **Home** key takes you to the start of the field and the **End** key takes you to the end.

Saving and recalling a customized workspace

If you customize your workspace as described in "Customizing your workspace" on page 19 you can save the workspace layout for later recall. You can save and recall up to two separate workspace layouts.

To save a customized workspace

Follow the procedure below to save a customized workspace.

Step	Action
1.	Change your workspace as desired.
2.	Select **View/Save Workspace**. **Response**: A submenu appears, listing the available workspaces.
3.	Select any one of the workspace and enter a name for the saved workspace.
4.	Enter up to 24 characters and click on OK. ✍ *You can include spaces in the name, if you want.*

To recall a customized workspace

Follow the procedure below to recall a customized workspace.

Step	Action
1.	Select **View/Use Workspace**. **Response**: A submenu appears, showing the names of the workspaces you have saved.
2.	Select one of the saved workspaces. **Response**: LANtegrity loads the workspace layout and adjusts your screen accordingly.

3 Protecting Server Data

Overview

When you initially enable protection for a server, it is automatically placed under continuous protection. The protected files provide the basis for LANtegrity's stand-in capability and also its ability to recover from system or disk failure.

✍ *You can remove files from continuous protection or place them on a schedule. However, with a few exceptions that are discussed in this chapter, you should leave your files under continuous protection.*

This chapter describes continuous protection and how to change the settings.

For information about how to place a server under protection, see Chapter 9, "Managing the Servers." LANtegrity can perform stand-in only on those servers that are under its protection.

For information about removing files from continuous protection or placing files on a protection schedule, see Chapter 8, "Customizing File Protection."

Continuous Protection

Continuous protection is a process by which the LANtegrity Server constantly monitors protected files for any changes. As soon as the server detects a change in a file, it copies the file to its cache. LANtegrity minimizes the amount of work that is at risk by automatically saving files as they change. By default, the LANtegrity Server saves a changed file within 15 minutes after the change occurs.

When a server is first placed under LANtegrity's protection, LANtegrity saves all of its files. From then on, LANtegrity saves only changed files. By copying an unchanged file only once, LANtegrity conserves network resources.

Once a file is protected, it is available during stand-in or for restoration whenever the need arises. If a problem on a protected server prevents users from accessing files, the LANtegrity Server can provide stand-in services for that server usually with no file out of date by more than the time you specified in the protection cycle.

How does LANtegrity protect files?

LANtegrity protects files by:

- Detecting file changes, to identify files that need to be saved.
- Copying the changed files to the Intelligent Data Vault (the LANtegrity Server's disk cache, the Online tapes, and the Offsite tapes.

The following figure shows how changed files are copied from a protected server to LANtegrity's Intelligent Data Vault.

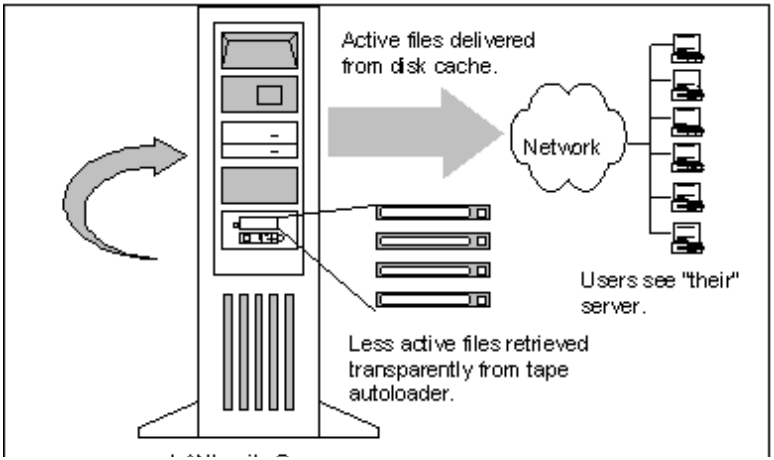


Figure 3-1. Replication of Changed Files

Is LANtegrity's default protection adequate for my needs?

LANtegrity's default continuous protection is designed to provide maximum coverage for your server with no changes required on your part. LANtegrity automatically protects all files that are not otherwise excluded on an ongoing, regular basis (by default, once every 15 minutes). This procedure ensures that all required files will be available for stand-in or restorations.

A LANtegrity Server provides continuous protection for all files on the protected servers except for a few files that are on the Master Exclusion sheet. Print queue files, for example, are on this sheet. You can add items to this sheet or remove them and place them back under protection. See Chapter 8, "Customizing File Protection," for more information.

What about deleted files and other types of data?

LANtegrity provides a verification process that together with continuous protection provides full coverage for your files. Verification saves the changes to NDS and Bindery information. In addition, it detects file and directory deletions, and keeps the cache up to date with read-active files, which are files that users opened to read but not update.

Can I change the protection method?

Yes. While the continuous method provides the most complete protection, there may be some files that you would want to remove from continuous protection. For example, you might consider using a protection schedule for a set of files that are internally consistent only at a certain time, such as database files.

Remember that if you change the method of protection on a file, you remove it from continuous protection. For safety's sake, you should leave nearly all of your files under continuous protection.

For a complete description of the ways in which you can modify LANtegrity's default continuous protection, see Chapter 3, "Protecting Server Data."

Managing Continuous Protection

Continuous protection requires only minimal management on your part. You may, however, from time to time want to change or review some of the settings for continuous protection. Most of the settings are accessible from the Configure LANtegrity Server panel. The settings specify the following:

- Protection cycle
  The protection cycle specifies how frequently the LANtegrity Server scans a protected server for changed files.

- Verify schedule
  Verification is the process whereby LANtegrity collects the mostly static data about files, such as file security and attributes. By default, a verify job runs nightly at 7 PM.

- NetWare 4 Directory Services (NDS) container that you want to protect

- The NDS container in which to store protected NetWare 3 Bindery objects
  These settings enable logins during stand-in.

- Change detection method for continuous and scheduled protection
  You can specify the archive bit or date/time stamp method. The default is the archive bit method.

- Maximum latency period for continuous protection
  Maximum protection latency is how long LANtegrity waits before sending an alert if it is taking longer than a specified time to check all files.

- Logging options for continuous protection
  These options include logging all files, error, and active files.

You can also remove selected files from continuous protection by placing them on the Never Protect sheet, Master Exclusions sheet, or a custom protection schedule. These methods are described in Chapter 8, “Customizing File Protection.”

Changing the protection cycle

The protection cycle specifies how often LANtegrity scans a protected server for changed files. The default setting for the protection cycle is 15 minutes. A faster scan rate consumes more server and network resources. A slower scan rate uses less resources but increases the time between saves. In this case, if stand-in occurs, the saved files will be older and users may not find their latest work.

Before setting a new protection cycle for a server, monitor LANtegrity's protection statistics for the server. For instructions on how to do this, see Chapter 4, "Checking Protection Statistics."

You can also set the **Maximum protection latency *before* an alert is issued** for the LANtegrity Server. Protection latency is how long it takes LANtegrity to respond to a detected change. It is usually equal to the scan rate but may increase during unusually busy times. For information on how to set the maximum protection latency, see "Setting the maximum protection latency period" on page 35.

Follow the procedure below to set the protection cycle for a server

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 showing a list of the available servers.
3.	Select the server whose protection cycle you want to change.
4.	For **Protection Cycle Time**, type the number of minutes for the new scan rate.

You can continue to set the protection cycle for additional servers or you can close the Configure Protected Servers panel.

Changing the verify schedule

Verification complements continuous protection to assure full coverage. The following changes are saved only when a verify job is active:

- Changes to a NetWare 3 Bindery and, optionally, to a NetWare 4 NDS.
- Deleted files and directories.
  If a file or directory was deleted from the protected server since completing the last verify job, LANtegrity marks the file or directory as deleted in the Intelligent Data Vault.
- Changes to file security and extended attributes.
- Restored files whose archive bit was cleared or older restored files when the date/time stamp method is used.
- Read-active files.
  A read-active file is a file that a user accessed recently but did not change. LANtegrity identifies and maintains these files in its disk cache. If a file has been read but not changed, LANtegrity ensures that the file is in its cache so that stand-in service can respond quickly

  To conserve network resources, LANtegrity copies read-active files to the cache from the Online tape set, not from the protected servers.

LANtegrity does not consider a server protected until it successfully complete its first verify job. Until then, LANtegrity does not have a copy of the files on the protected server under continuous protection and the Bindery on a NetWare 3 server is not protected. Also, LANtegrity does not allow you to initiate stand-in service for a server until at least one verify job completed. During the initial verify job, the LANtegrity Server copies all files under continuous protection from the protected server. If the protected server contains a large amount of data, this may take a long time.

Subsequent verify jobs are started by default on the verify (7PM) schedule, which you can change. While running the nightly verify job, LANtegrity scans only files that are under continuous protection.

✍ *To keep protected servers available for stand-in service, schedule the verify jobs on a regular basis. You should run at least one verify job per week.*

How does the verification work?

The verify job compares each directory or file under continuous protection in the LANtegrity Server's Intelligent Data Vault to the corresponding directory or file on the protected server. It detects file system changes that are not detected by continuous protection. If the file on the protected server is different, LANtegrity copies it to the LANtegrity Server. For example, continuous protection cannot detect changes to file attributes or NDS. A verify job also ensures that the most recently active files are available for instant access during stand-in.

LANtegrity displays all active verify jobs in the Current Jobs window. See Chapter 4, "Monitoring LANtegrity Operations," for more information about jobs.

When should I schedule a verify job?

You should schedule verify jobs during off hours, when network traffic is at a minimum. A verify job may require a significant commitment of system and network resources.

To set the time to run the verify schedule, use **Configure Verify Schedule**. Follow the procedure below to set the verify schedule.

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 'Verify Schedule'.

Response: LANtegrity displays the Configure Verify Schedule panel.

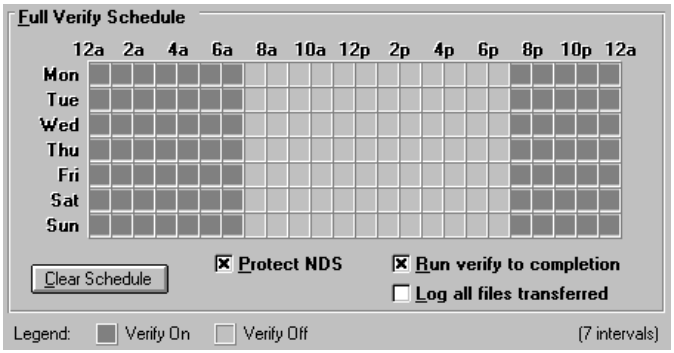


Figure 3-2. Configure Verify panel

Figure 3-2 shows a matrix consisting of hours of the day (columns) and days of the week (rows).

3. Identify the verify job by clicking one or more contiguous squares.

   ✍ *If you want the verify job to run to completion, select the **Run verify to completion** check box. This is the default.*

4. To specify a duration for a verify job run, after you click the starting square, click subsequent squares.

5. If you want the verify job to protect the NetWare Directory Services tree, click the Protect NDS check box. A verify job always saves Bindery information for each NetWare 3.x server.

6. If you want a record of the files that are being protected during a verify job, select 'Log all files transferred'.

   ✍ *By default, this option is deselected. Use 'Log all files transferred' only when you need the information because the log files can get quite large. To view the information provided by this option, open the Job Logs window as described in Chapter 4, "Monitoring LANtegrity Operations."*

7. When you finish making changes to this panel, select another option from the panel on the left or click Close.

Verifying a server on demand

There may be occasions when you want to start a verify job apart from the scheduled verify job (for example, before scheduled maintenance or after a major change to NDS). Follow the procedure below to verify a server on demand.

Step	Action
1.	Click the Protected Servers button or select **Tools/Protected Servers**. **Response**: LANtegrity displays the Protected Servers window.

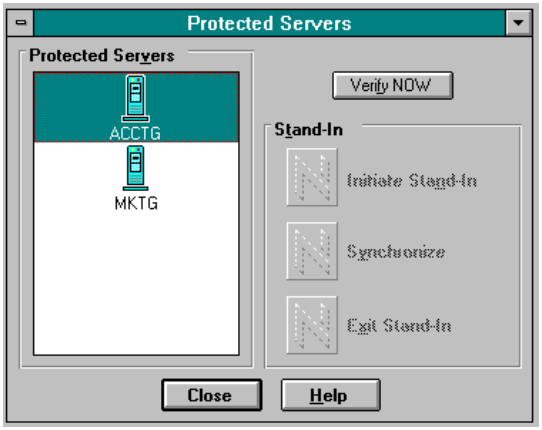


Figure 3-3. Protected Servers window

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.

Protecting NetWare 4 NDS

LANtegrity allows you to identify the NDS container that you want to have the LANtegrity Server protect. LANtegrity protects the designated NDS container and the subtree of which it is the root during a verify job. This protection provides a safe copy of NDS on tape in case of a disaster.

Novell recommends that you replicate all partitions of the NDS tree on multiple servers using the facilities provided by NetWare 4.

Follow the procedure below to identify the NDS Protection Container.

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 container name for the NDS container in the NDS Protection input box.

Protecting NetWare 3 Bindery

You can identify the destination NDS container in which to store protected NetWare 3 Bindery objects. To do this, you enter the distinguished name of a container that you created on the LANtegrity Server. See the *Setup Guide* for more information.

When you protect the NetWare 3 bindery, LANtegrity does the following:

- Protects the files that represent the bindery files to tape.
- Converts objects stored in the NetWare 3 bindery to NetWare 4 NDS objects.
- Creates two OU's for each NetWare 3x server at that location

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 container that you created in the Bindery Protection: input box.

Choosing a different detection method

You can configure LANtegrity to use either of two methods for detecting changed files. Specifically, you can instruct LANtegrity to check each file's archive bit, or last modified date/time stamp. Both methods provide full coverage for all files. By default, LANtegrity uses the archive bit method.

How LANtegrity uses the Archive Bit

Using the archive bit is the default method for detecting file changes. It is the preferred method because it is more efficient and provides better accuracy and performance.

The archive bit is a NetWare file attribute. NetWare turns it on each time a file is saved (that is, written to disk). LANtegrity scans for any files that have the archive bit on and saves them to the LANtegrity Server's Intelligent Data Vault. Once LANtegrity saves a file it sets the file's archive bit to off or change the protection method.

✍ *Other programs on your network (typically backup utilities) may also use and re-set the archive bit. To ensure that LANtegrity can correctly detect changed files, make sure that the protected servers contain no other program that clears the archive bit while LANtegrity is running.*

How LANtegrity uses the Date/Time Stamp

Every file has a date/time stamp that identifies when the file was last written to disk. With this method, LANtegrity compares a protected file's current date/time stamp against the date/time stamp it had when LANtegrity last copied it to the Intelligent Data Vault. If the current date/time stamp is different, LANtegrity copies the updated file to its Data Vault.

You should use this method only if your users' systems contain programs (for example, backup utilities) that modify the file archive bit setting. Follow the procedure below to change the detection method.

Step	Action
1.	Click the 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.

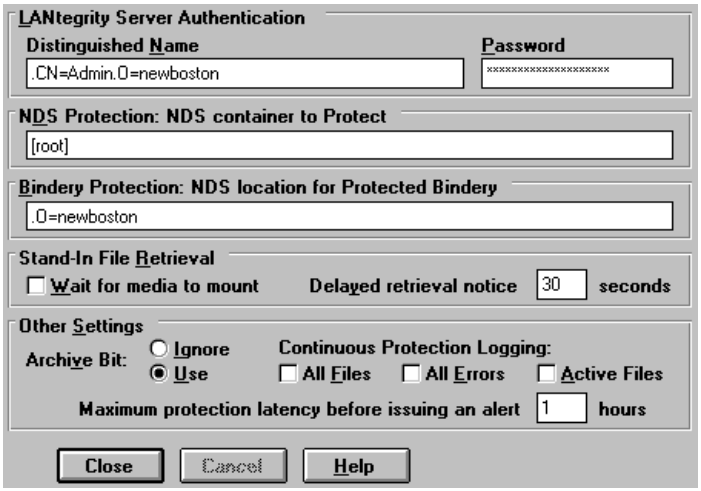


Figure 3-4. Configure LANtegrity Server panel

3. To use the archive bit method, click Use. To use the date/time stamp method, click Ignore.

4. When you are finished making changes to this panel, click Close.

Setting the maximum protection latency period

Protection latency is the difference between the time a file is changed and the time at which the LANtegrity Server saves the file. Optimally the protection latency period is equal to the setting for the protection cycle, which by default is 15 minutes.

The maximum protection latency period is how long the LANtegrity Server waits to send an alert if it is taking longer than a specified time to check all files. The default is 8 hours. The seemingly high number for maximum protection latency is to allow for protection slowdowns at unusually busy times (for example, during stand-in or peak network usage. Follow the procedure below to change the maximum latency period.

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 number of hours that LANtegrity waits in the ‘Maximum protection latency before issuing an alert’ input box.

Setting continuous protection logging

Continuous protection logging allows you to select logging for all files, all errors, or active files only. Usually you will leave these options off and use them only when you are testing protection.

✍ *Selecting either All Files or All Errors quickly increases the size of the **System Log**.*

- **All files.** Logs all of the files that are copied during each scan of the file system.
- **All errors.** Logs all of the errors that occur during each scan of the file system. Errors such as open files happen frequently during continuous protection. Daily verify jobs also report these errors.
- **Active files only.** Logs only files that change many times during a day. You can use this option when you're trying to decide if a frequently changing file needs to be put on a schedule.

Follow the procedure below to set continuous protection logging.

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.	Set the type(s) of protection logging you want by clicking **All Files**, **All Errors**, and/or **Active Files**.
4.	Close the window.

4 Monitoring LANtegrity Operations

Overview

This chapter describes how to monitor and control LANtegrity's operations by using the following tools:

- ***Job Log.*** Jobs are requests initiated by a user either manually or on a schedule. You can cancel any job. LANtegrity writes one top-level entry for each job to this log. The first entry is always the System Log. Each entry is associated with additional details.

- ***Alert Status Log.*** LANtegrity writes alerts to this log. Alerts are messages that inform you of conditions that may require your attention.

- ***System Log.*** LANtegrity writes system-wide messages, details of alerts, and errors to this log.

- ***Configure Alert Dispatching Panel.*** LANtegrity provides this control panel so you can distribute alerts to more people and thereby increase the chances that they will be quickly noticed and resolved.

- ***Current Jobs Window.*** LANtegrity provides you with information about each active job that you can update by pressing F5.

- ***Statistics Window.*** LANtegrity provides a statistical display that shows the protection effectiveness for individual protected servers.

Monitoring the Job Log

LANtegrity uses the **Job Log** to post a one-line, top-level entry for each job. The entry includes the job ID number, a description of the job, the creation time, the time of the latest update, and status. When you double-click on an entry, you can view details about the job. Periodically, LANtegrity monitors the Job Log and removes older entries when the log contains more than 100 entries.

What type of information is posted in the Job Log?

The Job Log contains a reverse chronological list of LANtegrity Server operations that start jobs. These activities include scheduled protection, verification, file restoration, and stand-in. In addition, the Job Log contains an entry for the **SYSTEM LOG**. SYSTEM LOG is always the first entry.

Accessing the Job Log

Follow the details below to access the Job Log.

Click the Logs and Alert Status button or select **Tools/Logs** and **Alert Status**. LANtegrity displays the Job Log, showing the reverse chronological list of job entries.

✍ *If the Alert Status window is displayed, click the Job Log button to switch to the Job Log.*

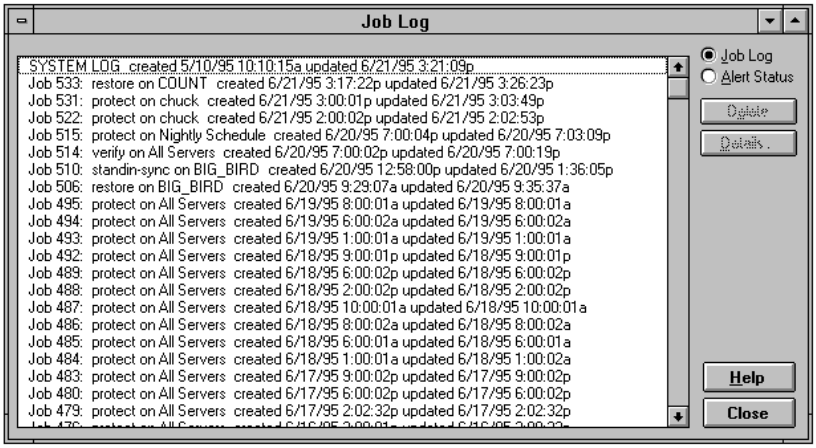


Figure 4-1. Sample Job Log

Interpreting Job Log entries

The entries in the Job Log identify specific jobs. Each entry consists of:

- **The LANtegrity-assigned ID for the job** (for example, “Job 149"). Jobs are listed in reverse chronological order according to their assigned IDs. Recent jobs appear first, followed by older jobs.

- **The message text describing the job** (for example, “restore on server name”). The message text typically identifies the request that originated the job.

- **Progress information** (for example, “created 8:58:04 updated 8:58:04”). As the job progresses, the update information may change. Press F5 to update the information on the screen.

- **Completion status** (for example, “1 error”). The completion status indicates whether the job was successful or experienced errors. A successful job has no completion status.

Viewing Job Log entry details

For each job in the Job Log, you can access additional, more detailed information. Follow the directions below to view Job Log entry details.

Step	Action
1.	On the Job Log, select the entry for which you want more information.
2.	Click Details or double-click the selected entry. **Response**: LANtegrity displays the detailed log for the selected job. The detailed log provides an entry for each of the steps in the job's processing.

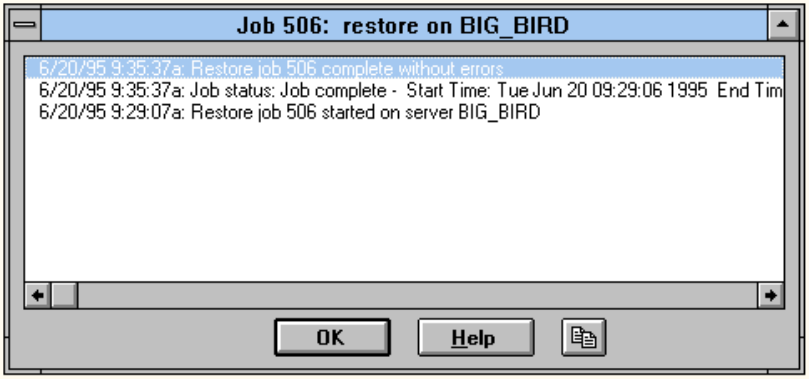


Figure 4-2. Sample log for server Big_Bird

You may have to scroll the window horizontally to display all of the message text.

Steps at which an error occurred are shown highlighted in red. For each reported error, LANtegrity provides an explanation and a recommended remedy.

3. After examining the job details, click OK to return to the Job Log.

Copying Job Log entry details

Follow the details below to copy Job Log entry details.

With the desired job displayed in the Job detail window, click the Copy icon. LANtegrity sends the job detail information to the Clipboard from which you can paste it into a file.

Deleting Job Log entries

When the Job Log expands beyond one hundred entries, LANtegrity purges the oldest entry. You can also manually delete entries. Follow the procedure below to delete Job Log entries.

Step	Action
1.	On the Job Log, select the entries you want to delete. ✍ *To select a sequence of entries, hold down the* SHIFT *key and click the first and last entries in the sequence. To select multiple individual entries, hold down the* CTRL *key and click each entry.*
2.	Click Delete. **Response**: LANtegrity asks you to confirm the deletion.
3.	Click Yes to delete or No to cancel.

Monitoring Alerts

LANtegrity uses the **Alert Status window** to provide a reverse chronological list of all recorded alerts. An alert is a message that notifies you about a significant event or that signals an error condition to which you may have to respond.

What actions do alerts require?

Some alerts request you to insert or remove tapes from the autoloader. Other alerts notify you that a protected server is no longer communicating and may need stand-in services. Most alerts, however, notify you about the successful completion of jobs and do not require any action.

You can view a complete list of the possible alerts in the Configure Alert Dispatching panel. See "Dispatching Alerts" on page 49.

What if I fail to respond to an alert that requires action?

LANtegrity continues to operate as long as it can and then it suspends its operations. Protection and stand-in service may degrade in the case of a long delay.

Responding to alerts in a timely fashion is a critical part of your job as a LANtegrity administrator.

How do I know if someone else has responded first?

LANtegrity maintains the alert in the **Alert Status** window until it is deleted. Whoever responds to an alert should delete the alert from the Alert Status window. The details of the alert remain in the System Log or in the Job details log.

Accessing the Alert Status window

Follow the details below to access the Alert Status window.

Click the Job Logs and Alert Status button or select **Tools/Logs** and **Alert Status**. LANtegrity displays the Alert Status window, showing the reverse chronological list of alerts.

✍ *If the Job Log is displayed, click the Alert Status button to switch to the Alert Status window.*

Interpreting alerts

The entries in the Alert Status window are messages that inform you of conditions that may require your attention. Each entry consists of:

- The severity level of the alert. LANtegrity indicates the relative importance of each alert by assigning it a severity level. There are four levels, each distinguished by a separate icon:

This icon...	Signifies...
	Information only.
	A minor problem.
	A severe problem.
	A critical problem.

- The LANtegrity-assigned ID for the alert (for example, “739”). Alerts are listed in reverse chronological order according to their assigned IDs. Recent alerts appear first, followed by older alerts.

- The event date and time (for example, “5/18/95 11:30:16”). This is the date and time of the event that produced the alert.
- The description text (for example, “Autoloader attention requested”). LANtegrity provides a message text that describes the event responsible for the alert.

Viewing alert details

For each alert in the Alert Status window, you can access additional, more detailed information. Follow the procedure below to view alert details.

Step	Action
1.	On the Alert Status window, select the alert for which you want more information.
2.	Click Details or double-click on the alert. **Response**: LANtegrity displays the details in a Job details window or the System Log. If the alert is related to a job, LANtegrity displays the details in the Job details window. The detailed log for the job provides an entry for each of the steps in the job’s processing. For a description of the detailed information provided, see “Viewing Job Log entry details” on page 40.

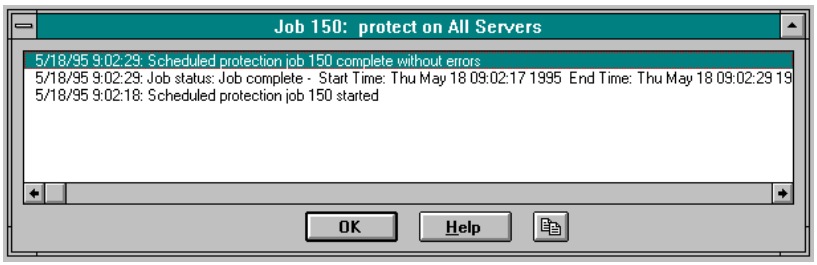


Figure 4-3. Job log for All Servers

If the alert is not related to a job, LANtegrity displays the details in the System Log. LANtegrity displays the System Log with the status message for the alert highlighted. When the alert signals a critical condition, LANtegrity highlights it in red.

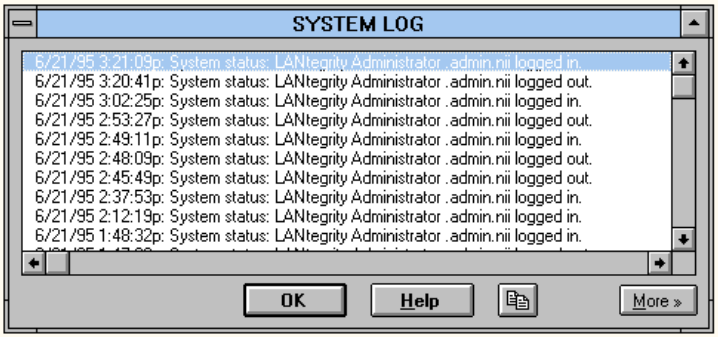


Figure 4-4. Sample system log

The status message provides detailed information about the event that produced the alert. If LANtegrity resolved the problem by taking some action on its own, the message indicates what this action was.

✍ *You may have to scroll the window horizontally to display all of the text in a message.*

3. After examining the alert details, click OK to return to the Alert Status window.

Deleting alerts

To indicate that you responded to an alert, delete it from the Alert Status window. The details of the alert remain in the log where they were recorded: the System Log or the Job Log. When the Alert Status log expands beyond one hundred entries, LANtegrity purges the oldest entry.

Follow the procedure below to delete alerts.

Step	Action
1.	On the Alert Status window, select the alerts you want to delete. ✍ *To select a sequence of entries, hold down the* SHIFT *key and click the first and last entries in the sequence. To select multiple individual entries, hold down the* CTRL *key and click each entry.*
2.	Click Delete. **Response**: LANtegrity asks you to confirm the deletion.
3.	Click Yes to delete or No to cancel.

Monitoring the System Log

LANtegrity uses the **System Log** to maintain detailed information about its operations and its interactions with the network and the protected servers. LANtegrity posts details for alerts and significant events to the log, where they are available for monitoring.

The System Log contains messages that are not specific to a job. For example, it includes login and logout times and system configuration errors.

You can access the System Log from the Job Log window.

Accessing the System Log

This section explains how to access the System Log from the Job Log window. You also access the System Log when you view the details of some alerts. For more information, see "Viewing alert details" in the previous section. Follow the procedure below to access the System Log.

Step	Action
1.	Click the Job Logs and Alert Status button or select **Tools/Logs** and **Alert Status**. **Response**: LANtegrity displays the Job Log. SYSTEM LOG is always the first entry in the Job Log. ✍ *If the Alert Status window is displayed, click the Job Log button to switch to the Job Log.*
2.	Select SYSTEM LOG and click Details or double-click on SYSTEM LOG. **Response**: LANtegrity displays the System Log. Entries associated with critical errors are shown highlighted in red. When the System Log has more than one screen of entries, it displays the More button.
3.	If you want to view the next screen, press the More button. If you want to view the previous screen, press the Back button.

Interpreting System Log entries

The entries in the System Log identify specific events and alerts. Each entry consists of:

- **The date and time** (for example, “5/18/95 8:24:40”). This is the date and time that the event or alert occurred.
- **Status indicator** (for example, “System Status”). This indicates whether the entry is associated with a system activity (such as an Administrator login) or a specific operation request (such as a tape load).
- **Message text** (for example, “LANtegrity Administrator logged out”). This is the text description of the event or alert.

Note that the System Log, unlike the Job Log and the Alert Status window, does not provide more detailed information for its entries.

Saving the System Log

Before you clear the System Log, you can save a copy of it. Follow the details below to save the System Log. With the System Log displayed, click the Copy icon. LANtegrity sends the entire contents of the System Log to the Clipboard from which you can paste it into a file.

Clearing the System Log

The System Log, unlike the Job Log and the Alert Status window, does not allow you to delete individual entries from it. If you want to clear out the log, you can delete it. After that, LANtegrity automatically recreates the System Log as soon as it needs to record new information. Follow the procedure below to clear the System Log.

Step	Action
1.	On the Job Log, select the SYSTEM LOG entry.
2.	Click Delete and confirm the deletion.
3.	Click Yes to delete or No to cancel.

Dispatching Alerts

LANtegrity always posts alerts to the **Alert Status** window. In addition, it allows you to route them to the following destinations:

- An SNMP-compatible application program.
- Up to five separate NDS users.
- The system console on the LANtegrity Server.

LANtegrity provides these additional destinations to make sure that important alerts receive prompt attention. You establish additional destinations for alerts by using the Configure Alert Dispatching panel. Follow the procedure below to access the Configure Alert Dispatching panel.

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 ‘Alert Dispatching’. **Response**: LANtegrity displays the Configure Alert Dispatching panel. The list box shows all of the possible LANtegrity alerts. Some alerts may require you to do something.

Selecting additional destinations for alerts

LANtegrity supports three types of additional destinations for alerts. Each alert in the list box has three buttons associated with it. You control routing for a given alert by clicking one or more of these destination buttons. LANtegrity assigns SNMP as a default location for all alerts. This is why, when you first access the Configure Alert Dispatching panel, all the entries in the list have the rightmost button set to on.

What are the possible destinations for alerts?

The three available destination choices are as follows:

- ***Generate SNMP Alert.*** This choice instructs LANtegrity to generate an SNMP (Simple Network Management Protocol) trap message and broadcast it over the network to be received by any SNMP network management applications that are listening. LANtegrity does this for each occurrence of the associated alert.

  The LANtegrity installation software includes a customized MIB (Management Information Base) file for use by your SNMP-compatible applications. The MIB file specifies the appropriate text string translation for any alerts. It also provides network identification for the LANtegrity Server that broadcasts the trap.

- ***Send Message.*** This choice tells LANtegrity to send an alert to a specific NetWare user when the user logs in. For each alert, you can select up to five different users.

  LANtegrity uses a NetWare send message function to distribute alerts to the selected users. Alerts are displayed one at a time, in reverse chronological order.

  To ensure that dispatched alerts receive prompt attention, you should select only users who are available during the main hours of LANtegrity operation. However, you can also instruct LANtegrity to hold alerts for a specified number of hours and send them when the user logs on within a period that you specify.

  You identify the user recipients for a given alert by entering their usernames in the Configure Send window.

- ***Display on LANtegrity Server System Console.*** This choice tells LANtegrity to send the associated alert to the LANtegrity Server's system console, where it can be viewed locally or remotely by using a NetWare RCONSOLE feature.

Follow the procedure below to select additional destinations.

Step	Action
1.	On the Configure Alert Dispatching panel, click the alert you want to dispatch. Note that each alert has three buttons, one for each of the three possible destinations. ✍ *To select a sequence of entries, hold down the* SHIFT *key and click the first and last entries in the sequence. To select multiple individual entries, hold down the* CTRL *key and click each entry.*
2.	Click the button that corresponds to the destination you want. To select multiple destinations, click the additional buttons.
3.	If you selected Send Message, click Send To to identify users to receive the alert. ✍ *See* *"Identifying user recipients" on page 51*.
4.	When you finish selecting destinations for alerts, click Close.

Identifying user recipients

When you select Send Message on the Configure Alert Dispatching panel, you must identify users to receive the alert. Follow the procedure below to identify user recipients.

Step	Action
1.	On the Configure Alert Dispatching panel, select Send Message for a given alert and then click Send To. **Response**: LANtegrity displays the Configure Send window.
2.	Type a valid NetWare username in the Username box. ✍ *The user must have login rights to the LANtegrity Server. Be careful to specify the NetWare username.*

3. In the Hold message for box, type the number of hours that LANtegrity will retain the alert. The default hold time is 72 hours and the maximum is 999 hours.

   Response: When the time expires, LANtegrity discards the alert.

4. Click Add to add the user to the recipient list.

5. Start with the username again and repeat steps 2 through 4 for any additional users.

   You can add up to five users to the recipient list. For each user, you can specify a different hold time. To remove a user from the list, select the username and then click Delete.

6. When you finish identifying users, click OK to return to the Configure Alert Dispatching panel.

Managing Current Jobs

For each job that the LANtegrity Server starts, LANtegrity creates a job entry in the Current Jobs window. Using the Current Jobs tools, you can monitor the progress of these jobs and cancel them. When a job is complete, LANtegrity deletes the entry from the window. Follow the procedure below to access the Current Jobs window.

Click the Current Jobs button or select **Tools/Current Jobs**. LANtegrity displays the Current Jobs window. To sort the list, click on a column heading.

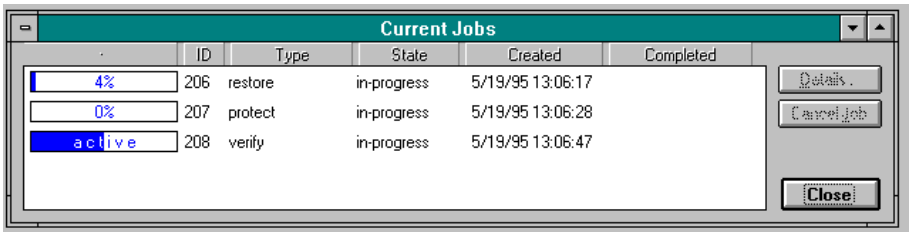


Figure 4-5. Current Jobs dialog

Interpreting job information

The Current Jobs window displays six fields for each job entry. The six fields are described below.

- ***Percent Completion.*** How much of the job is complete. LANtegrity displays a progress indicator and either a percent or the word “active.”
- ***ID***. The system-assigned ID number for the job.
- ***Type.*** The job’s type:
  - *Exit Stand-in.* A user request to exit stand-in with synchronization.
  - *Protect.* A user or scheduled request to protect files on a specific protection schedule.
  - *Restore.* A user request to restore files to a protected server.
  - *Restore-NDS.* A user request to restore the NetWare NDS.

  - *Stand-in Sync.* A user request to synchronize while the LANtegrity Server is standing in for a protected server.
  - *Verify.* A user or scheduled request to compare the file copies on the LANtegrity Server against a protected server's files.

- ***State***
  - In-Progress. The job is processing. The Percent Completion indicates how much of the job has completed.
  - Canceling. The job is canceled.

- ***Created.*** The date/time that the job was requested.

- ***Completed.*** The date/time when the job completed.

Viewing job details

LANtegrity provides a detailed view of the status of a job, including information on the amount of work needed to complete the request. Follow the procedure below to view job details.

Step	Action
1.	Click the Current Jobs button or select **Tools/Current Jobs**. **Response**: The Current Jobs window appears.
2.	Select a job entry.
3.	Click Details.

Response: LANtegrity displays the Job Detail window.

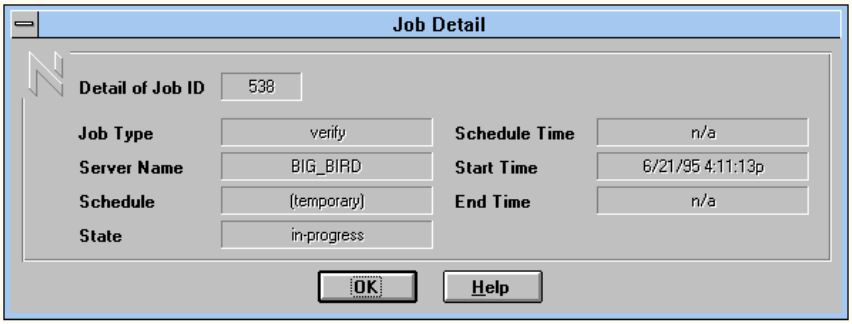


Figure 4-6. Job Detail dialog

The job detail fields are defined as follows:

Field	Description
Job ID	The ID of the job selected in the Current Jobs window.
Job Type	The type of request. For the list of valid requests, see "Interpreting job information" on page 53.
Schedule	For scheduled requests, the name of the schedule that initiated the job.
State	The current state of the request. For the list of possible states, see "Interpreting job information" on page 53.
Schedule TIme	For delayed requests, the time that the request will execute next.
Start Time	The date/time that the request was entered.
End Time	The date/time that the request completed or was canceled.

Canceling a job in progress

You can cancel a job request prior to its completion. Follow the procedure below to cancel a job in progress.

Step	Action
1.	From the Current Jobs window, select the job entry you want to cancel.
2.	Click Cancel Job.
3.	Click Yes to confirm your request. **Response**: LANtegrity removes the job from the window, but the Job Log still retains the entry.

Checking Protection Statistics

Since file protection is one of LANtegrity's most crucial operations, LANtegrity provides a way to check on its effectiveness. Use the Statistics window so you can determine how well file protection is working on the LANtegrity Server and each of your protected servers.

Accessing the Statistics window

You can open as many **Statistics** windows as you want to view at once and select a different server in each window. By arranging the windows on your desktop, you can compare LANtegrity's file protection performance with respect to the different servers. Follow the procedure below to access the Statistics window.

Step	Action
1.	Click the Statistics button or select **Tools/Statistics**. **Response**: LANtegrity displays the Statistics window.

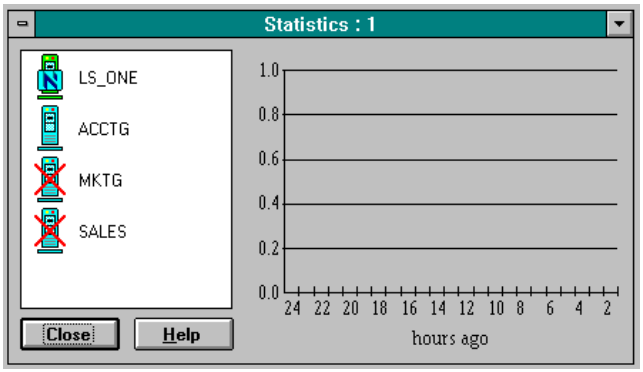


Figure 4-7. Sample Statistics window

2. In the list box, select the server whose statistics you want to view.

Response: If you choose a protected server, LANtegrity updates the graph to show the server's file protection latency (in minutes) over the last 24 hours.

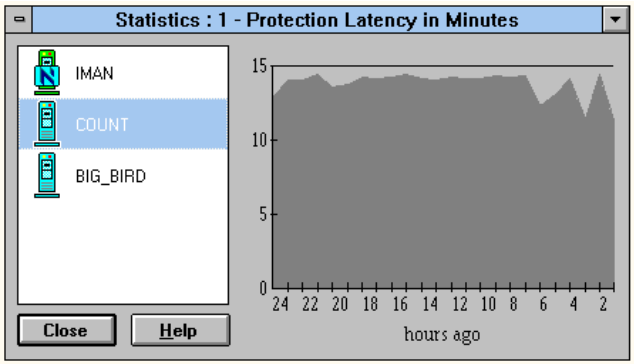


Figure 4-8. Sample Statistics Graph

If you choose the LANtegrity Server, LANtegrity displays a graph showing the ages of files in the disk cache.

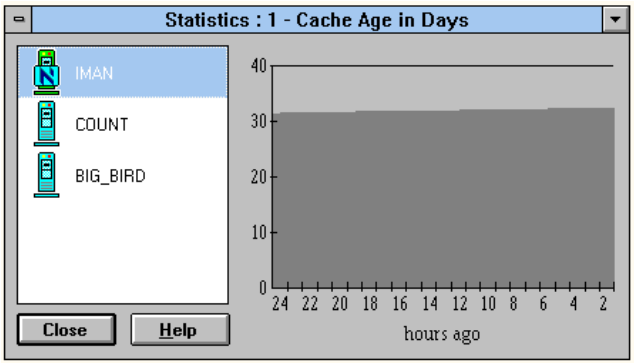


Figure 4-9. Cache Age Graph

✍ *To update a server's Statistics window, press* F5.

Interpreting statistics information

On the LANtegrity Server, the effectiveness of file protection is measured by the ages of files in disk cache. On a protected server, LANtegrity represents file protection effectiveness as protection latency. Once you open a window for a protected server, LANtegrity recalculates the latency value on that protected server only and updates the window.

What is cache age?

For a LANtegrity Server, cache age is the measure of how long an unmodified file remains in cache before it is removed to make room for new files. Ideally, a server's cache should hold unmodified files for 5-6 days. Thus, when the LANtegrity Server provides stand-in services, all files accessed in the last few days are instantly available.

If the cache age is consistently low (1-2 days) on a LANtegrity Server, you probably need to increase the amount of disk space configured as the cache volume. See the Setup Guide for information about recommended configurations.

What is protection latency?

For a protected server, protection latency is the average time it takes the LANtegrity Server to protect an updated file. It is calculated as the difference between the file's update time and the time at which LANtegrity copies the file to the LANtegrity Server's cache for protection. If the protection latency is consistently higher than expected, the number of files changing on the protected server may exceed the ability of the LANtegrity Server to protect them within an acceptable period of time.

The latency value identifies how current the LANtegrity Server's copies of protected files are. If a failure causes a protected server to go down, the copies of your files on the LANtegrity Server should be no older than the time indicated by the latency value.

5 Managing the Autoloader and Media Library

Overview

The autoloader provides the Online and Offsite tape storage, which together with the disk cache, forms the hierarchy of LANtegrity's Intelligent Data Vault. Each LANtegrity Server requires at least one autoloader to provide automated tape storage for files. The tapes in the autoloader contain your recovery files for stand-in service, restoring files, and disaster recovery. The autoloader also creates and provides access to the historic library of all of the protected files on your network.

Except for removing, inserting. and labeling tapes, you do not have to manage the autoloader or tape library. LANtegrity automatically operates the autoloader and media rotation. LANtegrity places at least two copies of every protected file on tape: one to the Online tape set, which remains in the autoloader at all times, and one to the Offsite tape set which is intended for storage at another site. These tapes allow you to restore both current and historic files or recover the LANtegrity Server in the event of a disaster.

This chapter describes the types of LANtegrity tapes. It also explains how to configure and manage the autoloader and tapes using the following tools:

- ***Configure Autoloaders.*** LANtegrity provides this window so you can change the settings for selecting an autoloader, add an additional tape compare process, and determine what types of tapes to overwrite.
- ***Autoloader Management.*** Use this tool when you need to remove or insert tapes, pause or activate the autoloader, obtain information about the autoloader, and view the status and details of the autoloader and its tapes.
- ***Configure Media Rotation.*** LANtegrity provides this window so you can change the settings for rotating tapes.
- ***Media Inventory.*** Use this tool to review the contents of your entire tape library.

LANtegrity Tapes

Because LANtegrity automatically manages file protection, file restoration, and tape storage, you only have to occasionally insert or remove tapes, and label them.

You can configure the autoloader and media library. To perform these tasks, you should know how LANtegrity handles tapes. The LANtegrity Server typically contains the following types of tapes in its autoloader(s):

- One or more Online tapes, as members of the Online tape set.
- One current Offsite tape.
- Sometimes a full Offsite tape waiting to be removed.
- Sometimes a Legacy tape waiting to be removed.
- One Cleaning tape, if required by your autoloader.
- “Blank” tapes in the remaining tape slots.

The following figure shows how LANtegrity manages the Online, Legacy, and Offsite tapes.

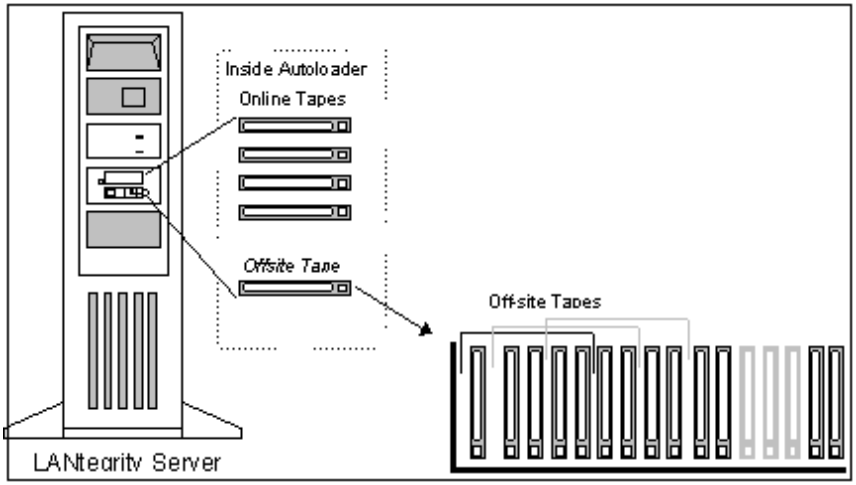


Figure 5-1. LANtegrity Management of Tapes: Onsite and Offsite

The following sections describe each type of tape.

Types of tapes

LANtegrity specifies the type of tape by its current use. While a tape is managed by LANtegrity, it may be used for several different purposes. For example, a blank tape can become an Online tape and finally a Legacy tape.

Online tape set

For each server that a LANtegrity Server protects, the Online set contains:

- At least one copy of all protected files.
- Most recently deleted files.
- Older files.

LANtegrity continuously updates the Online tape set with copies of the latest saved files. These files are used during stand-in or restoration if the files were purged from disk cache or if an older version of a file is needed.

✍ *Keep the Online tape set in the autoloader at all times. The LANtegrity Server keeps a list of the tapes that are currently in the set and warns you if you remove or select one for removal from the autoloader. If you remove a tape that LANtegrity needs from the autoloader, it sends you an alert.*

Periodically LANtegrity reviews the contents of the Online set and consolidates it. See "Consolidation of the online set" on page 62 for more information.

Consolidation of the online set

Consolidation is an automatic process that compacts the Online tape set. Consolidation allows LANtegrity to prevent the Online set from becoming unnecessarily large by replacing the oldest tape with a new one.

LANtegrity's continuous protection constantly sends copies of the newest modified files to the Online tapes. Eventually, the oldest Online tape has mostly older versions of files and deleted files.

During consolidation, LANtegrity reviews the oldest Online tape. Any files that are the most recent versions and are still active are copied to the newest Online tape. This old Online tape is no longer needed in the Online set. LANtegrity labels it a Legacy tape and marks it for removal from the autoloader.

✍ *Be sure to place the information from the electronic label on the Offsite tape's paper label when you remove the tape from the autoloader. Unless the paper label matches the electronic label, you cannot identify which tapes LANtegrity is requesting for a restore job, stand-in, or a recovery.*

Legacy tapes

Legacy tapes are old Online tapes that contain copies of all files that LANtegrity made daily, up to a time when it consolidated the Online set.

LANtegrity maintains an expiration schedule for the Legacy tapes so that you may keep them as an on-site history archive. You may find Legacy tapes useful for restoring older files. By default, LANtegrity expires the tapes after 90 days, after which you can make them available for reuse. For more information, refer to "Configuring Media Rotation" on page 86.

Offsite tape set

Like the Online set, the Offsite tape set contains at least one copy of all of the files currently stored on each protected server and those that were deleted. However, the Offsite set typically contains fewer file versions than the Online set because it is written to less frequently (every 6 hours or less).

An autoloader contains one or more Offsite tapes. As LANtegrity reaches the end of an Offsite tape, it sends an alert, marks the tape for removal, and starts a new tape. You can wait until the Offsite tape fills and then remove it or you can remove it every day; for example, every morning, which is equivalent to doing a full network backup. This routine increases the number of tapes in the set but it does keep the offsite tape set more up to date. You would use Offsite tapes under two conditions:

- When you need to restore older versions of files that pre-date the contents of your Legacy tape storage.
- In a disaster where you lose the LANtegrity Server and the Online tape set.

Therefore, we recommend that you store your Offsite tapes in a safe place at a **separate** site.

Offsite tape recovery sets

Each Offsite tape belongs to a set of tapes called a recovery set. A recovery set is the collection of Offsite tapes needed to fully recover a LANtegrity Server and all of the protected servers. It is equivalent to a full backup. The newest Offsite tape has the latest files. Combined with one or more tapes from the previous Offsite set, it completes a recovery set.

LANtegrity manages Offsite tapes on a rotation schedule and expires tapes that are no longer needed. See "Configuring Media Rotation" on page 86 for more information.

When the Offsite tape is marked for removal from the autoloader, LANtegrity creates an electronic label. For more information about labels, see "Tape labels" on page 66.

✍ *Be sure to place the information from the electronic label on the Offsite tape's paper label when you remove the tape from the autoloader. Unless the paper label matches the electronic label, you cannot identify which tapes LANtegrity is requesting for a restore job, stand-in, or a recovery.*

Cleaning tapes

If your autoloader requires a cleaning tape for regular maintenance, reserve one slot in each autoloader for the cleaning tape. LANtegrity assumes that the cleaning tape is in the last slot.

✍ *Unless you use a cleaning tape regularly in autoloaders that require one, you risk damaging the autoloader.*

LANtegrity manages the cleaning tapes and the schedule for cleaning the tape drive heads in the autoloader. It does the following automatically:

- Keeps track of the number of read/write actions performed by each of its tape drives.
- Loads a cleaning tape and cleans the drive heads when the manufacturer's recommended head cleaning interval is reached.
- Keeps track of the number of times a particular cleaning tape is used and notifies you when the cleaning tape must be replaced.

Blank tapes

Blank tapes are tapes that a LANtegrity Server uses for writing. By default, a LANtegrity Server writes to only two types of tapes:

- a new tape
- an expired tape that it marked expired.

As LANtegrity assigns new ID numbers to expired tapes, it keeps track of how many times the tape has been used. When a tape exceeds its useful life span, the LANtegrity Server notifies you that it no longer accepts it as a blank tape.

LANtegrity also accepts the following tapes as blank if you selected the corresponding overwrite option on the Configure LANtegrity Server window:

- A tape recorded by another product or other unrecognizable format, which LANtegrity identifies as an *other* type
- A tape written to by another LANtegrity Server, which this LANtegrity Server identifies as an *unknown* type

Tape errors

If LANtegrity detects a read error on any tape in the recovery set or on a tape from which you are restoring a file, it tries to read it several more times. If unsuccessful, the LANtegrity Server automatically looks for a duplicate of the file on the next most recent tape. If another tape is needed and it is not in the autoloader, the LANtegrity Server sends an alert to the **Alert Status** window. When you view the alert, click on it to see on which tape LANtegrity is requesting another copy of the file and insert that tape into the autoloader.

If LANtegrity detects a write error, it sends an alert and moves to another tape.

Tape labels

LANtegrity identifies each tape with an electronic label that you will see displayed in many windows in the LANtegrity Administrator interface. You need to write this information on the paper label of a tape when you remove it from the autoloader so that you can respond to LANtegrity requests for tape.

An example of a label is Off 55,6/13/95 46,5/17/95 7.

The following table describes the fields:

Field	Identifies
Type	A letter that indicates the type of tape. On=Online, **Cln**=cleaning, **Leg**=Legacy, and **Off**=Offsite. If the label does not start with a letter, it is a blank tape. If the type is **unknown**, the tape was created by another LANtegrity Server.
ID	A unique number that LANtegrity assigns to the tape.
Date	The date of the last write.
[ID, Date]	The ID and date of the first tape in the recovery set.
[N]	The number of tapes in this recovery set.

Configuring an Autoloader

You can use the Configure Autoloaders window on the General Configuration window to review the autoloader configuration settings. You can also

- Specify the autoloaders that the LANtegrity Server uses for Online and Off-site tape sets.
- Require a second read-compare for each tape in addition to the auto-loader's read-after-write operation.

Use this option on Offsite tapes only if you are concerned that your autoloader is not functioning correctly.

- Instruct the LANtegrity Server to overwrite tapes written by another product or another LANtegrity Server.

Follow the procedure below to access the Autoloader Management window.

Step	Action
1.	Click the General Configuration button or select **Tools/General Configuration**.
2.	Select 'Autoloaders' from the list box on the left. **Response**: LANtegrity displays the Configure Autoloaders window.

Dedicating an Autoloader for online or offsite tapes

When more than one autoloader is installed on a LANtegrity Server, you can specify which autoloader you want to use for Online tapes and which to use for Offsite tapes. We recommend that you retain the default setting of **Any Autoloader** for each setting. This enables the LANtegrity Server to:

- Retrieve files from all autoloaders simultaneously during stand-in.
- Distribute daily activities between the tape drives.
- Automate more of the tape management and minimize the number of tapes you have to handle.

Follow the procedure below to specify an autoloader for online or offsite tapes.

Step	Action
1.	Click the General Configuration button or select **Tools/General Configuration**.
2.	Select ‘Autoloaders’ from the list box on the left. **Response**: LANtegrity displays the Configure Autoloaders window. The autoloaders are listed in the ‘Online Autoloader’ and ‘Offsite Autoloader’ list boxes at the top of the window.
3.	Select a tape device from each list box.
4.	Click OK. ✍ *If you change windows within **General Configuration** without clicking Close or Cancel, any alterations you made to the previous window are saved.*

Requiring additional tape read comparisons

You can use LANtegrity to require an *additional* read comparison on the data after it is written to tape. You may want to use this option if you’re concerned that your autoloader is not functioning correctly. The options are:

- No compare options (the default).
- Compare offsite only.
- Compare online and offsite media.

Usually you do not select an additional read comparison. The autoloader automatically performs a read-after write, tape media have become extremely reliable, and the Onsite tapes are read a second time during LANtegrity’s consolidation process.

✍ *The second read compare process halves the speed of tape processing and doubles the wear on the drive.*

Follow the procedure below to require additional tape read comparisons.

Step	Action
1.	Click the General Configuration button or select **Tools/General Configuration**.
2.	Select ‘Autoloaders’ from the list box on the left. **Response**: LANtegrity displays the Configure Autoloaders window.
3.	Select the autoloader you want to manage.
4.	Under ‘Compare Option’, select the option you want to use. Select ‘Compare only offsite media’ to require another read comparison of the Offsite tapes. Select ‘Compare online & offsite media’ to require another comparison of Online and Offsite tapes.

Changing overwrite options

By default, a LANtegrity Server overwrites only tapes it marked expired. If you want a LANtegrity Server to overwrite tapes written by another LANtegrity Server or another product, you can change the overwrite options.

Follow the procedure below to change the tape overwrite options.

Step	Action
1.	Click the General Configuration button or select **Tools/General Configuration**.
2.	Select ‘Autoloaders’ from the list box on the left. **Response**: LANtegrity displays the Configure Autoloaders window.
3.	Select the autoloader you want to manage.

4. In the ‘Overwrite Options’ section, select or deselect the overwrite option(s).

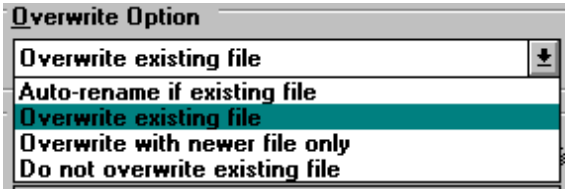


Figure 5-2. Overwrite Option group box

5. Select the overwrite option you want the LANtegrity Server to use.

   To overwrite tapes written by another LANtegrity Server, select ‘Unknown LANtegrity media’. To overwrite tapes written by another vendor or product, select ‘Unknown other-vendor media’.

Managing the Autoloader

Managing the autoloader is primarily a matter of responding to requests from LANtegrity to insert or remove a tape, and then labeling it. Otherwise, LANtegrity manages the autoloader and the tapes.

The LANtegrity tapes can be located:

- In the autoloader drive.
- In the autoloader magazine.
- Out of the autoloader, in your media library.

LANtegrity maintains the Offsite and Legacy tapes on a rotation schedule. For more information, see "Legacy tapes" on page 63 and "Configuring Media Rotation" on page 86.

LANtegrity automatically loads the tape that it needs if it is in the autoloader. When the tape is not in the autoloader, LANtegrity sends an alert. You can view alerts and other messages related to the autoloader in the **System Log** and the **Alert Status** window. See "Viewing log entries and alerts for tape activities" on page 72.

To respond to requests for a tape, you can use the **Autoloader Management** tool. From this window, you can:

- Pause or activate the autoloader.
- Insert or remove tapes.
- View the media.
- View the details of the tapes.

✍ *Unless you use the LANtegrity Autoloader Management window to pause the autoloader and notify the LANtegrity Server that you are removing or inserting tapes, you risk interrupting tape read/write activities and misapplying or losing track of tapes. See "Removing and inserting the tape magazine" on page 77 for more information.*

Viewing log entries and alerts for tape activities

Messages and alerts related to an autoloader are automatically posted to the System Log and to the Alert Status window. These messages notify you:

- When the autoloader requires you to insert or remove a tape.
- When autoloader activities such as an inventory occur.
- When any autoloader failure occurs.

You can also dispatch certain tape messages to the system console, or an SNMP-compatible notification systems, or broadcast to selected user's workstations by using the **Alert Dispatching** tool. See Chapter 4, "Monitoring LANtegrity Operations."

Accessing the Autoloader Management tool

You can view the media in an autoloader from the Autoloader Management window. Follow the details below to access the Autoloader Management tool.

Click the Autoloader Management button or select **Tools/Autoloader Management** to display the Autoloader Management window.

✍ *LANtegrity refers to the slots starting at 1. However, the slots on some autoloaders start at 0 (zero). So if you are using such an autoloader and LANtegrity refers to a tape for a particular slot, decrement the number by 1. For example, when LANtegrity requests you to insert a tape into slot 1, insert the tape into slot 0 (zero).*

From this window you can select one of two panels: **Remove Media** and **Insert Media.** The Remove Media panel displays the tapes in the autoloader. The Insert Media panel displays the tapes the LANtegrity Server needs and the other types of tapes you can insert.

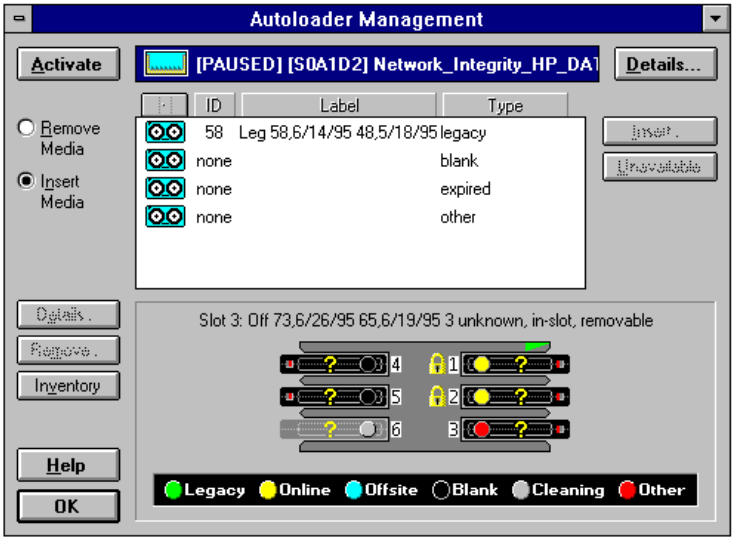


Figure 5-3. Autoloader Management dialog

Viewing the media you can remove

While the Remove Media panel is open, you can view information about the autoloader and its contents, force an inventory of the contents, pause and activate the autoloader, and notify LANtegrity that you are removing a tape. Follow the procedure below to view the Online Media.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
2.	Select the autoloader you want to view.
3.	Select ‘Remove Media’.

Response: The panel displays the contents of the selected autoloader.

The column headings on the panel are as follows:

Column	Description
Slot	The number of the magazine slot where the tape is located. LANtegrity refers to the slots starting at 1. However, some autoloaders start with 0 (zero). If you are using such an autoloader, when LANtegrity refer to a tape, decrement the number by 1.
ID	The number LANtegrity assigns to the tape.
Label	The information that identifies the tape. When you remove a tape from the magazine, use this information to label it. See "Tape labels" on page 66 for more information.
Type	Whether the tape is a blank, cleaning, expired, legacy, offsite, online, other (vendor), or unknown (other LANtegrity Server) tape. See "LANtegrity Tapes" on page 61 for more information.
Status	Where the tape is located (**in-slot** or **in-drive**) and if you can remove it from the autoloader (**removable** or **locked**). When the status is locked, leave it in the drive or else the files may not be accessible during stand-in.

Viewing the media you can insert

When the Insert Media panel is open, you can:

- View the requested tapes.
- Notify the LANtegrity Server that you are inserting the selected tape.
- Indicate that the requested tape is not available.

You can also view information about the autoloader and its contents, force an inventory of the contents, and pause and activate the autoloader. Follow the procedure below to view a request for a tape in the Insert Media panel.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
2.	Select the autoloader you want to view.
3.	Select 'Insert Media'. **Response**: The Insert Media panel lists any specific tape that the LANtegrity Server needs, followed by other types of tapes you may want to load into the autoloader: blank, expired, and other tapes.
4.	Select **View/Update View** to update the display or click F5. If you want to copy the list of tapes, copy them to the Clipboard. The column headings on the panel are described in the following table.

Column	Description
ID	A number LANtegrity assigns to the tape.
Label	Information used to identify the tape. See "Reviewing the Media Inventory" on page 89 for more information.
Type	Whether the tape is an online, blank, cleaning, expired, legacy, offsite, or other. In this case, "other" is an option to insert a LANtegrity tape. When you click on this option, LANtegrity prompts you for the tape ID.

5. If you have the requested tape, continue to "Responding to requests for a tape" on page 76.

✍ *LANtegrity refers to the slots starting at 1. However, the slots on some autoloaders start at 0 (zero). So if you are using such an autoloader and LANtegrity refers to a tape for a particular slot, decrement the number by 1. For example, when LANtegrity requests you to insert a tape into slot 1, insert the tape into slot 0 (zero)*

Responding to requests for a tape

When the LANtegrity Server needs a tape for the autoloader, it does the following:

- Sends an alert, which you can dispatch to several locations.

  For example, LANtegrity sends an alert when it needs a blank tape. Alerts range from a low level to critical. See Chapter 4, "Monitoring LANtegrity Operations," for more information.

- Places an entry in the **System Log** that gives you specific instructions about which tapes to remove or insert.

- Updates the **Insert Media** and **Remove Media** panel on the Autoloader Management window.

When you receive the alert, you can use the Insert Media panel to see the request for the tape. For information about how to access the panel, see "Viewing the media you can insert" on page 74.

Then use the instructions in the following sections to remove or insert the tape magazine, and to remove and insert tapes.

Removing and inserting the tape magazine

Before you remove the magazine from the autoloader, you need to suspend its operation. To do this, use the **Pause** button on the Autoloader Management window. When Pause has changed to **Activate**, you can eject the magazine and remove or insert tapes.

✍ *Unless you use the Autoloader Management window to pause and activate the autoloader, you risk interrupting tape read/write activity and mislabeling or losing track of tapes. Do not eject the magazine until the pause operation is complete.*

When you are finished and the magazine in back in place, press Activate on the Autoloader Management window. LANtegrity uses the information you supply from this window to update its inventory of tapes in the autoloader. Follow the procedure below to remove the magazine from the autoloader.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
2.	Select the autoloader you want to manage.
3.	Click Pause and wait for the operation to complete. **Response**: LANtegrity pauses the autoloader and changes the Pause button to Activate.
4.	At the autoloader, eject the magazine.

Follow the procedure below to insert the magazine into the autoloader.

Step	Action
1.	Insert the magazine into the autoloader.
2.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
3.	Select the autoloader you want to manage.
4.	Click Activate. **Response**: LANtegrity activates the autoloader and changes the Activate button to Pause.

Removing tapes

When tapes are no longer required by the LANtegrity Server, you should remove them from the autoloader. The LANtegrity Server animates the tape that needs to be removed in the Autoloader Management window.

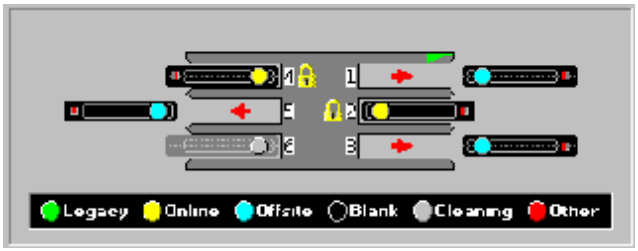


Figure 5-4. Animated tapes from the Autoloader Management window

You should remove these tapes regularly and replace them with blank tapes. Sometimes, when the LANtegrity Server requests a specific tape, no tapes are waiting to be removed. In this case, you have to decide which tape to remove.

What tapes you can remove

The first candidate for removal is a blank tape. If there is no blank tape in the magazine, then you can remove any tape that is in the magazine (not in the drive) and is unlocked.

✍ *Avoid removing Online tapes. Without Online tapes in the autoloader, the LANtegrity Server cannot stand-in for a protected server.*

Follow the procedure below to remove a tape.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
2.	Open the ‘Remove Media’ or the ‘Insert Media’ panel. You can notify LANtegrity about removing a tape when either panel is open. However, Insert is available only when the Insert Media panel is open.
3.	Select the autoloader you want to manage.
4.	Click Pause and wait for the operation to complete. **Response**: LANtegrity pauses the autoloader and changes the Pause button to Activate.
5.	Remove the magazine from the autoloader.
6.	In the magazine displayed in the Autoloader Management window, select the tape you want to remove. If a tape needs to be inserted and a tape is not animated for removal, select a blank tape. If there is no blank tape in the magazine, select a tape that is unlocked. If possible, avoid removing an online tape.

✍ *Avoid removing Online tapes. Without Online tapes in the autoloader, the LANtegrity Server cannot stand-in for a protected server.*

7. Click Remove and confirm your choice.

   Response: The magazine shows an animated tape sliding in and out of the slot. LANtegrity displays an information popup reminding you to remove the tape from the autoloader.

8. Remove the tape from the magazine and label the tape.

9. Click OK.

   Response: The animated tape disappears from the magazine slot in the Autoloader Management window.

10. If you do not have to insert any tapes, place the magazine back into the autoloader. Otherwise, insert the tape(s). See "Inserting tapes" on page 80.

11. When you are finished, click Activate to start the autoloader.

    Response: The Activate button toggles to Pause. LANtegrity marks any slot you did not select with a question mark until it inventories the autoloader.

Inserting tapes

The LANtegrity Server needs blank or expired tapes to write new data and may need Legacy, and Offsite tapes for restore jobs or stand-in service.

✍ *If you do not have the requested tape, click **Unavailable**. LANtegrity sends an alert if it finds a duplicate of the file on another tape.*

Follow the procedure below to insert a tape.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**. **Response**: LANtegrity displays the Autoloader Management window.
2.	Select the autoloader you want to use.
3.	Open the 'Insert Media' panel.
4.	Click Pause and wait for the operation to complete.
5.	Go to the autoloader and remove the magazine.
6.	On the Autoloader Management window, locate an empty slot in the autoloader. ✍ *If there are no empty slots, remove a tape. See "Removing tapes" on page 78 for information about which tape to remove.*
7.	On the Insert Media panel, select the type of tape you want to insert.

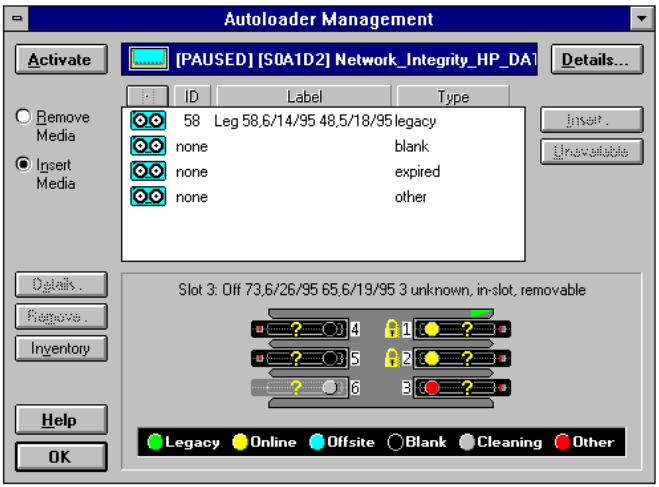


Figure 5-5. Autoloader Management window

The list of tapes includes specific tapes that the LANtegrity Server needs and tapes that you may want to load.

If you want to insert...	Choose...
A new blank tape.	Blank
An expired tape.	Expired
A cleaning tape or tape you removed and want to re-insert.	Other
A specific tape requested by LANtegrity.	The tape displayed in the panel.

8. Click Insert and confirm your choice.

   Response: A tape moves in and out of the selected magazine slot. If the tape you selected is “other,” LANtegrity prompts you for the tape ID. If the tape is “blank,” LANtegrity will create a label. LANtegrity displays an information popup reminding you to insert the tape into a specific slot in the magazine.

9. Insert the tape into the specified slot in the magazine.

10. Click OK.

    Response: The moving tape disappears from the magazine slot.

11. When you have finished inserting and removing tapes, place the magazine back into the autoloader.

12. On the Autoloader Management window, click Activate to start the autoloader.

    Response: The Activate button changes to Pause.

    When you place the tape in the magazine, LANtegrity checks to make sure that you inserted the tape it expected. Then it marks the rest of the slots for an inventory (indicated by a question mark). If LANtegrity finds that the tape is different than one specified on the Insert Media panel, it sends and alert.

Later, if LANtegrity finds an unexpected tape in any other slots, it immediately suspends all tape read/write activities to inventory the autoloader's slots and looks for the expected tape. This requires loading and reading the header information on each tape and may take a few minutes. Depending on which tapes are incorrectly loaded, you may receive messages asking you to supply the expected tapes.

Viewing details of a tape

LANtegrity provides additional information about a selected tape on the Autoloader Management window. Follow the procedure below to view details of a tape.

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**.
2.	Select a tape record.
3.	Click Details or double click on the media entry. **Response**: LANtegrity displays the Media Details window. An example is shown below.

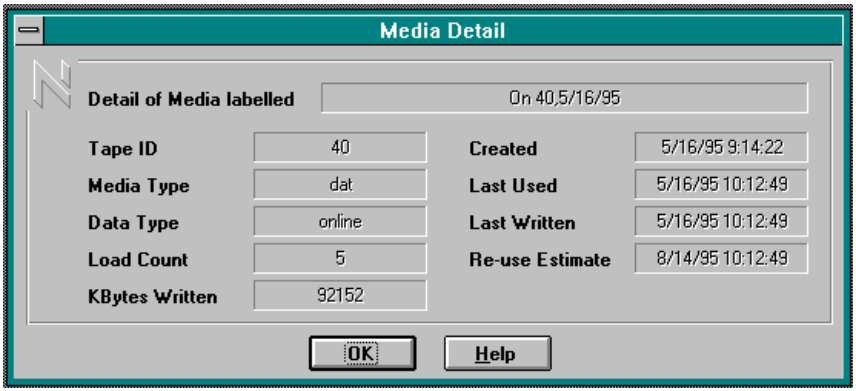


Figure 5-6. Media Detail dialog

✍ *The information on this window is not updated when the tape is in the drive.*

The Media Detail window displays information about the tape identified by its label contents at the top of the window.

Field	Identifies
Tape ID	The unique number that LANtegrity assigns to the tape.
Media Type	The format of the tape (for example, DAT). For the current list of supported tape formats, contact your Technical Support representative.
Data Type	The type of data stored on the tape. Possible types include: Blank, Cleaning, Expired, Legacy, Online, and Offsite.
Load Count	The number of times the tape has been loaded into the autoloader drive. LANtegrity notifies you when the number exceeds the tape's recommended use.
Kbytes Written	The number of kilobytes of data currently stored on the tape.
Created	The date and time that LANtegrity first wrote to the tape.
Last Written	The date and time that LANtegrity last wrote to the tape.
Last Used	The date and time that LANtegrity last read from, or wrote to, the tape.
Re-use Estimate	An estimate of when this tape will expire. The estimate may change depending on where the tape is located in the rotation schedule.

Inventory the contents of the Autoloader on demand

Any tape that LANtegrity has not inventoried is marked with a question mark. An inventory is the process by which LANtegrity updates the information about tapes it had not inventoried and removes the question marks from the slots in the magazine. After you insert a tape into the magazine and press Activate, LANtegrity checks to make sure that you inserted the tape it expected and marks the rest of the slots for an inventory. To force LANtegrity to perform an inventory immediately, you can select Inventory. This requires loading and reading the header information on each tape and may take several minutes for each tape.

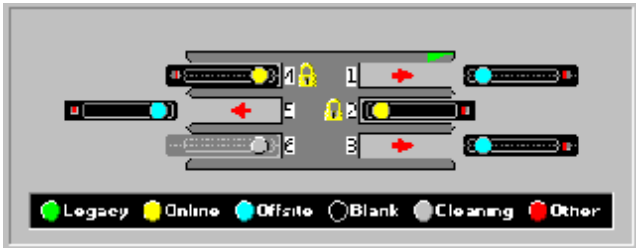


Figure 5-7. Tape details

Step	Action
1.	Click the Autoloader Management button or select **Tools/Autoloader Management**.
2.	Select the autoloader you want to inventory.
3.	Click Pause and wait for the operation to complete.
4.	Click Inventory.
5.	Click Activate. **Response**: LANtegrity inventories the autoloader and removes the question marks from the slots in the tape magazine.

✍ *You can also inventory the autoloader on demand without clicking Pause. In this case, all other activities in the autoloader are suspended while LANtegrity performs the inventory.*

Configuring Media Rotation

LANtegrity automatically maintains the Offsite and Legacy tapes on a rotation schedule. Media rotation allows the LANtegrity Server to

- Minimize the number of file records it has to maintain in its catalog.
- Minimize the number of tapes you have to store.
- Reuse tapes.

As each set of tapes moves in rotation, LANtegrity expires tapes that are no longer needed. When a Legacy or Offsite tape expires, the LANtegrity Server removes all references to the tape's files from its records and identifies it as expired. You can now recycle the tape for reuse in the autoloader.

On the Configure Media Rotation window, you can retain Offsite or Legacy sets in a three-level rotation, similar to a Grandfather/Parent/ Child rotation, and designate the intervals and retention periods.

✍ *We recommend that you retain the default rotation configuration. Changing the rotation configuration may have some unexpected results.*

In most cases, the default retention periods allow LANtegrity to satisfy a request to restore an old file. (To satisfy the more typical request to restore the latest version of a file; LANtegrity goes to cache or an Online tape, not to an Offsite or Legacy set.)

If you retain the defaults, the Offsite and Legacy tapes are kept as follows:

Tape	Type	Default Retention Period
Offsite	Current Offsite	90 days
	Monthly Offsite	12 months
	One monthly set per quarter	20 quarters
Legacy	All	90 days

✍ *The changes made on the last day of each month are included with each monthly set. LANtegrity keeps one extra tape with a set to guarantee that it captures the last day.*

Although expired Offsite tapes disappear from LANtegrity's records and therefore cannot be used for file restoration, you can if necessary, use them for disaster recovery, as long as a full recovery set is available and all tapes load without error.

Follow the procedure below to configure tape expiration policy.

Step	Action
1.	Click the General Configuration button or select **Tools/General Configuration**.
2.	Select 'Media Rotation' from the list box on the left. **Response**: LANtegrity displays the Configure Media Rotation window. The following illustration shows the Offsite panel.

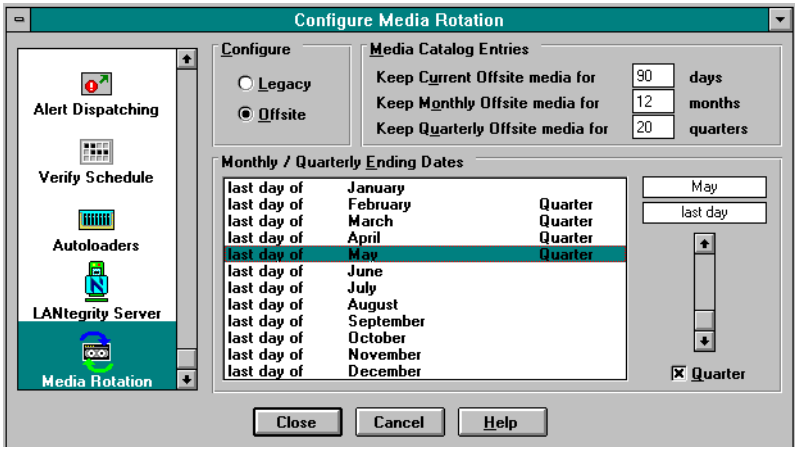


Figure 5-8. Configure Media Rotation

3. Select ‘Legacy’ or ‘Offsite’.

4. In ‘Media Catalog Entries’, specify the retention period for the current, monthly, and quarterly Offsite/Legacy media.

5. In the Monthly/Quarterly panel, set the quarter. Select the month in the panel and click the Quarter check box:

   - To deselect a month as the end of the quarter, select the designated month in the panel and click the ‘Quarter’ box.

   - To select another ending day for rotation, select the month in the panel and use the sliding bar (at right).

Reviewing the Media Inventory

LANtegrity maintains a record of every tape it creates. Using LANtegrity's 'Media Inventory' tools, you can

- View a list of all the tapes in your tape library.
- Display details on a tape-by-tape basis.
- Sort the list based on the fields in the tape records.
- Copy the contents of the Media Inventory to the clipboard.

How long is each tape record maintained?

LANtegrity maintains each tape record until the data on the tape expires and you reuse the tape for the Online or Offsite set.

The data on a tape expires according to your Media Rotation settings in the Protection Policy. When this happens, LANtegrity sets the tape's Type field to "expired." You can now re-use the tape in any LANtegrity Server that requests a blank tape.

Should I always re-use tapes in the same LANtegrity Server?

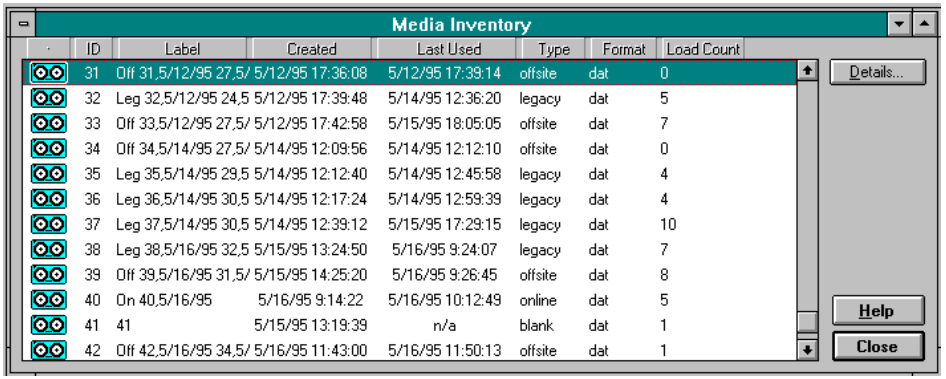
This is recommended, but not necessary. If you re-use the tape in the same LANtegrity Server, LANtegrity deletes the record of the tape but keeps track of the load count. Expiring a tape deletes the record with the data. When it is used again, LANtegrity deletes the reference to the tape but keeps a record of the load count.

Interpreting Media Inventory Data

You can view your complete inventory of LANtegrity tapes from the Media Inventory window. When you open the window, the list shows the most recently written tape at the top. You can sort the list for viewing or reporting purposes by double-clicking on a column heading. To have LANtegrity update the list, press F5.

You can also copy the list to the clipboard and then paste it into a document. Follow the details below to access the Media Inventory.

Click the Media Inventory button or select **Tools/Media Inventory**. LANtegrity displays the Media Inventory window. A sample display appears below.



ID	Label	Created	Last Used	Type	Format	Load Count
31	Off 31,5/12/95 27,5/	5/12/95 17:36:08	5/12/95 17:39:14	offsite	dat	0
32	Leg 32,5/12/95 24,5	5/12/95 17:39:48	5/14/95 12:36:20	legacy	dat	5
33	Off 33,5/12/95 27,5/	5/12/95 17:42:58	5/15/95 18:05:05	offsite	dat	7
34	Off 34,5/14/95 27,5/	5/14/95 12:09:56	5/14/95 12:12:10	offsite	dat	0
35	Leg 35,5/14/95 29,5	5/14/95 12:12:40	5/14/95 12:45:58	legacy	dat	4
36	Leg 36,5/14/95 30,5	5/14/95 12:17:24	5/14/95 12:59:39	legacy	dat	4
37	Leg 37,5/14/95 30,5	5/14/95 12:39:12	5/15/95 17:29:15	legacy	dat	10
38	Leg 38,5/16/95 32,5	5/15/95 13:24:50	5/16/95 9:24:07	legacy	dat	7
39	Off 39,5/16/95 31,5/	5/15/95 14:25:20	5/16/95 9:26:45	offsite	dat	8
40	On 40,5/16/95	5/16/95 9:14:22	5/16/95 10:12:49	online	dat	5
41	41	5/15/95 13:19:39	n/a	blank	dat	1
42	Off 42,5/16/95 34,5/	5/16/95 11:43:00	5/16/95 11:50:13	offsite	dat	1

Figure 5-9. Media Inventory

LANtegrity provides the following information for each tape currently stored in your tape library.

Field	Description
Label	The tape's electronic label information. If the information on the tape's paper label doesn't match the contents of this field, update the paper label. Each label contains the following fields: ▪ ID number and type of this tape ▪ Date of the last write to this tape ▪ ID number and type of first tape in recovery set ▪ Date of last write to first tape in recovery set ▪ Number of tapes in this recovery set If this field displays untitled, it means that this server has not written to it.
Created	The date and time that LANtegrity first wrote to the tape.
Last Used	The date and time that LANtegrity last read or wrote the tape.
Type	The type of data stored on the tape. The type can change depending on the current use of the tape. For example, a blank tape can become an Online tape and finally, a Legacy tape. Possible types include: Blank, Cleaning, Expired, Legacy, Online, and Offsite.
Format	The format of the tape (for example, DAT). For the current list of supported tape formats, contact your Technical Support representative.
Load Count	The number of times the tape has been loaded into the autoloader drive. This is a measure of the amount of wear and tear a tape has experienced. LANtegrity notifies you when the number exceeds the tape's recommended use level. LANtegrity can read data from a tape after it exceeds its recommended load count, but we recommend that you do not use it again for writing.

Viewing Details of a Tape

LANtegrity provides additional information on a selected tape when you open the Media Detail window. Follow the procedure below to view details of a tape in the library.

Step	Action
1.	Click the Media Inventory button or select **Tools/Media Inventory**.
2.	Select a tape record.
3.	Click Details or double click on the media entry.

Response: LANtegrity displays the Media Details window. An example is shown below.

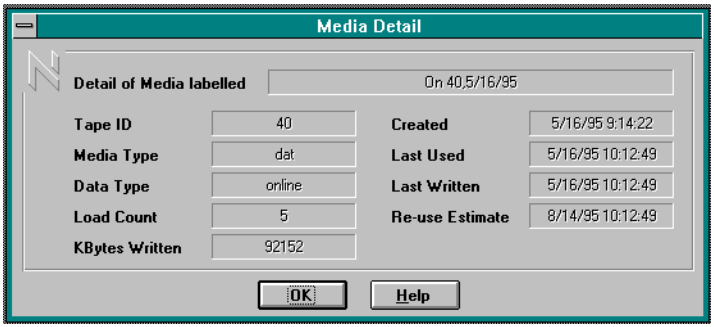


Figure 5-10. Media Detail

The Media Detail window displays information about the tape identified by its label contents at the top of the window.

6 Operating Stand-in Service

Introduction

When a protected server is down and its files are no longer accessible to its users, you can instruct the LANtegrity Server to take the place of the down server. This mode of operation is known as **stand-in service**.

When the LANtegrity Server loses contact with a protected server, it issues an alert informing you of this. You can investigate the problem and initiate the stand-in service manually or have the LANtegrity Server initiate the stand-in service automatically after a configurable period. When stand-in is enabled, LANtegrity issues another alert.

Users can log in again as soon as the stand-in service is in place. Stand-in service can be transparent to users. They log in to the *same server, with the same user ID and password.* The LANtegrity Server simply adopts the down server's name, and manages its security information. Unauthorized users cannot gain access to the down server's files during stand-in service.

✍ *The LANtegrity Server can stand-in for a protected server only if LANtegrity has completed at least a verify job on the server and you have kept all of the files required for its operation under protection. For details, see* *"Changing the verify schedule" on page 28* *in Chapter 3.*

The following figure illustrates how the LANtegrity Server stands in for a protected server that is down.

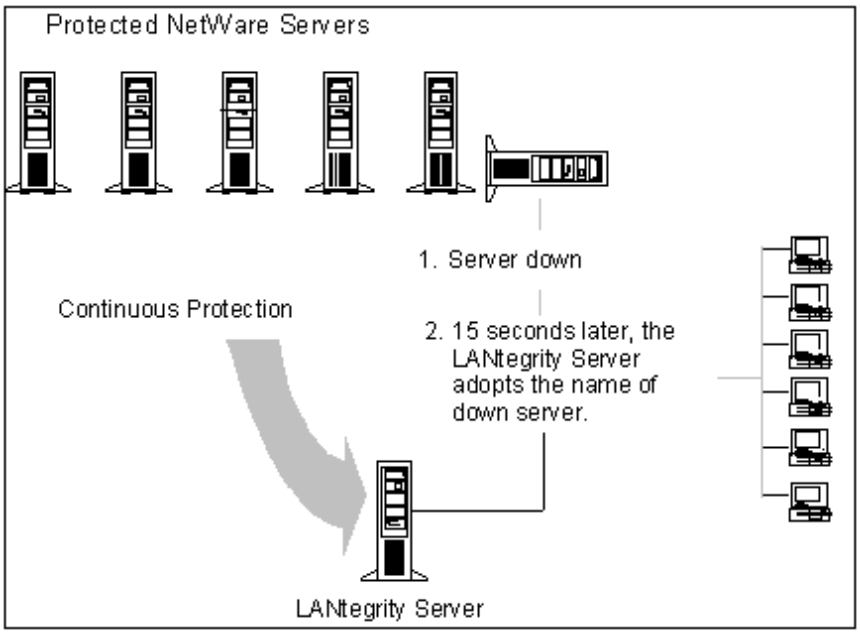


Figure 6-1. Sample of a LANtegrity server standing in for a downed server

This chapter describes how to operate LANtegrity's stand-in service for protected servers. Specifically, it describes:

- **Preparing for Stand-in.** Before a LANtegrity Server can stand-in for a server, you need to ensure that the server is protected and verified, and that the LANtegrity Server has the capacity to offer stand-in services while it continues to protect other servers.
- **Initiating Stand-in.** You can initiate stand-in service for a down server, either manually or automatically, after receiving an alert from LANtegrity.
- **What Happens During Stand-in.** You and your users should know what to expect during stand-in service.
- **Exiting Stand-in.** When the down server is ready to come back online, you can synchronize it with the LANtegrity Server to obtain the latest file changes made during stand-in and then return it to network operation.

Preparing for Stand-in Service

Stand-in service requires that you plan ahead to ensure its smooth operation. This section discusses the following issues that you need to consider for each protected server:

- Can all users of the protected server access the LANtegrity Server via network routing?
- Does the LANtegrity Server have the capacity to stand-in for a specific protected server?
- Are all the required files protected so that the stand-in service will have copies of them?
- Will you provide a message to your users to let them know that stand-in service is operating?
- Will the stand-in service also need to enable other services such as printing?
- Have the users been informed about what to expect when their server goes down?

You should answer each of these questions and plan your stand-in procedures for each protected server accordingly. Your choices may differ depending on each server's user community and the types of files it stores.

Verifying access for Stand-in service

All users with access rights to the protected server must be able to reach the LANtegrity Server if they are to benefit from stand-in service. You should review network routing paths and may want to experiment with workstation access from each of the remote locations in your network.

✍ *The LANtegrity Server requires that clients use NCP for access during stand-in. Workstations that do not use NCP do not "see" the LANtegrity Server's stand-in service on the network, nor are they able to address it.*

For workstations that are not compatible with NCP, consider alternative access methods. For example, you might want to convert the workstations to NCP or move the required files to another protected server (that supports the required access protocol) while the original server is down. To move the files to another protected server, you can use LANtegrity's Restore tools, see Chapter 7, "Restoring Files."

✍ *Make sure that the NCP Packet Signatures are turned off on the LANtegrity Server or else users cannot log in to stand-in services.*

Monitoring capacity requirements

To stand-in for a protected server, the LANtegrity Server must have sufficient processing power and storage capacity not only to stand-in for a protected server but also to continue protecting other servers.

The *Setup Guide* describes in detail the capacity requirements for initial installation. As with any other server, you should plan for growth and periodically review the LANtegrity Server to ensure that it has the capacity to stand-in when it is needed. As the quantity of stored data grows on the protected servers, you may need to adjust the LANtegrity Server's configuration.

At a minimum, any increase in the capacity of a protected server should cause an automatic review of the LANtegrity Server's capacity.

Ensuring total file protection

As with capacity issues, you should review the protection policy for each protected server periodically to ensure that all required files are being protected.

If you maintain files under continuous protection rather than on other schedules, LANtegrity keeps the files as current as possible. If a protected server goes down, the latest possible versions of the files will be available to your users.

You should also review any files excluded from protection on the Master Exclusions and Never Protect rule sheets. If a protected server goes down, these files may ***not*** be available. See Chapter 8, “Customizing File Protection,” for more information about the rule sheets.

Providing a Stand-in message to users

LANtegrity allows you to define a NetWare broadcast message (up to 58 characters) that it will deliver to users as they log into the stand-in service. You can use this message to notify your users that stand-in service is in effect or, if necessary, that a change in available network services has occurred. You can prepare a separate message for each protected server. LANtegrity dispatches the message when a user begins using stand-in service.

The stand-in service message is optional. Without this message, the users may not even realize that they are using stand-in service. Follow the procedure below to provide a stand-in message.

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.

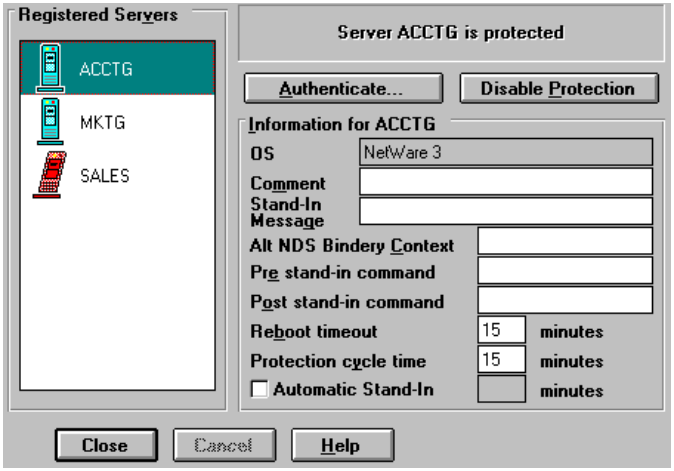


Figure 6-2. Configure Protected Servers panel

3. Select the protected server whose stand-in message you want to define.

4. Type your message in the ‘Stand-In Message’ box.

   You can type up to 58 alphanumeric characters, including punctuation marks and spaces. The text scrolls to the left as you type.

   If you leave this box empty, LANtegrity will not display a message to users as they begin using the stand-in service.

5. Press Close to save your changes.

Specifying pre- and post-Stand-in commands

Since networked servers are sometimes used for more than simple file storage, you can also use the LANtegrity Server to manage the print queues and other services provided by the down server. You can provide these services from the LANtegrity Server during stand-in if the appropriate printers is available on the network or connected to the LANtegrity Server.

✍ *The contents of print queues on the protected servers are not protected by the LANtegrity Server and are therefore lost when a protected server fails. Once the necessary equipment is available to the LANtegrity Server and the queues are initialized, users can resubmit jobs.*

For information about setting up printing services for stand-in, see the *Setup Guide*.

You can specify both a pre- and a post-stand-in command. These commands can be ***.NCF** batch files used to dynamically load NetWare NLMs such as print servers. Follow the procedure below to specify a pre- and post-stand-in command.

Step	Action
1.	Create one or two ***.NCF** files on the LANtegrity Server. One file can contain instructions that are executed when stand-in service is initiated. The other can contain corresponding instructions that are executed when stand-in service is exited and the down server is brought back online. You can create a pair of ***.NCF** files for each protected server. Alternatively, you can create one pair to be used for all protected servers. You must specify the ***.NCF** files for each protected server.
2.	Click the General Configuration button or select **Tools/General Configuration**. **Response**: LANtegrity displays the General Configuration window.
3.	In the list box on the left, select ‘Protected Servers’.

Response: LANtegrity displays the Configure Protected Servers panel.

4. Select the protected server for which you want to specify the pre-and post-stand-in batch files.

5. Type the name of the ***.NCF** batch file in the 'Pre stand-in command' box.

   For example, type ***filename*.ncf** where *filename* is the name of your batch file.

   If you want to specify a path other than the default SYS:SYSTEM, type the full path, including the volume. For example, type:

   `SYS:PUBLIC\`*filename***`.ncf.`**

6. Type the name of the ***.NCF** batch file in the 'Post stand-in command' box.

Informing users about what to expect

Although its possible that users may not notice any difference between stand-in service and the normal operation of their server, they may encounter some unexpected behavior such as a delay in accessing files they have not used for a while. Review "What occurs when a LANtegrity Server exits stand-in?" on page 118 and, in particular, "Effects of Stand-in service on users" on page 106.

Testing Stand-in service

We strongly suggest that you try out stand-in service regularly before you really need to use it. Stand-in is easy to test and gives your users a chance to use the software and see how it works. To try stand-in service, down a protected server or remove it from the network. Then use the instructions that follow.

Initiating Stand-in

You can initiate stand-in one of two ways: manually or automatically. To initiate stand-in manually, you use the **Protected Servers** tool. Your users can log into the stand-in service less than a minute after you start the service.

For information about automatic stand-in, see "Establishing Automatic Stand-in" on page 102. Follow the procedure below to initiate manual stand-in service.

Step	Action
1.	Click the Protected Servers button or select **Tools/Protected Servers**. **Response**: LANtegrity displays the Protected Servers window.

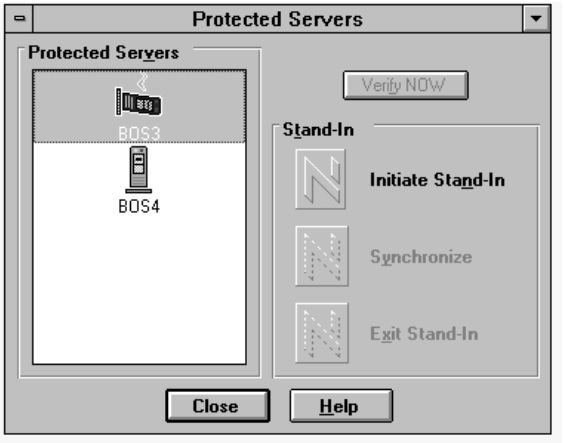


Figure 6-3. Protected Servers window

2. In the list box, select the protected server that requires stand-in service.

3. Each protected server name is shown with an icon that identifies the state of the server with regard to the LANtegrity Server.

Icon	Description
	Online and fully protected.
	Down and the LANtegrity Server is standing in for it.
	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 server.
	LANtegrity agent is loaded but server is not authenticated.
	Down and the LANtegrity Server is not standing in for it.

4. Click the Initiate Stand-In button.

The LANtegrity Server begins the stand-in process. The complete process takes less than a minute. Any users who attempt to log into the down server will actually log into the LANtegrity Server. See "What Happens During Stand-in Service" on page 104 for more information.

Establishing Automatic Stand-in

You can instruct LANtegrity to initiate stand-in automatically when it detects a down server-that is, when it loses connection to a server. Automatic stand-in may be useful when an administrator is not available.

The only thing you have to tell LANtegrity is how long to wait after it detects a down server and before it initiates automatic stand-in. This period is calculated from the time that the LANtegrity Server detects that a protected server is down. Follow the procedure below to establish automatic stand-in service.

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 window.
3.	Select the protected server for which you want to establish automatic stand-in.
4.	Click Automatic Stand-In.
5.	Type the number of minutes to wait before initiating stand-in. ✍ *Configure enough time to check for communication problems between the LANtegrity Server and the protected server. If you want to cancel stand-in, you can do so before it starts by pressing Cancel Automatic Stand-in on the Protected Servers window.*
6.	Select another server for which to establish automatic stand-in or click Close to save your changes and exit from the Configure Protected Servers window.

What Happens During Stand-in Service

This section describes what the LANtegrity Server does when stand-in starts and what it does during stand-in. It also explains what users might expect during stand-in and other considerations.

What the LANtegrity server does initially

As soon as stand-in starts, the LANtegrity Server performs these operations:

- Creates a file structure that parallels the protected server's file structure.
- Assumes the down server's security profile so that only authorized users are allowed access to their files.
- Adopts the server name of the down server and utilizes the same Service Advertising Protocol (SAP).
- Executes the stand-in ***.NCF** batch file, if you have defined one.
- If you have not defined such a batch file, you can manually start or stop the network services **after** stand-in is in place.
- Issues an alert when stand-in service is in effect.

The complete process takes less than a minute. From then on, any user who attempts to log into the down server actually logs into the LANtegrity Server.

What the LANtegrity server does during Stand-in

During stand-in, the LANtegrity Server does the following:

- Retrieves files that users need.

  Most of the files that users need are available immediately from disk cache. Any files that have not been accessed recently may have to be retrieved from tape. If the file is on a currently mounted tape, it is retrieved faster than a file on an unmounted tape.

- Protects the files that are maintained by stand-in service on the LANtegrity Server.

  File protection for the down server is unchanged. LANtegrity treats the stand-in LANtegrity Server as a local protected server and continues to copy updated files to its Intelligent Data Vault for protection.

- Continues to monitor the other protected servers and saves their files just as it does when it is not performing stand-in service.

  As long as the capacity requirements described in the *Setup Guide* are properly met, your LANtegrity Server and its stand-in service can operate indefinitely, balancing stand-in requirements and protection requirements on a dynamic basis.

Effects of Stand-in service on the LANtegrity server

To provide stand-in service and continued protection for other servers, the LANtegrity Server requires sufficient memory and disk space. These requirements depend on the amount of memory and disk space on the largest protected server and the amount of data on the protected servers. For information about configuration requirements, see the *Setup Guide*. You should review any changes in your network and determine whether you should upgrade the LANtegrity Server so that it can handle them.

During stand-in, user file access takes precedence over normal activities. Therefore, depending on the capacity of the LANtegrity Server and the number of requests for service during stand-in, you may notice the following:

- Some protection schedules may take longer to execute. If a scheduled protection does not complete in its allotted time, LANtegrity issues a message to this effect. You can then choose to:
- Run the schedule manually at a time of low demand, by using the **Protect NOW** option on the **Scheduled Protection** window (see "Executing a schedule on demand" on page 162).
- Select the **Run protection to completion** checkbox on the **Edit Schedule** window to ensure that the schedule is not interrupted.
- Tape activities, especially those that involve the Offsite tape, may be somewhat slower.
- Continuous protection latency may increase.

Effects of Stand-in service on users

For the most part, there are no changes for users who access stand-in service. However, they may encounter delays in system response depending, for example, on the configuration of the LANtegrity Server. They may also receive file retrieval messages if a file has to be retrieved from tape.

✍ *During stand-in, users will not be able to rename directories. In addition, they cannot use DOS wildcards to rename a file unless they use the Windows File Manager.*

During stand-in, users may:

- Log in to stand-in service using their normal login procedure.
- Receive a message when they log in, if a stand-in message was supplied on the Configure Protected Servers window.
- Access every file that was covered by continuous protection or on a protection schedule that completed successfully.

  Users can proceed with their work, just as if they were connected to the down server.
- Immediately obtain files that were recently accessed.

  This is because recently accessed files are in disk cache.
- Possibly find some files that do not contain their latest changes.

  These are files that either were not saved or were saved recently but not protected before their server went down.
- Possibly experience delays when trying to access a file that has not been accessed recently.

When there is a delay, the user's workstation pauses until LANtegrity sends a message indicating that the file is being retrieved from tape. After receiving the message, users can resume activities on their workstations that do not require this file. When the file is available, the user gets another message. However, you can choose not to wait for a tape to mount by selecting **Don't Wait for media to mount** on the Configure LANtegrity Server panel.

The following figure shows the availability of user files during stand-in.

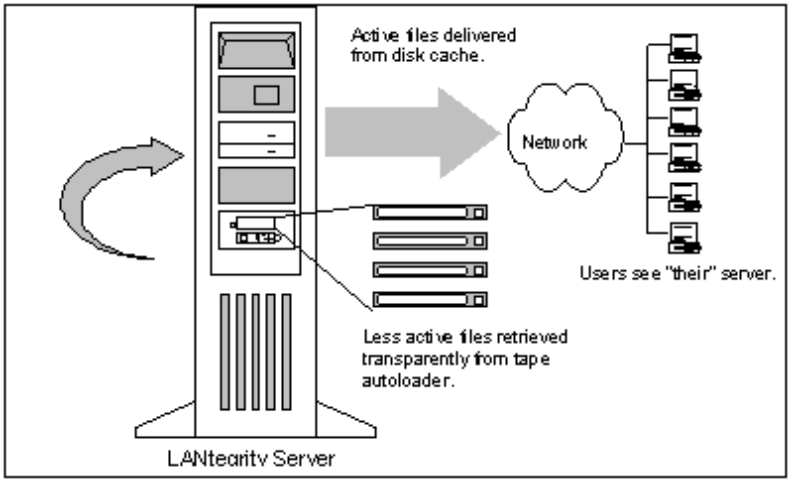


Figure 6-4. Available files during stand-in

If the LANtegrity Server is configured with a sufficiently large cache system as described in the LANtegrity *Setup Guide*, the file retrieval from tape should be minimal.

- When in stand-in, the LANtegrity Server does not provide NetWare accounting services nor does it enforce NetWare account restrictions (such as station restrictions, time restrictions, intruder detection, disk space requirements, etc.).

- Have access to services such as printing provided by the down server **if** you have configured the LANtegrity Server to take over these services.

For information about setting up printing services for stand-in, see Appendix A "Stand-In Printing Services" in the *Setup Guide*.

Other considerations for Stand-in

You do not have to change your normal routine while the LANtegrity Server provides stand-in service for a down server. However, to help maximize stand-in service, consider the following:

- Defer restore jobs when stand-in service starts.

  This will maximize the autoloader's ability to retrieve users' files during stand-in and allow faster file retrievals.

- When accessing applications that have not been used in a long time, users may initially receive errors and experience delay.

  Certain applications may require a large number of files from tape. Each file request may abort the application. After the file becomes available, the user will have to start the application again. You can alleviate this problem by increasing the size of the disk cache volume on the LANtegrity Server.

- If users have not logged in for a while, the login script must be retrieved from tape and they may get a file retrieval message.
- Monitor disk usage so that the down protected server's disk space is not over-subscribed.
- You can use non-privileged functions in commands such as FILER but you cannot use privileged system administration functions relative to the protected server.

  For example, when standing in for a NetWare 3.12 protected server, do not use SYSCON to make bindery changes (e.g., adding a new user to the protected server's bindery). If you do make these changes with SYSCON, they are not synchronized back to the protected server after the LANtegrity Server exits stand-in. In addition, you should not use SUPERVISOR to log in to or attach to a 3x server when the LANtegrity Server is standing in for that server. This is because NetWare 4.1 allows only one SUPERVISOR ID for the entire NDS tree.

- Do not disable logins on the protected server during stand-in because the LANtegrity Server needs to

- You may want to monitor the file protection latency to see what, if any, impact stand-in service has on file protection.

File protection latency is the average amount of time it takes LANtegrity to save a file after detecting a change in the file. Use LANtegrity's **Statistics** tool to view the latency. See "Checking Protection Statistics" on page 57.

Exiting Stand-in Service

When the down server is ready to go back online, you can update it with all of the files that were changed or created during stand-in service. LANtegrity updates the recovering server with a process called **synchronization**. During synchronization, the LANtegrity Server scans the file system of the protected server and transfers all of the necessary files to it. You can use synchronization to restore entire volumes and directories on the protected server.

✍ *Always restart the recovering server under the alternate name and IPX address created by LANtegrity during setup, **not under its original name**. If you do, there will be two servers on the network using the same name and you'll get copyright warnings. See* *"Preparing for synchronization" on page 111*.

This section describes how to prepare for, initiate, and exit stand-in service. The steps include:

- Bringing the recovering server up on the network under its alternate name created by LANtegrity during setup. The alternate name is the server's original name preceded by _PS_.
- Ensuring that all volumes on the recovering server are mounted and working properly.
- (Optional) If you decided to synchronize during stand-in, executing this first synchronization.
- Ensuring that users are logged out before the LANtegrity Server exits stand-in.
- Executing either **Exit Stand-in** with **Sync filesystem** or **Exit Stand-in** without **Sync filesystem** and ensuring that users remain logged out during the exit.

✍ *If printers or other peripherals are attached to the LANtegrity Server during stand-in service, their queues are not affected by the synchronization process.*

Preparing for synchronization

Synchronization requires the following:

- The LANtegrity Server is standing-in for the recovering server.
- The recovering server is brought up on the network under its alternate name _PS_*servername*.

✍ *Always restart the recovering server under the alternate name created by LANtegrity during setup,* ***not under its original name.*** *If you do, there will be two servers on the network using the same name and you'll get copy-right warnings.*

- The LANtegrity agent software is loaded on the recovering server.

If you need to install and setup the LANtegrity protected server software, load the LANtegrity INSTALL and SETUP programs as described in the *Setup Guide*. When the setup is complete, and you've rebooted the server to enable the changes in AUTOEXEC.BAT, LANtegrity displays:

```
What is the status of the LANtegrity Server?
Not Standing-In for this server
Standing-In for this server
```

To bring the server up under its alternate name, select **Standing-In for this server**. After the recovering server is operating properly under its alternate name, you can start synchronization.

When you are ready to bring the recovering server up on the network for the first time, perform the following system checks and actions **before** you initiate the first synchronization.

Follow the procedure below to prepare for synchronization.

Step	Action
1.	Bring up the recovering server and select **Standing-In for this server** when LANtegrity displays the following prompt: **What is the status of the LANtegrity Server?** **Not Standing-In for this server** **Standing-In for this server** The server comes up with the alternate name assigned by LANtegrity during its setup procedure. The server also uses the alternate IPX address entered during setup. The alternate name is the original name of the server prefixed by **_PS_**. This alternate name prevents conflict with the LANtegrity Server's stand-in service, which is using the original server's name. For example, for server FINANCE, the alternate name is _PS_FINANCE. The server's alternate name is defined in the **AUTOEXEC.NCF** file. If instead you selected **Not Standing-In for this server**, the protected server comes up under its original name. When LANtegrity detects that the protected server is being stood-in for, it downs the server and brings it back up under its alternate name.
2.	Logins must be enabled during synchronization so that the LANtegrity Server can log into the recovering server.
3.	Run **VREPAIR** on any volume that does not initialize properly when you bring up the system and make sure that NetWare is running properly. Recreate any volumes that were destroyed.
4.	Check that all volumes are mounted: ▪ Execute the **Volumes** command from the protected server's console to view the mounted volumes. ▪ Ensure that all non-DOS name spaces are added for the protected server's volumes.

5. Verify that the LANtegrity agent NLM is loaded and running.

   Press CTRL ESC to display the server console screens and make sure that the LANtegrity agent screen is listed. If the screen is not listed, install or load the LANtegrity agent software. See the *Setup Guide* for information.

6. If any unnecessary NLMs are running, we recommend that you unload them until after the synchronization process has completed to avoid the possibility of losing updates.

7. Verify that the username and password used by the LANtegrity Server to access this protected server is configured correctly for both the server itself and for the LANtegrity Server.

For information about supplying the username and password for the LANtegrity Server or a protected server, see "Changing Settings of the LANtegrity Server" on page 178 or "Authenticating the protected servers" on page 171.

Choosing the synchronization process

You can bring a recovering protected server back online the following way:

- **(Optional)** Perform a synchronization during stand-in.

  During this synchronization, users can access the stand-in service files while most of the synchronization occurs in background.

- **(Required)** Perform an exit with synchronization.

  During this synchronization, users cannot access their files on the protected server or the LANtegrity Server.

During synchronization, LANtegrity moves a file to the recovering server if no file by the same name exists or if a more recent version of an existing file is found on the LANtegrity Server. It also moves files that were deleted during stand-in service to the **LSDELETE** directory in the root of each protected volume.

What is the optional two-synchronization process?

The two-synchronization process allows users to access their files for as long as possible. The LANtegrity Server and recovering server communicate in the background during an initial synchronization process to compare file directories and ensure that the latest copy of each file is restored to the recovering server.

The following figure shows how the LANtegrity Server performs the first of the two synchronizations for a recovering server.

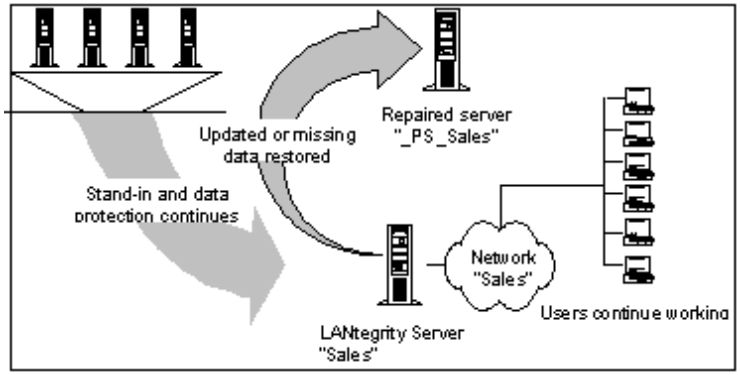


Figure 6-5. LANtegrity synchronizing for a recovering server

When the first synchronization completes, you may still have files that are more current on the LANtegrity Server — these are the files that were being modified by users during the first synchronization procedure. You now need to select a second synchronization when you exit stand-in. During this time, however, you must **prevent users from accessing their files**.

The time required for the second synchronization should be shorter than the first synchronization, depending on how many files were modified since the first synchronization started.

Performing synchronization during Stand-in

When you have verified that the recovering server is ready to be brought back to active service, you can start the synchronization process. Users can continue to access their current files from the LANtegrity Server's stand-in service while you execute this optional synchronization.

✍ *After this synchronization completes and you are ready to exit stand-in, you must select **Exit with Sync** to preserve any changes made during this optional synchronization.*

Follow the procedure below to perform the first synchronization.

Step	Action
1.	After the recovering server is connected to the network under its alternate name, click the Protected Servers button or select **Tools/Protected Servers**. **Response**: LANtegrity displays the Protected Servers window.
2.	Select the protected server for which the LANtegrity Server is standing in. **Response**: The server name is beneath the stand-in service icon.
3.	Click Synchronize. **Response**: LANtegrity asks you to confirm.
4.	Click OK. LANtegrity starts the synchronization job. Once the synchronization begins, it operates automatically until it completes. If you need to cancel a synchronization, see "Canceling a synchronization" on page 119.
5.	When this synchronization is complete, you can exit stand-in with synchronization as described in the next section.

Exiting Stand-in with synchronization

Use this procedure to exit stand-in with synchronization.

If you ran the optional synchronization during stand-in, the LANtegrity Server needs to update the recovering server only with the changes that were made since the optional synchronization started. Any changes that occurred during stand-in are already transferred to the recovering server.

On the other hand, if you did not use the optional synchronization, LANtegrity needs to update the recovering server with all the changes made during stand-in.

To execute this synchronization, you select the option **Sync filesystem** from a dialog box when you exit stand-in.

✍ *You must prevent users from logging in to access their files while the exit-with-synchronization is in progress.*

Follow the procedure below to exit stand-in with synchronization.

Step	Action
1.	Ensure that users log out and remain logged out during the time that the LANtegrity Server is exiting stand-in with synchronization.
2.	Click the Protected Servers button or select **Tools/Protected Servers**. **Response**: LANtegrity displays the Protected Servers window.
3.	Select the protected server for which the LANtegrity Server is standing in. **Response**: The name of the server is beneath the stand-in service icon. If the option **Exit Stand-in** is grayed out, it means that the protected server is not connected to the network under its alternate name. Check for communication problems and see “Initiating Stand-in” on page 101 for more information.

4. Click Exit Stand-In.

Response: LANtegrity displays the following window.

Figure 6-6. LANtegrity Administrator confirmation dialog

5. Ensure that the 'Sync filesystem' check box is selected and then click OK.

Response: LANtegrity starts the synchronization job, which runs automatically in the background until completion.

✍ *If **Sync filesystem** is deselected when you click OK, you will lose data. See "Exiting without synchronization" on page 119 for more information.*

6. Ensure that users are not connected to the recovering server or the LANtegrity Server's stand-in service.

To verify that no one is currently connected, you can access **Monitor** and check 'Connection Information'. If there are any entries in the list, notify the users, highlight the entries, and delete them.

You can check the Current Jobs window to check on the status of the synchronization job. Press F5 to ensure that you are seeing the latest information.

What occurs when a LANtegrity Server exits stand-in?

When the LANtegrity Server is exiting stand-in, the following steps occur:

- LANtegrity posts a message to the **System Log**.
- The LANtegrity agent on the protected server edits the recovered protected server's **AUTOEXEC.NCF** file.

  It comments out the alternate IPX address and the **Server File Name** statement referring to the **_PS_** prefixed name, and restores the original server's name.
- The LANtegrity Server stops advertising the original server name as its own on the network.
- The LANtegrity agent shuts down the recovering protected server and reboots it using its original name.

  If the reboot is successful, the protected server resumes operation. If the reboot is unsuccessful, the LANtegrity Server again stands in for the protected server and sends an alert. The amount of time that the LANtegrity Server waits for the server to reboot is determined by the **Reboot timeout** setting on the **Configure Protected Servers** panel. See Chapter 9, "Managing the Servers," for information.
- The LANtegrity Server clears out its stand-in file system.
- As a final step, the LANtegrity Server processes the stand-down ***.NCF** batch file, if one has been specified.

  Now you can let users know that they can log in to the protected server.

Exiting without synchronization

Under certain circumstances such as the following, you may decide to exit stand-in service without synchronizing:

- The down server becomes available quickly.
- No changes were made during stand-in.
- You are not bringing the protected server back online.

✍ *Use this option only under special circumstances because potentially you could lose valuable data.*

Canceling a synchronization

If you need to suspend or cancel a synchronization request, you can do so from the Current Jobs window. Synchronization requests appear in the Current Jobs window and can be canceled at anytime that the job remains active. Follow the procedure below to cancel a synchronization job.

Step	Action
1.	Click the Current Jobs button or select **Tools/Current Jobs**.
2.	Highlight the synchronization job. `Type = sync, State = in-progress.` **Response**: The active synchronization job appears in the Current Jobs window.
3.	Click Cancel Job. ✍ *When you decide to bring this recovering protected server back online, you need to restart the synchronization process again.*

7 Restoring Files

Overview

This chapter describes how you can restore the following files from a LANtegrity Server to a protected server:

- Current files
- Older versions of current files
- Deleted files
- NetWare bindery
- NDS information that you protected.

LANtegrity maintains copies of all protected files in the Intelligent Data Vault. You can always restore current files, recently deleted files, or older files from the Data Vault.

For any file that has been deleted for some time or that has been superseded by a later version, you can select the version that you want from LANtegrity's Data Vault. Once you browse for the file, LANtegrity identifies which Online, Legacy, or Offsite tape contains the target file. If the selected file is on an unmounted tape, LANtegrity requests you to insert the correct tape during the restoration process.

What can I restore?

You can restore a copy of any file, directory, or volume that resides in the Intelligent Data Vault. Every time a protected file changes, LANtegrity saves a copy of the updated file but it does not write all copies to tape. Therefore, you can restore most, but not all, of these file copies.

You can also restore full volumes, entire directory trees, or any number of files with a single restoration request. You can specify any number of files to restore in a single request or group files into separate requests according to their destinations or overwrite requirements.

How should I group files within restore requests?

LANtegrity imposes no restrictions on how you can group files within a restore request. However, you should consider the following:

- **Group files by destination.** With each restore job, you can restore only to a single destination.
- **Group files by overwrite option.** You can specify only one overwrite option for each restore job.

By default, LANtegrity restores files to their original directories. If the original directory no longer exists, LANtegrity recreates the directory and restores the file using the original pathname.

If you restore files to a location other than the original one, you can place all the files in a single directory or you can instruct LANtegrity to recreate the original directory structure at the new location. In the latter case, LANtegrity creates the complete directory path name, from the root, in this new location. You control this behavior with the **Preserve/Don't Preserve Directories** option on the Restore Options window.

Restoring File Copies

Using the **Restore** window, you can restore file copies from the LANtegrity Server to a protected server by performing the following procedures:

- Select **Restore Files**.
- Find and select the file(s) you want to restore.

  You can select current, deleted, or older versions of files. To identify the files for a restore request, you can select files, select an entire directory, or create a custom rule to select multiple files.
- If desired, set options for logging, overwriting, and restoring files to different locations.
- Click OK on the Restore Files window to start the restore job.

  You can view the status of the restore job in the Current Jobs window.

If you do not know the name or approximate date of a file, you can navigate through the list of protected volumes and directories.

Accessing the Restore tool

Follow the procedure below to access the restore tool.

Step	Action
1.	Click the Restore button or select **Tools/Restore**.

Response: LANtegrity displays the **Restore** window.

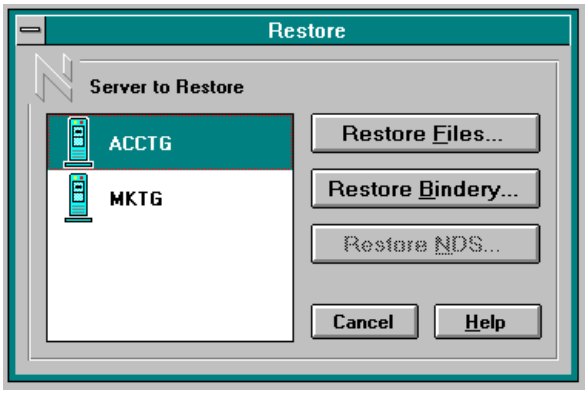


Figure 7-1. Restore window

2. Select the protected server that originally contained the files to be restored.

   ✍ *You must issue a separate restore job for each server whose files you want to restore.*

3. Click Restore Files.

Response: LANtegrity displays the Restore Files window showing the most recently protected volumes on the protected server. The content of the window is derived from the LANtegrity Server's Intelligent Data Vault.

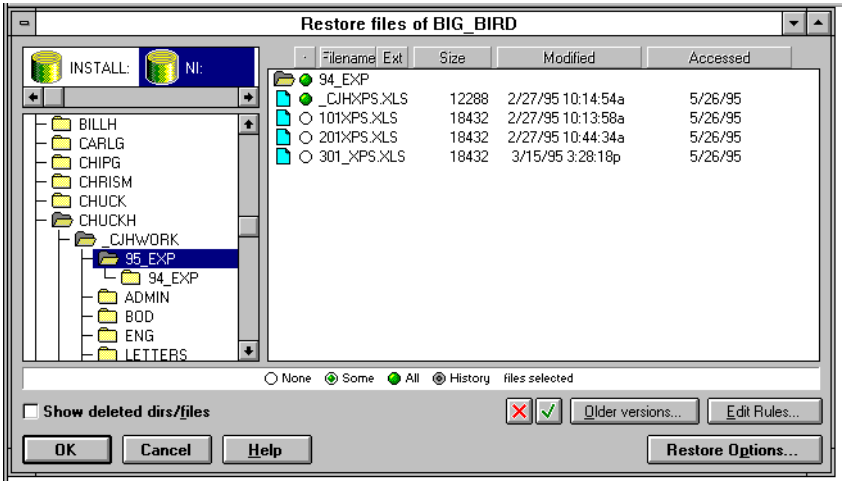


Figure 7-2. Restoring files from server Big_Bird

Viewing files and directories

The Restore window provides two list boxes that allow you to:

- Navigate the server file systems
- View and select items to restore.

Using the Navigation list box

The navigation list box (on the left) lets you navigate through the directories that the selected volume contains. By single clicking a directory in this box, you display its contents in the right-hand selection list box. By double-clicking items in this box, you open and close their contents in this box.

To change the volume that is currently displayed or to move up a directory level, select another volume in the volumes list box.

The lowest level that can be viewed in the navigation box is a directory; you cannot display files in the navigation list box.

Using the Selection list box

The selection list box (on the right) lets you view and select directories and files to restore.

Interpreting restore files information

The window displays the most recently protected file structure. The title bar displays the name of the protected server whose files you are currently viewing.

LANtegrity indicates the status of restores by preceding each item in the selection list box with an icon that indicates what kind of file it is and a circle that indicates the restore status of the file.

Icon	Description
	Files and directories that are not selected for restore.
	Files or entire directories that are selected for restore.
	Older files selected for restore.
	Directories and subdirectories that contain some files selected for restore.

✍ *Each click on a circle toggles the circle and creates a new rule. The new rule cancels the previous rule and all rules applying to subdirectories. For more information about the rules, see* *"Using Rules to Select Files" on page 130*.

Selecting current files to restore

Follow the procedure below to select current files to restore.

Step	Action
1.	On the **Restore Files** window, click on a volume in the volume list box. **Response**: LANtegrity displays the directories and files on the volume.
2.	In the navigation list box (on the left), double click on a directory to expand it. **Response**: LANtegrity displays a list of the directory's files in the selection list box (on the right). The display shows *only* the most recently protected files when it opens. If you choose just from these files, you should not need additional tapes to perform the restoration. The files are located on site in the LANtegrity Server's disk cache or Online tape set.
3.	To select a file for restoration, click once on the restore circle. **Response**: LANtegrity changes the associated circle to indicate the restore status. If you select a directory, you will restore the complete directory and all of its subdirectories. To restore a complete volume, you must select all of its directories and files in the root directory.
4.	After selecting the file(s) to restore, you can: ▪ View the rules that were created by clicking Edit Rules. See "Creating custom rules" on page 132 for information. ▪ Select other directories and files, edit rules, select restore options, or select older versions. ▪ Show deleted directories or files. ▪ Restore the item(s) you've selected.

Selecting deleted files to restore

If a volume, directory, or file does not appear in the list or if you know that it has been deleted from the protected server, you may still be able to restore it. Follow the procedure below to select deleted files.

Step	Action
1.	On the Restore Files window, select the 'Show deleted dirs/files' checkbox. **Response**: LANtegrity updates the display to add the names of directories and files that have been deleted from the protected server. Deleted items are displayed in red. Note that until the next verify job completes, any files that were deleted since the last verification are still shown as current (that is, not deleted). See Chapter 3, "Protecting Server Data," for information about verifications.
2.	Open volumes and directories to locate files to restore.
3.	Click on the file name (not the circle) in the selection list box.
4.	Click Older versions.
5.	Select the version of the file that you want to restore and then click OK. You can select only one older version of a file at a time. When you select deleted versions of files, you may have to load Legacy or Offsite tapes into the autoloader.
6.	After selecting the file you want to restore, you can: ▪ View the rules that were created by clicking Edit Rules. See "Creating custom rules" on page 132 for information. ▪ Select other directories and files or select restore options. ▪ Restore the item(s) you've selected.

Selecting older versions of current files

Follow the procedure below to select older versions of current files.

Step	Action
1.	On the Restore Files window, click on the file name (not the circle) in the selection list box.

✍ *Note that selecting an older version of a directory restores only the (empty) directory and its attributes. If you want to restore files within the directory, you have to select each file that it contains.*

2. Click Older versions.

Response: The History window opens showing all of the saved copies of the file that are currently available on tape.

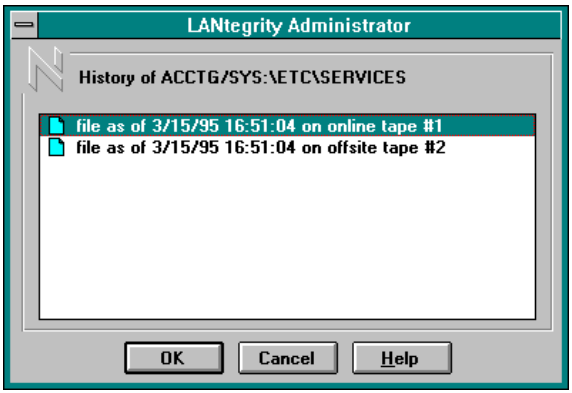


Figure 7-3. LANtegrity Administrator History window

Action: When you select older versions of files, you may have to load Legacy or Offsite tapes into the autoloader.

3. Select the version you want to restore and then click OK.

4. After selecting the version you want to restore, you can:

   - View the rules that were created by clicking Edit Rules. See “Creating custom rules” on page 132 for information.
   - Select other directories and files or select restore options.
   - Show deleted directories or files.
   - Restore the item(s) you’ve selected.

Using Rules to Select Files

A restore rule is a statement that specifies the criteria that LANtegrity uses to find matching items and restore them to the protected server.

You create restore rule in two ways:

- When you perform a file selection activity

  See "Restoring File Copies" on page 122.

- When you specifically define a custom rule

  See "Creating custom rules" on page 132.

✍ *For the most part, you will not have to create custom rules. You can simply click on the circles that precede the files you want to restore. If you want to create custom rules, make sure that you understand how they work before you begin.*

The file activities that create a rule are:

- Selecting a current file by clicking the restore circle.

  This action creates the rule *"include filename"* in the parent directory.

- Selecting current directories by clicking the restore circle.

  This action clears any previous rules in the selected directory and its subdirectories. Then it creates the include *.* or exclude *.* rule in the selected directory that applies to all of its subdirectories. It does not generate a rule in the parent directory. You must open the selected directory to view its rule.

  Note that if a directory is preceded by a filled green circle, it indicates that all of the files in the directory are selected for restore. A partially filled green circle indicates that some of the files in the directory are selected.

- Selecting older versions of current or deleted files.

  This action creates a rule such as *"file name as of date on tape n."* The history circle appears.

Viewing the restore rules

Rules are attached to directories, not to files. You have to navigate to the correct directory to view its rules. Follow the procedure below to view the rules for the directory.

Step	Action
1.	On the Restore Files window, navigate to the desired directory in the navigation list box.
2.	Click Edit Rules. **Response**: LANtegrity displays the Edit Rules window.

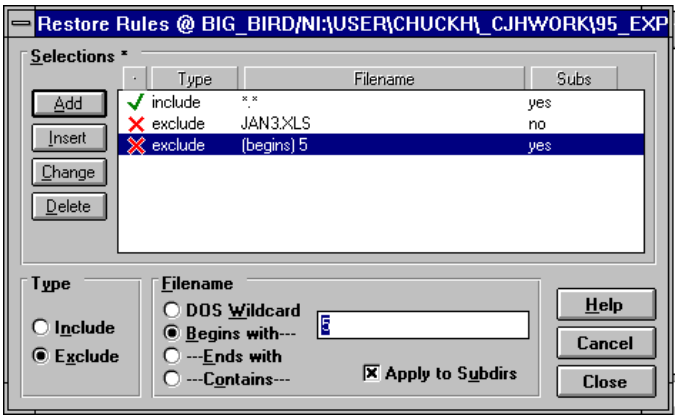


Figure 7-4. Restore/Edit Rules window

The column headings have the following meanings:

- **Type.** The rule type (**Include** or **Exclude**). The rule type indicates whether you want to include or exclude any files that match the **Filename** specification.

- **Filename.** The **Filename** specification. The filename specification supplies the search string that LANtegrity will use. For each file that matches the filename specification, LANtegrity applies the associated rule type. When defining a filename specification, you can use any printable characters, including punctuation marks and spaces. You cannot enter a pathname.

You can define a filename as:

- The actual filename.
- A DOS wildcard string. Select to specify a **DOS Wildcard** and then type the string in the input box. DOS wildcards are ***** (asterisk, designates any number of any characters) and **?** (question mark, designates a single occurrence of any character). For example, the string ***.dat** selects all files that have the **.dat** extension.
- LANtegrity applies this criterion only to the DOS name of the file.
- A pattern matching string that specifies one or more initial characters (**Begins with**), one or more ending characters (**Ends with**), or one or more sequential characters at any place within the filename (**Contains**). Select **Begins with**, **Ends with**, or **Contains**) and type the string in the input box. For example, if you select **Begins with** and specify the character **~** (tilde) as your string, LANtegrity will select all files whose names start with this character. With any of these options, ***** and **?** are interpreted as regular characters, not as wildcards.
- These patterns are matched to the name in its original name space.

- **Apply to Subdirs.** Select to apply the rule to all files located at any point below the volume and directory you selected. If you do not use this option, LANtegrity applies the rule only to those items within the selected volume and directory.

Creating custom rules

You can write rules to restore current files only.

✍ *For the most part, you will not have to create custom rules to restore files. You can simply click on the files you want to select. If you want to create custom rules, make sure that you understand how they work before you begin.*

Follow the procedure below to create custom rules.

Step	Action
1.	On the Restore Files window, select the volume and directory level where you want the rules to apply.
2.	Click Edit Rules.
3.	Define the rules: ▪ To create a new rule, specify the Type, DOS wildcard or pattern matching string, type a string if needed, and decide if you want the rule to apply to the subdirectories. See the section above for information about the fields. ✍ *The order in which you add rules is significant. Try to make your rules progress from the most general to the most specific. When performing a restore job, LANtegrity reads the rules from top of the list to bottom.* ▪ To insert a rule before an existing rule in the list, create the rule, click on the existing rule before which the new rule is to appear and click Insert. ▪ To modify an existing rule, click on the rule in the list, make the change, and then click Change. LANtegrity displays the rule's definition so you can change it. You cannot change rules for older versions. ▪ To remove a rule from the list, click on the existing rule and then click Delete.
4.	Click Add to add the rule to the end of the current list.
5.	Click Close to exit the Edit Rules window and return to the Restore Files window.

Selecting Restore Options

Once you have identified the items you want to restore, you can set various options for the restore operation. Follow the procedure below to access the restore options.

Step	Action
1.	On the Restore Files window, click Restore Options. **Response**: LANtegrity displays the Restore Options window.

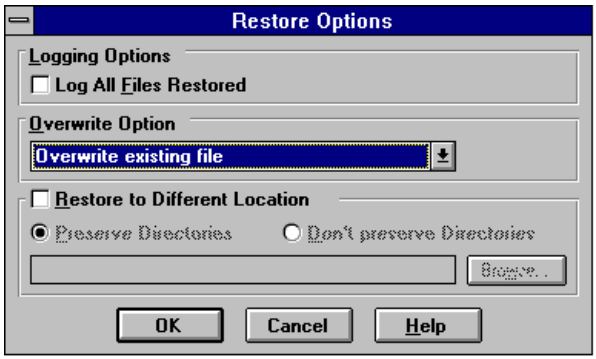


Figure 7-5. Restore Options window

To set logging options

You can instruct LANtegrity to produce a list of all files restored.

On the **Restore Options** window, click ‘Log All Files Restored’. Logs appear in the Job Log window.

To set the overwrite option

During the restoration process, LANtegrity may encounter existing files that have the same names as restored files. In the event that LANtegrity finds an existing file, you must provide instructions on how LANtegrity should proceed.

LANtegrity provides you with the following options for resolving filename conflicts:

- **Auto-rename if existing file.** LANtegrity renames the restored file and preserves the existing file.

  LANtegrity replaces the last character of the file extension with a number. If there is no extension, it adds an extension consisting of numbers.

  For example, LANtegrity would resolve a conflict for file **memo.doc** by renaming the restored file **memo.do1**. It would resolve a conflict for file **february.xls** by renaming the restored file **february.xl1**.

- **Overwrite existing file**. LANtegrity replaces the existing file with the restored file.

- **Overwrite with newer file only**. LANtegrity compares the two files and select the more recent one. If the restored file is more recent, LANtegrity overwrites the existing file. If the existing file is more recent, LANtegrity discards the restored file.

- **Do not overwrite existing file**. LANtegrity discards the restored file. Choose this option only if you want existing files to take precedence at all times.

Step	Action
1.	On the Restore Options window, click the arrow to the right of the 'Overwrite Option' input box. **Response**: LANtegrity displays the list of available options.

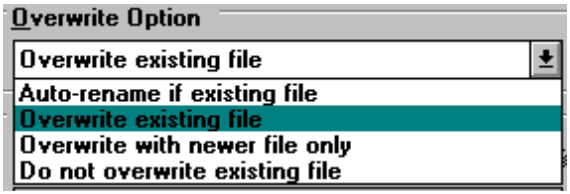


Figure 7-6. Overwrite Options group box

2.	Click on the option you want to set.

To restore to a different location

You can also choose to restore files to a location other than their original location. In this case, you have to decide if you want to preserve or not preserve the directory structure.

Preserve Directories restores the entire directory structure into the destination directory. This includes the full parent pathname from the root as well as all of the selected directories.

Don't preserve Directories restores all of the selected files from any selected directories to a single destination.

You can restore a file, directory, or volume to any protected server within the LANtegrity Server's domain and place the restored items anywhere in the server's directory structure. When restoring to a different server, you must include the server name in the path, using the following format:

```
server_name/volume_name:\directory_name\ ...
```

If you do not know the full pathname of the destination location, you can use the Browse feature, as described below.

Step	Action
1.	On the Restore Options window, click 'Restore to Different Location'.
2.	Type the pathname for the new location in the input box or click Browse to select the destination by browsing through the directory structure.
3.	If you want to restore all the files at the new location, regardless of their original paths, click 'Don't preserve Directories'. Otherwise, the default 'Preserve Directories' recreates the original directory structures at the new location.

✍ *When you restore any version of a file to a different location, some rights may be restricted by the directory rights. After restoring such a file, make sure that the intended users still have access.*

To identify a location via the browse feature

As an aid in identifying restore locations, LANtegrity provides a browse tool that lets you navigate through the directory structure and graphically select the volume and directory destinations.

Step	Action
1.	On the Restore Options window, click ‘Restore to Different Location’. **Response**: This activates Browse.
2.	Click Browse. LANtegrity displays the Restore-To Path window, with the left-hand list box showing the names of the servers within the LANtegrity Server’s domain.

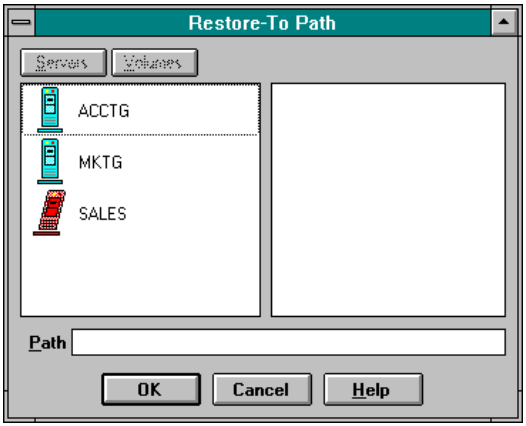


Figure 7-7. Restore-to Path dialog

3.	Double-click on the target server’s name. (You can select either the original server or another server.) LANtegrity displays the server’s name in the ‘Path’ input box at the bottom of the window and updates the display so that the left-hand list box now shows the names of the volumes on the selected server.

✍ *For each item you want to include in the pathname, double-click on its name in the left-hand list box.*

4. Double-click on the target volume's name. (You can select either the original volume or another volume.) LANtegrity displays the volume's name in the 'Path' input box at the bottom of the window and updates the display so that the left-hand list box now shows the names of the directories in the selected volume.

5. Double-click on the target directory's name. (You can select either the original directory or another directory.) LANtegrity displays the directory's name in the 'Path' input box at the bottom of the window and updates the display so that the right-hand list box now shows the names of any files or subdirectories contained in the selected directory.

6. When you complete the pathname for the restore destination, click OK to return to the Restore Options window.

   Response: LANtegrity displays the pathname you built with the browse feature in the 'Restore to Different Location' input box.

Executing the restore

After you have identified the volumes, directories, and files to restore, and after you have set your restore options, you are ready to execute the restore request. Follow the procedure below to execute the restore request.

Step	Action
1.	Make sure you are at the Restore Files window and then click OK. **Response**: LANtegrity asks you to confirm your action.
2.	Click Yes to confirm your restore request. **Response**: LANtegrity begins processing the restore job. If you do not want to confirm the restore request, press No to return to the Protected Servers window or Cancel to return to the Restore window.

Protecting restored files

When LANtegrity is using the date/time method to detect file changes, it may not protect restored files under continuous protection until the next full verify job completes. If a restored file's last modification date/time stamp is earlier than an overwritten file's previous date/time stamp, LANtegrity will not recognize that the file is changed. You may want to start a verify job now to make sure that all restored files are currently protected and that copies of them exist in the LANtegrity Server's cache. For instructions on how to perform a verification, see Chapter 3, "Protecting Server Data."

Restoring the Bindery

Follow the procedure below to restore the bindery to a protected server.

Step	Action
1.	On the Restore window, select the protected server and click Restore Bindery. **Response**: LANtegrity displays the following window showing the available versions of the saved Bindery for the protected server:

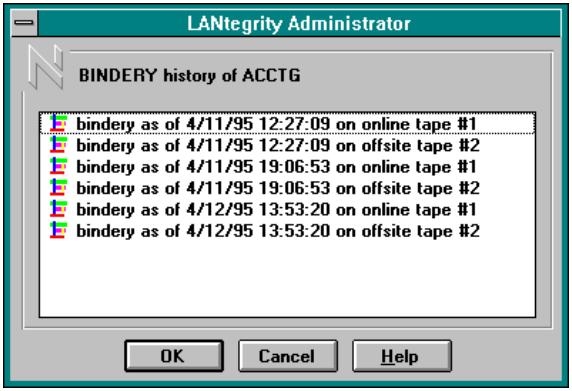


Figure 7-8. LANtegrity Administrator Bindery window

2.	Select the version you want to restore and then click OK. **Response**: LANtegrity restores the selected version and returns you to the Restore window.

Restoring NDS

Follow the procedure below restore the NDS subtree that was protected on the LANtegrity Server.

Step	Action
1.	On the Restore window, click Restore NDS. **Response**: LANtegrity displays a window showing the available versions of the saved NDS.

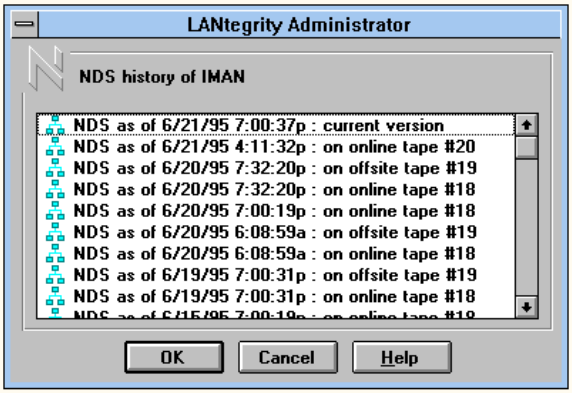


Figure 7-9. LANtegrity Administrator NDS window

The scope and content of the NDS subtree you can restore depends upon which container name you specified in the ‘NDS Protection’ field on the Configure LANtegrity Server window.

2.	Select the version you want to restore and then click OK. **Response**: LANtegrity restores the selected version and returns you to the Restore window.

8 Customizing File Protection

Overview

By default, LANtegrity provides continuous protection for all of the files on its protected servers except for files you specifically exclude. This default protection guarantees availability of all files that may be required during stand-in. It also ensures the protection of any files needed for restoration.

Each file is protected under continuous protection unless you specifically remove it from continuous protection by placing it on a protection schedule or on the Never Protect or Master Exclusions rule sheet. Note that by default, certain files are excluded. This chapter explains how you can make these changes to the default protection method.

Why would I change the default settings?

You might want to change the default settings for these types of files:

- Files that are internally consistent only at certain times, such as database files.
- Files that must remain exactly synchronized with other files, such as OLE-linked documents.
- Files that are extremely large and change very often, such as log files or accounting files.
- Mounted read-only volumes such as CD-ROMs.

Why exclude files from protection?

The purpose of protecting a file is to ensure that the file will be available during stand-in or for restoration.

Some files, however, are transient in nature and are never accessed by users. An application may create such files when it starts and then delete them when it shuts down. Saving copies of these files provides no recovery protection and needlessly consumes processing and storage resources.

How do I identify files to exclude?

LANtegrity supplies a default list of files on the Master Exclusions sheet. Consider keeping these files on the Master Exclusion list unless you are sure that a given file type or file should not be excluded.

You may want to exclude other file types or files from protection but do so carefully.

If you do not add any additional rules, at worst you are protecting some files that do not need protection.

What are my options?

In addition to continuous protection, LANtegrity provides three additional ways to create a customized file protection scheme:

- **Master Exclusions.** Use to identify specific files and file types that you want to globally exclude from protection, regardless of where they occur on any of the protected servers.
- **Never Protect.** Use to identify specific files and files types that you want to exclude from protection at locations on specific protected servers.
- **Scheduled protection.** Use to create protection schedules for files that must be saved at particular times.

Using Master Exclusions

You can use the Master Exclusions list to specify files that you want to exclude from protection, regardless of where they occur on the protected servers.

LANtegrity provides some default exclusions but you can change or delete them and add exclusions of your own.

You can identify the files to be excluded globally by specifying specific filenames or file types. These exclusions are actually rules that you can apply to all protected servers or to all servers of a given system type (NetWare 3x or NetWare 4x).

✍ *Use Master Exclusions with caution since placing a file on the Master Exclusions list means that it will not be available for stand-in or restoration.*

This section describes how to access the Master Exclusions list and how to define, add, change, or delete rules.

Accessing the Master Exclusions list

You can view the rules that make up the Master Exclusions list on the Master Exclusions panel, which is accessed from the Never Protect rule sheet. Follow the procedure below to access the Master Exclusions list.

Step	Action
1.	Click the Scheduled Protection button or select **Tools/Scheduled Protection**. **Response**: LANtegrity displays the Scheduled Protection window.
2.	Click on the ‘Never Protect’ tab. **Response**: LANtegrity displays the Never Protect rule sheet.
3.	Click on Master Exclusions.

Response: LANtegrity displays the Master Exclusions panel.

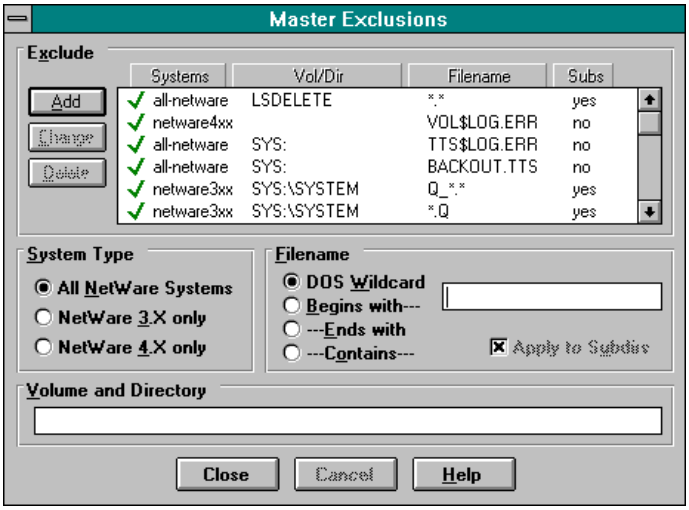


Figure 8-10. Master Exclusions panel

The window displays the list of files or file types that are excluded globally and the controls to add, change, or delete rules.

Defining Master Exclusion rules

To define a rule on the Master Exclusion panel, you specify a NetWare system type, a volume/directory path, a filename, and whether or not the exclusion applies to subdirectories. All of this information is required.

- **Systems.** The type of NetWare system to which you want to apply the rule. If you are working in a mixed environment containing both NetWare 3x and 4x servers, you may want to exclude certain files from systems running one of the versions. By default, LANtegrity applies the exclusion to all NetWare system types.

- **Vol/Dir.** A specific volume and directory path for exclusion. You must specify a complete DOS pathname.

  For example, if you want to exclude the SYS volume, you would enter SYS: If instead you wanted to exclude only a directory in the SYS volume, you would enter SYS:\USERS.

- **Filename.** The Filename specification. The filename specification supplies the search string that LANtegrity will use. For each file that matches the filename specification, LANtegrity applies the associated rule type. When defining a filename specification, you can use any printable characters, including punctuation marks and spaces. You cannot enter a pathname.

  You can define a filename as:

  - The actual filename.

  - A DOS wildcard string. Select to specify a **DOS Wildcard** and then type the string in the input box. DOS wildcards are ***** (asterisk, designates any number of any characters) and **?** (question mark, designates a single occurrence of any character). For example, the string ***.dat** selects all files that have the **.dat** extension.

  LANtegrity applies this criterion only to the DOS name of the file.

  - A pattern matching string that specifies one or more initial characters (**Begins with**), one or more ending characters (**Ends with**), or one or more sequential characters at any place within the filename (**Contains**). Select Begins with, Ends with, or Contains) and type the string in the input box. For example, if you select Begins with and specify the character ~ (tilde) as your string, LANtegrity will select all files whose names start with this character. With any of these options, * and ? are interpreted as regular characters, not as wildcards.

    These patterns are matched to the name in its original name space.

- **Apply to Subdirs.** Select to apply the rule to all files located at any point below the volume and directory you selected. If you do not use this option, LANtegrity applies the rule only to those items within the selected volume and directory.

Adding a new rule

You can add as many rules as necessary to the Master Exclusions list. The rules can appear in any order.

✍ *Remember that each rule you add identifies files that will not be protected by LANtegrity and therefore will not be available during stand-in or for restoration.*

Follow the procedure below to add a new Master Exclusion rule.

Step	Action
1.	On the Master Exclusions panel, define a new rule. Specify the NetWare system type, a volume/directory path, a filename, and whether or not the exclusion applies to subdirectories. See "Defining Master Exclusion rules" on page 145 for more information.
2.	When you finish defining the rule, click Add. **Response**: LANtegrity adds the new rule to the list. The rules can appear in any order.
3.	Click Close to return to the Scheduled Protection window and save your changes to the Master Exclusions list.

Changing a rule

You can modify a rule in the Master Exclusion list by changing its system type, filename specification, volume and directory path, and its applicability to subdirectories. Follow the procedure below to change a Master Exclusion rule.

Step	Action
1.	On the Master Exclusions panel, click on the rule you want to change. **Response**: LANtegrity shows the system type, filename, volume and directory path, and whether or not the rule applies to subdirectories.
2.	Make the necessary changes to the definition of a rule. See “Defining Master Exclusion rules” on page 145 for more information.
3.	When finished making your changes, click Change. **Response**: LANtegrity updates the rule in the Master Exclusions list.
4.	Continue changing rules or click Close to return to the Scheduled Protection window and save your changes to the Master Exclusions list.

Deleting a rule

You can delete rules from the Master Exclusion list. The files identified by a deleted rule revert to continuous protection, unless they are specified on the Never Protect rule sheet or on a protection schedule. Follow the procedure below to delete a Master Exclusion rule.

Step	Action
1.	On the Master Exclusions panel, click on the rule you want to delete. ✍ *To select a sequence of rules, hold down the* SHIFT *key and click on the first and last rules in the sequence. To select multiple individual rules, hold down the* CTRL *key and click on each rule.*
2.	Click on Delete. **Response**: LANtegrity removes the rule (s) from the list.
3.	Continue deleting rules or click Close to return to the Scheduled Protection window and save your changes to the Master Exclusions list.

Using the Never Protect Sheet

You can use the Never Protect rule sheet to specify files that you want to exclude from protection on a specific server. It contains a set of rules that define specific files or file types that you want exclude.

You can change or delete exclusions or add new exclusions of your own.

✍ *Use the Never Protect rule sheet with caution since placing a file on the sheet means that it will not be available for stand-in or restoration.*

This section describes how to access the Never Protect rule sheet and view the files and directories. It also explains how add or remove files and directories from the rule sheet. Follow the procedure below to access the Never Protect rule sheet.

Step	Action
1.	Click the Scheduled Protection button or select **Tools/Scheduled Protection**. **Response**: LANtegrity displays the Scheduled Protection window.
2.	Click on the NEVER Protect tab.

Response: LANtegrity displays the Never Protect rule sheet.

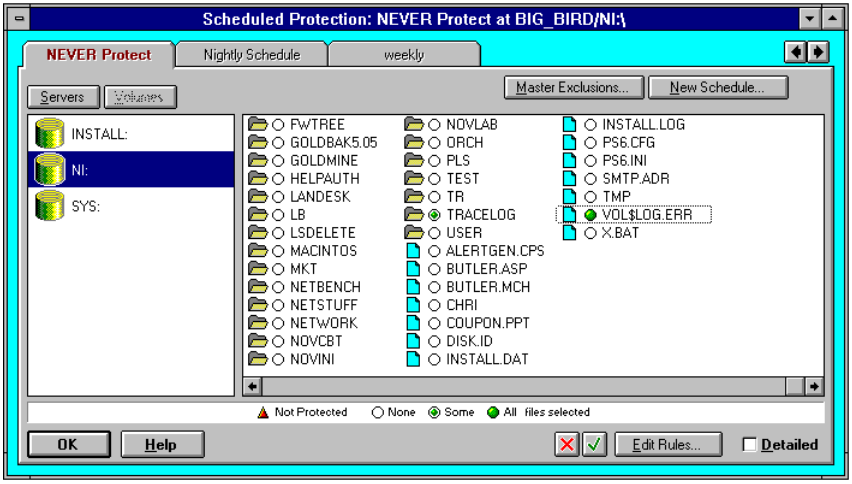


Figure 8-11. Never Protect rule sheet

Viewing files and directories

The Never Protect rule sheet and a schedule, such as the default Nightly schedule, provide two list boxes that allow you to:

- Navigate the server file systems
- View and select items in the current rule sheet.

Using the Navigation list box

The navigation list box (on the left) lets you navigate through the different servers and the volumes and directories that they contain. By single clicking a server, volume, or directory in this box, you display its contents in the right-hand selection list box.

By double-clicking items in this box, you open and close their contents in this box.

To change the volume or server that is currently displayed or to move up a directory level, click the **Servers** or **Volumes** button above the box.

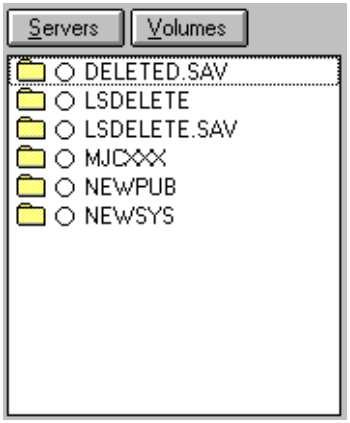


Figure 8-12. Navigation list box

The lowest level that can be viewed in the navigation box is a directory; you cannot display files in the navigation list box. LANtegrity updates the window's title bar as you move up and down the hierarchy.

Using the Selection list box

The selection list box (on the right) lets you view and select directories and files in the current rule sheet.

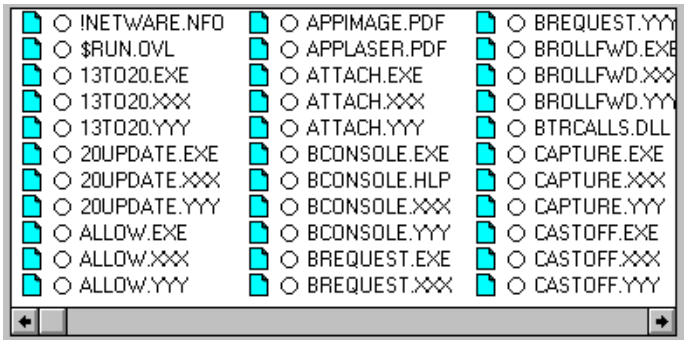


Figure 8-13. Selection list box

Interpreting file selection information

The title bar displays the name of protected server whose files you are currently viewing on the Never Protect rule sheet.

Each item in the selection list box is preceded by an icon that indicates whether it is a file or directory, and a circle that indicates the item's protection status. The following table describes the protection circles and their meanings.

Icon	Description
	Files and directories that are not selected for restore.
	Files or entire directories that are selected for restore.
	Older files selected for restore.
	Directories and subdirectories that contain some files selected for restore.
	Files or entire directories that are selected on the Never Protect or the Master Exclusions rule sheets. Note that this triangle appears on scheduled protection sheets but does not appear on the Never Protect sheet itself.

✍ *Each click on a circle toggles the circle and creates a new rule. The new rule cancels the previous rule and all rules applying to subdirectories. For more information about rules, see* *"Using Rules to Select Files" on page 165*.

Adding files and directories to a rule sheet

You can use the selection list box to add specific files or entire directories to the current rule sheet. An empty circle precedes items that are not on this rule sheet.

Follow the procedure below to add a file.

Step	Action
1.	Use the navigation list box to get to the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	If the file is under continuous protection (empty circle), click on the circle. **Response**: LANtegrity changes the circle to a filled circle, indicating that the file is now on the current rule sheet.

Follow the procedure below to add a directory and its subdirectories.

Step	Action
1.	Use the navigation list box to get to the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	If the directory or subdirectory is under continuous protection (empty circle), click on the circle. **Response**: LANtegrity changes the circle to a filled circle, indicating that the entire contents of the directory and all of its subdirectories are now on the current rule sheet.

Removing files and directories from a rule sheet

You can use the selection list box to remove specific files or entire directories from the current rule sheet. A filled circle precedes currently selected files and entire directories that are on this rule sheet. A partially filled circle precedes directories that contain some files that are on this rule sheet. Follow the procedure below to remove a file.

Step	Action
1.	Use the navigation list box to get to the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	Click on the file's filled circle. **Response**: LANtegrity removes the file from the current rule sheet and changes the circle to an empty circle, indicating that file has been removed from this rule sheet.

Follow the procedure below to remove a directory.

Step	Action
1.	Use the navigation list box to get to the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	Click on the directory or subdirectory's filled or partially filled circle. **Response**: LANtegrity removes the directory or subdirectory from the current schedule and changes the circle to an empty circle, indicating that the contents of the directory or subdirectory has been removed from this rule sheet. **Action**: Clicking on a filled or partially filled circle of a directory clears all the rules below that point.

Using Scheduled Protection

Scheduled protection allows you to remove files and directories from continuous protection and protect them at times that you specify. You should use schedules sparingly and only for files that must be saved at particular times. For these files, identify a time when they are quiesced and available for protection.

You can create multiple schedules for LANtegrity to execute automatically, and you can protect the same file under more than one schedule. This section describes how to access scheduled protection tools. It explains how to view, create, change, delete, or execute a schedule on demand. In addition, it explains how to add or remove files and directories from a schedule.

Continuous vs. scheduled protection

Whenever possible, you should use continuous protection. Continuous protection ensures that LANtegrity automatically detects and saves any file changes. It provides the most efficient protection for the majority of file types stored on network file servers.

However, there are some file types that you might want to handle with scheduled protection.

What types of files should I consider for scheduled protection?

You might want to consider these types of files for scheduled protection:

- Files that are internally consistent only at certain times, such as database files.
- Files that must remain exactly synchronized with other files, such as OLE-linked documents.
- Files that are extremely large and change very often, such as log files or accounting files.

Large files that change infrequently, however, should remain under continuous protection.

Accessing the scheduled protection tools

When you want to place a file under scheduled protection, you use the Scheduled Protection tool. Follow the procedure below to access the Scheduled Protection tools.

Step	Action
1.	Click the Scheduled Protection button or select **Tools/Scheduled Protection**. **Response**: LANtegrity displays the Scheduled Protection window.

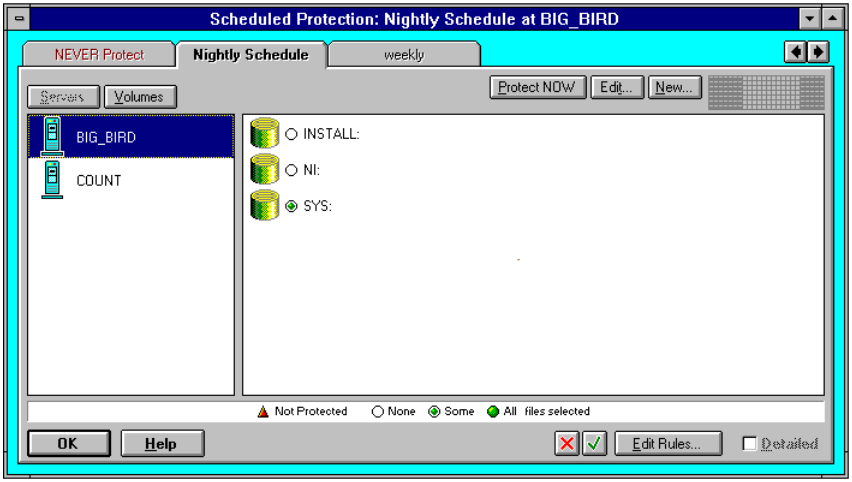


Figure 8-14. Scheduled Protection window

Viewing a schedule

LANtegrity allows you to view its default nightly schedule (running from 7 PM to 7 AM) or existing schedules that you have created. Follow the procedure below to view an existing schedule.

Step	Action
1.	On the Scheduled Protection window, click the tab for the desired schedule's folder or use the left and right arrow buttons to scroll through the list of schedules. **Response**: LANtegrity updates the Scheduled Protection window to show information about the selected schedule. LANtegrity lets you preview the current schedule by displaying a small image of the current schedule above the selection list box.
2.	To view the actual schedule, click Edit (above the selection list box). **Response**: LANtegrity displays the Edit Schedule window showing the starting time and duration (if any) for the schedule.
3.	To view another schedule, click the arrow to the right of the 'Save As' input box to pull down the list of schedules. Then double-click on the schedule you want to view
4.	Click Close to return to the Scheduled Protection window.

Creating a new schedule

You can create as many schedules as needed to provide custom protection for your network environment. LANtegrity provides default protection schedules that you can use as a starting point or you can start from an empty schedule. Follow the procedure below to create a new protection schedule.

Step	Action
1.	On the Scheduled Protection window, click New (above the selection list box) or if you want to start from an existing schedule, select Edit.

Response: LANtegrity displays the Edit Schedule window showing a blank schedule.

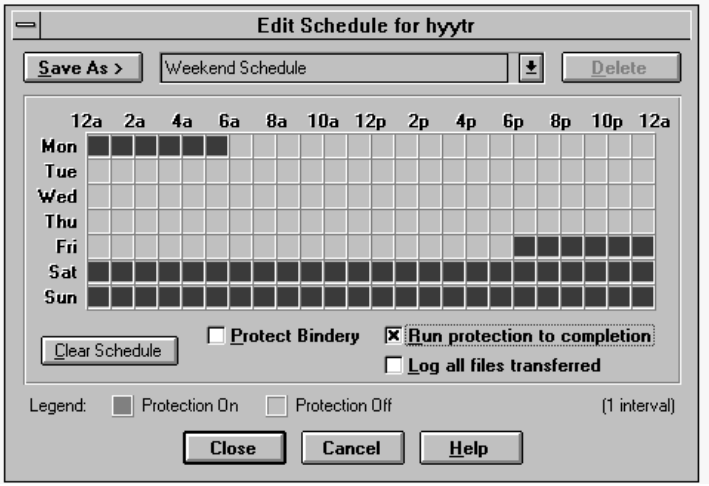


Figure 8-15. Edit schedule panel

The Edit Schedule window shows a matrix consisting of hours of the day (**columns**) and days of the week (**rows**). Each horizontal row identifies a day of the week, with Monday at the top. The first time period (left edge of the matrix) is 0 (12 AM, midnight). Protection periods are indicated by the shaded squares.

2. In the Save As input box, type a name for the new schedule.

   The name can contain up to 100 characters and any printable characters, including spaces. As a rule, use shorter names so that you can display them without having to scroll.

3. Identify the start of a schedule by clicking a square.

4. Click subsequent squares to specify the duration of the schedule.

   The figure above shows a schedule that runs from 6 PM Friday through 5AM Monday morning.

5. If you want to allow scheduled jobs to run until completed instead of terminating at a particular time, select ‘Run protection to completion’.

6. If you want to protect the Bindery in a NetWare 3x environment on a schedule, click the 'Protect Bindery' check box.

   A Bindery is also protected whenever a verify job runs to completion.

7. When you complete the schedule definition, click Save As to save the schedule and register it for use by the LANtegrity Server.

   You can continue to create additional schedules or change or delete existing schedules.

8. When finished with the Edit Schedule window, click Close to return to the Scheduled Protection window.

Changing a schedule

LANtegrity allows you to edit your schedules to reflect changing conditions and match them to the requirements of your site. Follow the procedure to change a protection schedule.

Step	Action
1.	On the Scheduled Protection window, click on a schedule's folder tab.
2.	Click Edit (above the selection list box). **Response**: LANtegrity displays the Edit Schedule window with the schedule's start times and duration (if any) shown.
3.	Change the schedule's start times or durations by clicking the appropriate squares.
4.	When you complete the schedule changes, click Save As.
5.	Click Close to return to the Scheduled Protection window.

Deleting a protection schedule

You can delete any protection schedule, even the default schedule **Nightly**.

✍ *If you delete all of the scheduled protection sheets, you can still create a new protection schedule from the Never Protect sheet, which you cannot delete.*

Follow the procedure to delete a protection schedule.

Step	Action
1.	On the Scheduled Protection window, click on a schedule's folder tab.
2.	On the Scheduled Protection window, click Edit (above the selection list box). LANtegrity displays the Edit Schedule window.
3.	Click Delete. **Response**: LANtegrity asks you to confirm the deletion.
4.	Click Yes. **Response**: LANtegrity removes the schedule from its protection policy. If the schedule has any rules, LANtegrity reassigns the identified files to continuous protection (if no other schedule applies).
5.	Click Close to return to the Scheduled Protection window.

Executing a schedule on demand

You can have LANtegrity execute a protection schedule at any time, without having to wait for the specified time. Regardless, the protection schedule will still execute at its regularly specified time. Follow the procedure below to execute a schedule on demand.

Step	Action
1.	On the Scheduled Protection window, click the tab for the desired schedule's folder or use the left and right arrow buttons to scroll through the list of schedules.
2.	Once the desired schedule is displayed, click Protect NOW. LANtegrity executes the schedule immediately

Adding files and directories to a schedule

You can use the selection list box on a protection schedule to add specific files or entire directories to the schedule. An empty circle precedes items that are not on this rule sheet.

Follow the procedure below to add a file.

Step	Action
1.	Use the navigation list box to position on the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	If you want to add a file that is not on this rule sheet (that is, it's preceded by an empty circle), click on the circle. **Response**: LANtegrity changes the circle to a filled circle, indicating that the file is now included on the current rule sheet.

Follow the procedure below to add a directory and all of its subdirectories.

Step	Action
1.	Use the navigation list box to position on the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	If the directory or subdirectory is not on this rule sheet (that is, it's preceded by an empty circle), click on the circle. **Response**: LANtegrity changes the circle to a filled circle, indicating that the entire contents of the directory or subdirectory are now selected on the current schedule.

✍ *If you click a partially filled circle, the circle clears indicating that the directory and all of its files and subdirectories are removed from this rule sheet. Click the circle again to add the entire directory to this rule sheet.*

Removing files and directories from a schedule

You can use the selection list box to remove specific files or entire directories from the current schedule. A filled circle precedes items on this schedule. A partially filled circle precedes directories that contain some files that are on this rule sheet. Follow the procedure below to remove a file.

Step	Action
1.	Use the navigation list box to position on the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*

2. Click on the file's filled circle.

   Response: LANtegrity removes the file from the current rule sheet and changes the circle to an empty circle, indicating that file has been removed from this rule sheet.

Follow the procedure below to remove a directory.

Step	Action
1.	Use the navigation list box to position on the desired point in a server's file system. ✍ *See "Using the Navigation list box" on page 151 for information about navigating through the file system of a server.*
2.	Click on the directory's filled or partially filled circle. **Response**: LANtegrity removes the directory and all of its subdirectories from the current rule sheet and changes the circle to an empty circle, indicating that the contents of the directory and its subdirectories have been removed from this rule sheet.

Using Rules to Select Files

A protection rule is a statement that specifies the criteria that LANtegrity uses to find matching items and include or exclude them from a rule sheet on the Scheduled Protection window. This section explains how rules are created. Then it describes how to view rules for all protected servers and rules for a directory, create custom rules or delete them.

How rules are created

You create a protection rule in two ways:

- When you perform a file selection activity on the rule sheets. See "Using the Never Protect Sheet" on page 150 and "Using Scheduled Protection" on page 156.
- When you specifically define a custom rule. See "Creating custom rules" on page 168 for details.

✍ *For the most part, you will not have to create custom rules. You can simply click on the circles that precede the files you want to select. If you want to create custom rules, make sure that you understand how they work before you begin.*

The file activities that create a rule are:

- Selecting a current file by clicking the circle that precedes it.

  This creates the rule "include filename" in the parent directory.

- Selecting current directories by clicking the circle that precedes it.

  This clears any previous rules in the selected directory and its subdirectories. Then it creates the include *.*, exclude *.*, or exclude-if-open rule in the selected directory that applies to all of its subdirectories. It does not generate a rule in the parent directory. You must open the selected directory to view its rule.

If a directory is preceded by a filled green circle, it indicates that all of the files in the directory are selected. A partially filled green circle indicates that some of the files in the directory are selected.

Viewing the rules for all protected servers

After adding and removing files and directories to a scheduled protection sheet or the Never Protect sheet, you may want to view the rules you have created.

LANtegrity allows you to check on the rules for the current schedule from **Tools/Scheduled Protection Rules** or at current directory location. Follow the procedure below to view the rules.

Step	Action
1.	Select Tools | Schedule Protection Rules. **Response**: LANtegrity displays the Schedule Protection Rules window which shows a list of volumes and pathnames of directories that contain rules, sorted by schedule.
2.	Select the directory whose rules you want to view. **Response**: LANtegrity displays the Rule Items panel, showing the specific rules for that directory. If you want to define custom rules, see "Creating custom rules" on page 168. If you want to view the Master Exclusion rules, see the Master Exclusions panel.

Viewing the rules for a directory

Rules are attached to directories, not to files. You have to navigate to the correct directory to view its rules. Follow the procedure below to view the rules for the directory.

Step	Action
1.	On the Scheduled Protection window, navigate to the desired directory in the navigation list box.
2.	Select the file or directory in the selection list box.
3.	Click Edit Rules.

Response: LANtegrity displays the Protection Rules window.

The column headings have the following meanings:

- **Type.** The rule type (**Include** or **Exclude**). The rule type indicates whether you want to include or exclude any files or directories that match the **Filename** specification.

- **Filename.** The **Filename** specification. The filename specification supplies the search string that LANtegrity uses. For each file that matches the filename specification, LANtegrity applies the associated rule type. When defining a filename specification, you can use any printable characters, including punctuation marks and spaces. You cannot enter a pathname.

You can define a filename as:

- The actual filename.
- A DOS wildcard string. Select to specify a **DOS Wildcard** and then type the string in the input box. DOS wildcards are ***** (asterisk, designates any number of any characters) and **?** (question mark, designates a single occurrence of any character). For example, the string ***.dat** selects all files that have the **.dat** extension.
- LANtegrity applies this criterion only to the DOS name of the file.
- A pattern matching string that specifies one or more initial characters (**Begins with**), one or more ending characters (**Ends with**), or one or more sequential characters at any place within the filename (**Contains**). Select Begins with, Ends with, or Contains) and type the string in the input box. For example, if you select Begins with and specify the character ~ (tilde) as your string, LANtegrity will select all files whose names start with this character. With any of these options, * and ? are interpreted as regular characters, not as wildcards.

These patterns are matched to the name in its original name space.

- **Apply to Subdirs.** Select to apply the rule to all files located at any point below the volume and directory you selected. If you do not use this option, LANtegrity applies the rule only to those items within the selected volume and directory.

- **Size.** You can optionally specify a size criterion for selecting files. LANtegrity will apply the rule type only to those files that qualify on the basis of their size.

To use a size qualification, click the 'Size' check box and either the 'Larger' or 'Smaller' check box. Then, type the number of bytes to use in the 'bytes' input box. For example, if you specify Smaller than 2,097,152 bytes, LANtegrity will select only those files that are smaller than 2 MB.

✍ *If a file's size changes and it no longer matches this criterion, LANtegrity reassigns the file to continuous protection.*

Creating custom rules

You can create rules on the Protection Rules window.

✍ *For the most part, you will not have to create custom rules. You can simply click on the circle that precedes the files you want to select. If you want to create custom rules, make sure that you understand how they work before you begin.*

Follow the procedure below to create custom rules.

Step	Action
1.	On the Scheduled Protection window, select the volume and directory level where you want the rules to apply.
2.	Click Edit Rules.
3.	Define the rules:

- To create a new rule, specify the Type, DOS Wildcard or pattern matching string. Type a string if needed, and decide if you want the rule to apply to the subdirectories. See the preceding section for information about the fields.

  ✍ *The order in which you add rules is significant. Try to make your rules progress from the most general to the most specific. When performing a scheduled protection job, LANtegrity reads the rules from the top of the list to bottom.*

- To insert a rule before an existing rule in the list, create the rule, click on the existing rule before which the new rule is to appear and click Insert.

- To modify an existing rule, click on the rule in the list, make the change, and then click Change. LANtegrity displays the rule's definition so you can change it. You cannot change rules for older versions.

- To remove a rule from the list, click on the existing rule and then click Delete.

4. Click Add to add the rule to the end of the current list.

5. Click Close to exit the Edit Rules window and return to the Scheduled Protection window.

Deleting a rule

You can delete rules from any rule sheet. The files identified by a deleted rule revert to continuous protection, unless they are covered by another rule in the same or a different rule sheet. Follow the procedure below to delete a rule.

Step	Action
1.	On the Scheduled Protection window, click the tab for the desired folder or use the left and right arrow buttons to scroll through the list of rule sheets.
2.	Once the desired schedule is displayed, click Edit Rules (in the lower right corner of the window).

Response: LANtegrity displays the Protection Rules window.

3. Click on the rule you want to delete.

4. Click on Delete.

   Response: LANtegrity removes the rule from the rule sheet.

5. Continue deleting rules or click Close to return to the Scheduled Protection window.

✍ *If, after deleting rules, you decide you don't want to change the rule, click Cancel instead of Close.*

9 Managing the Servers

Placing a Server Under Protection

Before a server is protected by LANtegrity, you use the **Configure Protected Servers** panel do the following:

- Authenticate the server
- Enable protection.

LANtegrity verifies the server with its regularly scheduled verification and automatically places it under continuous protection.

You can also disable protection for a server. See "Disabling protection" on page 177.

Authenticating the protected servers

A LANtegrity Server functions as the server and the protected NetWare servers function as clients. To support communications between the LANtegrity Server and its protected servers, you must authenticate the servers by supplying a username and password for each protected server. The LANtegrity Server uses this name to log in to the protected server to protect and restore files.

Use this procedure if you are authenticating a new server or if you are changing the username or password on an existing protected server. Follow the procedure below to authenticate a protected server.

Step	Action
1.	Make sure that the LANtegrity agent is running on the protected server. ✍ *If it is not running, see the Setup Guide for information about installing the LANtegrity software.*
2.	Click the General Configuration button or select **Tools/General Configuration**. **Response**: LANtegrity displays the General Configuration window.
3.	In the list box on the left, select 'Protected Servers'. **Response**: LANtegrity displays the Configure Protected Servers panel showing a list of the NetWare file servers that have LANtegrity agents running on them.

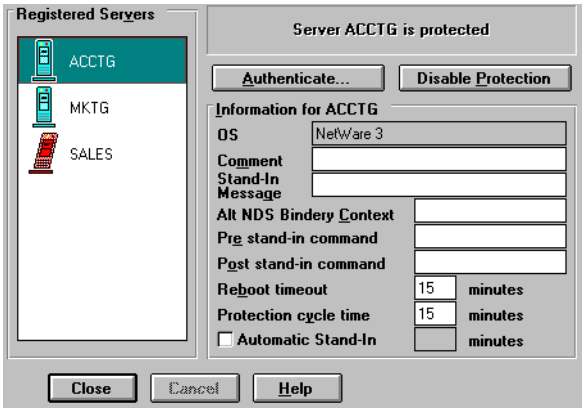


Figure 9-1. Configure Protected Servers panel

You can quickly identify servers that are not authenticated by checking their icons. The icon for unauthenticated servers is red and tilted. The following table describes all of the icons you may see.

Icon	Description
	Online and fully protected.
	Down and the LANtegrity Server is standing in for it.
	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 server.
	LANtegrity agent is loaded but server is not authenticated.
	Down and the LANtegrity Server is not standing in for it.

4. Select the server you want to authenticate and click Authenticate.

   Response: LANtegrity displays a LANtegrity dialog.

5. Type the LANtegrity Server's valid NetWare username in the 'Username' input box and the appropriate password in the 'Password' input box.

   - The username must be a Supervisor or Supervisor-equivalent for the file server.
   - For a NetWare 4 server, a Supervisor-equivalent is a user with supervisor rights to the NDS object of the protected server. Enter the typed or typeless NDS distinguished name.
   - For a NetWare 3 server, the username must have supervisor or supervisor-equivalent privileges on the protected server.

6. Supply or change information if needed in the ‘Information’ area.

   ✍ *Pay special attention to the description of **Reboot timeout**. The value should be about twice the time it normally takes to reboot the protected server. If the value is too low, the LANtegrity Server may not be able to exit Stand-in.*

7. Click OK to register the username and password with the LANtegrity Server and return to the Configure Protected Servers panel.

   You can enable protection for the server or continue authenticating other servers.

Enabling protection

Follow the procedure below to 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 showing a list of the available NetWare file servers. ✍ *Remember that you can enable protection only for an authenticated server.*
3.	Select the authenticated server you want to protect and click Enable Protection. **Response**: When you select the icon, the information box at the top of screen indicates the status of the server.

LANtegrity changes the server's icon from tilted to upright and shows an **X** through it. When you add or restore protection to a server, the **X** through its icon indicates that LANtegrity has not yet verified the server. Until a server is verified, the LANtegrity Server cannot stand-in for it. By default, verification is run nightly when network traffic is at a minimum. See "Changing the verify schedule" on page 28 for more information about verification.

Alternatively, you can verify now but note that a verification requires a significant commitment of system and network resources. For instructions on how to verify now, see "Verifying a server on demand" on page 31.

You can continue enabling protection for authenticated servers or you can fill in the rest of the information on the Configure Protected Servers panel.

Filling in information fields for a protected server

This table describes the fields in the 'Information' area. Some of the fields are optional.

✍ *Pay special attention to the description of* **Reboot timeout**. *The value is critical to the proper operation of Stand-in. Also check the description of* ***Automatic Stand-in***.

Use this field...	To...
OS	View the version of the NetWare system running on the server that you selected.
Comment	(Optional) Type a comment.
Stand-in Message	(Optional) Type a message that the LANtegrity Server automatically sends when each user logs into the protected server in stand-in. For example, you could type **`Server EXEC in off-line for repairs`**. For information about stand-in, see Chapter 6, "Operating Stand-in Service."

Use this field...	To...
Alt NDS Bindery Context	(Optional; for 3x protected servers only) Type the NDS context you use to handle other than file services for a 3x server during stand-in. For example, you could set up services for printing or a fax modem. For example, .o=exec_cx. For information, refer to the appendix in the *Setup Guide*, “Providing Stand-in Printing Services.”
Server Bindery Context	(Optional; for 4x protected servers only) Type the NDS context that is used to enable Bindery logins. This distinguished name appears in a set Bindery context command on the protected server.
Pre stand-in command	(Optional) Type console commands that the LANtegrity Server executes when it starts stand-in service. Typically, the commands are .NCF command files that start NLMs.
Post stand-in command	(Optional) Type console commands that LANtegrity executes when it exits stand-in.
Reboot timeout	Type 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 default is 15 minutes. **Important:** The amount of time must be approximately twice the time it takes to reboot the selected server or else the LANtegrity Server will not be able to exit stand-in. The default is 15 minutes.
Protection cycle time	Type the amount of time that you want the LANtegrity Server to take to complete a protection cycle. This option allows you to manually control the requirements for CPU time. The default 15 is minutes.
Automatic Stand-in	Select if you want the LANtegrity Server to automatically stand-in for the protected server when it loses connection with the protected server. The default is 15 minutes. The period specified should give you enough time to determine if the problem is communications (e.g., the router went down) and to solve it.

Disabling protection

You can disable protection for a server from the Protected Servers panel. When you remove protection from a server, LANtegrity suspends all protection. Follow the procedure below to remove protection from a server.

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 showing a list of the available servers.
3.	Select the server you want to remove from protection.
4.	Click Disable Protection. **Response**: LANtegrity asks you to confirm the operation.
5.	Click Yes. **Response**: LANtegrity suspends its scans of the server until you return the server to protection. The icon for the server now appears tilted.

Changing Settings of the LANtegrity Server

You can control the operation of the LANtegrity Server by the values that you set for several parameters. This section describes how to change:

- The LANtegrity Server's NetWare username and password
- The stand-in service file retrieval behavior

Refer to Chapter 2 for information about changing parameters related to continuous protection such as the detection method. Follow the procedure below to access the Configure LANtegrity Server panel.

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.

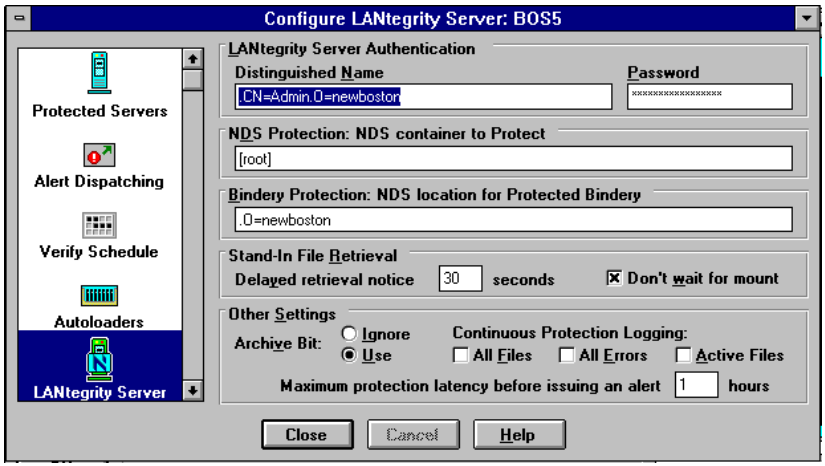


Figure 9-2. Configure LANtegrity Server window

3. When you complete all changes to this panel, select another option from the panel on the left or click Close.

✍ *LANtegrity saves changes to a configuration panel when you click on another selection in the list box on the left or when you click Close.*

Changing the name and password

LANtegrity does not require that you change your username and password at regular intervals, but you do need to update them to reflect any changes required by your NDS security schedule.

The LANtegrity Server is a NetWare Loadable Module (NLM) that communicates with other NetWare services. To communicate with NetWare, the LANtegrity Server must have a valid NDS username and password with NetWare Supervisor rights to the LANtegrity Server on the objects in the NDS tree. The username and password you supply is authenticated by NDS.

This username and password remains in effect until you explicitly change them on the Configure LANtegrity Server panel. Note that only the username name is displayed. The password is never displayed. Follow the procedure below to change the LANtegrity Server's username/password.

Step	Action
1.	On the Configure LANtegrity Server panel, type the new username in the 'Distinguished Name' input box. The name must be registered with NDS.
2.	Type the password for the new username in the 'Password' input box. **Response**: LANtegrity protects your password by displaying it as a sequence of asterisks (*******). If you make a typing error, delete the contents of the input box and start again.

Changing the Stand-In file retrieval behavior

When the LANtegrity Server is standing in for a down server, users may need to use files that are not available in the disk cache or in a currently loaded tape. In this case, users may experience some delay while the LANtegrity Server accesses the requested files from another Online tape or from an Offsite tape.

While waiting for the file, the user's workstation pauses. LANtegrity waits a specified amount of time to try to get the file. If it is not available within that time, LANtegrity releases the workstation and sends a message.

LANtegrity allows you to specify how it should interact with users while it accesses such files. Follow the details below to set the file retrieval behavior.

On the Configure LANtegrity Server panel:

- To pause the user's workstation until the required tape is mounted, deselect the 'Don't Wait for media to mount' check box. Then type the number of seconds to wait before sending a file retrieval message. This is the default setting.

- To allow users to continue without pausing their workstations until the required tape is mounted, select the 'Don't Wait for media to mount' check box. Then type the number of seconds to wait before sending a file retrieval message.

Index

B

Bindery
- restoring, 120

C

Continuous protection
- defined, 23

I

Instant server recovery
- *see* Stand in

L

LANtegrity
- components, 6

LANtegrity Administrator
- Windows application, 6

LANtegrity Server
- NLM, 6

LSAGENT.NLM
- defined 6

LSSERVER.NLM
- defined 6

LSSTART.NLM
- defined 6

N

NDS
- restoring, 120

NLMs
- LSAGENT.NLM, 6
- LSSERVER.NLM, 6
- LSSTART.NLM, 6

P

Protected server
- NLMs, 6
- SAP assumed by LANtegrity Server, 7
- stand in for, 7

R

Restore
- accesing, 123
- destinations, 121
- grouping files by destination, 121
- grouping files by overwrite option, 121

Restore window
- defined 122

S

SAP
- used during stand in, 7

Service Advertising Protocol
- *see* SAP

Stand in
- transfer of protected serverís SAP, 7

Stand-in
- when used, 93

Stand-in service
- *see* Stand-in

V

Verification
- default verify schedule, 22