

COURSE 570

NetWare® 5 Advanced Administration

INSTRUCTOR GUIDE

Education

Novell®

100-004318-001
Revision 1.0

Proprietary Statement

Copyright © Novell, Inc. 1995, 1996, 1997, 1998. All rights reserved.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express prior consent of the publisher. This manual, and any portion thereof, may not be copied without the express written permission of Novell, Inc.

Novell, Inc.
1555 North Technology Way
Orem, Utah 84097-2399

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to revise this publication and to make changes in its content at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software at any time, without obligation to notify any person or entity of such changes.

This Novell Training Manual is published solely to instruct students in the use of Novell networking software. Although third-party application software packages are used in Novell training courses, this is for demonstration purposes only and shall not constitute an endorsement of any of these software applications.

Further, Novell, Inc. does not represent itself as having any particular expertise in these application software packages and any use by students of the same shall be done at the students' own risk.

Software Piracy

Throughout the world, unauthorized duplication of software is subject to both criminal and civil penalties.

If you know of illegal copying of software, contact your local Software Antipiracy Hotline.

For the Hotline number for your area, access Novell's World Wide Web page at <http://www.novell.com> and look for the piracy page under "Programs."

Or, contact Novell's anti-piracy headquarters in the U.S. at 800-PIRATES (747-2837) or 801-861-7101.

Trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell, Inc.

NetWare, the N-Design, and Novell are registered trademarks of Novell, Inc. in the United States and other countries. The NetWare Logotype (teeth logo) is a trademark of Novell, Inc.

CNE is a registered service mark of Novell, Inc. CNA and CNI are service marks of Novell, Inc. Master CNE is a trademark of Novell, Inc.

ConsoleOne is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

Internet Packet Exchange is a trademark of Novell, Inc.

IPX and IPX/SPX are trademarks of Novell, Inc.

NetSync is a trademark of Novell, Inc.

NetWare 2 is a trademark of Novell, Inc.

NetWare 3 is a trademark of Novell, Inc.

NetWare 4 is a trademark of Novell, Inc.

NetWare 5 is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare DOS Requester is a trademark of Novell, Inc.

NetWare/IP is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare MultiProtocol Router is a trademark of Novell, Inc.

NetWare Name Service is a trademark of Novell, Inc.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

Novell Application Launcher is a trademark of Novell, Inc.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services and NDS are trademarks of Novell, Inc.

Novell Distributed Print Services is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

Novell Technical Support is a service mark of Novell, Inc.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Packet Burst is a trademark of Novell, Inc.

Remote Console is a trademark of Novell, Inc.

Storage Management Services and SMS are trademarks of Novell, Inc.

Transaction Tracking System is a trademark of Novell, Inc.

Other Trademarks

386 and 486 are trademarks of Intel Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.

ARCnet is a registered trademark of Datapoint Corporation.

DATASHOW is a registered trademark of Sayett Technology, Inc.

DynaText is a registered trademark of Electronic Book Technologies, Inc.

IBM is a registered trademark of International Business Machines Corporation.

Intel is a registered trademark of Intel Corporation.

Java is a registered trademark of Sun Microsystems, Inc. in the United States and other countries.

JavaSoft is a registered trademark of Sun Microsystems, Inc.

LANSchool is a registered trademark of Lan Fan Technologies.

Macintosh is a registered trademark of Apple Computer, Inc.

Microsoft is a registered trademark of Microsoft Corporation.

NetBasic is a registered trademark of High Technology Software Corporation

Netscape FastTrack is a trademark of Netscape Communication Corporation.

OS/2 is a registered trademark of International Business Machines Corporation.

Pentium is a registered trademark of Intel Corporation.

Persuasion is a registered trademark of Adobe Systems Incorporated.

PS/2 is a registered trademark of International Business Machines Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Windows, Windows 95, and Windows NT are registered trademarks of Microsoft Corporation.

Contents

Preparation and Setup

Audience.....	IG Prep-1
Prerequisites.....	IG Prep-1
Agenda	IG Prep-2
Classroom Requirements	IG Prep-4
Classroom Setup Instructions.....	IG Prep-5
Setting Up the Classroom Server	IG Prep-5
Setting Up the Student Servers.....	IG Prep-61
Classroom 3.12 Server.....	IG Prep-61
Install Online Documentation	IG Prep-62
Configure the Workstations	IG Prep-62
Using Presentation Graphics.....	IG Prep-63
Displaying the Graphics	IG Prep-63
Printing the Graphics.....	IG Prep-64
Using Classroom Animations	IG Prep-64

Introduction

Introduction.....	IG Intro-3
Audience.....	IG Intro-3
Prerequisites.....	IG Intro-5
Certification Tests.....	IG Intro-5
Relationship to Other Courses in the Curriculum	IG Intro-7
Course Overview	IG Intro-9
Exercises	IG Intro-9

Section 1 **Upgrading to NetWare 5**

Upgrading to NetWare 5.....	IG 1-3
Objectives.....	IG 1-3
Choosing an Upgrade Method and a Protocol	IG 1-5
Upgrading an Existing Server with the Installation Program.....	IG 1-7
Migrating a Server with the Novell Upgrade Wizard.....	IG 1-9
Choosing a Protocol	IG 1-11

Using the Installation Program to Upgrade a NetWare 4.1x Server	IG 1-13
Preparing for the Upgrade	IG 1-13
Performing the Upgrade	IG 1-15
Completing Post-Upgrade Procedures.....	IG 1-17
Hands-On Exercise 1-1: Upgrading a NetWare 4.11 Server to NetWare 5.....	IG 1-19
Using the Novell Upgrade Wizard to Upgrade a NetWare 3.1x Server	IG 1-23
Installing the Novell Upgrade Wizard	IG 1-23
Preparing for the Upgrade	IG 1-25
Launching the Utility	IG 1-31
Creating a Project.....	IG 1-31
Moving Objects from the Project Window	IG 1-33
Verifying That Objects and Files Can Be Upgraded.....	IG 1-35
Upgrading Across the Wire	IG 1-37
Completing Post-Upgrade Procedures.....	IG 1-39
Hands-On Exercise 1-2: Upgrading a NetWare 3.12 Server to NetWare 5.....	IG 1-41
Summary	IG 1-47

Section 2 Using the Server Console

Using the Server Console.....	IG 2-3
Objectives	IG 2-3
NetWare Server Overview	IG 2-5
The NetWare Kernel.....	IG 2-5
The Server Console	IG 2-11
NetWare Loadable Modules	IG 2-13
Executing Console Commands	IG 2-19
SET Parameters	IG 2-21
Console Hot Key Sequences	IG 2-23
Loading and Unloading NLMs	IG 2-25
Hands-On Exercise 2-1: Using Console Commands and NLMs	IG 2-27
Server Configuration Files	IG 2-31
STARTUP.NCF	IG 2-33
AUTOEXEC.NCF	IG 2-35
Customizing the Server Configuration Files	IG 2-37

Creating Server Script Files.....	IG 2-39
Hands-On Exercise 2-2: Customizing the Server AUTOEXEC.NCF File.....	IG 2-41
Hands-On Exercise 2-3: Creating Server Script Files	IG 2-43
Loading Support for Java Applications on the NetWare 5 Server	IG 2-47
Hardware Requirements for Java.....	IG 2-49
Java Support on NetWare	IG 2-51
GUI Support on NetWare	IG 2-55
Using the NetWare GUI.....	IG 2-57
Installing Other Novell Products	IG 2-57
Configuring Video Resolution	IG 2-59
Keyboard Configuration.....	IG 2-59
Configuring the Background.....	IG 2-61
Adding Java Programs and Applets to the NetWare GUI	IG 2-61
Using ConsoleOne	IG 2-63
Server Administration with ConsoleOne.....	IG 2-67
NDS Administration with ConsoleOne.....	IG 2-79
Customizing the ConsoleOne Interface.....	IG 2-85
Hands-On Exercise 2-4: Using ConsoleOne	IG 2-89
Accessing the Server Console from a Workstation	IG 2-103
Setting Up the Server for Remote Console	IG 2-105
Executing the Remote Console Software.....	IG 2-109
Protecting Your Server	IG 2-113
Locking Up the Server.....	IG 2-113
Secure Console.....	IG 2-113
SCRSAVER.NLM	IG 2-115
Loading Remote Console Agents with a Password	IG 2-115
Hands-On Exercise 2-5: Accessing and Securing the Server Console Remotely.....	IG 2-121
Summary	IG 2-127

Section 3 Setting Up Queue-Based Network Printing

Setting Up Queue-Based Network Printing	IG 3-3
Objectives.....	IG 3-3
Network Printing Setup Overview	IG 3-5

- Creating and Configuring Printing Objects IG 3-7
 - Critical Properties IG 3-7
 - Printing Object Creation Steps IG 3-11
 - Creating Printing Objects in NetWare Administrator IG 3-13
- Activating the Print Server IG 3-17
- Connecting a Printer to the Network..... IG 3-19
 - Activating a Printer Attached to the Print Server IG 3-21
 - Activating a Printer Not Attached to the Print Server IG 3-21
 - Activating a Printer Attached to a Windows 95 Workstation IG 3-23
- Hands-On Exercise 3-1: Setting Up Network Printing IG 3-25
- Managing Network Print Services IG 3-33
 - Managing the Print Queue IG 3-33
 - Managing the Printer IG 3-39
 - Managing the Print Server..... IG 3-39
 - Network Printing Management Summary..... IG 3-43
 - Default Assignments IG 3-45
- Hands-On Exercise 3-2: Managing Network Printing IG 3-47
- Utility Summary IG 3-53
- Summary of the Print Services Setup Tasks IG 3-55
- Summary IG 3-57

Section 4 Setting Up the Network File System

- Setting Up the Network File System..... IG 4-3
- Objectives..... IG 4-3
- Planning and Creating a Customized Network File System IG 4-5
 - Suggestions on Creating Volumes IG 4-9
- System-Created Directories IG 4-11
- Suggestions on Creating Directories to Organize the File System..... IG 4-17
 - Home Directories..... IG 4-19
 - Application Directories..... IG 4-19
 - Shared Data Directories IG 4-19
- Possible Directory Structures IG 4-21
 - One-Volume Directory Structure IG 4-23
 - Multiple-Volume Directory Structure..... IG 4-25
- Written Exercise 4-1: Designing a Directory Structure IG 4-27

Understanding the NSS File System	IG 4-33
Advantages of NSS	IG 4-33
Limitations of NSS	IG 4-35
NSS Storage Concepts	IG 4-37
Setting Up NSS	IG 4-41
Designing an NSS Volume	IG 4-41
Creating NSS Components	IG 4-43
Hands-On Exercise 4-2: Creating an NSS Volume	IG 4-45
Summary	IG 4-49

Section 5 Optimizing the Network and Server

Optimizing the Network and Server	IG 5-3
Objectives	IG 5-3
NetWare 5 Memory Management	IG 5-5
Memory Allocation	IG 5-7
Memory Deallocation and Garbage Collection	IG 5-9
Virtual Memory	IG 5-11
Understanding Virtual Memory	IG 5-11
Considerations for Using Virtual Memory	IG 5-13
Avoiding Disk Thrashing with Virtual Memory	IG 5-15
Managing Virtual Memory	IG 5-17
Hands-On Exercise 5-1: Managing Virtual Memory	IG 5-19
Using Applications	IG 5-27
Understanding Threads	IG 5-27
Understanding Applications	IG 5-27
Configuring Applications	IG 5-29
Hands-On Exercise 5-2: Managing Applications	IG 5-31
Protected Memory	IG 5-35
Considerations for Using Protected Address Spaces	IG 5-37
Managing Protected Address Spaces	IG 5-39
Hands-On Exercise 5-3: Managing Protected Memory	IG 5-41
MONITOR Statistics	IG 5-45
Cache Utilization	IG 5-49
Setting Cache Read and Write Parameters	IG 5-51
Processor Utilization	IG 5-53
Memory Utilization	IG 5-53
Server Packets and Buffers	IG 5-55

Packets.....	IG 5-55
Maximum Physical Receive Packet Size	IG 5-57
Packet Receive Buffers	IG 5-57
Network Board Statistics	IG 5-61
Disk Drivers and Controllers.....	IG 5-63
Hands-On Exercise 5-4: Monitoring and Maintaining Network Performance	IG 5-65
Written Exercise 5-5: Interpreting MONITOR Information	IG 5-69
Optimizing Disk Space	IG 5-75
Block Suballocation	IG 5-77
Enabling Block Suballocation	IG 5-79
File Compression.....	IG 5-81
File Compression Process	IG 5-81
Compression Ratio.....	IG 5-83
Managing File Compression.....	IG 5-83
File Compression Options	IG 5-85
Setting File Compression Attributes	IG 5-87
Viewing Compression Statistics	IG 5-89
Packet Burst Protocol	IG 5-91
How the Packet Burst Protocol Works	IG 5-93
Large Internet Packets (LIPs).....	IG 5-97
Enabling Routers for Larger Packets	IG 5-99
Using LIP and Packet Burst Protocol	IG 5-99
Written Exercise 5-6: Optimizing Network Performance	IG 5-101
Summary	IG 5-103

Section 6 Backing Up Servers and Workstations

Backing Up Servers and Workstations	IG 6-3
Objectives.....	IG 6-3
Introduction to Storage Management Services	IG 6-5
Choosing a Backup Strategy	IG 6-7
Time Requirements for Completing a Backup.....	IG 6-9
Time Requirements for Restoring a Backup	IG 6-13
Assigning Backup Responsibility.....	IG 6-15
Written Exercise 6-1: Choosing a Backup Strategy.....	IG 6-17

Backing Up Servers and Workstations	IG 6-19
Understanding Backup Terminology	IG 6-21
NetWare Backup/Restore Guidelines.....	IG 6-23
Backing Up a NetWare Server	IG 6-25
Backing Up Windows 95 or Windows NT Workstations	IG 6-27
Hands-On Exercise 6-2: Backing Up NDS and File System Information.....	IG 6-29
Hands-On Exercise 6-3: Backing Up Workstations	IG 6-45
Restoring Data.....	IG 6-55
Hands-On Exercise 6-4: Restoring NDS and File System Information.....	IG 6-57
Hands-On Exercise 6-5: Restoring Workstations	IG 6-69
Summary	IG 6-75

Section 7 Using DNS/DHCP Services

Using DNS/DHCP Services.....	IG 7-3
Objectives.....	IG 7-3
DNS/DHCP Overview	IG 7-5
DNS.....	IG 7-5
DHCP	IG 7-7
Snap-Ins for NetWare Administrator	IG 7-9
DNS/DHCP Management Console	IG 7-9
DNS/DHCP Objects	IG 7-11
Installing DNS/DHCP Services.....	IG 7-19
Extending the NDS Schema and Creating Default DNS/DHCP Objects	IG 7-19
Installing the Novell Client	IG 7-25
Installing the DNS/DHCP Management Console	IG 7-25
Hands-On Exercise 7-1: Installing Novell DNS/DHCP Services.....	IG 7-27
Configuring and Starting DHCP Services.....	IG 7-29
Running the DNS/DHCP Management Console	IG 7-29
Configuring a DHCP Server Object.....	IG 7-33
Configuring a DHCP Subnet Object	IG 7-37
Configuring a Subnet Address Range Object	IG 7-41
Configuring an IP Address Object	IG 7-45
Configuring a Subnet Pool Object	IG 7-47

Starting the DHCP Server	IG 7-51
Configuring the Workstation for DHCP	IG 7-51
Configuring DHCP Options.....	IG 7-53
Setting Global DHCP Options	IG 7-55
Setting DHCP Options at the Subnet Level.....	IG 7-59
Setting DHCP Server Options	IG 7-61
Hands-On Exercise 7-2: Configuring and Starting DHCP Services.....	IG 7-63
Importing DHCP Databases	IG 7-75
Hands-On Exercise 7-3: Importing DHCP Databases.....	IG 7-79
Configuring and Starting DNS Services	IG 7-81
DNS Zones in NDS	IG 7-83
Designated Servers.....	IG 7-85
Configuring a DNS Server Object	IG 7-89
Configuring a DNS Zone Object.....	IG 7-91
Configuring a Resource Record Object.....	IG 7-97
Starting the DNS Server.....	IG 7-99
Configuring the Workstation for DNS	IG 7-99
Hands-On Exercise 7-4: Configuring and Starting DNS Services.....	IG 7-101
Importing DNS Databases.....	IG 7-111
Hands-On Exercise 7-5: Importing DNS Databases	IG 7-113
Summary	IG 7-117

Section 8 Installing a Web Server and an FTP Server

Installing a Web Server and an FTP Server	IG 8-3
Objectives.....	IG 8-3
Overview of the Netscape FastTrack Server.....	IG 8-5
Understanding Web Servers	IG 8-5
Introduction to the Netscape FastTrack Server for NetWare	IG 8-7
Installing the Netscape FastTrack Server.....	IG 8-9
System Requirements.....	IG 8-9
Installing the Netscape FastTrack Server	IG 8-11
Changes Made During Installation	IG 8-15
Hands-On Exercise 8-1: Installing the Netscape FastTrack Server for NetWare.....	IG 8-21

Using the Administration Server	IG 8-25
Introduction to the Administration Server	IG 8-25
Introduction to Server Manager	IG 8-29
Configuring the FastTrack Server.....	IG 8-35
Modifying Basic Server Parameters	IG 8-35
Modifying Directories in the Document Tree	IG 8-41
Configuring Document Preferences	IG 8-47
Restricting Access	IG 8-51
Hands-On Exercise 8-2: Configuring the Netscape FastTrack Server for NetWare.....	IG 8-57
Tuning and Troubleshooting the Netscape FastTrack Server	IG 8-73
Tuning Server Performance	IG 8-73
Setting the Maximum Packet Receive Buffers	IG 8-81
Regulating Web Server Content.....	IG 8-85
Overview of Novell FTP Services for NetWare.....	IG 8-87
Understanding FTP Servers	IG 8-87
Introduction to Novell FTP Services for NetWare.....	IG 8-89
Installing Novell FTP Services for NetWare	IG 8-91
System Requirements	IG 8-91
Installing the Server.....	IG 8-91
Hands-On Exercise 8-3: Installing the Novell FTP Server.....	IG 8-97
Configuring the Novell FTP Server	IG 8-101
Configuring FTP Server Parameters	IG 8-101
Setting File System Rights	IG 8-107
Hands-On Exercise 8-4: Configuring the Novell FTP Server	IG 8-109
Using Novell FTP Services.....	IG 8-113
Downloading Files	IG 8-115
Uploading Files.....	IG 8-115
Hands-On Exercise 8-5: Transferring Files Using Netscape.....	IG 8-117
Troubleshooting FTP	IG 8-119
Network Failure	IG 8-119
FTP Server Not Running	IG 8-119
Overloaded FTP Server	IG 8-121
FTP Client Configuration Errors	IG 8-121
FTP Server Configuration Errors.....	IG 8-123
User Error	IG 8-123
Summary	IG 8-125

Section 9 Securing the NDS Tree

Securing the NDS Tree	IG 9-3
Objectives	IG 9-3
Group Exercise 9-1: NDS Security Review	IG 9-5
Understanding NDS Default Rights	IG 9-11
Default Rights Granted at Initial Tree Creation	IG 9-11
Default Rights Granted to New Containers	IG 9-13
Default Rights Granted at Server Installation	IG 9-15
Default Rights Granted to New User Objects	IG 9-19
Guidelines for Implementing NDS Security	IG 9-23
Using Network Resources	IG 9-23
Managing NDS Objects and Properties	IG 9-25
Additional Administrative Security	IG 9-29
Understanding Centralized and Distributed Administration	IG 9-33
Centralized Administration	IG 9-35
Distributed Administration	IG 9-37
Setting Up the Container Administrator	IG 9-37
Exclusive Container Administrator	IG 9-43
Determining Suggested Administrative Roles and Rights Assignments	IG 9-47
Rights for Administrative Roles	IG 9-53
Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator	IG 9-57
Summary	IG 9-69

Section 10 Maintaining Novell Directory Services

Maintaining Novell Directory Services	IG 10-3
Objectives	IG 10-3
Understanding Replication and Synchronization	IG 10-5
The Directory	IG 10-5
Partitions	IG 10-5
Replicas	IG 10-5
Changing the Directory	IG 10-9
NDS Maintenance Utilities	IG 10-11
Understanding Preventive Maintenance	IG 10-13
Planning Replica Placement Carefully	IG 10-13
Regulating Partition Management Rights	IG 10-15

Backing Up the Directory.....	IG 10-17
Maintaining a Standard NDS Version.....	IG 10-19
Preventing the SYS Volume from Running Out of Space	IG 10-25
Preparing a Server for Downtime	IG 10-27
Troubleshooting NDS Inconsistencies.....	IG 10-29
Identifying NDS Database Inconsistencies	IG 10-29
Finding Help for Resolving Inconsistencies.....	IG 10-37
Repairing NDS.....	IG 10-41
Correcting Database Inconsistencies.....	IG 10-41
Removing a Server from the Network	IG 10-45
Recovering from a Crashed SYS Volume	IG 10-49
Hands-On Exercise 10-1: Identifying NDS Errors	IG 10-55
Summary	IG 10-59

Section 11 Setting Up Server Remote Access and Mobile Clients

Setting Up Server Remote Access and Mobile Clients	IG 11-3
Objectives.....	IG 11-3
Understanding the Capabilities and Requirements of NIAS Remote Access	IG 11-5
Network Services Available Anywhere.....	IG 11-7
Differences Between NIAS Remote Access Connections and Direct LAN Connections	IG 11-9
Overview of Required Tasks to Enable Remote Access.....	IG 11-11
Evaluating the Current Network and User Environment.....	IG 11-13
Selecting the Best Physical Server Locations	IG 11-13
Determining Users and Services.....	IG 11-13
Selecting an Appropriate Data Transmission Technology.....	IG 11-15
Evaluating Common Data Transmission Choices	IG 11-17
Written Exercise 11-1: Selecting the Best Data Transmission Technologies for Your Organization.....	IG 11-23
Designing a Secure Remote Access Solution	IG 11-25
Determining an Organizational Security Policy	IG 11-25
Determining a Network Security Policy	IG 11-27
Determining a Data-Level Security Policy	IG 11-27
Isolating a Remote Access Server	IG 11-29
Special Security Concerns	IG 11-31

- Designing Optimal Remote Access Performance IG 11-33
 - Maximizing Client Performance..... IG 11-33
 - Maximizing Server Performance IG 11-35
 - Optimizing Remote Access Administration IG 11-37
- Written Exercise 11-2: Optimizing Performance and Administration for a Remote Access Solution IG 11-41
- Configuring NIAS Remote Access on the Server IG 11-45
 - Overview of Remote Access Server Tasks IG 11-45
- Hands-On Exercise 11-3: Configuring the NIAS Remote Access Server IG 11-47
- Configuring Windows 95 or Windows NT Clients for Remote Access IG 11-55
 - The Novell Client and Remote Access..... IG 11-55
 - Overview of Tasks to Configure a Remote Access Windows Client..... IG 11-55
- Hands-On Exercise 11-4: Configuring Windows for Remote Access IG 11-57
- Connecting Remotely to a Server..... IG 11-69
 - Connecting a Remote Client IG 11-69
- Hands-On Exercise 11-5: Connecting to the Remote Server with Windows IG 11-71
- Understanding Remote Authentication Dial-In User Service (RADIUS)..... IG 11-77
 - RADIUS Proxy..... IG 11-77
 - RADIUS and Internet Service Providers (ISPs) IG 11-79
- Summary IG 11-81

Section 12 Integrating Other Novell Services

- Integrating Other Novell Services IG 12-3
- Objectives IG 12-3
- Networking Services from Novell..... IG 12-5
- BorderManager Services IG 12-7
- Firewalls and Firewall Components..... IG 12-9
 - Firewall Components and the OSI Model..... IG 12-13
- Firewall Components in BorderManager IG 12-15
 - NIAS 4.1 Software IG 12-15
 - Remote Access IG 12-15
 - IP Gateway Software..... IG 12-17
 - Proxy Cache Software..... IG 12-17

Virtual Private Network (VPN) Encryption Software IG 12-23

BorderManager Components, the OSI Model, and
Firewalls IG 12-27

NDS for NT IG 12-29

Administering All Components of a Network from a
Single Database IG 12-31

NDS Support for Applications That Require Domains..... IG 12-33

Single Login to the Network IG 12-33

Additional Management Capabilities of NDS IG 12-35

NDS for NT Components and Their Functions IG 12-41

SAMSRV.DLL..... IG 12-43

Domain Object Wizard IG 12-47

Novell NDS for NT Client..... IG 12-47

NetWare Administrator IG 12-47

Mailbox Manager for Exchange..... IG 12-49

GroupWise 5 and NetWare IG 12-51

GroupWise 5 System Components IG 12-55

The Client IG 12-57

The Message Transfer System IG 12-59

GroupWise 5 Administration Program..... IG 12-61

The Message Store IG 12-61

The Directory Store IG 12-65

The Document Store IG 12-69

How the GroupWise System Components Work Together IG 12-71

Network Management Using ManageWise IG 12-73

Asset Inventory and Management..... IG 12-75

Server Monitoring and Management IG 12-79

Desktop Management IG 12-83

Network Traffic Analysis and Management..... IG 12-83

Network-Wide Virus Protection IG 12-89

ManageWise Software Components IG 12-91

Summary IG 12-95

Appendix A

Answers to Exercises A-1

Appendix B

NDS Security Review Exercise B-1

Notes

Preparation and Setup

Use this section to help you prepare for and set up the course.

Audience

This course is intended for network administrators who have completed the NetWare 5™ Administration course and Networking Technologies course. A typical student has acquired the necessary knowledge and skills from the NetWare® 5 Administration course and the Networking Technologies course or has had practical job experience administering a NetWare 4™ network.

After students have completed the NetWare 5 Administration course, we recommend that the students return to their jobs to use what they have learned before taking this course.

The course is also intended for NetWare 3™ network administrators who are preparing to upgrade to NetWare 5.

This course is intended for the CNE® and Master CNE™ candidate satisfying the NetWare 5 certification requirements.

Prerequisites

Prerequisite courses:

- Course 560, NetWare 5 Administration
- Course 565, Networking Technologies

Students should be able to perform the following tasks on a NetWare 5 network:

- Plan, implement, and manage the basic network services—user login, file storage, network printing, and Novell Directory Services™ (NDS™)—on a small network.
- Set up login security, file system security, and NDS security.
- Automate the user's environment and access to network resources with login scripts, Novell Application Launcher™, and Workstation Manager.
- Install the Novell Client.
- Create and manage the following objects: group, organizational role, user, printing, alias, directory map, application, workstation, template, organization, and organizational unit.

Agenda

This is a five-day course.

Day 1

Section	Duration (hrs: mins)
Introduction	00:30
Section 1: Upgrading to NetWare 5	02:30
Section 2: Using the Server Console	03:30

Day 2

Section	Duration (hrs: mins)
Section 3: Setting Up Queue-Based Network Printing	02:00
Section 4: Setting Up the Network File System	02:00
Section 5: Optimizing the Network and Server	02:30

Day 3

Section	Duration (hrs: mins)
Section 6: Backing Up Servers and Workstations	02:00
Section 7: Using DNS/DHCP Services	03:00
Section 8: Installing a Web Server and an FTP Server	01:30

Day 4

Section	Duration (hrs: mins)
Section 8: Installing a Web Server and an FTP Server <i>(continued)</i>	02:45
Section 9: Securing the NDS Tree	02:30
Section 10: Maintaining Novell Directory Services	01:15

Day 5

Section	Duration (hrs: mins)
Section 10: Maintaining Novell Directory Services <i>(continued)</i>	01:15
Section 11: Setting Up Server Remote Access and Mobile Clients	02:30
Section 12: Integrating Other Novell Services	02:00

Classroom Requirements

The following table identifies the basic hardware and software requirements for this course. Instructions for classroom setup follow.

Setup	Requirements
Classroom	Level 2 Novell® classroom (see http://education.novell.com/chaninfo/classreq.evy)
NetWare 5 Server	7 servers: 1 for instructor, 6 for students
Hardware	A Pentium® computer, with 64 MB of RAM, a 2 GB hard disk, and a CD-ROM drive
Software	NetWare 5 and NetWare 4.11
NetWare 3.12 Server	1 server
Hardware	A 486/66 computer, with 20 MB of RAM and a 300 MB hard disk
Software	NetWare 3.12
Workstations	7 workstations: 1 for instructor, 6 for students
Hardware	A Pentium computer, with 64 MB of RAM and a 2 GB hard disk For the instructor: connection to a large-screen monitor at the front of the classroom
Software	Windows NT® or Windows 95™, Novell Client

Table Prep-1: Classroom Requirements

Classroom Setup Instructions

You will need two to three hours to set up your classroom for this course.

Allow time not only to set up the system, but to test the setup as well. (Test the setup by performing the exercises and ensuring that the students can complete the exercises as presented.)

Also, test your workstation display software (such as LANSchool®) with the NetWare programs you plan to demonstrate.

Setting Up the Classroom Server

Complete the following:

1. Install the NetWare 5 operating system:
 - Server name: **FS1**
 - Tree name: **EMA_TREE**
2. During installation, create and mount the following volumes:
 - SYS (at least 750 MB)
 - DATA (at least 250 MB)
 - MAIL (at least 250 MB)
3. Create the following objects:
 - An organization object named **EMA**.
 - In EMA, an organizational unit object named **NYC**.
 - In NYC, an organizational unit object named **CORP**.
4. Place the server object and all volume objects in **CORP.NYC.EMA**.
5. Place an **Admin** object having the password of *novell* in the **CORP.NYC.EMA** context.



Using *novell* as the password allows you to use the RESTORE5.NLM default values to restore the Directory and file system.

6. Configure the server for IPX™ and IP. The instructor's server must have IPX bound in order to communicate with the NetWare 4.11 student servers.

7. Install the following options:
 - Storage Management Services™
 - Remote Access Services
 - Novell Documentation CD
8. Install the NetWare 5 documentation to the root of FS1\DATA.
9. After server installation is complete, restore the EMA_TREE backup from your instructor CD.
 - a. Copy the following files from the SETUP directory to FS1_SYS:SYSTEM:
 - EMUIF.NLM
 - TPEMU.HAM
 - NOVED_DS.BCK
 - NOVED_FS.BCK
 - NWTAPE.CDM
 - RESTORE.NLM
 - b. At the server console, enter
LOAD RESTORE5
For more information, refer to RESTORE5.TXT on the Instructor CD.



Using FS1 as the server name allows you to use the RESTORE5.NLM default values.

If you do not use RESTORE5.NLM, you need the information on the following pages to complete the network setup.

10. Install the Z.E.N.works Starter Pack.
 - a. On the client CD, run **WINSETUP.EXE**.
 - b. Click the appropriate *language*.
 - c. Click **Install Z.E.N.works**.
 - d. Follow the prompts.
11. Verify NetWare server operation.
12. Install a printer.
13. Prepare the instructor workstation to use a video projection unit.

File System for FS1

The following outlines the file system that is restored after running RESTORE.NLM.

- SYS:
 - PUBLIC\MESSAGE.TXT
- DATA:
 - APPS\DB
 - APPS\NETSCAPE\USERS\DEFAULT\ARCHIVE
 - APPS\NETSCAPE\USERS\DEFAULT\CACHE
 - APPS\WP (contains EMAWP.EXE)
 - DOCUMENT\DB
 - DOCUMENT\WP
 - SETUP (contains LIST.CTL, LIST.DAT, DHCP3TAB, DNSBIND, CFGRD5.EXE, CONFIG.NLM, and NOVELL.BMP files)
 - SHARED\ACCTG
 - SHARED\ENGR
 - SHARED\MRKTG
 - SHARED\SALES
 - SHARED\TRANSFER (contains EXPENSE.TXT, PROJECTS.TXT, and STATUS.TXT)
 - USERS
 - USERS\ACCTBEI
 - USERS\ACCTBER
 - USERS\ACCTCAI
 - USERS\ACCTMOS
 - USERS\ACCTNYC
 - USERS\ACCTRIO
 - USERS\ACCTTOK
 - USERS\CORPNYC
 - USERS\ENGRBEI
 - USERS\ENGRBER
 - USERS\ENGRCAI
 - USERS\ENGRMOS
 - USERS\ENGRNYC
 - USERS\ENGRRIO
 - USERS\ENGR TOK

USERS\MKTGBEI
USERS\MKTGBER
USERS\MKTGCAI
USERS\MKTGMOS
USERS\MKTGNYC
USERS\MKTGRIO
USERS\MKTGTOK
USERS\SALEBEI
USERS\SALEBER
USERS\SALECAI
USERS\SALEMOS
USERS\SALENYC
USERS\SALERIO
USERS\SALETOK

USERS*location**username* (created by the system when user objects are created) **Note:** location corresponds to the user's department and location.

USERS\SETUP\APPS\ACCTAPP
USERS\SETUP\APPS\DBAPP
USERS\SETUP\APPS\EMAILAPP
USERS\SETUP\APPS\WPAPP
USERS\SETUP\SHARED\ACCTNG\DB\ACTPAY
USERS\SETUP\SHARED\ACCTNG\DB\ACTRECV
USERS\SETUP\SHARED\ACCTNG\DB\GENLED
USERS\SETUP\SHARED\ACCTNG\REP
USERS\SETUP\SHARED\MRKTG\DB
USERS\SETUP\SHARED\MRKTG\REP
USERS\SETUP\SHARED\TRANSFER
USERS\SETUP\USERS\EHEINER
USERS\SETUP\USERS\KHERD
USERS\SETUP\USERS\MJENSEN
USERS\SETUP\USERS\MAVILLA

■ MAIL:

APPS\EMAIL
DOCUMENT\EMAIL
DOCUMENT\EMAIL\TEMPLATE

NDS

Each user object is created using the template object located in the same container.

Object Type	Object Name	Property	Value
O=EMA			
Organizational Unit	BEI		
	BER		
	CAI		
	MOS		
	NYC	Postal (Zip) Code	10001
	RIO		
	TOK		
OU=NYC.O=EMA			

Table Prep-2: NDS Setup

Object Type	Object Name	Property	Value
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	CORP	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=NYC.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	CMiner	Last Name	Miner
		Given Name	Carolyn
	DCook	Last Name	Cook
		Given Name	Doug
	JNesbit	Last Name	Nesbit
		Given Name	John
	MSanchez	Last Name	Sanchez
		Given Name	Manuel
		Title	Director
		Telephone	x7453
Admin	Last Name	Student	
Template	Accounting	Telephone	(212) 555-7878
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERSVACCTNYC
		Street	342 South Technology Way
		City	New York
		State	NY
		Zip Code	10001
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	CMiner
			DCook
	WPUSERS	Members	JNesbit
			MSanchez
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	DCook	
			JNesbit	
OU=CORP.OU=NYC.O=EMA				
User	EAlder	Last Name	Alder	
		Given Name	Elise	
		Telephone	x6723	
		Fax Number	555-1000	
	EHeiner	Last Name	Heiner	
		Given Name	Ethan	
	KHerd	Last Name	Herd	
		Given Name	Kim	
	MAvilla	Last Name	Avilla	
		Given Name	Maria	
		Title	International Marketing Director	
		Telephone	x9991	
	MJensen	Last Name	Jensen	
		Given Name	Marc	
	RClark	Last Name	Clark	
		Given Name	Russ	
		Title	Domestic Marketing Director	
		Telephone	x1212	
	Admin			
	GWAgent	Last Name	Student	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Template	Management	Telephone	(212) 555-7000
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\CORPNYC
		Street	342 South Technology Way
		City	New York
		State	NY
		Zip Code	10001
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	EAlder
			EHeiner
	WPUSERS	Members	KHerd
			MJensen
	EMAILUSERS	Members	EAlder
			EHeiner
			MAvilla
			RCClark
	Container_Admins	Members	Admin.ACCT.BEI.EMA
			Admin.ENGR.BEI.EMA
			Admin.MKTG.BEI.EMA
			Admin.SALE.BEI.EMA
			Admin.ACCT.BER.EMA
			Admin.ENGR.BER.EMA
			Admin.MKTG.BER.EMA
			Admin.SALE.BER.EMA
Admin.ACCT.CAI.EMA			
Admin.ENGR.CAI.EMA			
Admin.MKTG.CAI.EMA			
Admin.SALE.CAI.EMA			
Admin.ACCT.MOS.EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Group (continued)	Container_Admins (continued)	Members (continued)	Admin.ENGR.MOS.EMA
			Admin.MKTG.MOS.EMA
			Admin.SALE.MOS.EMA
			Admin.ACCT.NYC.EMA
			Admin.ENGR.NYC.EMA
			Admin.MKTG.NYC.EMA
			Admin.SALE.NYC.EMA
			Admin.ACCT.RIO.EMA
			Admin.ENGR.RIO.EMA
			Admin.MKTG.RIO.EMA
			Admin.SALE.RIO.EMA
			Admin.ACCT.TOK.EMA
			Admin.ENGR.TOK.EMA
			Admin.MKTG.TOK.EMA
Admin.SALE.TOK.EMA			
Server	FS1		
Volume	FS1_SYS		
	FS1_DATA		
	FS1_MAIL		
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	EMAILDOC	Volume	FS1_MAIL.CORP.NYC.EMA
		Path	DOCUMENT\EMAIL
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	EHeiner
			KHerd

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Application	ConsoleOne	Application icon title	ConsoleOne
		Path to executable file	\\FS1\SYS\PUBLIC\MGMT\CONSOLE1.EXE
		Associations	Container_Admins.CORP.NYC.EMA
			Admin.CORP.NYC.EMA
	Operating System	Windows 95 Windows NT	
	NETSCAPE404	Application icon title	Netscape 404
		Path to executable file	\\FS1\DATA\APPS\NETSCAPE\PROGRAM\NETSCAPE.EXE
		Associations	Container_Admin
			Admin
	OS	Windows 95 Windows NT	
OU=ENGR.OU=NYC.O=EMA			
User	HFranks	Last Name	Franks
		Given Name	Heide
	LWarner	Last Name	Warner
		Given Name	Les
	MBanks	Last Name	Banks
		Given Name	Maria
	RSimpson	Last Name	Simpson
		Given Name	Rebecca
		Title	Design Engineer
		Telephone	x7887
	Admin	Last Name	Student

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Template	Engineer	Telephone	(212) 555-7880
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ENGRNYC
		Street	342 South Technology Way
		City	New York
		State	NY
		Zip Code	10001
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	HFranks
			LWarner
	WPUSERS	Members	MBanks
			RSimpson
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	LWarner
			MBanks
OU=MKTG.OU=NYC.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	APratt	Last Name	Pratt
		Given Name	Amy
	BPritchard	Last Name	Pritchard
		Given Name	Bob
	DMAughan	Last Name	Maughan
		Given Name	David
	SWong	Last Name	Wong
		Given Name	SuLin
		Title	Manager
		Telephone	x7423
Admin	Last Name	Student	
Template	Marketing	Telephone	(212) 555-7400
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\MKTGNYC
		Street	342 South Technology Way
		City	New York
		State	NY
		Zip Code	10001
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	APratt
			BPritchard
	WPUSERS	Members	DMAughan
			SWong
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	BPritchard	
			DMaughan	
OU=SALE.OU=NYC.O=EMA				
User	ELundskog	Last Name	Lundskog	
		Given Name	Elsa	
	JChen	Last Name	Chen	
		Given Name	Joan	
	JGrahm	Last Name	Grahm	
		Given Name	Jeff	
	WFruehan	Last Name	Fruehan	
		Given Name	Wayne	
		Title	Manager	
		Telephone	x7787	
	Admin		Last Name	Student
	Template	Sales	Telephone	(212) 555-7700
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\SALENYC	
Street			342 South Technology Way	
City			New York	
State			NY	
Zip Code			10001	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections	2			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Group	DBUSERS	Members	ELundskog
			JChen
	WPUSERS	Members	JGrahm
			WFruehan
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=BEI.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=BEI.O=EMA			
User	CChen	Last Name	Chen
		Given Name	Ching-Chi
	CYan	Last Name	Yan
		Given Name	Cui
	HLee	Last Name	Lee
		Given Name	Hwa-Wei
	ZTeng	Last Name	Teng
		Given Name	Zhongting
		Title	Director
		Telephone	x458
Admin	Last Name	Student	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Template	Accounting	Telephone	86 10 62751243
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ACCTBEI
		Street	28 Dongzhimenwai Dajie
		City	Beijing
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	CChen
			CYan
	WPUSERS	Members	HLee
			ZTeng
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	CYan
			ZTeng
OU=ENGR.OU=BEI.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	BHong	Last Name	Hong
		Given Name	Baochen
	SXiao	Last Name	Xiao
		Given Name	Shen
	YLi	Last Name	Li
		Given Name	Youmei
	ZQiang	Last Name	Qiang
		Given Name	Zhu
		Title	Design Engineer
		Telephone	x743
Admin	Last Name	Student	
Template	Engineer	Telephone	86 10 62751244
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ENGRBEI
		Street	28 Dongzhimenwai Dajie
		City	Beijing
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	BHong
			SXiao
	WPUSERS	Members	YLi
			ZQiang
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Organizational Role	Manager	Occupant	SXiao	
			YLi	
OU=MKTG.OU=BEI.O=EMA				
User	FLao	Last Name	Lao	
		Given Name	Fengzhi	
	JZhang	Last Name	Zhang	
		Given Name	Juyin	
	LJiang	Last Name	Jiang	
		Given Name	Luding	
	ZHe	Last Name	He	
		Given Name	Zhicheng	
		Title	Manager	
		Telephone	x251	
	Admin	Last Name	Student	
	Template	Marketing	Telephone	86 10 62751245
			Home Directory Volume	FS1_DATA.CORP.NYC.EMA
			Path	USERS\MKTGBEI
Street			28 Dongzhimenwai Dajie	
City			Beijing	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	FLao	
			JZhang	
	WPUSERS	Members	LJiang	
			ZHe	
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA	
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA	
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	JZhang	
			LJiang	
OU=SALE.OU=BEI.O=EMA				
User	ELundskog	Last Name	Lundskog	
		Given Name	Elsa	
	JChen	Last Name	Chen	
		Given Name	Joan	
	JGrahm	Last Name	Grahm	
		Given Name	Jeff	
	WFruehan	Last Name	Fruehan	
		Given Name	Wayne	
		Title	Manager	
		Telephone	x7787	
	Admin		Last Name	Student
	Template	Sales	Telephone	86 10 62751243
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\SALEBEI	
Street			28 Dongzhimenwai Dajie	
City			Beijing	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	ELundskog	
			JChen	
	WPUSERS	Members	JGrahm	
			WFruehan	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=BER.O=EMA			
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=BER.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	GSchmidt	Last Name	Schmidt
		Given Name	George
	HKies	Last Name	Kies
		Given Name	Hilda
	MZiegler	Last Name	Ziegler
		Given Name	Manfred
	PBusche	Last Name	Busche
		Given Name	Petra
		Title	Director
		Telephone	x523
Admin	Last Name	Student	
Template	Accounting	Telephone	49 30 5556 3450
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ACCTBER
		Street	17 Burkhart Strasse
		City	Berlin
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	GSchmidt
			HKies
	WPUSERS	Members	MZiegler
			PBusche
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Role	Manager	Occupant	HKies
			MZiegler
OU=ENGR.OU=BER.O=EMA			
User	MFischer	Last Name	Fischer
		Given Name	Michael
	MWinkler	Last Name	Winkler
		Given Name	Marcus
	SWassermann	Last Name	Wassermann
		Given Name	Sylvia
	WFehlman	Last Name	Fehlman
		Given Name	Wilhelm
		Title	Design Engineer
		Telephone	x675
	Admin	Last Name	Student
	Template	Engineer	Telephone
Home Directory Volume			FS1_DATA.CORP.NYC.EMA
Path			USERS\ENGRBER
Street			17 Burkhart Strasse
City			Berlin
Login Time Restrictions			No login on Saturday or Sunday
Concurrent Connections			2
Group	DBUSERS	Members	MFischer
			MWinkler
	WPUSERS	Members	SWassermann
			WFehlman
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	MWinkler	
			SWasserman	
OU=MKTG.OU=BER.O=EMA				
User	ABothmann	Last Name	Bothmann	
		Given Name	Amanda	
	EHuber	Last Name	Huber	
		Given Name	Eva	
	JHofer	Last Name	Hofer	
		Given Name	Jurgen	
	MHein	Last Name	Hein	
		Given Name	Monika	
		Title	Manager	
		Telephone	x963	
	Admin		Last Name	Student
	Template	Marketing	Telephone	49 30 5556 7800
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\MKTGBER	
Street			17 Burkhart Strasse	
City			Berlin	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	ABothmann	
			EHuber	
	WPUSERS	Members	JHofer	
			MHein	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	EHuber
			JHofer
OU=SALE.OU=BER.O=EMA			
User	ELundskog	Last Name	Lundskog
		Given Name	Elsa
	JChen	Last Name	Chen
		Given Name	Joan
	JGrahm	Last Name	Grahm
		Given Name	Jeff
	WFruehan	Last Name	Fruehan
		Given Name	Wayne
		Title	Manager
		Telephone	x7787
Admin		Last Name	Student
Template	Sales	Telephone	49 30 5556 7900
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\SALEBER
		Street	17 Burkhart Strasse
		City	Berlin
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Group	DBUSERS	Members	ELundskog
			JChen
	WPUSERS	Members	JGrahm
			WFruehan
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=CAI.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=CAI.O=EMA			
User	ADarwish	Last Name	Darwish
		Given Name	Ahmed
	EBishay	Last Name	Bishay
		Given Name	Emil
	IOthman	Last Name	Othman
		Given Name	Ibrahim
	OOsman	Last Name	Osman
		Given Name	Omar
		Title	Director
		Telephone	x458
Admin	Last Name	Student	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Template	Accounting	Telephone	20 2 4188970
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ACCTCAI
		Street	14 Osoris St.
		City	Cairo
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	ADarwish
			EBishay
	WPUSERS	Members	IOthman
			OOsman
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	EBishay
			IOthman
OU=ENGR.OU=CAI.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	AAhram	Last Name	Ahram
		Given Name	Aly
	GBadawy	Last Name	Badawy
		Given Name	Gamal
	LKarnouk	Last Name	Karnouk
		Given Name	Liliane
	NElsalhy	Last Name	Elsalhy
		Given Name	Nabil
		Title	Design Engineer
		Telephone	x743
Admin	Last Name	Student	
Template	Engineer	Telephone	20 2 4188980
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ENGRCAI
		Street	14 Osoris St.
		City	Cairo
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	AAhram
			GBadawy
	WPUSERS	Members	LKarnouk
			NElsalhy
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Role	Manager	Occupant	GBadawy
			LKarnouk
OU=MKTG.OU=CAI.O=EMA			
User	AHaggag	Last Name	Haggag
		Given Name	Amr
	AOsman	Last Name	Osman
		Given Name	Ahmed
	HElsharkawy	Last Name	Elsharkawy
		Given Name	Hassan
	SSaad	Last Name	Saad
		Given Name	Sherif
		Title	Manager
		Telephone	x251
	Admin	Last Name	Student
	Template	Marketing	Telephone
Home Directory Volume			FS1_DATA.CORP.NYC.EMA
Path			USERS\MKTGCAI
Street			14 Osoris St.
City			Cairo
Login Time Restrictions			No login on Saturday or Sunday
Concurrent Connections			2
Group	DBUSERS	Members	AHaggag
			AOsman
	WPUSERS	Members	HElsharkawy
			SSaad
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	AOsman	
			HEIsharkawy	
OU=SALE.OU=CAI.O=EMA				
User	ELundskog	Last Name	Lundskog	
		Given Name	Elsa	
	JChen	Last Name	Chen	
		Given Name	Joan	
	JGrahm	Last Name	Grahm	
		Given Name	Jeff	
	WFruehan	Last Name	Fruehan	
		Given Name	Wayne	
		Title	Manager	
		Telephone	x7787	
	Admin		Last Name	Student
	Template	Sales	Telephone	20 2 4188960
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\SALECAI	
Street			14 Osoris St.	
City			Cairo	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	ELundskog	
			JChen	
	WPUSERS	Members	JGrahm	
			WFruehan	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=MOS.O=EMA			
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=MOS.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
User	AKhokhlov	Last Name	Khokhlov	
		Given Name	Anatoly	
	AVedyaev	Last Name	Vedyaev	
		Given Name	Alexander	
	BWasilev	Last Name	Vasil'ev	
		Given Name	Boris	
	NStrokov	Last Name	Strokov	
		Given Name	Nikolai	
		Title	Director	
		Telephone	x458	
Admin	Last Name	Student		
Template	Accounting	Telephone	7 095 263 67 30	
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA	
		Path	USERS\ACCTMOS	
		Street	10 Krasnopresnenskaya Nab.	
		City	Moscow	
		Login Time Restrictions	No login on Saturday or Sunday	
		Concurrent Connections	2	
Group	DBUSERS	Members	AKhokhlov AVedyaev	
		Members	BWasilev NStrokov	
	Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
		FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
FS1_MAIL		Aliased Object	FS1_MAIL.CORP.NYC.EMA	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Role	Manager	Occupant	AVedyaev
			BVasilev
OU=ENGR.OU=MOS.O=EMA			
User	ADneprovskiy	Last Name	Dneprovskiy
		Given Name	Alexi
	IMaslov	Last Name	Maslov
		Given Name	Irina
	PTverdislov	Last Name	Tverdislov
		Given Name	Pavel
	Vilyushin	Last Name	Ilyushin
		Given Name	Vladimir
		Title	Design Engineer
		Telephone	x743
	Admin	Last Name	Student
	Template	Engineer	Telephone
Home Directory Volume			FS1_DATA.CORP.NYC.EMA
Path			USERS\ENGRMOS
Street			10 Krasnopresnenskaya Nab.
City			Moscow
Login Time Restrictions			No login on Saturday or Sunday
Concurrent Connections			2
Group	DBUSERS	Members	ADneprovskiy
			IMaslov
	WPUSERS	Members	PTverdislov
			Vilyushin
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	IMaslov	
			PTverdislov	
OU=MKTG.OU=MOS.O=EMA				
User	GAdo	Last Name	Ado	
		Given Name	Georgy	
	OKeldysh	Last Name	Keldysh	
		Given Name	Oleg	
	VKunitsin	Last Name	Kunitsin	
		Given Name	Valerii	
	YMikhailin	Last Name	Mikhailin	
		Given Name	Yuri	
		Title	Manager	
		Telephone	x251	
	Admin		Last Name	Student
	Template	Marketing	Telephone	7 095 263 67 50
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\MKTGMOS	
Street			10 Krasnopresnenskaya Nab.	
City			Moscow	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	GAdo	
			OKeldysh	
	WPUSERS	Members	VKunitsin	
			YMikhailin	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	OKeldysh
			VKunitsin
OU=SALE.OU=MOS.O=EMA			
User	ELundskog	Last Name	Lundskog
		Given Name	Elsa
	JChen	Last Name	Chen
		Given Name	Joan
	JGrahm	Last Name	Grahm
		Given Name	Jeff
	WFruehan	Last Name	Fruehan
		Given Name	Wayne
		Title	Manager
		Telephone	x7787
Admin		Last Name	Student
Template	Sales	Telephone	7 095 263 67 60
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\SALEMOS
		Street	10 Krasnopresnenskaya Nab.
		City	Moscow
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Group	DBUSERS	Members	ELundskog
			JChen
	WPUSERS	Members	JGrahm
			WFruehan
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=RIO.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=RIO.O=EMA			
User	CChaves	Last Name	Chaves
		Given Name	Celeste
	DCuritiba	Last Name	Curitiba
		Given Name	Dileide
	HSantos	Last Name	dos Santos
		Given Name	Helveci
	MPaula	Last Name	de Paula
		Given Name	Marcia
		Title	Director
		Telephone	x623
Admin	Last Name	Student	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Template	Accounting	Telephone	55 21 6673590
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ACCTRIO
		Street	Av Paulista 293
		City	Rio do Janeiro
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	CChaves
			DCuritiba
	WPUSERS	Members	HSantos
			MPaula
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	DCuritiba
			HSantos
OU=ENGR.OU=RIO.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	ANeves	Last Name	Neves
		Given Name	Almir
	JFerreira	Last Name	Ferreira
		Given Name	Joao
	MMenezes	Last Name	Menezes
		Given Name	Maria
	PFernandes	Last Name	Fernandes
		Given Name	Paulo
		Title	Design Engineer
		Telephone	x875
Admin	Last Name	Student	
Template	Engineer	Telephone	55 21 6673480
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ENGRRIO
		Street	Av Paulista 293
		City	Rio do Janeiro
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	ANeves
			JFerreira
	WPUSERS	Members	MMenezes
			PFernandes
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Role	Manager	Occupant	JFerreira
			MMenezes
OU=MKTG.OU=RIO.O=EMA			
User	AOliveira	Last Name	de Oliveira
		Given Name	Antonio
	CHasse	Last Name	Hasse
		Given Name	Claudia
	EMontenegro	Last Name	Montenegro
		Given Name	Eurico
	VLaube	Last Name	Laube
		Given Name	Valerio
		Title	Manager
		Telephone	x563
	Admin	Last Name	Student
	Template	Marketing	Telephone
Home Directory Volume			FS1_DATA.CORP.NYC.EMA
Path			USERS\MKTGRIO
Street			Av Paulista 293
City			Rio do Janeiro
Login Time Restrictions			No login on Saturday or Sunday
Concurrent Connections			2
Group	DBUSERS	Members	AOliveira
			CHasse
	WPUSERS	Members	EMontenegro
			VLaube
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	CHasse	
			EMontenegro	
OU=SALE.OU=RIO.O=EMA				
User	ELundskog	Last Name	Lundskog	
		Given Name	Elsa	
	JChen	Last Name	Chen	
		Given Name	Joan	
	JGrahm	Last Name	Grahm	
		Given Name	Jeff	
	WFruehan	Last Name	Fruehan	
		Given Name	Wayne	
		Title	Manager	
		Telephone	x7787	
	Admin		Last Name	Student
	Template	Sales	Telephone	55 21 6673580
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\SALERIO	
Street			Av Paulista 293	
City			Rio do Janeiro	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	ELundskog	
			JChen	
	WPUSERS	Members	JGrahm	
			WFruehan	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm
OU=TOK.O=EMA			
Organizational Unit	ACCT	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	ENGR	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	MKTG	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
	SALE	Incorrect login attempts	3
		Intruder attempt reset interval	15 minutes
		Intruder lockout reset interval	30 minutes
OU=ACCT.OU=TOK.O=EMA			

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
User	KFuruya	Last Name	Furuya
		Given Name	Kazuko
	KOsako	Last Name	Osako
		Given Name	Keiko
	SNakamura	Last Name	Nakamura
		Given Name	Shinji
	YOkamoto	Last Name	Okamoto
		Given Name	Yoshi
		Title	Director
		Telephone	x458
Admin	Last Name	Student	
Template	Accounting	Telephone	81 3 3405-9880
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\ACCTTOK
		Street	Shibuya-ku
		City	Tokyo
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2
Group	DBUSERS	Members	KFuruya
			KOsako
	WPUSERS	Members	SNakamura
			YOkamoto
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Organizational Role	Manager	Occupant	KOsako
			SNakamura
OU=ENGR.OU=TOK.O=EMA			
User	HMatsubara	Last Name	Matsubara
		Given Name	Hiroki
	JNishioka	Last Name	Nishioka
		Given Name	Jun
	STanaka	Last Name	Tanaka
		Given Name	Sumiko
	TTakahata	Last Name	Takahata
		Given Name	Taichi
		Title	Design Engineer
		Telephone	x743
	Admin	Last Name	Student
	Template	Engineer	Telephone
Home Directory Volume			FS1_DATA.CORP.NYC.EMA
Path			USERS\ENGR TOK
Street			Shibuya-ku
City			Tokyo
Login Time Restrictions			No login on Saturday or Sunday
Concurrent Connections			2
Group	DBUSERS	Members	HMatsubara
			JNishioka
	WPUSERS	Members	STanaka
			TTakahata
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value	
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\DB	
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA	
		Path	DOCUMENT\WP	
Organizational Role	Manager	Occupant	JNishioka	
			STanaka	
OU=MKTG.OU=TOK.O=EMA				
User	HMatsumoto	Last Name	Matsumoto	
		Given Name	Hirokazu	
	HSuzuki	Last Name	Suzuki	
		Given Name	Hiroko	
	KInoue	Last Name	Inoue	
		Given Name	Kiichiro	
	SSaito	Last Name	Saito	
		Given Name	Sanae	
		Title	Manager	
		Telephone	x251	
	Admin		Last Name	Student
	Template	Marketing	Telephone	81 3 3405-9820
Home Directory Volume			FS1_DATA.CORP.NYC.EMA	
Path			USERS\MKTGTOK	
Street			Shibuya-ku	
City			Tokyo	
Login Time Restrictions			No login on Saturday or Sunday	
Concurrent Connections			2	
Group	DBUSERS	Members	HMatsumoto	
			HSuzuki	
	WPUSERS	Members	KInoue	
			SSaito	

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	HSuzuki
			KInoue
OU=SALE.OU=TOK.O=EMA			
User	ELundskog	Last Name	Lundskog
		Given Name	Elsa
	JChen	Last Name	Chen
		Given Name	Joan
	JGrahm	Last Name	Grahm
		Given Name	Jeff
	WFruehan	Last Name	Fruehan
		Given Name	Wayne
		Title	Manager
		Telephone	x7787
Admin		Last Name	Student
Template	Sales	Telephone	81 3 3405-9830
		Home Directory Volume	FS1_DATA.CORP.NYC.EMA
		Path	USERS\SALETOK
		Street	Shibuya-ku
		City	Tokyo
		Login Time Restrictions	No login on Saturday or Sunday
		Concurrent Connections	2

Table Prep-2: NDS Setup (continued)

Object Type	Object Name	Property	Value
Group	DBUSERS	Members	ELundskog
			JChen
	WPUSERS	Members	JGrahm
			WFruehan
Alias	FS1_SYS	Aliased Object	FS1_SYS.CORP.NYC.EMA
	FS1_DATA	Aliased Object	FS1_DATA.CORP.NYC.EMA
	FS1_MAIL	Aliased Object	FS1_MAIL.CORP.NYC.EMA
Directory Map	DBDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\DB
	WPDOC	Volume	FS1_DATA.CORP.NYC.EMA
		Path	DOCUMENT\WP
Organizational Role	Manager	Occupant	JChen
			JGrahm

Table Prep-2: NDS Setup (continued)

NDS Security

The following table lists the NDS security rights. Each SALE container has an IRF blocking the B right.

Object	Trustee	Rights Granted
[Root]	[Public]	Browse object (default)
	Container_Admins.CORP.NYC.EMA	[S] object [RC] All properties
	ADMIN.CORP.NYC.EMA	[SI] object (default)
	GWAGENT.CORP.NYC.EMA	[S] object
EMA	Container_Admin.CORP.NYC.EMA	[BI] object
CORP.NYC.EMA	CONTAINER_ADMINS.CORP.NYC.EMA	[BI] object [RCI] All Properties
	ADMIN.CORP.NYC.EMA	[SI] object [SI] All Properties
	MANAGER.CORP.NYC.EMA	[SI] object [SI] All Properties
FS1.CORP.NYC.EMA	ADMIN.CORP.NYC.EMA	[S] object [S] All Properties

Table Prep-3: NDS Security Setup

Object	Trustee	Rights Granted
ACCT.BEI.EMA	ADMIN.ACCT.BEI.EMA	[S] object [S] All Properties
	MANAGER.ACCT.BEI.EMA	[S] object [S] All Properties
ENGR.BEI.EMA	ADMIN.ENGR.BEI.EMA	[S] object [S] All Properties
	MANAGER.ENGR.BEI.EMA	[S] object [S] All Properties
MKTG.BEI.EMA	ADMIN.MKTG.BEI.EMA	[S] object [S] All Properties
	MANAGER.MKTG.BEI.EMA	[S] object [S] All Properties
SALE.BEI.EMA	ADMIN.SALE.BEI.EMA	[S] object [S] All Properties
	MANAGER.SALE.BEI.EMA	[S] object [S] All Properties
ACCT.BER.EMA	ADMIN.ACCT.BER.EMA	[S] object [S] All Properties
	MANAGER.ACCT.BER.EMA	[S] object [S] All Properties
ENGR.BER.EMA	ADMIN.ENGR.BER.EMA	[S] object [S] All Properties
	MANAGER.ENGR.BER.EMA	[S] object [S] All Properties
MKTG.BER.EMA	ADMIN.MKTG.BER.EMA	[S] object [S] All Properties
	MANAGER.MKTG.BER.EMA	[S] object [S] All Properties
SALE.BER.EMA	ADMIN.SALE.BER.EMA	[S] object [S] All Properties
	MANAGER.SALE.BER.EMA	[S] object [S] All Properties
ACCT.CAI.EMA	ADMIN.ACCT.CAI.EMA	[S] object [S] All Properties
	MANAGER.ACCT.CAI.EMA	[S] object [S] All Properties

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
ENGR.CAI.EMA	ADMIN.ENGR.CAI.EMA	[S] object [S] All Properties
	MANAGER.ENGR.CAI.EMA	[S] object [S] All Properties
MKTG.CAI.EMA	ADMIN.MKTG.CAI.EMA	[S] object [S] All Properties
	MANAGER.MKTG.CAI.EMA	[S] object [S] All Properties
SALE.CAI.EMA	ADMIN.SALE.CAI.EMA	[S] object [S] All Properties
	MANAGER.SALE.CAI.EMA	[S] object [S] All Properties
ACCT.MOS.EMA	ADMIN.ACCT.MOS.EMA	[S] object [S] All Properties
	MANAGER.ACCT.MOS.EMA	[S] object [S] All Properties
ENGR.MOS.EMA	ADMIN.ENGR.MOS.EMA	[S] object [S] All Properties
	MANAGER.ENGR.MOS.EMA	[S] object [S] All Properties
MKTG.MOS.EMA	ADMIN.MKTG.MOS.EMA	[S] object [S] All Properties
	MANAGER.MKTG.MOS.EMA	[S] object [S] All Properties
SALE.MOS.EMA	ADMIN.SALE.MOS.EMA	[S] object [S] All Properties
	MANAGER.SALE.MOS.EMA	[S] object [S] All Properties
ACCT.NYC.EMA	ADMIN.ACCT.NYC.EMA	[S] object [S] All Properties
	MANAGER.ACCT.NYC.EMA	[S] object [S] All Properties
ENGR.NYC.EMA	ADMIN.ENGR.NYC.EMA	[S] object [S] All Properties
	MANAGER.ENGR.NYC.EMA	[S] object [S] All Properties

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
MKTG.NYC.EMA	ADMIN.MKTG.NYC.EMA	[S] object [S] All Properties
	MANAGER.MKTG.NYC.EMA	[S] object [S] All Properties
SALE.NYC.EMA	ADMIN.SALE.NYC.EMA	[S] object [S] All Properties
	MANAGER.SALE.NYC.EMA	[S] object [S] All Properties
ACCT.RIO.EMA	ADMIN.ACCT.RIO.EMA	[S] object [S] All Properties
	MANAGER.ACCT.RIO.EMA	[S] object [S] All Properties
ENGR.RIO.EMA	ADMIN.ENGR.RIO.EMA	[S] object [S] All Properties
	MANAGER.ENGR.RIO.EMA	[S] object [S] All Properties
MKTG.RIO.EMA	ADMIN.MKTG.RIO.EMA	[S] object [S] All Properties
	MANAGER.MKTG.RIO.EMA	[S] object [S] All Properties
SALE.RIO.EMA	ADMIN.SALE.RIO.EMA	[S] object [S] All Properties
	MANAGER.SALE.RIO.EMA	[S] object [S] All Properties
ACCT.TOK.EMA	ADMIN.ACCT.TOK.EMA	[S] object [S] All Properties
	MANAGER.ACCT.TOK.EMA	[S] object [S] All Properties
ENGR.TOK.EMA	ADMIN.ENGR.TOK.EMA	[S] object [S] All Properties
	MANAGER.ENGR.TOK.EMA	[S] object [S] All Properties
MKTG.TOK.EMA	ADMIN.MKTG.TOK.EMA	[S] object [S] All Properties
	MANAGER.MKTG.TOK.EMA	[S] object [S] All Properties

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
SALE.TOK.EMA	ADMIN.SALE.TOK.EMA	[S] object [S] All Properties
	MANAGER.SALE.TOK.EMA	[S] object [S] All Properties
DBDOC.ACCT.BEI.EMA	DBUSERS.ACCT.BEI.EMA	[B] object [RC] Path Property
DBDOC.ENGR.BEI.EMA	DBUSERS.ENGR.BEI.EMA	[B] object [RC] Path Property
DBDOC.MKTG.BEI.EMA	DBUSERS.MKTG.BEI.EMA	[B] object [RC] Path Property
DBDOC.SALE.BEI.EMA	DBUSERS.SALE.BEI.EMA	[B] object [RC] Path Property
DBDOC.ACCT.BER.EMA	DBUSERS.ACCT.BER.EMA	[B] object [RC] Path Property
DBDOC.ENGR.BER.EMA	DBUSERS.ENGR.BER.EMA	[B] object [RC] Path Property
DBDOC.MKTG.BER.EMA	DBUSERS.MKTG.BER.EMA	[B] object [RC] Path Property
DBDOC.SALE.BER.EMA	DBUSERS.SALE.BER.EMA	[B] object [RC] Path Property
DBDOC.ACCT.CAI.EMA	DBUSERS.ACCT.CAI.EMA	[B] object [RC] Path Property
DBDOC.ENGR.CAI.EMA	DBUSERS.ENGR.CAI.EMA	[B] object [RC] Path Property
DBDOC.MKTG.CAI.EMA	DBUSERS.MKTG.CAI.EMA	[B] object [RC] Path Property
DBDOC.SALE.CAI.EMA	DBUSERS.SALE.CAI.EMA	[B] object [RC] Path Property
DBDOC.ACCT.MOS.EMA	DBUSERS.ACCT.MOS.EMA	[B] object [RC] Path Property
DBDOC.ENGR.MOS.EMA	DBUSERS.ENGR.MOS.EMA	[B] object [RC] Path Property
DBDOC.MKTG.MOS.EMA	DBUSERS.MKTG.MOS.EMA	[B] object [RC] Path Property
DBDOC.SALE.MOS.EMA	DBUSERS.SALE.MOS.EMA	[B] object [RC] Path Property
DBDOC.ACCT.NYC.EMA	DBUSERS.ACCT.NYC.EMA	[B] object [RC] Path Property

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
DBDOC.ENGR.NYC.EMA	DBUSERS.ENGR.NYC.EMA	[B] object [RC] Path Property
DBDOC.MKTG.NYC.EMA	DBUSERS.MKTG.NYC.EMA	[B] object [RC] Path Property
DBDOC.SALE.NYC.EMA	DBUSERS.SALE.NYC.EMA	[B] object [RC] Path Property
DBDOC.ACCT.RIO.EMA	DBUSERS.ACCT.RIO.EMA	[B] object [RC] Path Property
DBDOC.ENGR.RIO.EMA	DBUSERS.ENGR.RIO.EMA	[B] object [RC] Path Property
DBDOC.MKTG.RIO.EMA	DBUSERS.MKTG.RIO.EMA	[B] object [RC] Path Property
DBDOC.SALE.RIO.EMA	DBUSERS.SALE.RIO.EMA	[B] object [RC] Path Property
DBDOC.ACCT.TOK.EMA	DBUSERS.ACCT.TOK.EMA	[B] object [RC] Path Property
DBDOC.ENGR.TOK.EMA	DBUSERS.ENGR.TOK.EMA	[B] object [RC] Path Property
DBDOC.MKTG.TOK.EMA	DBUSERS.MKTG.TOK.EMA	[B] object [RC] Path Property
DBDOC.SALE.TOK.EMA	DBUSERS.SALE.TOK.EMA	[B] object [RC] Path Property
WPDOC.ACCT.BEI.EMA	WPUSERS.ACCT.BEI.EMA	[B] object [RC] Path Property
WPDOC.ENGR.BEI.EMA	WPUSERS.ENGR.BEI.EMA	[B] object [RC] Path Property
WPDOC.MKTG.BEI.EMA	WPUSERS.MKTG.BEI.EMA	[B] object [RC] Path Property
WPDOC.SALE.BEI.EMA	WPUSERS.SALE.BEI.EMA	[B] object [RC] Path Property
WPDOC.ACCT.BER.EMA	WPUSERS.ACCT.BER.EMA	[B] object [RC] Path Property
WPDOC.ENGR.BER.EMA	WPUSERS.ENGR.BER.EMA	[B] object [RC] Path Property
WPDOC.MKTG.BER.EMA	WPUSERS.MKTG.BER.EMA	[B] object [RC] Path Property
WPDOC.SALE.BER.EMA	WPUSERS.SALE.BER.EMA	[B] object [RC] Path Property

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
WPDOC.ACCT.CAI.EMA	WPUSERS.ACCT.CAI.EMA	[B] object [RC] Path Property
WPDOC.ENGR.CAI.EMA	WPUSERS.ENGR.CAI.EMA	[B] object [RC] Path Property
WPDOC.MKTG.CAI.EMA	WPUSERS.MKTG.CAI.EMA	[B] object [RC] Path Property
WPDOC.SALE.CAI.EMA	WPUSERS.SALE.CAI.EMA	[B] object [RC] Path Property
WPDOC.ACCT.MOS.EMA	WPUSERS.ACCT.MOS.EMA	[B] object [RC] Path Property
WPDOC.ENGR.MOS.EMA	WPUSERS.ENGR.MOS.EMA	[B] object [RC] Path Property
WPDOC.MKTG.MOS.EMA	WPUSERS.MKTG.MOS.EMA	[B] object [RC] Path Property
WPDOC.SALE.MOS.EMA	WPUSERS.SALE.MOS.EMA	[B] object [RC] Path Property
WPDOC.ACCT.NYC.EMA	WPUSERS.ACCT.NYC.EMA	[B] object [RC] Path Property
WPDOC.ENGR.NYC.EMA	WPUSERS.ENGR.NYC.EMA	[B] object [RC] Path Property
WPDOC.MKTG.NYC.EMA	WPUSERS.MKTG.NYC.EMA	[B] object [RC] Path Property
WPDOC.SALE.NYC.EMA	WPUSERS.SALE.NYC.EMA	[B] object [RC] Path Property
WPDOC.ACCT.RIO.EMA	WPUSERS.ACCT.RIO.EMA	[B] object [RC] Path Property
WPDOC.ENGR.RIO.EMA	WPUSERS.ENGR.RIO.EMA	[B] object [RC] Path Property
WPDOC.MKTG.RIO.EMA	WPUSERS.MKTG.RIO.EMA	[B] object [RC] Path Property
WPDOC.SALE.RIO.EMA	WPUSERS.SALE.RIO.EMA	[B] object [RC] Path Property
WPDOC.ACCT.TOK.EMA	WPUSERS.ACCT.TOK.EMA	[B] object [RC] Path Property
WPDOC.ENGR.TOK.EMA	WPUSERS.ENGR.TOK.EMA	[B] object [RC] Path Property
WPDOC.MKTG.TOK.EMA	WPUSERS.MKTG.TOK.EMA	[B] object [RC] Path Property

Table Prep-3: NDS Security Setup (continued)

Object	Trustee	Rights Granted
WPDOC.SALE.TOK.EMA	WPUSERS.SALE.TOK.EMA	[B] object [RC] Path Property
EMAILDOC.CORP.NYC.EMA	EMAILUSERS.CORP.NYC.EMA	[B] object [RC] Path Property

Table Prep-3: NDS Security Setup (continued)

File System Security

The IRF for MAIL:DOCUMENT\EMAIL\TEMPLATE blocks all rights except Supervisor, Read, and File Scan.

Directory	Trustee	Rights Granted
SYS:PUBLIC	CORP.NYC.EMA	[RF] (default)
	<i>dept.location.EMA</i>	[RF]
DATA:SETUP	CONTAINER_ADMIN.S.CORP.NYC.EMA	[RWF]
DATA:USERS\ <i>location</i> \ <i>username</i>	<i>username.dept.location.EMA</i>	[SRWCEMFA] (default)
DATA:SHARED	MANAGER. <i>dept.location.EMA</i>	[SRWCEMFA]
DATA:SHARED\ACCTG	ACCT. <i>location.EMA</i>	[RWCEF]
DATA:SHARED\ENGR	ENGR. <i>location.EMA</i>	[RWCEF]
DATA:SHARED\MKTG	MKTG. <i>location.EMA</i>	[RWCEF]
DATA:SHARED\SALES	SALE. <i>location.EMA</i>	[RWCEF]
DATA:SHARED\TRANSFER	<i>location.EMA</i>	[RWCEF]
DATA:APPS\DB	DBUSERS. <i>dept.location.EMA</i>	[RF]
DATA:APPS\WP	WPUSERS. <i>dept.location.EMA</i>	[RWF]
DATA:DOCUMENT\DB	DBUSERS. <i>dept.location.EMA</i>	[RWF]
DATA:DOCUMENT\WP	WPUSERS. <i>dept.location.EMA</i>	[RWF]
MAIL:APPS\EMAIL	EMAILUSERS.CORP.NYC.EMA	[RWF]
	CONTAINER_ADMIN.S.CORP.NYC.EMA	[RWF]
MAIL:DOCUMENT\EMAIL	EMAILUSERS.CORP.NYC.EMA	[RWF]
	CONTAINER_ADMIN.S.CORP.NYC.EMA	[RWF]
DATA:	CONTAINER_ADMIN.S.CORP.NYC.EMA	[S]
MAIL:	[PUBLIC]	[S]

Table Prep-4: File System Security Setup

Login Scripts

The following is the login script for all departmental containers:

```
MAP DISPLAY OFF
NO_DEFAULT

;MAP A SEARCH DRIVE TO PUBLIC
MAP ROOT INS S1:=%<PREFERRED_SERVER>\SYS:PUBLIC

;MAP NETWORK DRIVES
MAP F:=%<PREFERRED_SERVER>\SYS:
MAP ROOT H:=%HOME_DIRECTORY
MAP G:=%<PREFERRED_SERVER>\DATA:
MAP I:=%<PREFERRED_SERVER>\MAIL:

;CONDITIONAL MAPPING
IF MEMBER OF "DBUSERS" THEN MAP S16:=DBDOC
IF MEMBER OF "WPUSERS" THEN MAP S16:=WPDOC

;SHOW CURRENT DRIVES
MAP DISPLAY ON
MAP
```

All ADMIN user objects should have the following login script:

```
#NAL
```

Partitions and Replicas

After restoring NDS, you need to create partitions for and place replicas of your tree. Each departmental container which contains a server should be made a partition.

The corresponding server should hold the master replica of that partition. FS1 should hold the master replica of the [Root] partition.

Place read/write replicas of all partitions on each server.

Setting Up the Student Servers

In Section 1, students upgrade from a NetWare 4.11 server to NetWare 5. Use FDISK to create a 30 MB DOS partition on each server.

Install NetWare 4.11 on the student servers (750 MB SYS volume).

Add the servers to the existing NetWare 5 NDS tree. Place each server into its own department container.

During installation, create the DATA volume (at least 250 MB) and the MAIL volume (at least 250 MB).

After installation, add the long name space to the SYS, DATA, and MAIL volumes.

Make the container where the DATA and MAIL volumes are located a trustee of the root directory for each volume and assign the RF rights.

Classroom 3.12 Server

In Section 1, students upgrade information from a NetWare 3.12 server located in the classroom to NetWare 5.



Do not use your classroom server for this process.

Install NetWare 3.12 and configure the server by doing the following:

1. Call the server **FS312**.
2. Copy the NET\$*.OLD file from the instructor CD SETUP directory to the SYS:SYSTEM directory.
3. To create users and groups, run BINDREST.



This changes SUPERVISOR's password to NOVELL.

Install Netscape Navigator

Install Netscape Navigator to DATA:\APPS\NETSCAPE for use with the application object by running
DATA:\NOVDOCS\INSTALL\NETSCAPE\SETUP.EXE.

You might want to perform a custom installation and only install Communicator 4.04.

Configure the Workstations

Complete the following tasks on each student workstation:

1. Install Windows[®].
2. If you are using Windows 95, install the latest Windows 95 Support Pack (downloadable from www.microsoft.com).
3. Install the Novell Client using the Custom installation option, and choose the following:
 - Novell Distributed Print Services
 - Novell TSA for Windows 95/98
 - Novell Remote Access Dialer
4. Install the appropriate 32-bit LAN driver for each workstation's network board.
5. Configure each workstation to connect to a selected server by setting the following parameters:
 - Preferred Server = **FSx**
 - Preferred Tree = **EMA_TREE**
 - Name Context = **OU=department.OU=region.O=EMA**
 - Show Advanced Button on Login = **On**
 - Show Variables Button on Login = **On**
 - Show Clear Connections on Login = **On**
6. Restart the workstations.

Supplemental Setup Information—Future Setup

After you have installed all the servers, you can use an imaging application to reduce the time needed to set up for future classes.

Using Presentation Graphics

Each section has corresponding presentation graphics on the course CD in Adobe® Acrobat® PDF format. Use the graphics by

- Displaying them from the instructor's workstation
- Printing them on laser-quality transparency sheets for use with an overhead projector

Displaying the Graphics

To display the graphics from the instructor workstation, use Adobe Acrobat Reader and an external display device, such as DATASHOW®.

Using Acrobat Reader

1. Install Acrobat Reader on the workstation.
For Windows 95, use the installation file ACRORD.EXE, found in the ACROBAT directory on the course CD.
You can also download the Installation files from the Adobe home page at <http://www.adobe.com>.
2. Read the README.TXT file for instructions on using your version.
3. Make sure your monitor's resolution is set to 800 x 600 pixels. Otherwise, some colors and text will not display clearly.
4. To display the graphics, choose one of the following:
 - From Windows, display a PDF file by double-clicking the filename. This launches Acrobat Reader, and the graphic appears in full-screen view.
 - If Acrobat Reader is open, from the main menu click **File | Open** and browse for and select the file. The graphic appears in full-page view.
5. To switch between views, choose one of the following:
 - To switch from full-page to full-screen view, from the main menu click **View | Full Screen**.
 - To switch from full-screen to full-page view, press **Esc**.
6. To scroll forward between graphics use Enter or the Up- or Right-arrow keys; to scroll backward use the Down- or Left-arrow keys.

Printing the Graphics

To print a graphic file you must have the following:

- A PostScript® printer with at least 2 MB RAM
- A PostScript driver

Windows 95 comes with a PostScript driver. PostScript drivers can be downloaded from <http://www.adobe.com>.

Printing from Acrobat Reader

1. Open the PDF file for the course.
2. From the menu bar, click **File | Print**.
You can print graphics by page number or you can print all graphics in the file.
3. In the Print dialog, click **Setup** and make sure the orientation is set to Landscape.
4. To ensure that the graphics print completely on an 8 1/2" by 11" output, from the Print dialog select **Shrink to Fit**.
5. For each file you want to print, repeat Steps 1 through 4.

Printing from Windows

1. Highlight a file to print from.
2. From the menu bar, click **File | Print**.
This launches Acrobat Reader and your selected file, with the Print dialog open.
3. Use the instructions "Printing from Acrobat Reader" (above) and follow Steps 1 through 4.

Using Classroom Animations

The animations supplied with this course require a 486/50 PC that can display a minimum of 256 colors. To use the animations, do the following:

1. Launch the animation.
The Novell logo appears.
2. Choose from the following:
 - To move to the title screen, click the mouse.
 - To advance to the animation menu from the title screen, click the mouse.
 - To view an animation, click a menu item.

After the animation loads, it pauses to allow you to explain what occurs during the animation.

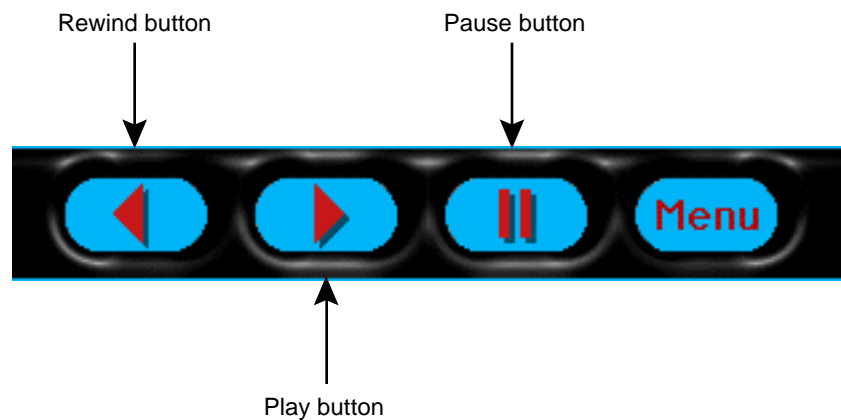


Figure Prep-1: Animation Control Bar

- Control the animation by using the standard control bar, shown in Figure Prep-1:
 - To begin an animation, click **Play**.
 - To rewind an animation, click **Rewind**.
 - To pause an animation, click **Pause**.
 - To return to the main menu, click **Menu**.
3. To exit the animation, click **Exit**.

Introduction

Duration 00:30

Introduction

This course provides you with the knowledge and skills needed to configure and administer a complex network. The course is designed to provide you with an advanced skill set and abilities to handle more challenging network situations than were presented in the NetWare 5™ Administration course.

Audience

The NetWare® 5 Advanced Administration course is intended for network administrators who have completed the NetWare 5 Administration course and Networking Technologies course.

A typical student has acquired the necessary knowledge and skills from the NetWare 5 Administration course and the Networking Technologies course or has had practical job experience administering a NetWare 4™ network.

After you have completed the NetWare 5 Administration course, we recommend that you return to your job to use what you learned before taking this course.

The course is also intended for NetWare 3™ network administrators who are preparing to upgrade to NetWare 5.

This course is intended for the CNE® and Master CNE™ candidate satisfying the NetWare 5 certification requirements.

Presentation**Notes****Introduction**

- Introduce yourself and the students.

- Familiarize students with their surroundings and their materials.

- Introduce the course.

- Determine if students have hearing, vision, or other problems.
- Explain how you like to handle questions and comments (during sections or after).

- Explain the location of bathrooms, drinking fountains, etc.
- Remind students to turn off their cell phones, pagers, etc.
- Point out the Reader Comments form at the back of the student manual.

Audience

- Describe who the course is for.

Find out what students expect from the course.

Prerequisites

You should have completed Course 560, NetWare 5 Administration, and Course 565, Networking Technologies, or have equivalent experience. You should also have a working knowledge of Windows 95™ or Windows NT® Workstation 4.0.

You should be able to perform the following tasks on a NetWare 5 network:

- Plan, implement, and manage basic network services—user login, file storage, network printing, and Novell Directory Services™ (NDS™)—on a small network.
- Set up login security, file system security, and NDS security.
- Automate the user's environment and access to network resources with login scripts, Novell Application Launcher™, and Workstation Manager.
- Install the Novell Client.
- Create and manage the following objects: group, organizational role, user, printing, alias, directory map, application, workstation, template, organization, and organizational unit.

Certification Tests

This course helps you prepare for the following certification tests:

- CNE 050-640
- CNI 050-840

You should arrange to take the certification test for this course within six weeks of acquiring the course materials. Thereafter, the test might be replaced by one based on an updated version of the course.

Presentation**Notes****Prerequisites**

- Explain the course prerequisites.

Assess the knowledge of the students regarding the information to be covered.

Certification Tests

- Mention the tests related to this course.

Relationship to Other Courses in the Curriculum

This course is one of five courses in the NetWare 5 curriculum. These courses teach network administrator responsibilities. The following table provides brief descriptions of each course in the NetWare 5 curriculum.

Course	Responsibilities Description
560 NetWare 5 Administration	Manage, protect, organize file system. Set up and manage basic network services: create users, set up security, manage printing, and manage workstations. Install NetWare 5.
565 Networking Technologies, Volumes 1 and 2	Understand the basic operation of computer networks. Understand the Open Systems Interconnection (OSI) reference model and how it relates to NetWare. Understand networking protocols such as TCP/IP and IPX/SPX™.
570 NetWare 5 Advanced Administration	Upgrade to NetWare 5. Configure the server and the file system. Manage the NDS database, manage a diverse network, and tune the server. Set up and manage TCP/IP portions of the network such as Web servers, DHCP, and DNS.
575 NDS Design and Implementation	Work as a design project team on a case company. Create a design document for NDS for the case company. Implement the NDS design.
580 Service and Support	Install and maintain network hardware, including network boards, cables, and storage devices. Troubleshoot problems with the server, workstations, network, and printing.
529 NetWare 4.11 to NetWare 5 Update	Upgrade and migrate to NetWare 5. Manage the NetWare server using Java® utilities. Set up DHCP, DNS, and Web servers. Manage client workstations by managing the workstations remotely, configuring NDS for the Application Launcher, and configuring workstations with Workstation Manager. Manage Novell Distributed Print Services™.

Table Intro-1: NetWare 5 Course Descriptions

Presentation

Notes

**Relationship to Other Courses
in the Curriculum**

- Explain the relationship of the course to the curriculum.

Course Overview

Upon completing this course, you should be able to

1. Upgrade a NetWare 4.11 network to a NetWare 5 network and migrate a NetWare 3.12 bindery to the NetWare 5 server. (Section 1)
2. Execute console commands, load NetWare Loadable Modules™ (NLMs™), access the server from a remote console, execute Java-based utilities on a NetWare 5 server, and describe NetWare 5 server security strategies. (Section 2)
3. Configure the network for queue-based printing. (Section 3)
4. Plan and set up a network file system. (Section 4)
5. Optimize the NetWare server by monitoring server statistics and taking appropriate actions using various server utilities. (Section 5)
6. Back up and restore NDS and file system information on a NetWare server using SBACKUP. (Section 6)
7. Provide appropriate TCP/IP functionality for client workstations by configuring the NetWare server and client workstations for DNS and DHCP. (Section 7)
8. Install and configure a Netscape FastTrack™ Web server and an FTP server on a NetWare server. (Section 8)
9. Plan NDS security by considering the impact of default rights assignments, determining NDS administrative roles, and choosing a centralized or distributed security model. (Section 9)
10. Perform preventive maintenance on the NDS database and troubleshoot synchronization inconsistencies. (Section 10)
11. Configure a NetWare 5 network for access by remote and traveling users. (Section 11)
12. Explain the uses and benefits of other Novell technologies in enhancing network services. (Section 12)

Exercises

This course provides both written and hands-on exercises to give you experience performing the tasks you will learn.

When doing exercises, continue until you see **(End of Exercise)**.

Presentation**Notes****Course Overview**

- Briefly describe what is covered in the course.

- Provide a course agenda.

Indicate daily starting time, breaks, lunch time, etc.

Exercises

- Briefly discuss the types of exercises found in this course.

Students should continue exercises until they come to the **(End of Exercise)** line.

Notes

SECTION 1 Upgrading to NetWare 5

Duration 02:30

Preparation

Install the Novell® Upgrade Wizard on the instructor's workstation.

SECTION 1

Upgrading to NetWare 5

In this section you learn how to upgrade existing servers to NetWare 5.

Objectives

Upon completing this section, you should be able to

1. Choose an upgrade method and a protocol.
2. Use the Installation program to upgrade a NetWare 4.1x server to NetWare 5.
3. Use the Novell Upgrade Wizard to upgrade the bindery of a NetWare 3.1x server to NetWare 5.

Presentation

Notes

Upgrading to NetWare 5

- Introduce the section.

Objectives

- Present the section objectives.

Choosing an Upgrade Method and a Protocol

Upgrading or migrating an existing NetWare system to NetWare 5 provides many new features and reduces network administration costs.

You can upgrade an older network operating system to NetWare 5 in one of two ways:

- You can install NetWare 5 on the same machine over existing files. This type of upgrade is called an *in-place upgrade*.
- You can use the Novell Upgrade Wizard to move the file system and the bindery (or NDS) to another server. This method is called an *across-the-wire upgrade*.

The minimum hardware requirements for a NetWare 5 server include the following:

- An IBM[®] PC or PC-compatible with a Pentium[®] processor
- 64 MB of RAM
- 30 MB DOS partition
- 200 MB of free disk space for volume SYS
- A network board

How you upgrade your existing server to NetWare 5 depends on the operating system you are running, your available hardware, and the NetWare 5 features (such as suballocation, compression, and block size) that you want to implement.

Choosing an Upgrade Method and a Protocol

- Discuss the two ways to upgrade.
- List the system requirements for a NetWare 5 server.
- Introduce the main factors for determining how to upgrade an existing server.

Upgrading an Existing Server with the Installation Program

You can use the NetWare 5 Installation program to upgrade an existing server running any of the following NetWare versions:

- NetWare 3.1x
- NetWare 4.x
- intraNetWare[®]
- intraNetWare for Small Business

The installation program (INSTALL.BAT) runs in a Java[®]-based mode with a graphical user interface. After running the program, choose “Upgrade from 3.1x or 4.1x” in the first text screen.

Advantages

- If your existing server meets hardware requirements for a NetWare 5 server, you do not need additional hardware.
- You can use suballocation and disk compression on the volume.

Disadvantages

- A very slight chance of data loss exists. For example, if a power outage occurs during the upgrade and both your backups are defective, you might lose data.
- NetWare 2[™] servers and non-NetWare servers cannot be upgraded to NetWare 5 using this option. You must first upgrade to NetWare 3 or NetWare 4.

Presentation**Notes****Upgrading an Existing Server with the Installation Program**

- List the versions of NetWare that can be upgraded to NetWare 5.
- Mention that the NetWare 5 Installation program is used to upgrade a server.
- Discuss the advantages of upgrading an existing server.
- Discuss the disadvantages of upgrading an existing server.
- Mention that insufficient hardware is the most common reason preventing administrators from using this option.

Migrating a Server with the Novell Upgrade Wizard

You can use the Novell Upgrade Wizard to migrate a NetWare 3.1x server to a NetWare 5 server. The Novell Upgrade Wizard allows you to move your NetWare 3.x bindery, passwords, security rights, and file system “across the wire” to a location in an existing NetWare 5 NDS tree.

Advantages

- Graphical modeling capabilities allow you to organize the new server structure offline before the upgrade. You accomplish this by dragging network objects, files, and volumes from the NetWare 3 server to any location in the new NDS tree.
- If a power outage occurs or a connection is lost during a migration, the source server remains intact and still contains the bindery and all stored data.
- You can migrate all or part of the file system (complete volumes only).
- You can migrate multiple servers to a single destination server. Organizations with older server hardware can consolidate network data as they upgrade to newer, more powerful server hardware.
- The Novell Upgrade Wizard checks for potential conflicts and errors (such as object name conflicts, NDS security, and disk space limitations) between the NetWare 3 server and the NDS tree and then gives you several options for resolution.

Presentation**Notes****Migrating a Server with the Novell Upgrade Wizard**

- Mention the information that the Novell Upgrade Wizard allows administrators to migrate.

- Discuss the advantages of the Novell Upgrade Wizard.

Choosing a Protocol

When you upgrade or migrate to NetWare 5, you must determine which protocol you want to use: pure Internet Protocol (IP), Internet Packet Exchange™ (IPX™), or both.

Pure IP

If you choose IP, your network can share data with other IP networks, including the Internet. To use IP, you must have an IP address, a subnet mask, and a router or gateway address.

Any IPX data will be encapsulated using the IP protocol.

IPX

If you choose IPX, Novell's traditional protocol, you can continue using legacy NetWare IPX applications.

NetWare automatically loads and binds all detected IPX frame types for your network board. If no frame types are detected, the server loads and binds to Ethernet_802.2. You can remove frame types when customizing upgrades.

IP and IPX

You can use both IP and IPX on the same network in compatibility mode. IP nodes can communicate over IPX segments and IPX nodes can communicate over pure IP segments. Compatibility mode also identifies and processes encapsulated packets from NetWare IP (NWIP) clients.



You can bind both protocols to a single network board.



For more on IP/IPX compatibility and migration, see the IPXTOIP.HTM file on the *NetWare 5* CD.

Presentation**Notes****Choosing a Protocol**

- Explain that administrators can choose pure IP, IPX, or both as the protocol.
- Discuss binding pure IP as the sole protocol.
- Discuss binding IPX as the sole protocol.
- Discuss binding both protocols.

Using the Installation Program to Upgrade a NetWare 4.1x Server

If you decide to use the Installation program to upgrade your NetWare 3 or NetWare 4 server, you must do the following:

- Prepare for the upgrade
- Perform the upgrade
- Complete post-upgrade procedures

Preparing for the Upgrade

Complete the following tasks before performing an upgrade to NetWare 5:

1. Make at least two backups of your NetWare 4.x system.



Make sure the backup software supports both the existing operating system and NetWare 5. We recommend using SBACKUP.

2. Document the hardware settings (such as interrupt number and I/O port) for the server's network boards.
3. Broadcast a console message asking users to log out of the server you are upgrading.
Users must stay logged out until the upgrade is complete.
4. If you use third-party NLMs, disk drivers (*.HAM), or LAN drivers (*.LAN), ask your Novell Authorized ResellerSM about compatibility issues before upgrading your network.



NetWare 5 requires a HAM driver for each host bus adapter; it does not support DSK drivers. For more information, contact your hard disk manufacturer.



To avoid base schema conflicts in NDS, always upgrade the server holding the master replica of the [Root] partition first.

Using the Installation Program to Upgrade a NetWare 4.1x Server

- List the NetWare versions that administrators can upgrade to NetWare 5.

Preparing for the Upgrade

- Discuss the preparation steps for upgrading a server.
- Caution students to upgrade the server holding the master replica of the [Root] partition before upgrading additional servers.

Performing the Upgrade

To upgrade a server to NetWare 5, complete the following tasks:

1. Load the Installation program at the server's DOS prompt by entering **INSTALL** and selecting **Upgrade from 3.1x or 4.1x**.
2. Select the mouse and video drivers.
3. If needed, modify the following automatically detected hardware devices:
 - Storage devices
 - Network boards
 - Platform Support Module

The Installation program mounts volume SYS and loads the Java virtual machine.

4. Select the protocols for network boards.
5. Upgrade NDS.
6. Install licenses for NetWare 5 by selecting an .NLF file.
7. Mark additional products you want to install.
8. (Optional) Customize the installation.
9. Exit the Installation program and reboot the server.

Presentation**Notes****Performing the Upgrade**

- Discuss how to upgrade a NetWare 4.11 server to NetWare 5.

- Point out that NetWare 5 requires a HAM driver for each host bus adapter.

Completing Post-Upgrade Procedures

After you upgrade a server, consider performing the following tasks:

1. Upgrade your printing configuration with NDPS.
2. Modify container and user login scripts. Consider the following:
 - If you renamed a server, modify references to it.
 - Make sure drives are mapped to directories containing adequate rights.
 - Modify or delete the MAP login script commands.

When you map a drive to a directory that is located on a NetWare 5 NDS volume, modify the volume name to correspond to the new NDS name.

However, when you map a drive to a server that is running an earlier version of NetWare, the MAP command functions as it did originally and must include the server name.



The majority of login commands work the same under NetWare 5 as they did under previous NetWare versions. If the server is not specified in MAP commands (MAP F:=SYS:*directory*), the user's Message Server attribute is used.

3. Upgrade NetWare clients if needed. Version 2.2 or higher is required for access to NetWare 5 servers.

Presentation

Notes

Completing Post-Upgrade Procedures

- Discuss the post-upgrade steps.

Hands-On Exercise 1-1: Upgrading a NetWare 4.11 Server to NetWare 5

In this exercise you upgrade a NetWare 4.11 server to NetWare 5.

Complete the following:

1. Bring down your NetWare 4.11 server.
 - a. Enter **DOWN**.
 - b. Enter **EXIT**.
2. Launch the NetWare 5 Installation program.
 - a. From the DOS prompt on your NetWare 4.11 server, change to the drive containing the NetWare 5 installation files.
 - b. Enter **INSTALL**.
3. After reading the license agreement, accept it by pressing **F10**.
4. In the Options menu, do the following:
 - a. Select **Modify**.
 - b. In the "Is this a new server or an upgrade?" field, select **Upgrade from 3.1x or 4.1x**.
 - c. Press **Tab** to toggle to the Options window.
 - d. To set advanced settings for your server, press **F2**.
 - e. Select **Continue**.
5. Select the appropriate *mouse type* and *video driver* for your server.
6. Wait while the Installation program copies files to the hard disk.
7. Make sure the correct storage adapter is selected; then select **Continue**.
8. Make sure the correct storage device is selected; then select **Continue**.

The Installation program mounts volume SYS.

Presentation**Notes****Hands-On Exercise 1-1:
Upgrading a NetWare 4.11
Server to NetWare 5**

- Introduce the exercise.

- Let students know which local drive contains the NetWare 5 installation files.

- Provide the students with the names and settings for the drivers of their hardware.

- Assign the following to each student:
 - A unique IP address
 - A subnet mask

:35



Conduct the exercise.

Assist the students as necessary.

9. Make sure the correct network board is selected and configured; then select **Continue**.
10. Wait for the Installation program to copy files and load the Java virtual machine.
All SYS:SYSTEM driver files are copied to the SYS:SYSTEM\DRIVERS.OLD directory, and the program loads the Java console.
11. If prompted, click **Next** in the Configure File System window.
12. In the Mount Volumes window, click **No, mount volumes now**.
13. Click **Next**.
14. In the Protocols window, click the **network board icon**.
15. Click **IP**; then enter your **IP address**, **subnet mask**, and **router** information.
16. Click **Next**.
17. Configure NDS.
 - a. Enter your **Admin object's name** and **context**.
 - b. Click **Next**.
18. In the Licenses screen, do the following:
 - a. Click the **Browse** button.
 - b. Click the **.NLF file** specified by your instructor.
 - c. Click **OK**.
 - d. Click **Next**.
19. Install additional products and services.
 - a. Click **Deselect All**.
 - b. Click **Storage Management Services**.
20. Click **Next**.
21. Review the Summary screen and click **Finish**.
22. If prompted to replace existing files, select the option to replace all existing files.
23. When the file copy is complete, click **Yes**.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 1-1:
Upgrading a NetWare 4.11
Server to NetWare 5** *(continued)*

- Provide students with the path to the license file.

- Point out that in Step 22, the Customize button is optional for further tailoring the upgrade.

- Move on to the next subsection when students have completed Step 22.

- Review the exercise.

During the file copy, you can discuss the upgrade of the NetWare 3.1x server.

Using the Novell Upgrade Wizard to Upgrade a NetWare 3.1x Server

To upgrade your server using the Upgrade Wizard, complete the following tasks:

1. Install the Novell Upgrade Wizard.
2. Prepare for the upgrade.
3. Launch the utility.
4. Prepare a *project* (a model that you use to place NetWare 3.1x objects in the NDS tree).
5. Move objects from the Project window.
6. Verify that objects and files can be upgraded as specified.
7. Upgrade the server components across the wire.
8. Complete the post-upgrade steps.

Installing the Novell Upgrade Wizard

Novell Upgrade Wizard is *not* installed during NetWare 5 installation. To install the program, do the following:

1. At the workstation where you want to run the Novell Upgrade Wizard, insert the *NetWare 5 Operating System CD*.
2. Locate the following self-extracting executable:
 \PRODUCTS\UPGRDWZD\UPGRDWZD.EXE
3. Execute the self-extracting file and follow the prompts.

Using the Novell Upgrade Wizard to Upgrade a NetWare 3.1x Server

- Introduce the tasks involved in using the Novell Upgrade Wizard.

Installing the Novell Upgrade Wizard



Demonstrate how to install the Novell Upgrade Wizard.

Preparing for the Upgrade

Before you use the Novell Upgrade Wizard, do the following:

1. To protect against possible file loss or corruption during the upgrade, always create a backup of NDS and the volumes to which you will migrate the NetWare 3.1x file system.
2. If you are upgrading a NetWare 3.1x server to an existing NDS tree, gather the following information:
 - Tree name
 - Desired NDS context for this server
 - Administrator's name (user ADMIN or another user with Supervisor object rights to this context)
 - Administrator's password (for authentication to NDS)
3. If you are upgrading several servers to the same NDS context, do the following before upgrading:
 - Consolidate names of users who exist under different names on different servers.

For example, user Mark Peters might be MARK on server FS1 and MPETERS on server FS2. If you upgraded both servers to the same context, two user objects would be created for the same user, Mark Peters.
 - Change the names of users with the same names on different servers that are upgraded to the same context.

For example, the user MARK might exist on server FS1 and a different user MARK might exist on server FS2.
4. Upgrade Windows[®] 95 client workstations to Novell Client for Windows 95 version 2.2 or higher. You can find the client version by holding down **Alt** and double-clicking **Network Neighborhood**.

If you do not have access to Network Neighborhood, you can still find the client version by doing the following:

 - Select **Start | Settings | Control Panel**.
 - Double-click **Network**.
 - Click **Novell NetWare Client** or **IntranetWare Client**.
 - Click **Properties**.

The Novell Client page appears with the client version at the bottom.

Presentation

Notes

Preparing for the Upgrade

- Discuss the preparation steps for using the Novell Upgrade Wizard.



If this procedure does not access the client version number for you, you must upgrade your client. You can get a free client upgrade at <http://www.novell.com/download/>.

5. Upgrade Windows NT[®] client workstations to Novell Client[™] for Windows NT version 4.11 or higher. You can find the client version on the title bar of the Login dialog.

6. Verify that you have sufficient rights.

You need Supervisor or equivalent rights to both the NetWare 3.1x and NetWare 5 servers. If you are not authenticating to the NDS tree as user Admin, you must have console operator rights.

7. (Conditional) Disable SAP filtering on each server involved in the migration.

If you cannot disable SAP filtering, ensure that the default server (preferred server) for the client is on the same LAN segment as the other servers you are migrating to and from.

8. Update NLMs on the NetWare 3.1x server.

For the Novell Upgrade Wizard to work properly, you must update several NLMs. If you installed the Novell Upgrade Wizard to the default path, the NLMs are in the following directory:

C:\PROGRAM FILES\NOVELL\UPGRADE\PRODUCTS\NW3X

9. Unload the following NetWare 3.1x server NLMs in the order indicated:

- TSA311.NLM or TSA312.NLM
- SMDR.NLM
- SMDR31x.NLM
- SPXS.NLM
- TLI.NLM
- AFTER311.NLM
- CLIB.NLM
- A3112.NLM
- STREAMS.NLM

Presentation

Notes

Preparing for the Upgrade *(continued)*

- Continue discussing the preparation steps.

10. Load the new **TSA312.NLM**. This updates all the NLM programs that you copied earlier.

11. (Conditional) Load and add name spaces.

If any of the volumes you are going to migrate contain files that use non-DOS naming conventions, you must load the appropriate name space on the NetWare 5 server and then add the name space to the volume prior to the upgrade.

Windows 95, Windows NT, and OS/2[®] name spaces are loaded through LONG.NAM. The NFS name space is loaded through NFS.NAM, and the Macintosh[®] name space is loaded through MAC.NAM.

12. Determine which objects to upgrade.

The Novell Upgrade Wizard allows you to upgrade the entire NetWare 3.1x bindery and the contents of the individual NetWare 3.1x volumes.

In most cases, you will upgrade both. However, you might want to upgrade only the bindery (for example, to quickly add users in an NDS tree) or the contents of an individual volume.

Presentation**Notes****Preparing for the Upgrade** *(continued)*

- Continue discussing the preparation steps.



Demonstrate how to prepare the classroom NetWare 3.12 server for an upgrade.

Students will upgrade a NetWare 3.12 bindery in Exercise 1-2. Use this demonstration to prepare for this exercise.

Launching the Utility

To run the Novell Upgrade Wizard, do the following:

1. Click the **Start** menu.
2. Select **Programs | Novell | Novell Upgrade Wizard | Novell Upgrade Wizard**.

The Startup dialog box appears and allows you to create a new project.

Creating a Project

Create and complete a project by doing the following:

1. In the Startup dialog box, click **Create New Upgrade Project**; then click **OK**.
2. Type a **project name** and use the **Browse** button to indicate the location where you want to save the project; then click **Next**.

A new page appears and requests the source NetWare 3.1x server you are upgrading and the destination server where NDS resides.

3. Use the two drop-down lists to indicate the **source server** and **destination tree**; then click **Next**.

If the desired source server or destination tree is not displayed, use the **Server** button or **Tree** button to log in to a server or NDS tree.

4. To create the upgrade project, click **Create**.

Presentation

Notes

Launching the Utility



Demonstrate how to launch the Novell Upgrade Wizard.

Creating a Project



Demonstrate how to create a project.

Moving Objects from the Project Window

The indicated source server and destination tree appear in the Project window. In this window, you can drag bindery objects and volume data from the source server to the desired location in the NDS tree. A sample Project window is shown in Figure 1-1.

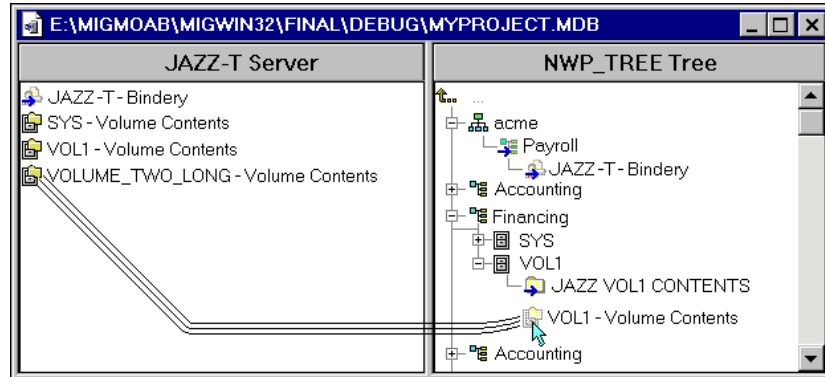


Figure 1-1: A Sample Project Window

To move objects, do the following:

1. Determine where you want each object to appear in the NDS tree.
2. (Conditional) If the container (for the bindery) or folder (for the volume data) does not already exist in the NDS tree, right-click the parent object and create a new container or folder.
3. Click and drag the bindery or volume objects from the Source area to the desired location in the Destination area.

Presentation**Notes****Moving Objects from the Project Window**

- Introduce the Project window.



1-1 (Figure 1-1: A Sample Project Window)



Demonstrate how to move objects in the Project window.

Verifying That Objects and Files Can Be Upgraded

After you move the bindery and volumes to the Destination area, verify that the upgrade can proceed as indicated in the Project window. The verification process checks for the following:

- Object conflicts
- Sufficient NDS and file system rights
- Disk space limitations
- Other criteria that could impede the upgrade

To perform the verification, do the following:

1. From the toolbar, click **Verification**, or select **Project | Verify Project**.
2. Read the Overview page and click **Next**.
3. To upgrade the NetWare 3.1x print information to a queue-based system, select a **volume** in the tree browser; then click **Next**. If you don't want to upgrade the print information, unmark the box.
4. To apply a template object to all users being upgraded, locate and click the **template** object; then click **Next**.
If you don't want to apply a template, unmark the appropriate box.
5. If you want to create a user template, mark the box; then enter a **name** and click **Next**.
6. Enter the **passwords** to the source server and destination tree; then click **Next**.
7. Mark the boxes to indicate the categories you want to verify; then click **Next**.

The utility verifies the selected items and reports any naming conflicts between same-type objects.

8. For each naming conflict the verification process finds, click the **object** and select one of the following options:
 - Let the wizard rename the object automatically.
 - Don't migrate the object.
 - Merge the objects and maintain the bindery properties.
 - Merge the objects and maintain the NDS properties.

By default, each object will be renamed. If no naming conflicts occur, the list box will be empty.

Verifying That Objects and Files Can Be Upgraded



Demonstrate how to verify that objects and files can be upgraded.

9. Click **Next**.

The next screen shows naming conflicts between different object types as well as objects (including print forms, print devices, and print configurations) that cannot be merged.

10. For each naming conflict between different object types, click the **object** and select one of the following options:

- Let the wizard rename the object automatically.
- Don't upgrade the object.

By default, each object will be renamed.

11. Click **Next**.

12. Resolve all additional errors; then click **Next**.

13. Read the verification summary results; then click **Finish**.

Upgrading Across the Wire

When you have verified that all objects and files can be upgraded, you can upgrade the bindery and file system across the wire by completing the following steps:

1. In the toolbar, click **Upgrade**, or select **Project | Upgrade**.

2. Read the Overview page; then click **Next**.

The program goes through the verification process again. Any previously shown conflicts that are not resolved are still marked.

3. Resolve any remaining issues.

4. To begin the upgrade process, click **Upgrade**.

A progress bar shows the relative percentage of objects that have been upgraded and those yet to be upgraded.

You can stop the upgrade process at any time by clicking **Stop** and then clicking **Yes** to confirm. All NetWare 3.1x bindery and file contents copied to that point remain in the destination NDS tree until you manually delete them.

Presentation**Notes****Verifying That Objects and Files
Can Be Upgraded** *(continued)*

- Continue the demonstration.

Upgrading Across the Wire

Demonstrate how to upgrade the bindery and file system across the wire.

Completing Post-Upgrade Procedures

Following the upgrade, perform any of the following applicable post-upgrade procedures:

- Modify login scripts.
- Modify your printing configuration.
- Check upgraded user information.
- Check upgraded file information.
- Check third-party applications.
- Move individual objects to different locations in the NDS tree.
- Upgrade Novell clients (version 2.2 or higher is required).



For more information on post-upgrade procedures, refer to the online Help in the Novell Upgrade Wizard.

Presentation

Notes

Completing Post-Upgrade Procedures

- Discuss the post-upgrade procedures.

Hands-On Exercise 1-2: Upgrading a NetWare 3.12 Server to NetWare 5

In this exercise you migrate a NetWare 3.12 bindery to the NetWare 5 server you created in Exercise 1-1.

Complete the following:

1. At your workstation, install the Novell Upgrade Wizard.
 - a. Run **UPGRDWZD.EXE**. Get the path to the file from your instructor.
 - b. Follow the prompts.
2. Log in to the NetWare 5 tree as your **Admin** object.
3. From Windows, select **Start | Programs | Novell | Novell Upgrade Wizard | Novell Upgrade Wizard**.
4. Create a project.
 - a. In the Startup dialog box, click **Create New Upgrade Project**; then click **OK**.
 - b. Name the project **Exercise**.
 - c. Use the **Browse** button to indicate the *location* where you want to save the project; then click **Next**.
 - d. Click the **server icon** by the Source field.
 - e. Click the **server icon** in the Novell Client window.
 - f. Browse to the **FS312** server.
 - g. Log in as **supervisor** with the password **novell**.
 - h. Click **OK**.
 - i. Click **Next**.
 - j. Click **Create**.
 - k. Read the Getting Started window; then click **Close**.
 - l. Drag **FS312-Bindery** from the left and drop it in your assigned NDS context on the right.

Presentation**Notes**

Hands-On Exercise 1-2: Upgrading a NetWare 3.12 Server to NetWare 5

- Introduce the exercise.



:10

- Conduct the exercise.

- Provide the path to the UPGRDWZD.EXE file.

Make sure you have prepared the NetWare 3.12 server for this upgrade by performing the demonstration discussed in "Preparing for the Upgrade" on page 1-13.

5. Upgrade across the wire.
 - a. In the toolbar, click **Start Migration**.
 - b. Read the **Migration Wizard** page; then click **Next**.
 - c. Unmark the **Migrate the Bindery Print Information** box; then click **Next**.
 - d. Select the **template object** found in your container; then click **Next**.
 - e. Click **Next**.
 - f. Click **Next**.
 - g. At the Duplicate File Resolution screen, select an option; then click **Next**.
 - h. Enter **novell** as the password to the source server and your password to the destination tree; then click **Next**.
 - i. Mark all boxes to indicate the categories to verify and click **Next**.
 - j. For each naming conflict the verification process finds, click the **object** and select one of the following options:
 - Let the wizard rename the object automatically.
 - Don't migrate the object.
 - Merge the objects and maintain the bindery properties.
 - Merge the objects and maintain the NDS properties.
 - k. Click **Next**.
 - l. For each naming conflict between different object types, click the **object** and select one of the following options:
 - Let the wizard rename the object automatically.
 - Don't upgrade the object.
 - m. Click **Next**.
 - n. Resolve all additional errors; then click **Next**.
 - o. To start the upgrade, click **Proceed** one student at a time.
6. Click **View Error Log**.

Notice that the Supervisor user does not upgrade. Why?

Presentation**Notes****Hands-On Exercise 1-2:
Upgrading a NetWare 3.12
Server to NetWare 5** *(continued)*

- Make sure students perform Step 5o one at a time.

- Review the answer.

The FS312 bindery files are locked once the first student performs this step. The files are not available again until the migration is complete.

Answer:

6. This user is no longer the supervisor of the NetWare 5 server. The Admin object now controls the NDS tree.

7. Click **View Success Log** and review the information.
8. Click **Close**.
9. In NetWare Administrator, verify the upgrade.
10. Exit the Novell Upgrade Wizard.

(End of Exercise)

**Hands-On Exercise 1-2:
Upgrading a NetWare 3.12
Server to NetWare 5** *(continued)*

- Review the exercise.

Summary

In this section you learned the following:

- Upgrading means installing NetWare 5 on the same machine over existing files or moving files to another server that already has NDS installed.
- To upgrade a server, use the NetWare 5 installation program (INSTALL.BAT) or the Novell Upgrade Wizard.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Choose an upgrade method and a protocol.
2. Use the Installation program to upgrade a NetWare 4.1x server to NetWare 5.
3. Use the Novell Upgrade Wizard to upgrade the bindery of a NetWare 3.1x server to NetWare 5.

Notes

SECTION 2 Using the Server Console

Duration 03:30

Preparation

Do the following:

- Disable the STARTX.NCF line in the AUTOEXEC.NCF file on the FS1 server.
- Reboot the server.

SECTION 2 Using the Server Console

In this section, you learn basic NetWare server skills such as executing console commands, loading NetWare Loadable Modules™ (NLMs™), maintaining server configuration files, and accessing the server from a Remote Console™. Additionally, you learn about NetWare server security strategies.

Objectives

Upon completing this section, you should be able to

1. Describe the function of a NetWare server and its interface, and identify the server components.
2. Execute server console commands and navigate the server console using hot keys.
3. Load and unload NetWare Loadable Modules (NLMs).
4. Identify and describe server configuration files.
5. Customize the server by editing the appropriate configuration files.
6. Create server script files to automate the execution of console commands.
7. Load Java® application support on the NetWare 5 server.
8. Launch Java programs and applets from the NetWare GUI.
9. Manage NetWare from the server using ConsoleOne™.
10. Describe remote console management; use various utilities to remotely manage the console.
11. Describe security strategies for a NetWare server; implement console security.

Presentation

Notes

Using the Server Console

- Introduce the section.

Objectives

- Present the section objectives.

NetWare Server Overview

A NetWare server is a computer running the NetWare operating system. NetWare runs in the server RAM and is the main software component that enables the server to provide network services to clients.

The NetWare operating system is started by executing a file called SERVER.EXE. Typically, NetWare runs on an Intel® or Intel-compatible computer. NetWare 5 runs on a Pentium® processor.

The server's main function is to regulate communication between itself, the workstations attached to the server, and other shared network resources, such as printers.

The NetWare server manages the transmission of data among network devices, stores data on and retrieves data from hard disks, manages one or more file systems, protects data integrity, manages printers and printing, and allocates and manages memory use.

The NetWare operating system is modular; it can be divided into the following categories:

- Kernel
- Server Console
- NetWare Loadable Modules (NLMs)

The NetWare Kernel

A kernel is the basis or core of an operating system. The NetWare operating system kernel provides the following:

- Multiprocessor support
- Memory protection
- Virtual memory
- Load balancing
- Scheduling
- Preemption

Presentation**Notes****NetWare Server Overview**

- Define *NetWare*.
- Review the function of the NetWare server.
- Discuss where NetWare resides.
- Discuss server RAM.

RAM is dynamic, electronic memory. Active software is stored in RAM and used by the server.

The NetWare Kernel

- Define *operating system kernel*.
- Briefly review some of the main features of the NetWare kernel.

Multiprocessor Support

The NetWare Multi-Processor Kernel (MPK) is both a uniprocessor kernel and a multiprocessor kernel. The same kernel can run on machines containing a single processor and on machines containing multiple processors.

NetWare automatically detects the number of processors in a server. The NetWare MPK can support machines with as many as 32 processors.

Memory Protection

Memory protection allows applications to run in a mode that prevents ill-behaved applications from crashing the server. Currently NetWare provides memory protection support for Java applications.

Virtual Memory

Virtual memory is a memory management scheme that permits execution of programs larger than the size of the physical memory configured on the server. Virtual memory is transparent to applications that request memory.

When memory resources are low, NetWare assesses all memory to see which data has been used less recently than the rest. It then moves least-used data out of physical memory to the hard disk, thus freeing memory for other programs.

When the data is needed again, it is returned to memory; it is swapped for other data which is then moved to the hard disk.

Because Java applications have high memory requirements, virtual memory support on NetWare reduces the actual amount of RAM a NetWare server needs.

Presentation

Notes

The NetWare Kernel *(continued)*

- Continue discussing the NetWare kernel features.

Load Balancing

The ability of the NetWare kernel to detect and intelligently distribute processing across multiple processors is called *load balancing*. When NetWare is running on a machine with multiple processors, the kernel automatically detects and distributes the processing load across all processors.

Scheduling

The NetWare kernel allows you to manage the amount of time each application uses the processor. By configuring the amount of time the processor allocates to each application, you can ensure that your high-priority and mission-critical applications receive a greater share of the processing bandwidth.

Preemption

Preemption is an operating system scheduling technique that allows the operating system to take control of the processor at any instant regardless of the state of the currently running application.

The preemptive nature of the NetWare kernel allows you to schedule the processor utilization of each application.

Presentation

Notes

The NetWare Kernel *(continued)*

- Continue discussing the NetWare kernel features.

The Server Console

You control and manage the NetWare server at the server console. The server console provides a command prompt (similar to the DOS command prompt) where console commands are executed and NLMs are loaded.

The following is a list of the types of tasks you can perform from the NetWare server console:

- View network traffic.
- Send messages.
- Set server configuration parameters.
- Shut down and restart the server.
- Load and unload programs.
- Edit configuration files and other batch files.
- Add name spaces to and remove name spaces from volumes.

Presentation

Notes

The Server Console

- Introduce the server console.

NetWare Loadable Modules

A NetWare Loadable Module (NLM) is a server software program that adds greater functionality and services to the NetWare server. NLMs link disk drivers, LAN drivers, name space modules, management utilities, and server enhancements with the operating system.

An NLM can be loaded into and removed from server memory, generally without affecting the overall operation of the server.

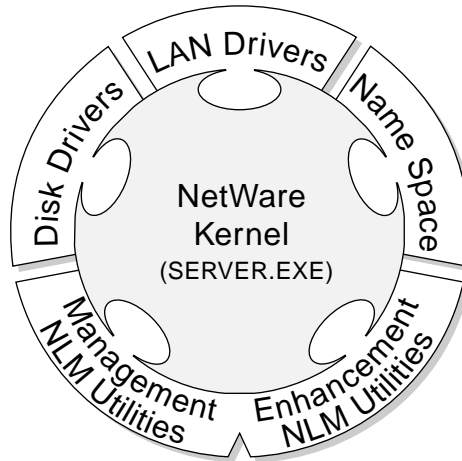


Figure 2-1: NetWare Loadable Modules


NLMs have the following advantages:

- You can remove inactive NLMs to free up RAM.
- You can load and unload NLMs without bringing down the server.
- Third-party developers can write their own NLMs for the NetWare operating system.

NetWare has four types of loadable modules:

- Disk drivers
- LAN drivers
- Name space modules
- NLM utilities

Presentation**Notes****NetWare Loadable Modules**

- Introduce NLMs.
-  2-1 (Figure 2-1: NetWare Loadable Modules)
- Point out operating system and NLM services in the graphic.

- Explain the advantages of NLMs.

- Introduce NLM types.

Give an explanation similar to the following:

“The NetWare operating system is loaded when the network administrator executes the SERVER.EXE file on the server.

“Once this file (plus LAN and disk drivers) is loaded, all the core operating system services are immediately available to clients.

“Most NLM services are not immediately available when SERVER.EXE is loaded. With NLMs, the network administrator chooses which NLMs the network needs and activates (or loads) them only on the servers where the administrator wants them to run.

“This allows the network administrator to use the specific services he or she wants and to distribute the workload among different servers.”

Disk Drivers

Disk drivers control communication between the server operating system and storage devices. Because disk drivers are NLMs, you can load and unload disk drivers with the server running.

NetWare 5 disk drivers are written to the NetWare Peripheral Architecture™ (NPA) specification. NPA separates NetWare driver support into two components:

- HAM (Host Adapter Module) controls the host adapter (bus).
- CDM (Custom Device Module) controls the hardware devices attached to the host bus adapter.



NetWare 5 does not support disk drivers with a .DSK extension.

LAN Drivers

LAN drivers control communication between the server operating system and the network boards. You can unload a LAN driver and load a new one with the server running. These modules have .LAN extensions.

Presentation**Notes****Disk Drivers**

- Explain NLM disk drivers.

- Define *NPA*, *HAM*, and *CDM*.

Disk drivers normally execute from the STARTUP.NCF file when the operating system is booted. Volume SYS on the associated disks will be mounted automatically during system boot. Any other volumes will need to be mounted manually by the AUTOEXEC.NCF file.

LAN Drivers

- Explain LAN drivers.

- Mention the .LAN extension for this NLM type.

If desired, provide an example such as NE2000. You do not need to list and define every LAN driver.

Name Space Modules

Name space modules allow non-DOS filenames to be stored on NetWare volumes. These modules have .NAM extensions.

Name space modules that are included in NetWare 5 are MAC.NAM, LONG.NAM, and NFS.NAM.

Long name support is loaded automatically when NetWare 5 mounts the SYS volume. New volumes are created with DOS and long name support.

NLM Utilities

Most NLMs are management utilities and server applications modules. They allow you to run services not built into the core operating system. These NLMs have .NLM extensions.

NetWare 5 NLMs provide many network services, including the following:

- Novell Directory Services™ (NDS™)
- File system
- Security
- Authentication
- Java Virtual Machine
- Network printing
- Storage Management Services™ (SMS™)
- Remote server console
- Routing
- Server monitoring*
- Network management*



*These NLMs do not come with the basic NetWare 5 package. They must be purchased separately.

Presentation**Notes****Name Space Modules**

- Introduce name space modules.
- Mention the .NAM extension.

NLM Utilities

- Introduce NLM utilities.
- Point out the .NLM extension.
- Point out the many services that are provided through NLMs.
- Point out that the NLMs used with the Novell Client are not the same as the NLMs that are loaded on the server.

Students might be confused about seeing NLM utilities under NLM types. This NLM type is the only one with the .NLM extension.

Executing Console Commands

Console commands are command line utilities that can only be executed at the server console. They are part of the NetWare core operating system.

Once the server has been installed, these commands assist you in performing various tasks required to manage the network environment.

To execute a console command, simply enter the command and any parameters at the server console prompt.

To see what console commands are available to you, enter HELP at the server console prompt. HELP is one of the console commands.

To get detailed help for a specific console command, enter

HELP *command name*

Presentation**Notes****Executing Console Commands**

- Introduce console commands.
- Explain that console commands are part of the NetWare core operating system.
- Emphasize that console commands and NLMs are the two major categories of server utilities.
- Compare console commands to internal DOS commands such as COPY, DEL, PATH, MD, and CD.



Demonstrate the console command HELP.



Demonstrate how to execute a console command.

Students need to remember the difference between console commands and NLMs.

SET Parameters

The default server configuration parameters in NetWare 5 have been set to maximize network performance in most situations. You can view or change these parameters using the SET console command.

To view the SET console screen, enter **SET** at the server console.

To change a parameter's setting, enter the following command:

SET *parameter = value*

Most SET parameters can be executed at the server console prompt, but the setting will last only until it is reset or until you bring down the server. To make the settings permanent, add them to the appropriate configuration files.



For more information on SET commands, see "SET" in *Utilities Reference* in the online documentation.

Presentation**Notes****SET Parameters**

- Briefly introduce the function of SET and SET parameters.



Demonstrate a few of the SET utility options.

- Discuss the purpose of executing SET from the system console.

Avoid discussing any parameters regarding communication and memory. These will be discussed in later sections.

The system default settings are usually acceptable and the SET command is usually used only in unique situations.

Console Hot Key Sequences

The NetWare console also supports some hot key sequences to help you navigate the console more easily.

Current Screens Menu

To bring up the Current Screens menu that lists all the NLM screens currently running on the server, hold down the **Ctrl** key and then press **Esc**.

Once the Current Screens menu appears, you can go to an NLM screen by typing in the menu number of that screen and pressing **Enter**.

Toggle Screens

You can toggle through the NLMs that are currently running by holding down the **Alt** key and then pressing **Esc**.

Hung Console Screen

The Hung Console Screen is useful to you if you are unable to execute any commands at the server console. It helps you bring down your server safely so that you can restart the server.

To bring up the Hung console screen, press **Ctrl+Alt+Esc**.

Once the menu comes up, you can choose to bring down the server or cancel a volume mount.

Presentation**Notes****Console Hot Key Sequences**

Demonstrate the hot key sequences supported on the console.

Note: In the Current Screens Menu, screens are listed in the same order that the modules are loaded. The Console screen is always number 1.

Loading and Unloading NLMs

NLMs are executed only on the NetWare server. To activate an NLM, enter the name of the NLM at the server console prompt. The syntax to load an NLM is as follows:

```
[path]NLMname [parameters]
```

The system assumes that the path is SYS:SYSTEM if you do not specify a path. Replace *NLMname* with the name of the NLM, such as NWCONFIG or MONITOR. For example, to load the MONITOR.NLM, enter the following:

```
MONITOR
```



You can also change SET parameters with the MONITOR console utility. This utility provides a menu interface that makes changing SET parameters easier.

You can also load NLMs with the LOAD console command at the server console prompt.

The LOAD command uses the following format:

```
LOAD [path]NLMname [parameters]
```

To terminate an NLM, unload it. Most NLMs that have a user interface will be unloaded when you choose the menu item to exit the NLM.

You can force an NLM to terminate by unloading it using the server console command UNLOAD. The syntax to unload an NLM is as follows:

```
UNLOAD NLMname
```

Loading and Unloading NLMs

- Explain how to load NLMs at the console prompt.
- Compare NLMs to external DOS commands such as FORMAT, DISKCOPY, and FDISK.
- Discuss support for the LOAD command.
- Point out that the LOAD command is not needed with NetWare 5, but it is required on earlier versions of NetWare.
- Explain how to unload NLMs at the console prompt.



Demonstrate how to load and unload NLMs.

Hands-On Exercise 2-1: Using Console Commands and NLMs

In this exercise, you learn about some common console commands and use some common NLMs. From your server console, do the following:

1. Shut down the NetWare GUI.
 - a. Click **Novell**.
 - b. Click **Exit GUI**.
 - c. Click **Yes**.
2. View the available console commands.
 - a. Enter **HELP**.

A screen of console commands is displayed.
 - b. To continue displaying console commands, press any key.
3. Use the HELP console command to determine what the following console commands do. Record what the console command does in the space provided below.

The syntax is **HELP command**. For example, to determine what the UNLOAD command does, you enter **HELP UNLOAD**.

CLS _____

VERSION _____

SPEED _____

MEMORY _____

Presentation**Notes**

Hands-On Exercise 2-1: Using Console Commands and NLMs

- Introduce the exercise.



:10

- Have the students complete the exercise.
- Review answers to the questions.

Consider showing students other helpful console commands such as ALIAS or the wild cards that can be used with console commands such as MODULES.

3. Console Commands

CLS: Clears the console screen

VERSION: Displays the file server version and copyright information

SPEED: Displays the processor speed of the server

MEMORY: Displays the amount of server RAM that the kernel recognizes as being available for use

VOLUME _____

TIME _____

MODULES _____

4. Use the SET console command to view the types of server parameters that can be set and to view the setting for the Minimum Service Processes parameter.
 - a. Enter **SET**.
 - b. To view the Miscellaneous SET parameters, enter **11**.
 - c. Continue pressing any key until you see the Minimum Service Processes parameter.
 - d. What is the Minimum Service Processes parameter currently set to?
 - e. Press **Esc**.
5. Use the SET command to set Minimum Service Processes to 70. At the console prompt, enter
SET MINIMUM SERVICE PROCESSES = 70
6. Load some common NLMs.
 - a. Enter **MONITOR**.
 - b. To toggle back to the console, press **Alt+Esc**.
 - c. Enter **NWCONFIG**.
7. Unload the NLMs you just loaded.
 - a. Toggle back to the console.
 - b. Enter **UNLOAD NWCONFIG**.
 - c. Enter **UNLOAD MONITOR**.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 2-1: Using Console Commands and NLMs** *(continued)*

- Continue reviewing answers to the questions.

- Point out that these are only a few of the available commands and NLMs.

3. Console Commands (continued)

VOLUME: Displays a list of currently mounted volumes along with the name space supported on each volume

TIME: Displays the current date and time set on the server

MODULES: Displays a list of NLMs that are currently loaded in server memory

- 4d. Minimum Service Processes should be set to 60 by default

Refer the students to the online documentation for more detailed information on these and other commands and NLMs.

Server Configuration Files

NetWare allows you to create NetWare configuration files (NCFs). NetWare configuration files have an .NCF filename extension. These configuration files are similar to DOS batch (BAT) files; however, they include commands that are specific to the NetWare server.

You can specify a sequence of commands in a text file and then have the server execute those commands by specifying the NCF filename.

Just as DOS uses CONFIG.SYS and AUTOEXEC.BAT files to automate the boot process of the DOS operating system, NetWare uses the following NCF files to help automate its boot-up process:

- STARTUP.NCF
- AUTOEXEC.NCF

The NetWare operating system is loaded by executing the DOS executable SERVER.EXE which, in turn, looks for the STARTUP.NCF and AUTOEXEC.NCF files.

You can automate the loading of SERVER.EXE by placing it in the DOS AUTOEXEC.BAT file. The order in which these files are used is shown in Figure 2-2.

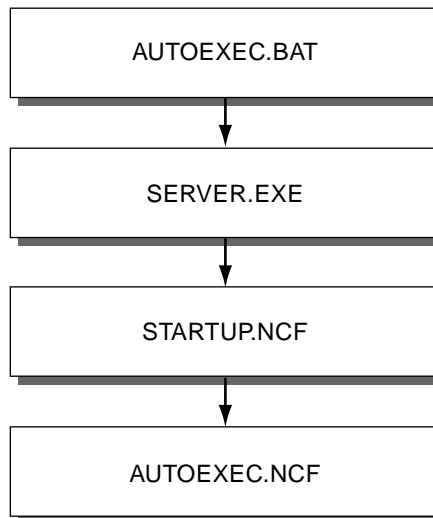


Figure 2-2: Execution Order of Server Startup Files

Presentation**Notes****Server Configuration Files**

- Briefly explain the purpose of configuration files.
- Compare configuration files to DOS batch files.
- Point out the files that will be covered in this section:
 - STARTUP.NCF
 - AUTOEXEC.NCF
- Compare STARTUP.NCF to CONFIG.SYS and AUTOEXEC.NCF to AUTOEXEC.BAT.



2-2 (Figure 2-2: Execution Order of Server Startup Files)

- Point out the order in which the server startup files are executed.

The NetWare operating system does not need the CONFIG.SYS file. Memory managers, such as HIMEM.SYS, can cause conflicts and should not be loaded.

STARTUP.NCF

The STARTUP.NCF file is a server boot file. It contains console commands that must be executed while SERVER.EXE is loading. These commands include disk drivers, name space NLMs, and SET commands.

A sample NetWare server STARTUP.NCF file might contain the following commands:

```
LOAD IDEATA.HAM PORT=1F0 INT=E
LOAD IDE.CDM
LOAD LONG.NAM
```

The STARTUP.NCF file is automatically generated during installation and stored on the DOS partition in the server's C:\NWSERVER boot directory. It can be edited using NWCONFIG.NLM, EDIT.NLM, or any other text editor.

To boot the server with an alternate STARTUP.NCF file (for maintenance purposes), use the following command:

```
SERVER -S \path\filename
```

To boot the server without a STARTUP.NCF file (for maintenance or troubleshooting), use the following command:

```
SERVER -NS
```



For more information about STARTUP.NCF, see "Using Server Batch Files" in the *NetWare Server Operating System* manual in the online documentation.

Presentation**Notes****STARTUP.NCF**

- Display the classroom server's STARTUP.NCF file.
- Discuss the STARTUP.NCF file, emphasizing its contents and method of creation.
 - Point out the sample commands and parameters.
 - Discuss STARTUP.NCF load options.

Mention any SET parameters that you have in the STARTUP.NCF file, but do not discuss them in detail.

The STARUP.NCF file is used for loading *disk* drivers. The AUTOEXEC.NCF file is for loading LAN drivers. Students might be confused if they do not notice this distinction. If students are interested in the order of execution of files and alternatives, explain the SERVER.EXE process and parameters.

Refer the students to the documentation for more information on STARTUP.NCF.

AUTOEXEC.NCF

The AUTOEXEC.NCF file, located in SYS:SYSTEM, guides the server during the boot process. It contains the following information:

- Time zone
- Bindery context
- NetWare server name
- Internal network number
- Calls to other .NCF files
- Other LOAD commands for NLMs (except those NLMs which belong in STARTUP.NCF)
- Other console commands (including SET commands)
- Comment lines (marked with a semicolon in the example below)

A sample AUTOEXEC.NCF file might contain the following commands:

```
;FS1's autoexec.ncf file, last modified 2-10-98 by Bob Cutler
set Time Zone = MST7MDT
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST 2:00:00 AM)
set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST 2:00:00 AM)
set Default Time Server Type = SINGLE

set Bindery Context = OU=CORP.OU=NYC.O=EMA
file server name FS1

ipx internal net 1011532
LOAD TCPIP
LOAD NE2000 INT=3 PORT=300 FRAME=Ethernet_802.2 NAME=NE2000_1_E82
BIND IPX NE2000_1_E82 NET=010107D0
LOAD NE2000 INT=3 PORT=300 FRAME=Ethernet_II NAME=NE2000_1_EII
BIND IP NE2000_1_EII ADDR=137.65.182.22. MASK=255.255.255.0

mount all
```

Figure 2-3: Sample AUTOEXEC.NCF File

Presentation**Notes****AUTOEXEC.NCF**

- Display the classroom server's AUTOEXEC.NCF file.
- Discuss the location and contents of the AUTOEXEC.NCF file.
 - Explain that NCF files can be invoked from within other NCF files.
 - Point out the lines in the figure that correspond to the bullet items.

Note: Do not explain bindery context at this point.

Note: This example contains only a few of the components that can be set or loaded in the AUTOEXEC.NCF file.

The AUTOEXEC.NCF file is created during installation. You can also create or edit it with NWCONFIG.NLM, EDIT.NLM, or any text editor.

To boot without an AUTOEXEC.NCF file (for maintenance or troubleshooting), use the following syntax:

```
SERVER -NA
```



For more information about AUTOEXEC.NCF, see “Using Server Batch Files” in the *NetWare Server Operating System* manual in the online documentation.

Customizing the Server Configuration Files

You can customize the configuration files to meet your needs for management and server performance. NLMs, console commands, and SET parameters can be added to automate the configuration you require upon server startup.

Certain parameters must appear in the STARTUP.NCF file; others must be added to the AUTOEXEC.NCF file.

You can create and edit the STARTUP.NCF and AUTOEXEC.NCF files using a text editor or the following NetWare utilities:

- NWCONFIG.NLM
- EDIT.NLM



For more information, see each command or utility in the *Utilities Reference* manual in the online documentation.

Presentation**Notes****AUTOEXEC.NCF** *(continued)*

- Explain where the AUTOEXEC.NCF file is created.

- Explain how a server can be initialized without an AUTOEXEC.NCF file.

Refer students to the documentation reference for more on AUTOEXEC.NCF.

Customizing the Server Configuration Files

- Introduce the utilities used to create and edit NCF files.

Later in this section, students learn to create and edit other NCF files using EDIT.NLM.

Creating Server Script Files

You can create your own batch files to automate procedures that you execute at the server console. These files can be executed from the server console prompt or called from other batch files such as AUTOEXEC.NCF.

Batch files executed from the server console require the .NCF extension.

You can create the batch files with a text editor and place them in the SYS:SYSTEM directory, or you can create and edit them at the server console using EDIT.NLM.

Use the following syntax to load EDIT:

```
EDIT path\filename
```



If no path is specified, NetWare will search for the file in the SYS:SYSTEM directory.

When you use EDIT, if you do not specify the path and filename, EDIT will prompt you for them. You must enter a file extension if you want one; EDIT will not create an extension for you.

EDIT.NLM can also be used to edit text files (such as AUTOEXEC.BAT) on the DOS partition of the server.

NCF files are also created by other products that are installed on NetWare. They are created to automate tasks that those products perform. For example, the NetWare GUI requires several different NLMs. NetWare includes a STARTX.NCF file to automatically load these NLMs with one convenient command.

Presentation**Notes****Creating Server Script Files**

- Explain how and why a network administrator would create NCF batch files.
- Compare server batch files with DOS batch files.



Demonstrate how to create a new .NCF file with EDIT.NLM.

- Discuss the following points about EDIT.NLM.



Demonstrate how to edit AUTOEXEC.BAT with EDIT.NLM.

DOS batch files are text files containing commands that can be executed at the DOS command prompt. *Server batch files* are text files containing commands that can be executed at the server console prompt.

Demonstrate the following EDIT.NLM commands:

- EDIT
- EDIT *path\filename*

Demonstrate the following keystrokes:

- F1 to access help
- F5 to mark text
- Del to delete text
- Ins to insert deleted text
- If no path is specified, EDIT searches for the file in SYS:SYSTEM.
- If the path and filename are not provided; EDIT will prompt for them.
- EDIT does not add any extension; you must include the extension with the filename if you want one.
- EDIT can be used to edit text files on the DOS partition.

Hands-On Exercise 2-2: Customizing the Server AUTOEXEC.NCF File

In this exercise, you customize the server AUTOEXEC.NCF file by loading MONITOR.NLM and changing a SET parameter.

Complete the following tasks.

1. Access the AUTOEXEC.NCF file.
 - a. At the server console prompt, enter
NWCONFIG
 - b. In the Installation Options menu, select **NCF Files Options**.
 - c. In the Available System Options menu, select
Edit AUTOEXEC.NCF File.
2. Add commands to the AUTOEXEC.NCF file that load NWCONFIG.NLM and set sound bells for alerts to off.
 - a. Enter the following commands at the bottom of the AUTOEXEC.NCF file:
NWCONFIG
SET SOUND BELL FOR ALERTS = OFF
 - b. Press **Esc**.
 - c. To exit AUTOEXEC.NCF and save the changes, select **Yes**.
3. Exit NWCONFIG.
4. To restart the server, enter the following at the server console prompt:
RESTART SERVER
5. Verify that the NWCONFIG.NLM was loaded.
6. Verify that the SET SOUND BELL FOR ALERTS was set to OFF.
 - a. From the NWCONFIG.NLM, toggle to the console prompt by pressing **Alt+Esc**.
 - b. At the server console prompt, enter
SET SOUND BELL FOR ALERTS
 - c. Was the SET parameter set to OFF?

(End of Exercise)

Presentation**Notes**

Hands-On Exercise 2-2: Customizing the Server AUTOEXEC.NCF File

- Introduce the exercise.



:05

- Have students complete the exercise.

- Review the exercise.

Answers:

- 6c. SOUND BELL FOR ALERTS should have been set to OFF.

Hands-On Exercise 2-3: Creating Server Script Files

In this exercise, you create an NCF file that automates the commands needed to provide you with additional configuration information about your NetWare server.

From your NetWare server console, do the following:

1. Create an NCF file named STATS.NCF that displays additional configuration information.

- a. Enter

EDIT STATS.NCF

- b. To create the STATS.NCF file, select **Yes**.

- c. Add the following commands to the file:

REM This program reports additional server information

CLS

VERSION

PAUSE

CLS

SPEED

PAUSE

CLS

MEMORY

PAUSE

CLS

VOLUME

PAUSE

CLS

TIME

PAUSE

CLS

MODULES

- d. To bring up the Save menu, press **Esc**.

- e. Select **Yes**.

- f. To exit, press **Esc**.

- g. To exit, select **Yes**.

Hands-On Exercise 2-3: Creating Server Script Files



Introduce the exercise.



:10

Have the students complete the exercise.

2. From the server console prompt, run your batch file. Enter

STATS

Your batch file should run and display additional information about your server.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 2-3:
Creating Server Script Files**
(continued)

- Continue conducting the exercise.

- Review the exercise.

Loading Support for Java Applications on the NetWare 5 Server

Users typically interact with NLMs on the NetWare server using a text interface. (See Figure 2-4.)



Figure 2-4: MONITOR.NLM with a Text Interface

NetWare 5 also supports the execution of applications written in Java. NetWare 5 provides a graphical user interface (GUI) for Java applications that require user interaction through a mouse and a graphical display.

Java applications requiring a GUI are typically developed using the Java Abstract Windowing Toolkit (AWT). NetWare 5 supports Java applications that are written using the Java AWT or the Java Foundation Class.

Loading Support for Java Applications on the NetWare 5 Server



2-3 (Figure 2-4:
MONITOR.NLM with a Text
Interface)

- Point out that NetWare 5 supports NLMs and Java applications, even those requiring a GUI.

Hardware Requirements for Java

Your server must meet the following requirements to run Java applications that use a GUI.

Memory Requirements

To run Java programs on the NetWare platform, you must have a server with a minimum of 48 MB of RAM. (We recommend at least 64 MB of RAM.)

Mouse Support

You can configure a mouse when you install NetWare 5. The NetWare GUI supports PS/2[®] and serial mice that conform to the Microsoft[®] protocol.

If your server does not have a mouse, you can configure the GUI (during the NetWare installation) to work with the numeric keypad.

Video Support

The NetWare GUI supports ISA, EISA, and PCI video cards. We recommend a PCI video card that conforms to the Video Emulation Standard Association (VESA) specification 1.2 or greater.

NetWare automatically detects and loads the proper video driver for your video card at the time you install NetWare:

- If your video card does not meet the VESA 1.2 or greater specification, NetWare loads a default video driver that supports 640 X 480 resolution with 16 colors.
- If your video card conforms to the VESA 1.2 or greater specification, NetWare loads a VESA video driver that uses the default setting of 640 X 480 resolution with 256 colors.



The VESA video driver supports greater resolutions, but it must be configured manually.

Presentation

Notes

Hardware Requirements for Java

- Discuss hardware requirements for running text-based and graphical Java applications.

Re-detecting Mouse and Video drivers

If you change the mouse or video card on your server and need to have NetWare re-detect the proper drivers, you must execute the SYS:\JAVA\NWGFX\VESA_RSP.NCF file.

To re-detect your mouse and video drivers, enter the following at the server console prompt:

VESA_RSP

Java Support on NetWare

Java applications exist in one of two forms: Java classes or Java applets. A *Java class* is a fully functioning application written in Java. A *Java applet* is a Java program written to run within a Java-compatible browser. NetWare 5 can execute both types of Java applications.

The JAVA.NLM provides Java support on the NetWare platform. This NLM is a port of the JavaSoft® Java Virtual Machine interpreter for Java classes. Once JAVA.NLM is loaded, NetWare can execute Java classes and applets.

Running Java Classes

To load the Java Virtual Machine on the NetWare platform, enter the following at the console prompt:

JAVA

To run a Java application from the console prompt, use the following syntax:

JAVA [-options] path_to_java_class

To view the available runtime options when running a Java application, enter the following at the console prompt:

JAVA -help



Names of Java classes are case sensitive and require the long name space.

Presentation**Notes****Hardware Requirements for Java**
(continued)

- Explain how to have NetWare re-detect the mouse and video drivers.

Note: Executing VESA_RSP.NCF will set the detected video driver back to the default resolution setting.

Java Support on NetWare

- Explain the difference between Java classes and applets.
- Discuss JAVA.NLM.

Running Java Classes

Demonstrate how to load JAVA.NLM.

Running Java Applets

NetWare provides an applet viewer. The applet viewer will run a Java applet that has been defined as part of a HyperText Markup Language (HTML) document. The applet runs as an application on the NetWare server.

The JAVA.NLM provides you with a server console command called APPLET. To run a Java applet from the console prompt, enter

APPLET HTTP://URL

or

APPLET *path_to_local_filename_of_HTML_document*

By providing the APPLET console command with the URL or filename of an HTML document, you can run applets defined in that HTML document.

An applet is defined in an HTML document between the <applet> and </applet> HTML code parameters. For example, the following HTML code would define an applet called Clock2.class with a width of 170 pixels and a height of 150 pixels:

```
<applet codebase="1.0.2" code="Clock2.class" width=170  
height=150> </applet>
```

The APPLET console command executes only what is defined as an applet and ignores all other HTML code in an HTML document. This means that an HTML document viewed by a Java-enabled browser will appear differently than an HTML document run by the APPLET console command.

Presentation**Notes****Running Java Applets**

- Explain how the APPLET console command works.



(Optional) In a Java-enabled browser, show the students an HTML document that has an applet defined in it.

- Point out that the APPLET console command only executes the applet part of an HTML document.

Once students have seen what the document looks like in a Java-enabled browser, show them the applet definition in the source HTML document.

GUI Support on NetWare

You can dynamically load and unload Java GUI support. When the GUI is loaded but not active, it consumes minimal system resources and has no residual effect on the server when it is unloaded.

GUI support on the NetWare platform is provided by an implementation of X-Windows. Java programs that conform to the Java AWT are displayed using X-Windows.



Although the NetWare GUI implementation runs on top of X-Windows, users and application developers cannot develop programs to the X-Windows layer directly. Access to the X-Server can only be obtained through the Java AWT.

By requiring GUI applications to conform to the Java AWT, Novell can implement whatever windowing system serves customers best. If Novell changes the GUI implementation in NetWare to something other than X-Windows, applications will run without having to be rewritten.

You can load GUI support on the NetWare server in one of two ways:

- At the server console prompt, enter

STARTX.NCF

STARTX.NCF loads JAVA.NLM, mouse and video drivers, and the NetWare GUI.



STARTX.NCF is launched automatically from the AUTOEXEC.NCF file when the server is started.

- Load a Java class or applet that requires GUI support.
STARTX.NCF will be launched automatically.

Presentation**Notes****GUI Support on NetWare**

- Explain that Java AWT support on NetWare is implemented through X-Windows.

- Point out that Java AWT programs will not have to be rewritten if Novell changes its GUI implementation.



Demonstrate how to load GUI support on the NetWare server console.

Using the NetWare GUI

The NetWare GUI allows you to run graphical Java programs and applets on your NetWare server. Its menu is preconfigured with Java utilities that allow you to manage your network and configure the NetWare GUI.

You can also configure the NetWare GUI to launch your own Java programs and applets.



The NetWare GUI is not intended to be a full-featured desktop environment or a high-performance graphical workstation.

Installing Other Novell Products

The NetWare GUI allows you to rerun the installation program so that you can install additional NetWare products and services you did not install during the initial installation.

To install additional NetWare products and services, do the following:

1. In the NetWare GUI, click **Novell**.
2. Click **Install**.
A list of NetWare products that are already installed appears.
3. To install additional NetWare products, click **New Product**.
4. Provide the **path** to the location of the source files.
5. Click **OK**.
6. In the Additional Products and Services window, select the **product** or **products** you want to install.
7. When all the products you want are selected, click **Next**.
Some products prompt you for additional configuration information.
A Summary window appears listing the products to be installed.
8. You can customize the installation of any of the products by clicking the **Customize** button.

Presentation

Notes

Using the NetWare GUI

- Discuss the role of the NetWare GUI.

Installing Other Novell Products



Demonstrate how to install additional NetWare products and services from the NetWare GUI.

9. To start the file copy, click **Finish**.
10. Once the product files are copied, you will be prompted to reboot.

Configuring Video Resolution

If your video card and monitor support video resolutions greater than 640 X 480, you can manually configure higher resolutions using the Display Properties configuration tool provided in the NetWare GUI.

To set higher video resolutions, do the following:

1. Click **Novell**.
2. Click **Tools**.
3. Click **Display Properties**.
4. From the list of available resolutions, select the **resolution** you want.
5. Click **Test**.
6. When asked to test the resolution mode, click **OK**.
A test pattern for that mode will be displayed for 10 seconds.
7. If the test pattern is displayed properly, click **OK**.
A message will appear telling you that you must restart the GUI for the change to take effect.
8. Click **OK**.

Keyboard Configuration

For keyboards that support international character sets, you can use the Keyboard Properties utility to specify the keyboard type you are using.

To set the keyboard type, do the following:

1. Click **Novell**.
2. Click **Tools**.
3. Click **Keyboard Properties**.
4. From the Available Keyboards list, select the keyboard type you want.
5. Click **Apply**.

Presentation**Notes****Installing Other Novell Products***(continued)*

Continue the demonstration.

Configuring Video Resolution

Demonstrate how to configure video resolution for the NetWare GUI.

Keyboard Configuration

Demonstrate how to set the keyboard type.

Configuring the Background

The NetWare GUI comes with a variety of backgrounds to choose from. You can add your own background graphics to use in the NetWare GUI by adding graphics in XPM format to the SYS:JAVA\NWGFX\PIXMAPS directory.

To change the NetWare GUI background, do the following:

1. Click **Novell**.
2. Click **Tools**.
3. Click **Backgrounds**.
4. Select the **background** that you want.
5. To display the background you selected, click **Test**.
6. Do one of the following:
 - To set the background and exit the utility, click **OK**.
 - To exit the utility without changing the background, click **Cancel**.

Adding Java Programs and Applets to the NetWare GUI

You can configure the NetWare GUI with menu items that launch your own Java programs or applets.

To add your own menu items to the NetWare GUI, do the following:

1. In a text editor, edit **SYS:JAVA\NWGFX\FVWM2\FVWM2RC5XX**.
2. Under the MENUS section, find the subsection where the menu you want to add an item to is defined.
3. Add your Java program or applet to the menu using the following syntax:

+ “menuitem” Exec command

For example, if you have a SYS:\JAVA\MYAPP.HTML document that contains a Java applet that you want to run on your server, use the following syntax to add that applet to the NetWare GUI:

+ “MyApp” Exec Applet SYS:\JAVA\MYAPP.HTML

4. To force the menu changes to take effect, restart the NetWare GUI.

Presentation**Notes****Configuring the Background**

Demonstrate how to change the NetWare GUI background.

Adding Java Programs and Applets to the NetWare GUI

Open the FVM2RC5XX file in a text editor and explain the syntax used to add menu items.

Note: NetWare GUI menu items can also be created for NLMs. If an NLM is launched as a NetWare GUI menu item, the display will switch to the NLM and the NLM will run outside the NetWare GUI.

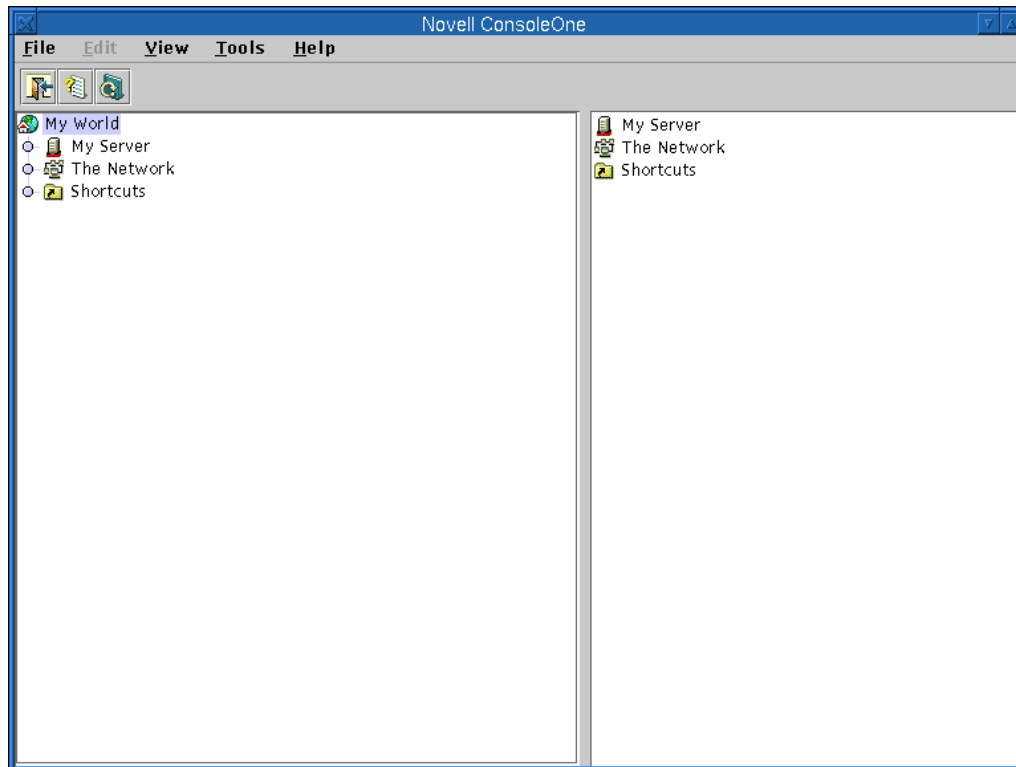


Figure 2-5: The ConsoleOne Utility

Using ConsoleOne

ConsoleOne is a graphical utility, written in Java, that allows you to perform basic server and NDS administration tasks.

You can start ConsoleOne in one of the following ways:

- Execute the C1START.NCF script file from a server console prompt or NCF file.



C1START.NCF will load Java and GUI support prior to executing ConsoleOne.

- Launch ConsoleOne from the NetWare GUI menu.

Presentation

Notes

Using ConsoleOne

- Explain the purpose of ConsoleOne.

- Discuss the various ways to start the ConsoleOne utility.

ConsoleOne allows you to browse objects and manage those objects from your NetWare server console. The left window pane allows you to browse objects; the right window pane displays the contents of the objects being browsed.

The left window pane allows you to navigate by expanding and collapsing container objects. To expand or collapse a container object, double-click the container object or click the dot to the left of the container object.

The right window pane displays the contents of ConsoleOne container objects, such as folders and NDS containers. The right window pane is also the place where screens from most applets launched from ConsoleOne are displayed.

Container objects in ConsoleOne contain other objects that pertain to the server, the file system, or NDS.

For example, when you browse the file system, volumes and subdirectories appear as browsable container objects. When you browse NDS, organization and organizational unit objects become browsable container objects.

The My World object in the left window contains all the object types you can browse using ConsoleOne. By default, the My World object contains the My Server, The Network, and Shortcuts objects.

The ConsoleOne interface allows developers to add custom object types that can also be browsed and managed from within ConsoleOne.



The options available in the menu bar and toolbar for object management will vary according to the object that is currently selected.

Presentation**Notes****Using ConsoleOne** *(continued)*

Demonstrate how to move a window by dragging the window's title bar.



Demonstrate various ways to resize windows in ConsoleOne.



Demonstrate how to expand and collapse objects in the left window pane of ConsoleOne.



Point out the three default object types under the My World object:

- My Server
- The Network
- Shortcuts

Resizing of ConsoleOne windows might be necessary on video displays that don't support high resolutions. The window can be resized by:

- Dragging any corner of the window.
- Clicking the up-arrow in the right-hand corner.

Note: Clicking the up-arrow in the right-hand corner again will return the window to its original size.

Server Administration with ConsoleOne

Most server management tasks supported by ConsoleOne are located under the My Server object. When you expand the My Server object, the Volumes, Configuration Files, and Tools objects are displayed:

- The Volumes object allows you to navigate your NetWare server's volumes and perform basic file system tasks.
- The Configuration Files object contains links to some of the common server configuration files. When you click the Configuration Files object, common server configuration files appear in the right window pane. When you select a server configuration file to edit, ConsoleOne will automatically open up the file in a Java text editor.
- The Tools object contains two tools that can be used in managing your server. The two tools provide local and remote server console access.

Using ConsoleOne, you can

- Edit server configuration files
- Access local and remote server consoles
- Manage the local server file system

Presentation

Notes

Server Administration with ConsoleOne

- Introduce the server management tasks that can be performed in ConsoleOne.

Editing Server Configuration Files

ConsoleOne includes a Java-based graphical text editor. You can use this editor to edit your server configuration files or any other text file that is found on your server's volumes.

To edit a server configuration file, do the following:

1. Expand the **My Server** object.
2. In the left window pane, click **Configuration Files**.
3. In the right window pane, double-click the *configuration file* you want to edit.

The graphical text editor is launched, and the selected server configuration file is opened.



You can also edit a file from the Configuration Files object by right-clicking it and clicking **Edit**.

To edit text files not listed under the Configuration Files object, do the following:

1. Expand the **My Server** object.
2. Expand the **Volumes** object.
3. Expand a *server volume*.
4. Navigate to the *directory* that contains the text file you want to edit.
5. Click the *directory* in which the file is located.
6. In the right window pane, click the *file* you want to edit.
7. In the File menu, click **Edit**.

Presentation

Notes

Editing Server Configuration Files



Demonstrate how to edit a server configuration file.



Demonstrate how to edit text files not listed under the Configuration Files object.

Accessing NetWare Console Screens

A *console screen* is the server console prompt or an NLM, such as MONTIOR.NLM, that has a text user interface. The ConsoleOne remote console tools do not allow you to remotely access any Java GUI console screens.

ConsoleOne provides two tools with which you can gain access to your NetWare console screens and remotely manage your servers. The two tools are Console Manager and RConsoleJ.

Console Manager and RConsoleJ can only gain access to the console screens of local and remote servers that are running the RConsole agent RCONAG6.NLM. The RConsole agent sets the password, TCP port, and SPX port used to gain access to the target server.

During NetWare 5 installation, an RCONAG6.NLM command line is added to the server's AUTOEXEC.NCF file.

The command line to load RCONAG6.NLM is disabled by default. RCONAG6 will not load from the AUTOEXEC.NCF file unless the command line is enabled by removing the semicolon at the beginning of the line.

Presentation**Notes****Accessing NetWare Console Screens**

- Introduce Console Manager and RConsoleJ.
- Discuss the RConsole agent RCONAG6.NLM.



Bring up AUTOEXEC.NCF in a text editor to show students the disabled RCONAG6.NLM command line that is added during NetWare 5 installation.



To demonstrate how the RCONAG6.NLM will prompt for password, TCP port, and SPX port, load RCONAG6 at the server console prompt.

Note: Use a password of *novell*, and press **Enter** to accept the default port numbers.

Console Manager. The Console Manager tool allows you to access consoles that are running on your local NetWare server by displaying them in their own windows on the Java GUI console.

To run Console Manager, do the following in ConsoleOne:

1. Select **My Server | Tools | Console Manager**.
2. Change any connection information and provide a password so that it will connect with the RConsole agent.
3. Click **Connect**.

Console Manager displays all the consoles available on your NetWare server.

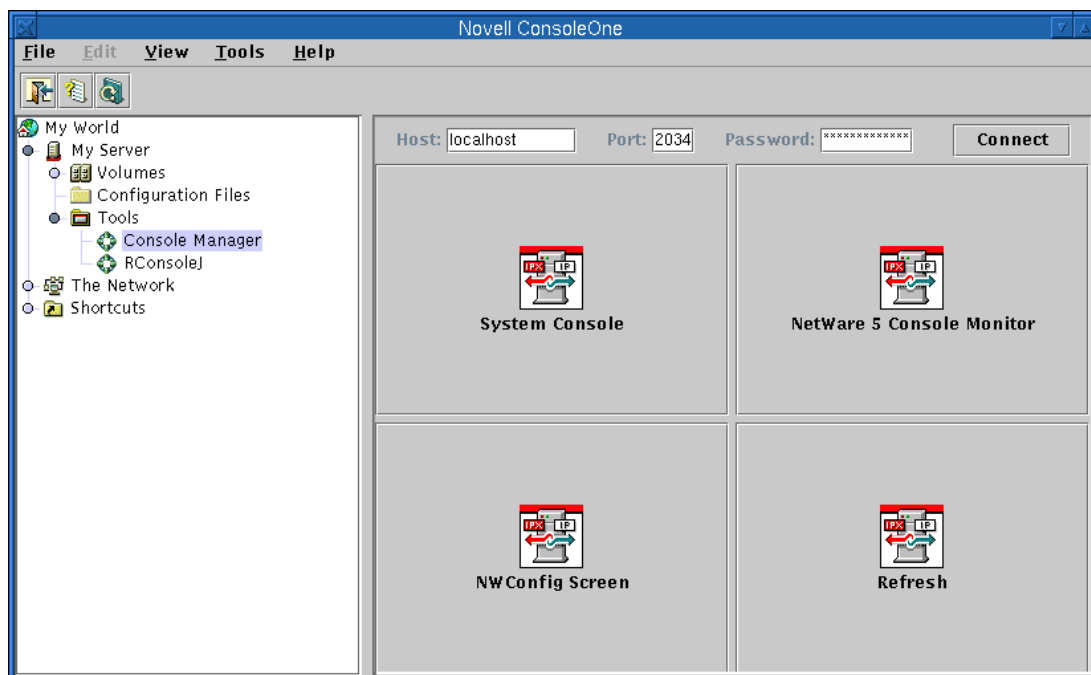


Figure 2-6: Available Local Console Screens in Console Manager

4. Click the console you want to view.



When the Console Manager is started, it displays NetWare consoles available at that time. If any other consoles become available later, they will not appear in Console Manager until you click **Refresh**.

Presentation**Notes****Accessing NetWare Console Screens** *(continued)*

- Discuss Console Manager.



Demonstrate how to access local console screens using Console Manager.

Note: You can connect to remote servers that have the RCONAG6.NLM remote console agent loaded by providing a remote IP address in the Host field.

RConsoleJ. The RConsoleJ tool allows you to access server consoles on remote NetWare servers.

To start RConsoleJ, do the following:

1. Select **My Server | Tools | RConsoleJ**.
2. In the right window pane, connect to the remote server directly or through a proxy.

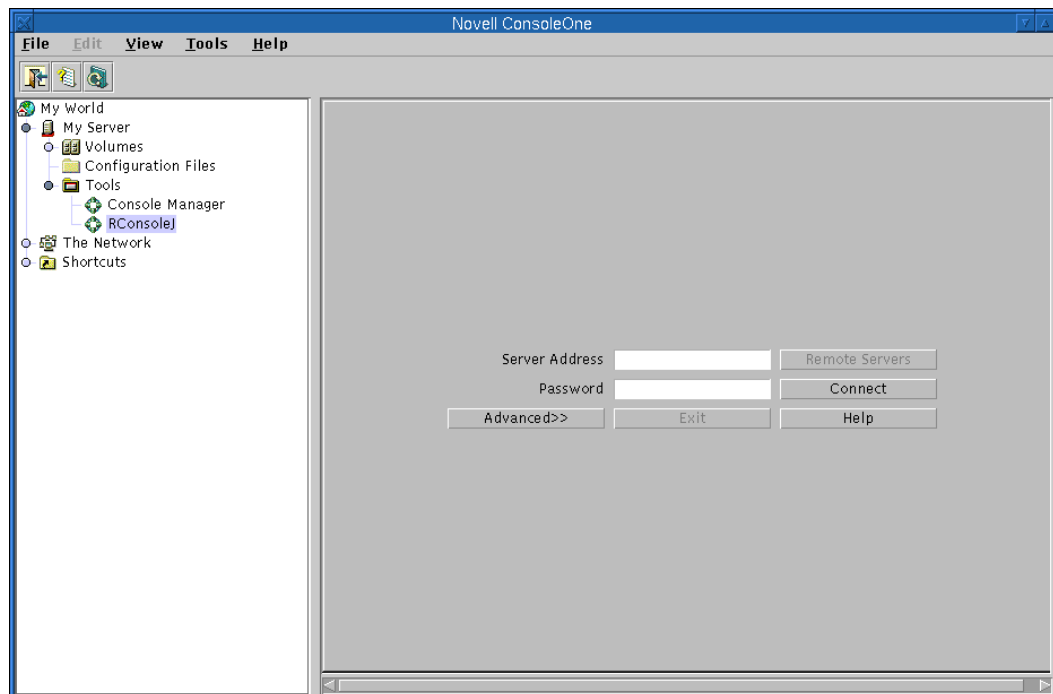


Figure 2-7: Accessing a Remote Server from ConsoleOne Using RConsoleJ

3. Authenticate to the remote server using the password set on the RCONAG6.NLM remote console agent.

Navigations through console screens using RConsoleJ are not seen on the screen of the remote server unless the console screen being accessed remotely matches the screen being displayed on the server itself.

You can make the screen on the remote server match the screen being displayed in RConsoleJ by

- Synchronizing screens
- Activating the current screen on the remote server

Presentation**Notes****Accessing NetWare Console Screens** *(continued)*

- Discuss RConsoleJ.



Demonstrate the RConsoleJ tool by accessing your local server as if it were a remote server.

Managing the Local Server File System

ConsoleOne lets you manage your server's file system under the Volumes object. From ConsoleOne, you can perform the following file system functions:

- Navigate the file system.
- Rename a file.
- Delete a file.
- Copy a file.
- Edit text files.

Presentation

Notes

Managing the Local Server File System

- Discuss the file system management capabilities of ConsoleOne.

NDS Administration with ConsoleOne

Besides server administration, ConsoleOne also allows you to administer NDS from your server console. You can access NDS objects through the The Network container object.

Under the The Network object, ConsoleOne displays all the trees discovered on your network. This allows you to administer all the NDS trees on your network from a single utility.

When you expand an NDS tree to which you are not authenticated, ConsoleOne provides a login window so you can authenticate to that tree. Once you have authenticated to the tree, you can create and manage NDS objects for that tree from within ConsoleOne.

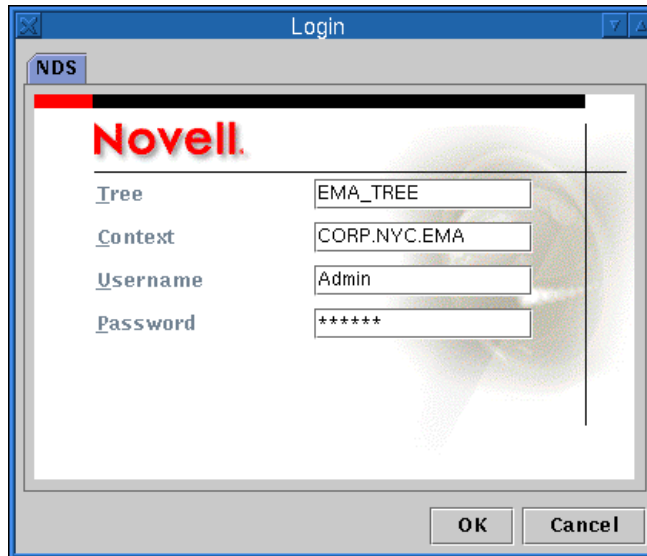


Figure 2-8: The NetWare Login Window in ConsoleOne

Presentation**Notes****NDS Administration with ConsoleOne**

- Point out that ConsoleOne allows the network administrator to administer NDS for all trees on the network.



Demonstrate how to browse NDS using the The Network object in ConsoleOne.



Demonstrate how to log in to an NDS tree.

- Introduce the NDS administration tasks that can be performed in ConsoleOne:
 - Creating NDS objects
 - Managing NDS objects

Show that ConsoleOne allows the administrator to browse multiple NDS trees.

Creating NDS Objects in ConsoleOne

ConsoleOne allows you to create four NDS object types: organization, organizational unit, group, and user objects.

To activate the ConsoleOne menu and toolbar for NDS creation capability, select an NDS container object in the left window pane. When a container object is selected, you can create an NDS object by doing the following:

1. In the File menu, click **New**.
2. Click the **NDS object type**.



You can also click the object type in the ConsoleOne toolbar.

Managing NDS Objects in ConsoleOne

ConsoleOne allows you to perform administration tasks for NDS objects that already exist in NDS while you are at the server console.

To administer an NDS object that already exists in the tree, do the following:

1. In the left window pane, browse to and click the **NDS container** that holds the object.
2. In the right window pane, right-click the **object** you want to administer. ConsoleOne displays a pop-up menu.

Presentation**Notes****Creating NDS Objects in ConsoleOne**

- Point out that four NDS object types can be created with ConsoleOne:
 - Organization
 - Organizational Unit
 - Group
 - User



Demonstrate how to create an NDS object using ConsoleOne.

Managing NDS Objects in ConsoleOne

- Point out that NDS objects can be managed in ConsoleOne.

3. Click **Properties**.

The details of the NDS object are displayed.

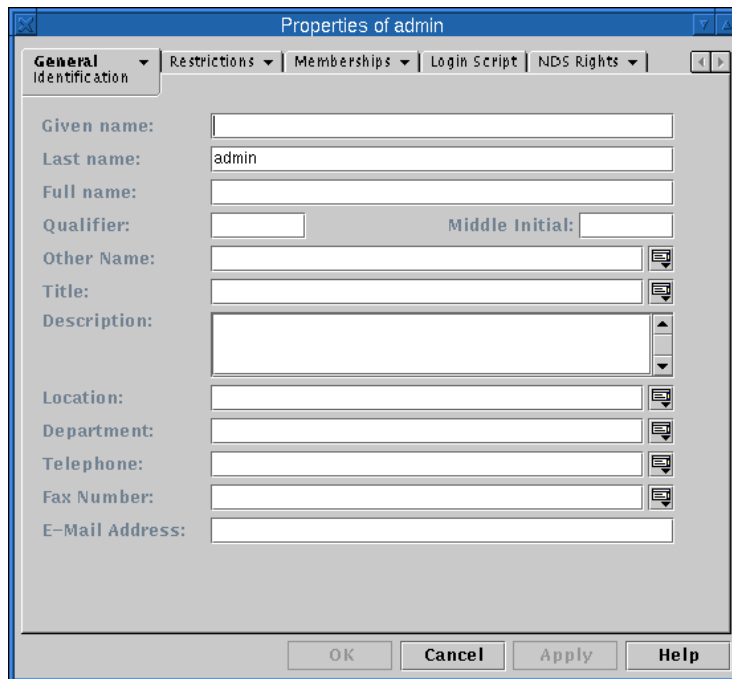


Figure 2-9: An NDS Properties Window in ConsoleOne

For convenience, ConsoleOne displays the details of an NDS object one property at a time. To view the details of another property, click the appropriate property tab.

Because an NDS property can have several details, each property tab can have multiple pages that can be viewed.

For example, each NDS object has an NDS Rights property tab. The NDS Rights property tab has a list of three NDS pages that can be viewed: Inherited Rights Filter, Effective Rights, and Trustees of this Object.

4. To view a different page of the property tab, select the **property page** you want from the drop-down list on the tab.
5. Make your modifications to the NDS property.
6. To save the changes, click **Apply**.

Presentation**Notes****Managing NDS Objects in ConsoleOne** *(continued)*

Demonstrate the following:

- How to view the properties of NDS objects in ConsoleOne.
 - How to access the properties of an object.
 - How to access different pages of a property tab.
-
- Point out that changes are saved and are in effect when the Apply button is clicked.

Customizing the ConsoleOne Interface

ConsoleOne provides a framework in which functionality is provided by components that snap in to the interface. Developers can add custom object types to the ConsoleOne interface using snap-ins.

Network administrators can customize the ConsoleOne interface by adding shortcuts to files, folders, and applets that make navigating to these objects easier.

A *ConsoleOne shortcut* is a text file that defines a file, folder, or applet to be added to the ConsoleOne interface. The name of a shortcut in ConsoleOne has the same name as the text file.

Shortcuts to Text Files

By default, ConsoleOne includes shortcuts to frequently accessed server configuration files. These shortcuts are found in ConsoleOne under the My Server | Configuration Files object.

To add your own text files to the list of files that appear under the Configuration Files object, do the following:

1. Use a text editor to create a text file containing only the path and filename of a text file.

For example, to add the NetWare GUI configuration file, type
SYS:JAVA\NWGFX\FVWM2\FVWM2RC5XX



The specified configuration file must be a local file.

2. Place the text file in the following directory:
SYS:PUBLIC\MGMT\CONSOLE1\CONFIGFILES
3. Save the text file with the name, such as GUI Config, you want it to have in ConsoleOne.



If you use a filename extension, the extension is displayed as part of the ConsoleOne shortcut object.

4. In the View menu, click **Refresh**.

Presentation**Notes****Customizing the ConsoleOne Interface**

- Point out that developers can customize ConsoleOne with snap-ins.
- Point out that administrators can customize ConsoleOne with shortcuts.
- Define *ConsoleOne shortcut*.

Note: ManageWise® is a product that adds functionality to ConsoleOne using its own snap-ins.

Shortcuts to Text Files

Demonstrate how to create a shortcut to a text file in ConsoleOne.

Note: Folders can be created under the ConsoleOne Configuration Files object by creating subdirectories in the SYS:PUBLIC\MGMT\CONSOLE1\CONFIGFILES directory.

Shortcuts to Folders

By default, ConsoleOne includes shortcuts to folders that are frequently used by administrators. These shortcuts are found in ConsoleOne under the Shortcuts | Folders object.

To add your own folder shortcuts to ConsoleOne, do the following:

1. Use a text editor to create a text file containing only the **path** of a directory.

For example, to add the Java directory, type

```
SYS:JAVA
```

2. Place the text file in the following directory:

```
SYS:PUBLIC\MGMT\CONSOLE1\SHORTCUTS\FOLDERS
```

3. Save the text file with the **name**, such as SYS_Java, you want it to have in ConsoleOne.
4. In the View menu, click **Refresh**.

Shortcuts to Applets

In ConsoleOne, creating a shortcut to launch an applet is similar to creating other shortcuts. The difference is that you are required to create a text file containing applet configuration information.



For more information regarding the syntax of applet configuration information files, see “Applet Configuration Keywords” in the online documentation.

Depending on where the applet configuration information file is saved, the applet shortcut will appear in one of two places:

- To have the shortcut appear in **My Server | Tools**, save the text file in SYS:PUBLIC\MGMT\CONSOLE1\SHORTCUTS\TOOLS.
- To have the shortcut appear in **Shortcuts | Applets**, save the text file in SYS:PUBLIC\MGMT\CONSOLE1\SHORTCUTS\APPLETS.

Presentation**Notes****Shortcuts to Folders**

- Review the steps used to create a shortcut to a folder in ConsoleOne.

Note: The rules for creating a shortcut to a text file also apply to creating a shortcut to a folder.

Shortcuts to Applets

- Point out that the applet menu items in ConsoleOne are defined using applet configuration information files.



Use a text editor to demonstrate the contents of an applet configuration information file.

- Discuss the locations for saving an applet configuration information file.
- Discuss the effects an applet configuration file will have on ConsoleOne.

Hands-On Exercise 2-4: Using ConsoleOne

In this exercise you use ConsoleOne to perform various administration tasks:

- In Part I, you perform common server administration tasks.
- In Part II, you perform NDS administration tasks.
- In Part III, you add shortcuts to customize the ConsoleOne interface.

Part I: Server Administration

1. Launch ConsoleOne.
 - a. In the NetWare GUI, click **Novell**.
 - b. Click **ConsoleOne**.
2. Use the Java editor to edit your server's AUTOEXEC.NCF file. Enable the RCONAG6.NLM command line.
 - a. In the left window pane, click the **dot** to the left of My Server.
 - b. In the left window pane, click **Configuration Files**.
 - c. In the right window pane, right-click **AUTOEXEC.NCF**.
 - d. Click **Edit**.
 - e. Find the line that reads
#LOAD RCONAG6 <your password here> 2034 16800
 - f. Remove the # sign and modify the line so that it reads
LOAD RCONAG6 novell 2034 16800
 - g. In the Java Editor File menu, click **Close**.
 - h. When asked if you want to save the file, click **Yes**.
3. Exit the NetWare GUI.
 - a. Click **Novell**.
 - b. Click **Exit GUI**.
 - c. Click **Yes**.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne



Introduce the exercise.



:20

Conduct the exercise.

4. To restart your NetWare server, enter the following:
RESTART SERVER
5. When the NetWare GUI starts again, launch ConsoleOne.
 - a. In the NetWare GUI, click **Novell**.
 - b. Click **ConsoleOne**.
6. Launch MONITOR.NLM from ConsoleOne by accessing your server's console prompt using Console Manager.
 - a. To expand the My Server object, click the **dot** to the left of the object.
 - b. To expand the Tools object, click the **dot** to the left of the object.
 - c. In the left window pane, click **Console Manager**.
 - d. In the Password field, type **novell**.
 - e. Click **Connect**.

To view the Connect button, you might need to resize the window by dragging the lower right-hand corner of the ConsoleOne utility.
 - f. Click **System Console**.

The System Console appears in its own window.
 - g. In the System Console window, enter **MONITOR**.

The server will make MONITOR the active screen.
 - h. Toggle back to ConsoleOne using **Alt + Esc**.

Notice that MONITOR does not appear in Console Manager.
 - i. To manually update Console Manager, click **Refresh**.
 - j. To open MONITOR in its own window, click **NetWare 5 Console Monitor**.
 - k. To minimize the NetWare 5 Console Monitor, click the **Down arrow** in the right-hand corner.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne *(continued)*

- Continue the exercise.

7. Access your server from within ConsoleOne using RConsoleJ.
 - a. In the left window pane, click **RConsoleJ**.
 - b. In the Server Address field, type your server's **IP address**.
 - c. In the Password field, type **novell**.



Password is case sensitive.

- d. Click **Connect**.

To view the Connect button, you might need to resize the window by dragging the lower right-hand corner of the ConsoleOne utility.
- e. To scroll through the available console screen, click the double **Right-arrow** button until you return to the System Console screen.
- f. To view all the console screens that are running on the server, click and hold down the **Server Screens** drop-down list.
- g. To make the System Console screen the active screen on the server, click **Activate**.
- h. Toggle back to ConsoleOne using **Alt + Esc**.
- i. To terminate the Remote Console session, click **Disconnect**.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne *(continued)*

- Continue the exercise.

Part II: NDS Administration

1. Use ConsoleOne to create an NDS user object in your container.
 - a. Click the **dot** to the left of the The Network object.
 - b. Click the **dot** to the left of Novell Directory Services.
 - c. In the left window pane, click the **dot** to the left of the EMA_TREE. ConsoleOne provides a login window.
 - d. Log in to the EMA_TREE as your **Admin** user object.
 - e. In the left window pane, navigate to and click your **container object**.
 - f. In the File menu, click **New**.
 - g. Click **User**.
 - h. In the Login name field, type **JCampbell**.
 - i. In the Last name field, type **Campbell**.
 - j. Click **Create**.
 - k. In the Create Authentication Secrets window, provide a new **password** for user JCampbell.
 - l. Click **OK**.
2. Use ConsoleOne to set user object JCampbell's concurrent connections to 4.
 - a. In the right window pane, right-click **JCampbell**.
 - b. Click **Properties**.
 - c. Click the **Restrictions** property tab.
 - d. If you cannot see all the fields in the Properties window, click the **Up-arrow** in the upper right corner of the window.
 - e. In the Restrictions drop-down list, click **Login Restrictions**.
 - f. Mark the **Limit Concurrent Connections** box.
 - g. In the Maximum Connections box, change the value to **4**.
 - h. Click **Apply**.
 - i. Click **Close**.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne *(continued)*

- Continue the exercise.

Part III: Customizing ConsoleOne

1. Create a shortcut to the NetWare GUI configuration file.
 - a. In the left window pane, click **Configuration Files**.
 - b. In the right window pane, right-click **Autoexec.ncf**.
 - c. Click **Edit**.
 - d. In the text editor's File menu, click **Close**.
 - e. In the empty text editor, type
SYS:\JAVAINWGF\X\FVWM2\FVWM2RC5XX
 - f. In the text editor's File menu, click **Save As**.
 - g. In the Save As field, type **NETWARE GUI**.
 - h. Browse to the **SYS:\PUBLIC\MGMT\CONSOLE1\CONFIGFILES** directory.
 - i. Click **Save**.
 - j. In the text editor's File menu, click **Exit**.
 - k. In the ConsoleOne View menu, click **Refresh**.
The NETWARE GUI menu item should appear in ConsoleOne.
 - l. Right-click **NETWARE GUI**.
 - m. Click **Edit**.
The FVWM2RC5XX file should open in the Java editor.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne *(continued)*

- Continue the exercise.

2. In ConsoleOne, create a shortcut to the SYS:\PUBLIC\MGMT\CONSOLE1 directory.
 - a. In the text editor's File menu, click **Close**.
 - b. In the empty editor, type **SYS:\PUBLIC\MGMT\CONSOLE1**.
 - c. In the text editor's File menu, click **Save As**.
 - d. In the Save As field, type **CONSOLE1**.
 - e. Browse to the following directory:
SYS\PUBLIC\MGMT\CONSOLE1\SHORTCUTS\FOLDERS
 - f. Click **Save**.
 - g. In the text editor's File menu, click **Exit**.
 - h. In the ConsoleOne View menu, click **Refresh**.
 - i. In the left window pane, click the **dot** to the left of Shortcuts.
 - j. Click the **dot** to the left of Folders.
 - k. In the left window pane, click **CONSOLE1**.
The contents of the SYS:\PUBLIC\MGMT\CONSOLE1 directory should appear in the right window pane.

Presentation

Notes

Hands-On Exercise 2-4: Using ConsoleOne *(continued)*

- Continue the exercise.

3. In ConsoleOne, create a shortcut to the clock applet under the Tools object.
 - a. In the left window pane, click the **dot** to the left of CONSOLE1.
 - b. Click the **dot** to the left of Shortcuts.
 - c. Click the **dot** to the left of Applets.
 - d. In the left window pane, click **JDK Demos**.
 - e. In the right window pane, right-click **Clock**.
 - f. Click **Edit**.
 - g. In the text editor's File menu, click **Save As**.
 - h. In the Save As field, type **Clock**.
 - i. Browse to the
SYS:\PUBLIC\MGMT\CONSOLE1\SHORTCUTS\TOOLS
directory.
 - j. Click **Save**.
 - k. In the text editor's File menu, click **Exit**.
 - l. In the ConsoleOne View menu, click **Refresh**.
 - m. In the left window pane, select **My Server | Tools | Clock**.
The clock applet should appear in the right window pane.
4. Exit the NetWare GUI.
 - a. Click **Novell**.
 - b. Click **Exit GUI**.
 - c. Click **Yes**.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 2-4: Using ConsoleOne** *(continued)*

- Review the exercise.

Note: You might want to have students disable the STARTX line from the AUTOEXEC.NCF file so that the NetWare GUI does not load in future exercises.

Accessing the Server Console from a Workstation

To obtain access to your NetWare server from your workstation, NetWare 5 includes two utilities. These two utilities are RConsoleJ and Remote Console.

Although these utilities are standalone programs, they have been integrated into the Tools menu of NetWare Administrator for easier access.

RConsoleJ

RConsoleJ can be used to gain remote access to your NetWare server text screens over an IP connection. RConsoleJ is the same Java utility that is available at the server in ConsoleOne.

To access the console screens of a NetWare 5 server over an IP connection, you must run the RConsole agent called RCONAG6.NLM on the NetWare 5 server you want to access.

The RConsole agent sets the password, TCP port, and SPX port used to gain access to the target server.

RConsoleJ can obtain access to NetWare servers running only the IPX protocol through the use of remote console proxy agents.



For more information on remote console proxy agents, see “RCONPRXY” in the online *Utilities Reference* manual.

To run RConsoleJ at the workstation do one of the following:

- Execute SYS:PUBLIC\RCONJ.EXE
- Select **Pure IP Remote Console** from the Tools menu in NetWare Administrator.

Presentation**Notes****Accessing the Server Console
from a Workstation**

- Introduce the two utilities that provide remote access to the NetWare server.

- Point out that RConsoleJ is the same Java utility available in ConsoleOne.

- Explain how to launch RConsoleJ on the workstation.

Remote Console

With RCONSOLE.EXE, you can use your workstation to reach your server console over SPX and asynchronous connections. You can execute console commands and load and unload NLMs just as you would at the actual server console.

Remote console management consists of both server and workstation pieces. To set up a remote console, complete the following tasks:

1. Set up the server for Remote Console.
2. Execute Remote Console software at the workstation.

Setting Up the Server for Remote Console

You can establish a remote console connection over the network (LAN connection) or over a modem (asynchronous connection).

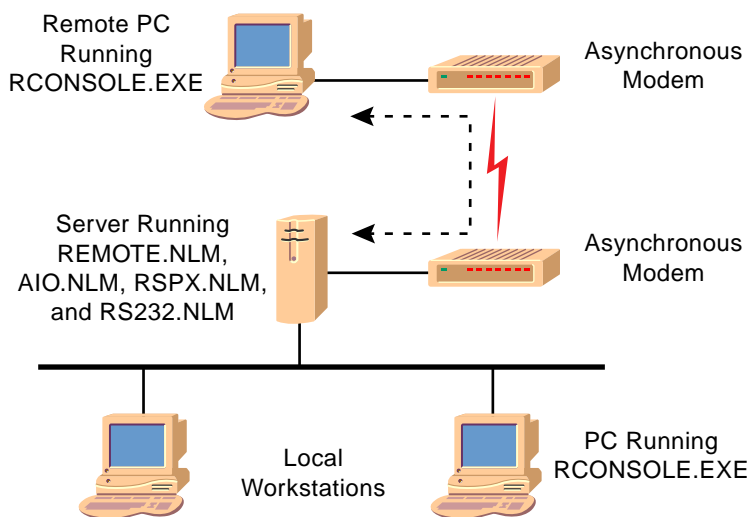


Figure 2-10: Network and Asynchronous Remote Console Connections

Presentation**Notes****Accessing the Server Console from a Workstation** *(continued)*

- Introduce the components of remote console management.
- Explain how to use RCONSOLE.

Emphasize that Remote Console (RCONSOLE.EXE) can be used only with servers running NetWare 3 and above.

Only users who know the REMOTE.NLM password can access the NetWare server console with RCONSOLE.EXE.

Setting Up the Server for Remote Console

2-4 (Figure 2-10: Network and Asynchronous Remote Console Connections)

- Explain LAN connections to the server.
- Explain asynchronous connections to the server.
- Explain performance differences between a LAN connection and an asynchronous connection.

Just like any other network activity, a LAN connection affects network traffic on the network cable. It does not greatly affect server utilization.

An asynchronous connection affects server utilization. For this reason, we recommend that asynchronous connections not be used during peak hours.

Each type of connection, LAN or asynchronous, requires different NLMs to be loaded at the server.

You can automate setting up the server for a LAN or asynchronous connection by adding the appropriate commands to the server's AUTOEXEC.NCF file.

Setting Up a LAN Connection

To establish a network remote console connection, you must load the following NLMs at the server:

- REMOTE.NLM
- RSPX.NLM

REMOTE.NLM manages the information exchange with workstations that are accessing the server remotely.

RSPX.NLM provides communications support and advertises the server's availability for remote access.

Setting Up an Asynchronous Connection

An asynchronous remote connection requires the following NLMs to be loaded at the server:

- REMOTE.NLM
- RS232.NLM
- AIO.NLM

The RS232.NLM and AIO.NLM initialize the NetWare server's communication port and transfers screen and keystroke information to and from REMOTE.NLM.

In addition, both the workstation and the server must have modems for an asynchronous connection. You might need to complete additional steps beyond those listed here to configure the modem.

Presentation**Notes****Setting Up the Server for Remote Console** *(continued)*

- Continue discussing setting up the server for Remote Console.

Setting Up a LAN Connection

- Discuss the software components for a LAN connection.



Demonstrate how to load the remote console software needed to establish a LAN connection.

Setting Up an Asynchronous Connection

- Discuss the software components needed for an asynchronous connection.
- Point out the need to have and configure a modem.



Demonstrate how to load the asynchronous software.

Executing the Remote Console Software

RCONSOLE.EXE is executed at the DOS prompt of the workstation. It is found in the SYS:PUBLIC directory of a NetWare server. It must reside locally on the workstation using an asynchronous connection.

You can also launch Remote Console from within NetWare Administrator by selecting Remote Console from the Tools menu.

To access the server from a workstation on the network, do the following:

1. In the Connection Type menu, select **LAN**.
2. From the list of Available Servers, select the **server** you want.
3. Enter the remote console **password**.

To connect the server over a modem, do the following:

1. In the Connection Type menu, select **Asynchronous**
2. In the Asynchronous Options menu, select **Connect To Remote Location**.
3. Enter the remote console **password**.

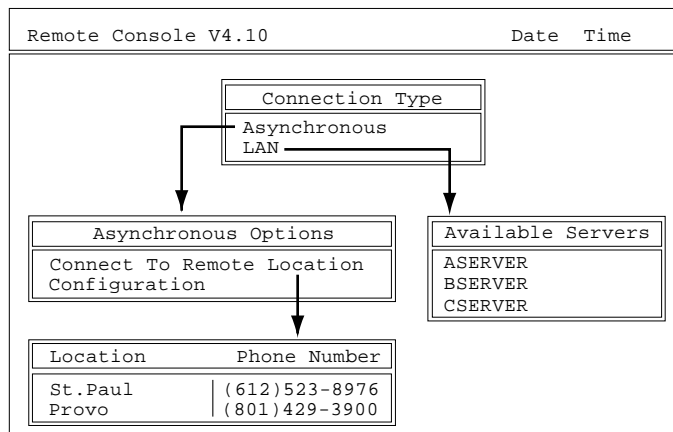


Figure 2-11: RCONSOLE Menus

Presentation**Notes****Executing the Remote Console Software**

2-5 (Figure 2-11:
RCONSOLE Menus)



Demonstrate how to load
RCONSOLE.

Make sure you have loaded REMOTE and RSPX (in that order) at the server console. Then you can run RCONSOLE at your workstation. Also be aware of rules for using remote management screens and menus.

Note: When you select to launch Remote Console from within NetWare Administrator, it launches it through the NWRCON.PIF file.

Because Remote Console is a DOS executable, the NWRCON.PIF file is set to warn you that you should exit Windows before running Remote Console.

If you want to configure the NWRCON.PIF file so that the warning message goes away, do the following:

1. Flag the SYS:PUBLIC\NWRCON.PIF file with a read/write attribute.
2. In Windows Explorer, view the properties of the NWRCON.PIF file.
3. Click the **Program** tab.
4. Click **Advanced**.
5. Click **Prevent MS-DOS-based programs from detecting Windows**.
6. Unmark **Suggest MS-DOS mode as necessary**.
7. To save the settings, click **OK**.
8. To close the Properties window, click **OK**.

When you have established the RCONSOLE session, your workstation screen will display the current server screen. From here, you can perform all tasks available at the server console.

In addition to completing standard console activities, you can complete the following tasks with RCONSOLE:

- Change screens.
- Scan server directories (including the server's DOS partition).
- Transfer files to the server.
- Change to DOS to view network directories.

You can perform these tasks with the RCONSOLE Available Options menu (Figure 2-12).

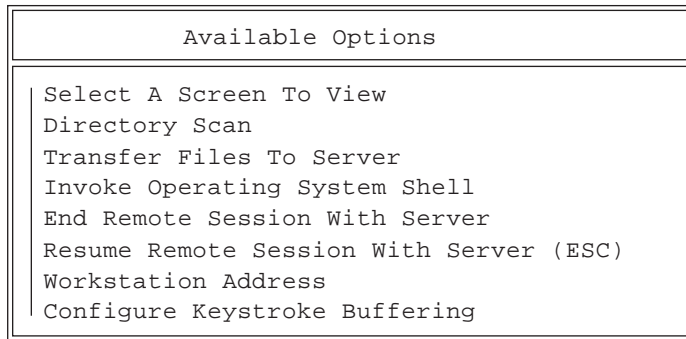


Figure 2-12: RCONSOLE Available Options

Additionally, you can complete some tasks with one or two keystrokes. Table 2-1 lists the function keys available in RCONSOLE.

Purpose	Keys
View the Available Options menu.	Alt+F1
Quit the Remote Console Session.	Alt+F2
Move forward through server console screens.	Alt+F3
Move backward through server console screens.	Alt+F4
Display the network and workstation address.	Alt+F5
Resume the remote session with the server.	Esc

Table 2-1: RCONSOLE Function Keys

Presentation**Notes****Executing the Remote Console Software** *(continued)*

Display the RCONSOLE Available Options menu.



Demonstrate and explain the function of each menu option.



Demonstrate and explain the function keys available in RCONSOLE.

Protecting Your Server

Because networks are such an important part of business, it is important that you protect the server and its data from unauthorized use or tampering.

You can physically protect your server in these ways:

- Lock up the server.
- Use the SECURE CONSOLE command.
- Prevent access to the server keyboard using the console locking feature in SCRSAVER.NLM.
- Add a password to remote console agents (this is required).

Locking Up the Server

One of the strongest features of NetWare is its security system. However, the software running on the server can only be as secure as the physical server.

Keeping the server in a safe place is critical to preventing unauthorized access.

The most secure way to keep a server safe is to lock the server in a room or closet to which access is restricted. You can also lock the server keyboard (if this option is available with the hardware).

Secure Console

The NetWare SECURE CONSOLE console command prevents unauthorized users from loading NLMs outside of the SYS:SYSTEM directory and from changing the date and time on the server.

Presentation**Notes**

Protecting Your Server

- Emphasize that the server needs to be secured.

Locking Up the Server

- Discuss the importance of physically locking up the server.

Secure Console



Demonstrate how to execute the **SECURE CONSOLE** command.

SCRSAVER.NLM

You can use the SCRSAVER.NLM to add a password and prevent any unauthorized keyboard entry at the console.

The SCRSAVER.NLM brings up a screen saver on the console screen that locks the console. When a key on the keyboard is pressed, the user is prompted to authenticate as an NDS user to gain access to the console prompt.

The SCRSAVER.NLM supports many parameters. To see what parameters are supported, enter the following at the server console:

SCRSAVER HELP

Loading Remote Console Agents with a Password

To help prevent unauthorized access to the server console, both RCONAG6.NLM and REMOTE.NLM require a password in order to be loaded. If no password is provided at the time you load a remote console agent, you will be prompted to provide one.

You can automate the loading of the remote console agent from the AUTOEXEC.NCF or from any other NCF file. Both remote console agents support password encryption, which prevents someone from reading the password out of an NCF file.

An encrypted password is a string of characters, generated using a remote console agent, that represent the actual password.

To load a remote console agent with an encrypted password, you must complete two steps:

1. Generate an encrypted password.
2. Load the agent using the encrypted password.

Presentation**Notes****SCRSAVER.NLM**

Demonstrate how to use the SCRSAVER.NLM.

Note: MONITOR.NLM no longer has the ability to lock the console keyboard. This function is now performed by SCRSAVER.NLM.

Loading Remote Console Agents with a Password

- Point out that both remote console agents require a password.
- Explain that both agents support password encryption.
- Explain that an encrypted password is represented by a string of characters.
- Introduce the steps required to use an encrypted password with a remote console agent.

RCONAG6.NLM

To load RCONAG6.NLM, enter the following at the server console prompt:

RCONAG6 *password TCPport SPXport*

If you execute RCONAG6 without providing any parameters, you will be prompted for a password, TCP port number, and SPX port number.

An RCONAG6 command line is placed in the AUTOEXEC.NCF file when NetWare is installed. The command line is disabled by default. RCONAG6 will not load from the AUTOEXEC.NCF file unless the command line is enabled.

To have the RCONAG6.NLM generate an encrypted password, do the following:

1. At the server console prompt, enter

RCONAG6 ENCRYPT

2. When prompted, provide a *password*.
3. When prompted, provide a *TCP port number*.
4. When prompted, provide an *SPX port number*.

RCONAG6.NLM displays the command to use the encrypted password.

You will be asked if you want to place the command in an NCF file.

5. To place the command into SYS:\SYSTEM\LDRCONAG.NCF, respond with **Yes**.
6. If you are executing RCONAG6 from a different NCF file and just need the encrypted password, write down the encrypted password so that you can place it into the appropriate NCF file.

To use an encrypted password, execute the following from the server console:

RCONAG6 -E *encrypted password TCPport SPXport*

To see all the supported RCONAG6 parameters, enter

RCONAG6 /?

Presentation**Notes****Loading Remote Console Agents
with a Password** *(continued)*

- Discuss the syntax for loading RCONAG6.NLM.



Demonstrate how to encrypt a password using RCONAG6.NLM.

Note: Be sure to save the command line to SYS:SYSTEM\LDRCONAG.NCF.

For added security, the LDRCONAG.NCF file can be renamed and placed into a different directory.

REMOTE.NLM

To load the REMOTE.NLM, enter the following at the server console prompt:

REMOTE *password*

If you do not provide a password with the command, NetWare will request a password.

You can place the REMOTE command with a password in the AUTOEXEC.NCF file to automate the process.

To have REMOTE.NLM generate an encrypted password, do the following:

1. At the server console prompt, enter

REMOTE ENCRYPT



ENCRYPT must be capitalized!

2. When prompted, provide a password.

REMOTE.NLM will display the command to execute in order to use the encrypted password.

You will be asked if you want to place the command in an NCF file.

3. To place the command in SYS:\SYSTEM\LDREMOTE.NCF, respond with **Yes**.
4. If you are executing REMOTE from a different NCF file and just need the encrypted password, write down the encrypted password so that you can place it in the appropriate NCF file.

To use an encrypted password, execute the following from the server console:

REMOTE -E *encrypted password*

To see all the supported REMOTE.NLM parameters, enter

REMOTE /?

Presentation**Notes****Loading Remote Console Agents
with a Password** *(continued)*

- Discuss the syntax used to load REMOTE.NLM.



Demonstrate how to encrypt a password using REMOTE.NLM.

Note: Be sure to save the command line to SYS:SYSTEM\LDREMOTE.NCF.

For added security, the LDREMOTE.NCF file can be renamed and placed into a different directory.

Hands-On Exercise 2-5: Accessing and Securing the Server Console Remotely

In this exercise, you access the server console using RCONSOLE.EXE from your workstation and secure the server console using SCRSAVER.NLM and the SECURE CONSOLE command.

Complete each of the following tasks.

1. Load remote console support on your NetWare server. At your NetWare server, enter the following:
REMOTE <password>
RSPX
2. From your workstation, do the following:
 - a. Log in to your server as your **Admin** object.
 - b. Open NetWare Administrator.
 - c. In the Tools menu, click **Remote Console**.
 - d. After reading the warning message, press **Enter** to continue.
 - e. Select **LAN**.
 - f. In the Available Servers menu, select **your server**.
 - g. Enter the password you provided when you loaded REMOTE.NLM on your server.

Presentation

Notes

Hands-On Exercise 2-5: Accessing and Securing the Server Console Remotely



Introduce the exercise.



:20

Have the students complete the exercise.

3. Try the following RCONSOLE keystrokes and describe what they do.
 - a. Press **Alt + F1**.

 - b. Press **Esc**.
 - c. Press **Alt + F2**.

 - d. Press **Esc**.
 - e. Press **Alt + F3**.

 - f. Press **Alt + F4**.

 - g. Press **Alt + F5**.

 - h. Press **Esc**.

Hands-On Exercise 2-5: Accessing and Securing the Server Console Remotely

(continued)

- Review answers.

Answers:

- 3a. Press **Alt+F1** to bring up the Available Options menu.
- 3c. Press **Alt+F2** to bring up the RCONSOLE Exit menu.
- 3e. Press **Alt+F3** to toggle through the running NLM screens in reverse order of what they would appear when toggling through them while actually at the console using Alt + Esc.
- 3f. Press **Alt+F4** to toggle through the running NLM screens in the same order as they would appear when toggling through them while actually at the console using Alt+Esc.
- 3g. Press **Alt+F5** to display the workstation address of the machine from which you are running RCONSOLE.

4. Use RCONSOLE to load SCRSAVER on your NetWare server.
 - a. Press **Alt + F1**.
 - b. Select **Select a Screen to View**.
 - c. Select **System Console**.
 - d. At the server console prompt, enter
SCRSAVER ACTIVATE
 - e. To stop the screen saver, press **any key**.
 - f. Enter the **fully distinguished name** of your Admin object.
 - g. Because your admin user has no password, press **Enter**.
 - h. To authenticate, press **Enter**.
5. Use RCONSOLE to secure your NetWare server.

At the console prompt, enter
SECURE CONSOLE

You should see a message stating that the console is secure.
6. Exit RCONSOLE.
 - a. Press **Alt+F2**.
 - b. In the Quit Remote Console Session menu, select **Yes**.
 - c. Press **Esc**.
 - d. To affirm your choice, select **Yes**.
7. Bring down your server and reboot it.
 - a. At the console prompt, enter
DOWN
 - b. When the DOS prompt appears, turn off the machine.
 - c. Turn on the machine.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 2-5:
Accessing and Securing the
Server Console Remotely***(continued)*

- Review the exercise.

Note: If students failed to let the NetWare installation update their AUTOEXEC.BAT file, they will need to manually start their server by executing C:\NWSERVER\SERVER.EXE.

Summary

In this section you learned about the basic software components needed to start a NetWare server. The section discussed the server start-up procedure, which initializes SERVER.EXE, disk drivers, and LAN drivers. Finally, it discussed the creation of batch files, such as STARTUP.NCF and AUTOEXEC.NCF, which are used to automate the server start-up procedure.

Server utilities are executed from the server console. They are classified as either console commands or NetWare Loadable Modules (NLMs).

Console commands, part of the NetWare core operating system, are used to monitor or control server activity; NLMs add functionality to the NetWare kernel.

These commands and utilities are controlled at the server. A remote management utility allows you to control the server's console from a workstation. As network administrator, you can remotely perform tasks that must otherwise be completed at the server.

The JAVA.NLM allows you to run Java classes and applets. Java applications requiring a GUI run on top of an X-Windows implementation on the NetWare platform.

Using the ConsoleOne GUI interface, you can perform NetWare server and NDS administration tasks from your server's console.

Protecting your server is an important administrative task. You can use the SCRSAVER.NLM, a password for REMOTE, and the SECURE CONSOLE command to help protect your valuable investment. You should also consider providing physical security for the server by placing the server in a secured room.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objective:

1. Describe the function of a NetWare server and its interface, and identify the server components.
2. Execute server console commands and navigate the server console using hot keys.
3. Load and unload NetWare Loadable Modules (NLMs).
4. Identify and describe server configuration files.
5. Customize the server by editing the appropriate configuration files.
6. Create server script files to automate the execution of console commands.
7. Load Java application support on the NetWare 5 server.
8. Launch Java programs and applets from the NetWare GUI.
9. Manage NetWare from the server using ConsoleOne.
10. Describe remote console management; use various utilities to remotely manage the console.
11. Describe security strategies for a NetWare server; implement console security.

Notes

2-64

SECTION 3 Setting Up Queue-Based Network Printing

Duration 02:00

Preparation

None

SECTION 3

Setting Up Queue-Based Network Printing

In this section, you will learn how to set up network printing by defining NDS printing objects, bringing up a print server, and connecting a printer to the network. You will also learn how to perform basic network printing maintenance by managing print jobs in the print queue and modifying the queue users and notification lists.

Objectives

Upon completing this section, you should be able to

1. Set up a network printing environment by creating and configuring related print queue, printer, and print server objects.
2. Set up network printing hardware by bringing up a print server on a NetWare 5 server and connecting a printer to the network through a NetWare server or workstation.
3. Regulate who can do any of the following: print to a print queue, manage print jobs in the print queue, be notified by a printer when a problem occurs, view the status of the print server, or manage the print server.
4. Manage the flow of print jobs into and out of a print queue by managing the status of the print queue.
5. Manage print jobs in a print queue by pausing, rushing, delaying, and deleting print jobs in the print queue.

Presentation

Notes

Setting Up Queue-Based Network Printing

- Introduce the section.

Objectives

- Present the section objectives.

Network Printing Setup Overview

Queue-based printing comprises printers, print queues, and print servers. (Figure 3-1 reviews the queue-based printing environment.) The queue-based printing setup process includes steps to configure the logical (NDS objects) and physical pieces of each component.

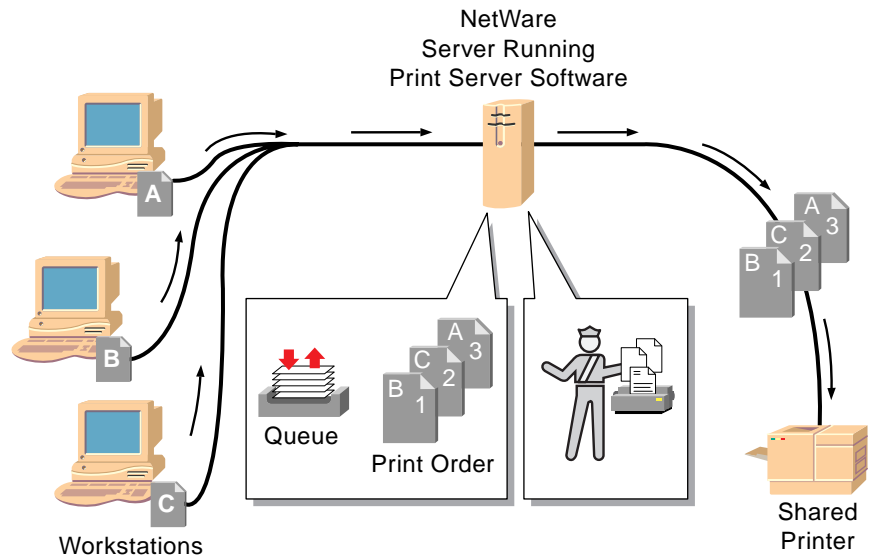


Figure 3-1: Network Printing Environment

To set up queue-based print services, you must complete the following tasks:

- Create and configure printing objects.
- Activate the print server.
- Connect printers to the network.

Each of these steps is discussed in detail in this section. A flow chart detailing the steps in setting up network printing is found at the end of this section. Additionally, this section discusses managing network printing and creating print job configurations.

Network Printing Setup Overview

- Review the network printing environment.



3-1 (Figure 3-1: Network Printing Environment)

- Provide an overview of the print services setup process.

Point out the major steps.

- Create and configure printing objects.
The network administrator uses NetWare Administrator to create and configure the print services objects.
- Activate the print server.
The network administrator selects the NetWare server to run the print server software and modifies the NetWare server's AUTOEXEC.NCF file to automatically load the print server software.
- Connect printers to the network.
The network administrator selects the NetWare servers and workstations where the network printers will be located, attaches the printers, and executes the proper utilities.

Creating and Configuring Printing Objects

You must create NDS objects to access the physical print server, print queues, and printers.

The graphic below shows the network printing objects and the properties required to set up functional network printing. It also shows the logical connection between the print queue, printer, and print server objects.

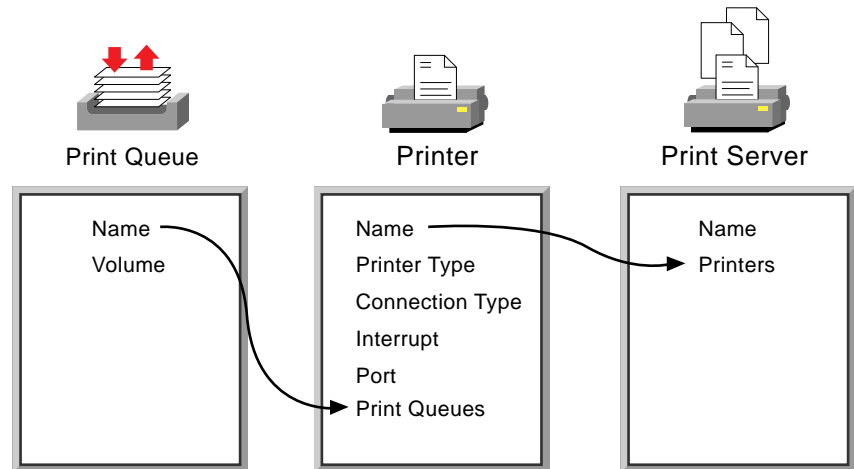


Figure 3-2: Network Print Objects and Critical Properties

Critical Properties

Each printing object is assigned critical properties. These properties enable basic network printing to occur.

You must understand each of these properties and know their corresponding values to set up a network printing environment.

Creating and Configuring Printing Objects

- Discuss creating the network printing objects.



3-2 (Figure 3-2: Network Print Objects and Critical Properties)

Critical Properties

- Explain critical properties.

The properties to point out are as follows:

- NDS objects must be created for the print queue, printer, and print server before the physical objects are accessible.
- Critical properties for each object are required.
- The Name property of a print queue object is added to a printer object's print queues property list to indicate that the print queue is serviced by the printer.
- The Name of a printer object is added to a print server object's Printer Property list to indicate that the printer object is managed by the print server.

Each printing component has properties that are required to enable network printing. Each printing component has additional properties that expand the functionality of the printing environment or are used to manage network printing. These additional properties are discussed later in this section.

Print Queue Critical Properties

A print queue object requires two critical properties: a name and a print queue volume on which the print queue directory will reside. To configure a print queue object, do the following:

1. Create and name the print queue object.
2. Identify the volume on which the print queue will be stored.

The print queue's name is used to link the print queue to a printer.

Printer Critical Properties

You must define several properties to create a functional printer object. These properties include the name, printer type, printer port, interrupt, and connection type. The following selections are the most common choices; however, other choices are available.

- Printer type: Parallel, Serial, AppleTalk®, or UNIX®
- Printer port: LPT or COM
- Interrupts: Use Interrupts or Polled mode
- Connection Type: Auto Load or Manual Load

Polled mode is the default setting for interrupts. However, a dedicated interrupt usually provides better printing performance.

If you do not know what interrupt to set or if you are having interrupt conflicts, try using the Polled mode. A polled mode printer might not be as fast as an interrupt-driven printer, but it avoids the difficulty of identifying an available interrupt and the conflicts that can arise from choosing an incorrect interrupt.

To configure a printer object, do the following:

1. Create and name the printer object.
2. Enter the critical properties.
3. Assign a print queue to the printer.



For more information on printer properties, see the online documentation.

Presentation**Notes****Print Queue Critical Properties**

- Discuss the critical properties of the print queue object:
 - Print queue name
 - Print queue volume

Printer Critical Properties

- Define the critical properties of the printer object:
 - Printer name
 - Printer type
 - Printer port
 - Interrupt
 - Connection type
- Compare polled mode and dedicated interrupt.
- Discuss the basic steps in creating a printer object.

The printer object can be created by simply specifying its name. However, the printer object must be configured to match the physical device that it represents.

The default configuration uses the following:

- Printer type: Parallel
- Port: LPT1
- Interrupts: Polled
- Connection Type: Manual Load (Remote from Print Server)

Print Server Critical Properties

The print server object requires a name and the names of the printer objects it manages. To configure a print server, do the following:

1. Create and name the print server object.
2. Add printers to the print server object's Printer List property.

Printing Object Creation Steps

The steps you use to create and configure the printing objects are summarized below:

1. Create the print queue object.
Identify the volume on which the print queue will reside.
2. Create the printer object.
 - Configure the properties to match the physical device the printer object represents.
 - Assign a print queue to the printer.
3. Create the print server object (this is optional if one already exists).
4. Add the printer to the print server object's Printer List property.



You need to gather critical information (such as the print queue volume name, connection type, type, interrupt, and port) before creating the objects.

Presentation**Notes****Print Server Critical Properties**

- Discuss the critical properties of the print server object:
 - Print server name
 - Names of printer objects

- Discuss the basic steps in creating a print server object.

The print server object can be created by specifying its name. It will not be functional until the printers that it will manage are identified. The printers are added to the print server's Printer List property.

Printing Object Creation Steps

- Discuss the steps required for setting up simple network printing.

- Emphasize the importance of gathering critical information before creating the objects.

Creating Printing Objects in NetWare Administrator

The objects used in network printing are created and modified with NetWare Administrator.

The print server object contains a Print Layout window that allows you to graphically view the relationship between the print server, printers, and print queues. Additionally, the Print Layout window provides status information on each of the network printing components.

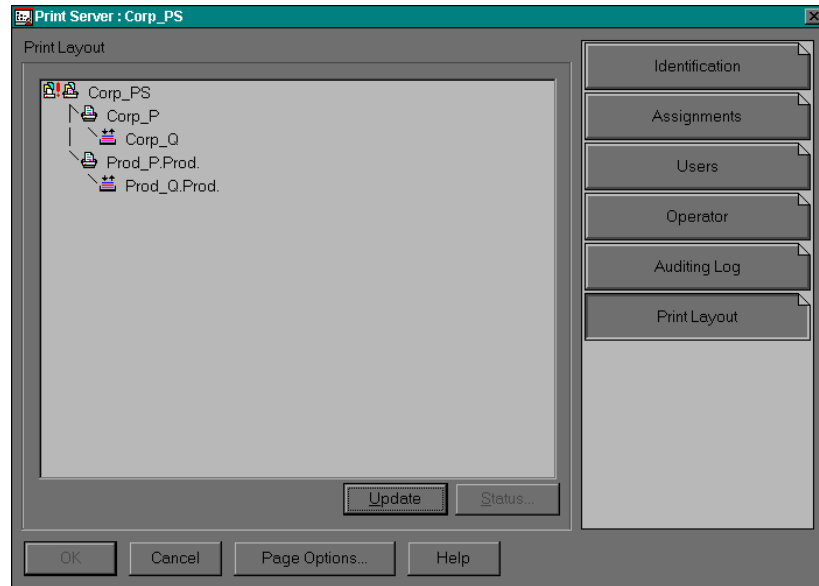


Figure 3-3: Print Layout Window in NetWare Administrator

Presentation**Notes****Creating Printing Objects in NetWare Administrator**

- Discuss using NetWare Administrator to create and manage print services.



Demonstrate how to create the print services objects with NetWare Administrator.



3-3 (Figure 3-3: Print Layout Window in NetWare Administrator)

- Discuss the Print Layout window.



Demonstrate how to use the Print Layout window.

The Print Layout window only works for print setups using a NetWare print server. It does not work for third-party print servers or printers connected directly to the network with their own print servers.

Performing a Quick Setup

You can use the Print Services Quick Setup option in NetWare Administrator to easily create the NDS print services objects and configure the basic properties necessary for setting up functional network printing.

Quick Setup provides a default name for each object; however, you can change the name. Quick Setup adds the print queue to the printer's list of print queues and adds the printer to the print server's list of printers.

Finally, Quick Setup provides default definitions for the printer type, connection type, interrupt, and port. These properties should be modified to match your printer definition.

To set up network printing objects using Quick Setup, do the following:

1. In the Tools menu in NetWare Administrator, click **Print Services Quick Setup (Non-NDPS)**.
2. In Print Server Name, type a ***name*** for this print server object.
3. In Printer Name, type a ***name*** for this printer object.
4. In Printer Type, type or select a ***printer type***.
After you specify a printer type, a dialog box specific to your printer type is displayed.
5. Complete the dialog box for your printer type.
6. In Print Queue Name, type a ***name*** for this print queue object.
7. In Print Queue Volume, type a ***name*** for this print queue volume (or browse to select a volume).
8. Click **Create**.

Performing a Quick Setup

- Discuss Quick Setup.

Initially, Quick Setup creates and configures a print server object named *PS_container* (where *container* is the name of the current NDS organization or organizational unit) if a print server does not exist.

Otherwise, it chooses the first print server in the container (print servers are listed alphabetically).

Quick Setup also creates a printer object named P1 and a print queue object named Q1. It places the printer object on the print server object's Printer Property list and the print queue object on the print object's Print Queues Property list.

Additionally, Quick Setup places the print queue object on the first volume found in the current container.

Quick Setup can be used to add a printer to the same context as an existing print server.

The utility will recognize an existing print server within the context and use it. It will also recognize printers with the default printer names and go to the next number; for example, if P1 exists, it will add P2 as the printer name.

Quick Setup is limited in the following ways:

- All objects are placed within the same context.
- Existing objects cannot be edited.
- Some object properties cannot be edited.



Demonstrate how to use Quick Setup.

Activating the Print Server

The physical print server is activated when the print server NLM (PSERVER.NLM) is loaded on a NetWare server.

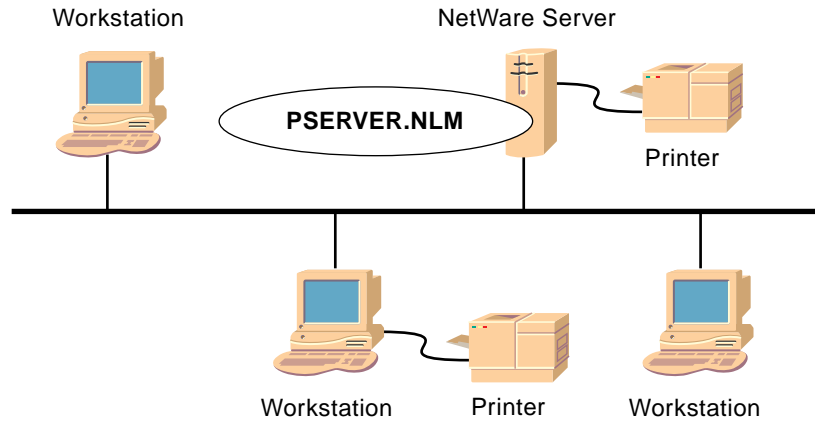


Figure 3-4: Print Server Software Running on a NetWare Server

If the print server and the NetWare server are in different contexts, you must include the print server's context in the LOAD statement.

For example, if you have a print server, Corp_PS, in the context OU=CORP.OU=NYC.O=EMA, and the server is in a different context, OU=ACCT.OU=NYC.O=EMA, you must enter the following at the server prompt:

```
LOAD PSERVER .Corp_PS.CORP.NYC.EMA
```

Activating the Print Server



3-4 (Figure 3-4: Print Server Software Running on a NetWare Server)



Demonstrate and discuss the LOAD procedure.



Demonstrate how to add the LOAD command to the NetWare server's AUTOEXEC.NCF file.

- Point out how PSERVER.NLM uses the print objects.

To add the print server service to a NetWare server, you must load PSERVER.NLM. PSERVER.NLM does not greatly impact the performance of the NetWare server.

The basic command syntax is shown below:

LOAD PSERVER *printservername*

To automate this procedure, you can add the LOAD command to the server's AUTOEXEC.NCF file.

PSERVER.NLM uses the print server name provided in the LOAD command to locate the print server object in NDS.

PSERVER.NLM reads the print server object's property values into server memory. The Printers property is used to locate all printer objects serviced by this print server.

The printers' property values are read and the Queues property of each printer object is used to locate the print queue objects in NDS.

The print queue object's property values are read and the print queue volume and directory are located. With this information, the print server manages each print queue and sends print jobs to the correct printer.

Note: If the network administrator makes changes to the print services objects after the print server has been loaded, the print server might not recognize the changes. If so, PSERVER must be reloaded.

Connecting a Printer to the Network

A network printer can be attached to any NetWare server or any Windows 95 workstation. It can also be connected directly to the network cable.



How a directly attached printer is configured depends on the printer. Consult your printer's documentation for details.

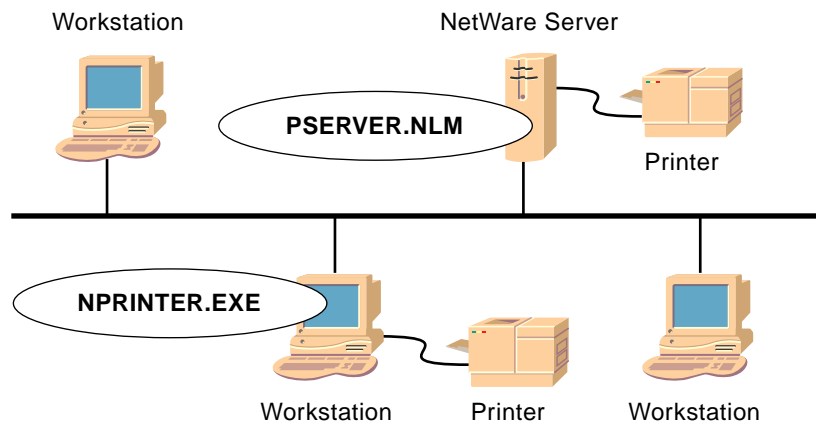


Figure 3-5: Connecting a Network Printer with NPRINTER

Generally, to make a printer available for network printing, you need to do the following:

1. Connect the printer cable to the NetWare server or workstation.
2. Create a printer object in NDS.
3. Activate the print server software.
4. Run NPRINTER.

These steps vary, depending on where the printer is attached.



When you choose the type of network printer connection, either a NetWare server or a workstation, you should also gather the critical property information for the printer.

Connecting a Printer to the Network



3-5 (Figure 3-5: Connecting a Network Printer with NPRINTERR)

- Point out how NPRINTERR makes a printer available as a network printer.
- Discuss the basic steps involved in connecting a printer to the network.
- Point out that the steps vary depending on where the printer is attached.

The transparency illustrates the following:

- A network printer can be attached to the print server or to any NetWare server by running NPRINTERR.NLM on the server.
- A network printer can be attached to a Windows 95 workstation by running NPTWIN95.EXE on the workstation.

When NPRINTERR is loaded at a NetWare server or a workstation, it advertises the printer name you provide and the network address of the NetWare server or workstation.

The print server responsible for this printer can then communicate with the printer and send print jobs based on the printer object information, such as printer port, interrupt, and printer buffer size.

Printer Connected to	NPRINTERR Type	Load
Print server	NLM	Auto or Manual
NetWare server not running PSERVER	NLM	Manual
Workstation	EXE	Manual

Activating a Printer Attached to the Print Server

To make a printer attached to the print server available for network printing, do the following:

1. Connect the printer cable to a port on the print server.
2. Create a printer object configured as Auto Load (Local).
3. Activate the print server software.



PSERVER.NLM will automatically load NPRINTER.NLM for any printer with the Location property defined as Auto Load (Local).

Activating a Printer Not Attached to the Print Server

To make a printer attached to a NetWare server other than the print server available for network printing, do the following:

1. Connect the printer cable to a port on the NetWare server.
2. Create a printer object configured as Manual Load (Remote).
3. Activate the print server software.
4. Load the network printer software on a NetWare server not running PSERVER.NLM by entering the following command at the server console:

LOAD NPRINTER *printservername printername*

Replace *printername* with the name of the printer object.

To automatically load NPRINTER.NLM on a NetWare server not running PSERVER.NLM, include the LOAD statement in the NetWare server's AUTOEXEC.NCF file.

Presentation**Notes****Activating a Printer Attached to the Print Server**

- Explain how NPRINTER.NLM is loaded on the print server.

Activating a Printer Not Attached to the Print Server

- Explain how to load NPRINTER.NLM on a NetWare server other than the print server.



Demonstrate how to load NPRINTER on a NetWare server.

NPRINTER.NLM should auto-load when PSERVER.NLM is loaded.

Activating a Printer Attached to a Windows 95 Workstation

To make a printer attached to a Windows 95 workstation available for network printing, do the following:

1. Connect the printer cable to a port on the workstation.
2. Create a printer object configured as Manual Load (Remote).
3. Activate the printer server software for the server.
4. Execute NPTWIN95. This activates NPRINT for Windows 95 (NetWare NPRINT Manager). In the Add Network Printer window, select the printer object that will print to the printer.

To make the connection permanent, mark the **Activate printer when Nprinter Manager loads** box. Otherwise, the printer will only be loaded for the current NPRINT Manager session.

Presentation

Notes

Activating a Printer Attached to a Windows 95 Workstation

- Explain how to execute NPTWIN95 on a Windows 95 workstation.

Hands-On Exercise 3-1: Setting Up Network Printing

In this exercise, you create and configure network printing objects, connect a local printer to the network, and send a print job to that printer.

This exercise is divided into two parts:

- Part I: Setting Up Network Printing in General
- Part II: Setting Up Network Printing in Windows 95



Do not delete objects created in this exercise; they will be used in the next exercise.

Presentation**Notes****Hands-On Exercise 3-1:
Setting Up Network Printing**

- Introduce the exercise.

- Prepare for the exercise.

- Explain the procedures for the exercise.



:20

Have the students complete the exercise.

By now students have been introduced to the main utilities of printing: PSERVER.NLM and NPRINT. They should also have seen a demonstration in which print queue, print server, and printer objects were created.

Do the following:

- Provide the students with the information they need to configure their printer objects.

- Read through the main steps in the procedure with students. Explain any modifications needed for your classroom setup.

- Encourage students to complete the exercise using only the numbered steps.

- Inform students if printers are not available for this exercise.

Part I: Setting Up Network Printing

1. Gather the following information from your instructor:

Printer Type	
Printer Interrupt	
Printer Port	

2. Log in as your **Admin** object.
3. Create a print queue object.
 - a. Click your department's **organizational unit**.
 - b. To initiate object creation, press **Ins**.
 - c. Select the **Print Queue** object; then click **OK**.
 - d. In the Print Queue Name field, type **Class_Q**.
 - e. In the Print Queue Volume field, click the **Select Object** button.



- f. Double-click your **FSx_DATA** volume object (under the Available Objects window).
 - g. Click **Create**.
4. Create a printer object.
 - a. Click your department's **organizational unit**.
 - b. To initiate object creation, press **Ins**.
 - c. Highlight the **Printer (Non NDPS)** object; then click **OK**.
 - d. In the Printer Name field, type **Class_P**.
 - e. Click **Define Additional Properties**.
 - f. Click **Create**.

Presentation

Notes

**Hands-On Exercise 3-1:
Setting Up Network Printing**
(continued)

- Help students if necessary.

5. Define Class_P according to the printer information you gathered in Step 1.
 - a. Click **Configuration**.
 - b. Change the Printer Type to the correct **type** according to the information gathered in Step 1.
 - c. Click **Communication**.
 - d. Change the **Port** and **Interrupts** fields to the values gathered in Step 1.
 - e. Set the Connection Type to **Manual Load (Remote from Print Server)**.
 - f. Click **OK**.
6. Assign the new print queue Class_Q to the Class_P printer.
 - a. Click **Assignments**.
 - b. Click **Add**.
 - c. Double-click the **Class_Q** object you created in Step 3.
 - d. Click **OK**.
7. Create your own print server object.
 - a. Click your department's **organizational unit**.
 - b. Press **Ins**.
 - c. Highlight the **Print Server (Non NDPS)** object and click **OK**.
 - d. In the Print Server Name field, type **Class_PS**.
 - e. Click **Create**.
8. Assign the Class_P printer to the print server.
 - a. Double-click the **Class_PS** print server object.
 - b. Click **Assignments**.
 - c. Click **Add**.
 - d. Double-click **Class_P**.
 - e. Click **OK**.

Presentation

Notes

**Hands-On Exercise 3-1:
Setting Up Network Printing**
(continued)

- Help the students if necessary.

9. Exit NetWare Administrator.



If there is only one printer in the classroom, you must take turns loading NPTWIN95.EXE.

Part II: Setting Up Network Printing in Windows 95

Complete the following steps:

1. Bring down and turn off your workstation.
2. Plug the printer into your workstation.
3. Turn on the workstation and log in as your Admin object.
4. Execute NPTWIN95 from the PUBLIC\WIN95 directory.
5. Click the **Browse** button for the NDS printer.
6. Select your printer from the available objects.
7. Click **OK**.
8. Send a print job to the printer.
9. If a printer is available, view the completed print job. If no printer is available, confirm that the print job arrived at the print queue.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 3-1:
Setting Up Network Printing**
(continued)

- Review the exercise.

Managing Network Print Services

The following basic network printing management tasks are covered in this section:

- Managing the print queue
- Managing the printer
- Managing the print server

Managing the Print Queue

Print queue management includes the following tasks:

- Controlling the print queue work flow
- Managing print jobs in the print queue
- Controlling access to the print queue

Controlling the Print Queue Work Flow

The flow of print jobs into and out of a print queue can be controlled in three ways:

- Stop print jobs from entering the queue.
- Stop print jobs from leaving the queue.
- Stop new print servers from adding print jobs to the queue.

Figure 3-6 shows the operator flags that regulate work flow into and out of the print queue. (Operator flags are located on the identification page of the print queue object.)

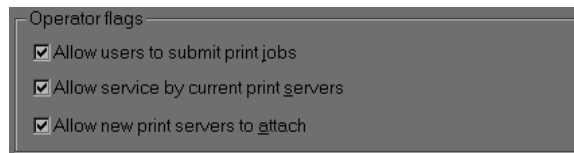


Figure 3-6: Print Queue Operator Flags

Presentation**Notes****Managing Network Print Services**

- Introduce network printing management.

Managing the Print Queue

- Introduce print queue management.

Controlling the Print Queue Work Flow

- Explain what the network administrator can do with Queue Status.
- Discuss three ways to control queue status.



3-6 (Figure 3-6: Print Queue Operator Flags)



Demonstrate how to modify the Print Queue Operator flags.

Remind the students that a print queue is a directory that holds a print job before it is sent to a network printer. The network administrator or print queue operator can control how print jobs are sent to the print queue and what happens to the print jobs in the print queue.

The network administrator or print queue operator can control movement of print jobs into and out of the print queue. Queue status provides information about how the print queue is being used. Specifically, it indicates how many jobs are in the queue and how many print servers are currently sending print jobs to the print queue.

Managing Print Jobs in the Print Queue

A print job can be managed while it is in the queue. You can manage print jobs in the Print Queue Job List by

- Changing the order of print jobs in a print queue
- Viewing the print jobs in a print queue
- Deleting print jobs from a print queue
- Placing a print job on hold in the print queue
- Identifying and modifying the print job attributes

Figure 3-7 shows the Print Queue Job List.

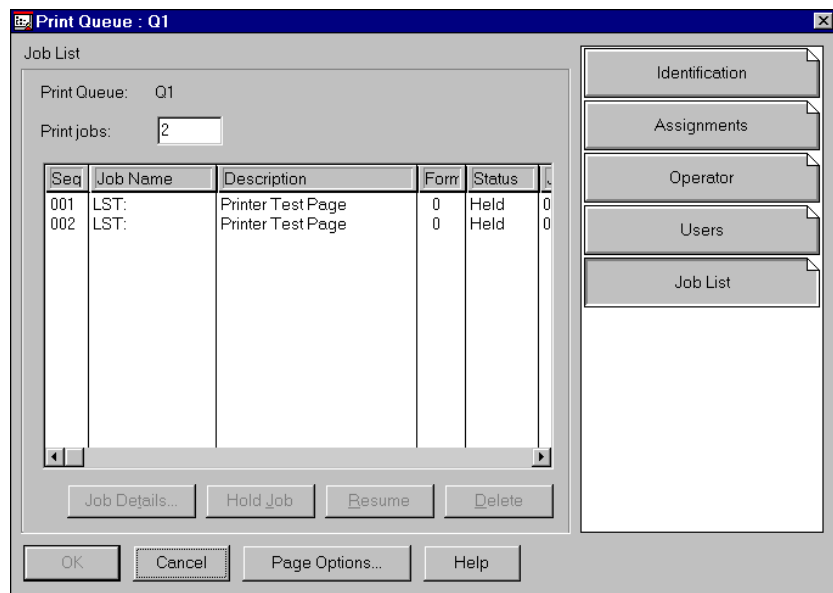


Figure 3-7: Current Print Queue Job List

You can use the Job Details button in the print queue window to customize your print job. Figure 3-8 illustrates what details are available to you through this option.

Presentation**Notes****Managing Print Jobs in the Print Queue**

3-7 (Figure 3-7: Current Print Queue Job List)

- Introduce the concept of managing print jobs in the print queue.
- Discuss each task on the student page.



Demonstrate tasks from the student page.

Steps:

1. Stop print jobs from leaving the print queue.
2. Send several print jobs to the print queue.
3. Manage the print jobs in the print queue.

Figure 3-8 shows the Print Job Detail window.

The screenshot shows the 'Print Job Detail' window with the following fields and options:

- Print job: 01805301
- File size: 43994
- Client: RussC
- Description: Printer Test Page
- Status: Print job has user hold
- User hold
- Operator hold
- Service sequence: 1
- Number of copies: 1
- File contents:
 - Byte stream
 - Text
 - Tab size: []
- Form feed
- Notify when job is printed
- Entry date: 1 / 2 / 96
- Entry time: 1 : 23 : 39 PM
- Form: []
- Print banner
 - Name: LST:
 - Banner name: RussC
- Defer printing
- Target date: / /
- Target time: : :

Figure 3-8: Print Job Detail Window

Controlling Access to the Print Queue

You can regulate access to the print queue in the following ways:

- Identify who can send print jobs to the print queue.
- Identify who can manage print jobs in the print queue.

To allow a user to send print jobs to the print queue, add the user to the Print Queue Users list. A print queue user can manage his or her print jobs in the print queue.

You can add a user to the Print Queue Operators list to allow the user to change the order of print jobs, edit other users' jobs, delete jobs, and change the print queue flags.

When a print queue object is created, some objects are automatically assigned to the Print Queue Users and Print Queue Operators lists. For details, see "Default Assignments" later in this section.

Presentation**Notes****Managing Print Jobs in the Print Queue** *(continued)*

3-8 (Figure 3-8: Print Job Detail Window)

Controlling Access to the Print Queue

- Discuss how to control access to the print queue.
- Point out how controlling access to the print queue controls access to the printer.
- Define *print queue operator* and *print queue user*.



Demonstrate how to create print queue users and operators.

Managing the Printer

Network printer management includes the following tasks:

- Viewing and controlling the printer status
- Managing printer error messages

Viewing and Controlling the Printer Status

The Printer Status window can give you important information about the printer, such as whether it is active, not connected, or out of paper. Additionally, you can make the following printer status changes to an active printer:

- Change service mode for forms
- Mount form
- Pause, stop, and start printer
- Select form feed
- Mark top of form
- Abort print job

These printer management tasks can be performed at the print server console or from a workstation using the NetWare print utilities.

Managing Printer Error Messages

When an error occurs on the printer, the printer sends out error messages. To identify users who will receive printer error messages, add users to the printer object's Notify list.

Managing the Print Server

To manage a print server, you need to complete the following tasks:

- View the print server status.
- Bring down the print server.
- Assign print server users and operators.

Presentation**Notes****Managing the Printer**

- Introduce printer management tasks.

Viewing and Controlling the Printer Status

Demonstrate how to view and modify the printer status.

Managing Printer Error Messages

Add a user to the Notify list.

Managing the Print Server

- Introduce print server management tasks.

Viewing Print Server Status

The following information can be displayed in the print server object using NetWare Administrator:

- Print server version
- Number of printers it supports
- Current status (Running or Down)
- Advertising name

Bringing Down the Print Server

You can bring down or unload a print server in the following ways:

- Unload the PSERVER.NLM at the NetWare server console.
- Click the Unload button on the print server object identification page in NetWare Administrator.

Assigning Print Server Users and Operators

A print server user can view print server status information, but cannot perform print server management tasks. To make a user a print server user, add him or her to the Print Server Users list.

A print server operator can perform tasks such as attaching other NetWare servers to the print server or bringing down the print server. To make a user a print server operator, add the user to the Print Server Operators list.

When you create the print server object, some assignments to the Print Server Users and Print Server Operators lists occur automatically. For details, see "Default Assignments" later in this section. You must add any other print server operators.

Presentation**Notes****Viewing Print Server Status**

Demonstrate how to view print server status.

Bringing Down the Print Server

Discuss the process of bringing down a print server.



Demonstrate how to bring down a print server.

Assigning Print Server Users and Operators

Define *print server operator* and *print server user*.



Demonstrate how to create print server users and operators.

**Network Printing
Management Summary**

Table 3-1 shows the printing capabilities granted to different types of users.

Task	A	PQO	PQU	PNL	PSO	PSU
Create and delete printer, print queue, and print server objects	X					
Modify print queue and print server user and operator lists	X					
Modify print queue assignments	X	X				
Modify the Notify list	X				X	
Modify printer status					X	
Modify print queue operator flags		X				
Use print queues			X			
Manipulate others' print jobs in print queue		X				
Manipulate own print jobs in print queue			X			
Receive printer error messages				X		X
Monitor print server	X					X
Bring down print server					X	

A	Administrator of container	PNL	Printer Notify List
PQO	Print Queue Operator	PSO	Print Server Operator
PQU	Print Queue User	PSU	Print Server User

Table 3-1: Printing Capabilities Granted to User Types

Presentation

Notes

Network Printing Management Summary

- Discuss the information in Table 3-1.

Default Assignments

When the printing objects are created, some objects are automatically added to the various printing lists. The following table summarizes the default assignments made when printing objects are created.

Print Queue Object	PQO	PQU
Creator of print queue	X	X
Parent container		X

Print Server Object	PSO	PSU
Creator of print server	X	
Parent container		X

PQO	Print Queue Operator List	PSO	Print Server Operator List
PQU	Print Queue User List	PSU	Print Server User List

Table 3-2: Default Print Queue and Print Server Assignments

Presentation

Notes

Default Assignments

- Discuss the information in Table 3-2.

Hands-On Exercise 3-2: Managing Network Printing

In this exercise, you manage access to network printing and manage print jobs in the print queue.

Complete the following network printing management tasks from NetWare Administrator.

1. Log in as your **Admin** object.
2. Launch Network Administrator.
3. Allow a user in your container to receive error messages from the printer.
 - a. Double-click the **Class_P** object you created.
 - b. Click **Notification**.
 - c. Click **Add**.
 - d. Locate and double-click the **user object** you want to make a print queue operator.
 - e. Click **OK**.
4. Verify that each user in your container can use the printer you set up in Exercise 3-1.
 - a. Double-click **Class_Q**.
 - b. Click **Users**.
 - c. Verify that your container is listed.
 - d. Click **Cancel**.

Presentation**Notes**

Hands-On Exercise 3-2: Managing Network Printing

- Introduce the exercise.

- Encourage students to complete the exercise using only the numbered steps.

:30



Have students complete the exercise.

5. Allow a user in your container to manage other users' print jobs in the print queue.
 - a. If you closed the Print Queue Object Details window, double-click the **Class_Q** object you created.
 - b. Click **Operator**.
 - c. Click **Add**.
 - d. Locate and double-click the **user object** you want to make a print queue operator.
6. Stop print jobs in the print queue from being sent to a printer.
 - a. Click **Identification**.
 - b. Click the **Allow Service By Current Print Servers** operator flag line. (The mark within the box disappears.)
 - c. Click **OK**.
7. Send multiple print jobs (at least two) to the print queue.
 - a. Capture your **print queue**.
 - b. Activate Notepad.
 - c. Create a small text file.
 - d. Send this file to print.
8. View the print jobs in the print queue.
 - a. If you closed the print queue object Details window (in NetWare Administrator), double-click the **Class_Q** object you created.
 - b. Click the **Job List** page button.
9. Place your *first* print job on hold.
 - a. Click the first **print job entry**.
 - b. Click **Hold Job**.

Presentation

Notes

**Hands-On Exercise 3-2:
Managing Network Printing**
(continued)

- Assist students as needed.

10. View and record the status of this print job.
 - a. Click the ***print job entry***.
 - b. Click **Job Details**.
Status:
11. Defer the printing of your *first* print job to another time.
Click **Defer Printing**.
12. Record the default **Target Date** and **Target Time** parameters.
Target Date:
Target Time:
13. Why do you think a default date and time are given?

14. Record the ***service sequence number*** of your *first* print job.
Sequence number:
15. Exit the Print Job Details window of your first print job.
Click **OK**.
16. Make your *last* print job the first print job in the Print Jobs list.
 - a. Click the last ***print job entry***.
 - b. Click **Job Details**.
 - c. Type **1** in the Service Sequence field.
 - d. Click **OK**.
17. Record the new order of your print jobs.

18. To delete your print jobs, highlight each print job and click **Delete**.
19. Allow print jobs in this print queue to be sent to the printer (reverse Step 6).
 - a. Click the **Identification** button.
 - b. Click the **Allow Service By Current Print Servers** operator flag.
(A mark appears within the box.)
 - c. Click **OK**.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 3-2:
Managing Network Printing**
(continued)

- Assist students as needed.

Answers:

10. Status indicates that the job is being held.

12. Answers vary.

13. A default date ensures the file will print. NetWare Administrator sets the target date and time to the date and time the print job entered the print queue. PCONSOLE sets the print date and time to the next day at midnight.

14. Answers vary.

17. The last job is now first.

- Review the exercise.

Utility Summary

Table 3-3 summarizes tasks that can be completed with each NetWare printing utility

Utility	Function
NetWare Administrator	Create and manage printing objects. Display the logical layout of network printing.
NPTWIN95 (EXE)	Use a printer attached to a Windows 95 workstation as a network printer.
NPRINTER (NLM)	Use a printer attached to a NetWare server as a network printer.
PSERVER (NLM)	Provide network print services; move print jobs from a print queue to a network printer; manage printers and print servers.

Table 3-3: Utility Summary

Presentation**Notes****Utility Summary**

- Briefly discuss the utility summary.

If students need to review the printing utilities, consider reading definitions at random and having students identify the utilities.

Of course, this activity works best with new network administrators who need a great deal of review to grasp concepts. If students seem confident, skip the review. Students can read the summary on their own.

Summary of the Print Services Setup Tasks

The following flowchart provides a summary of the network printing services setup tasks.

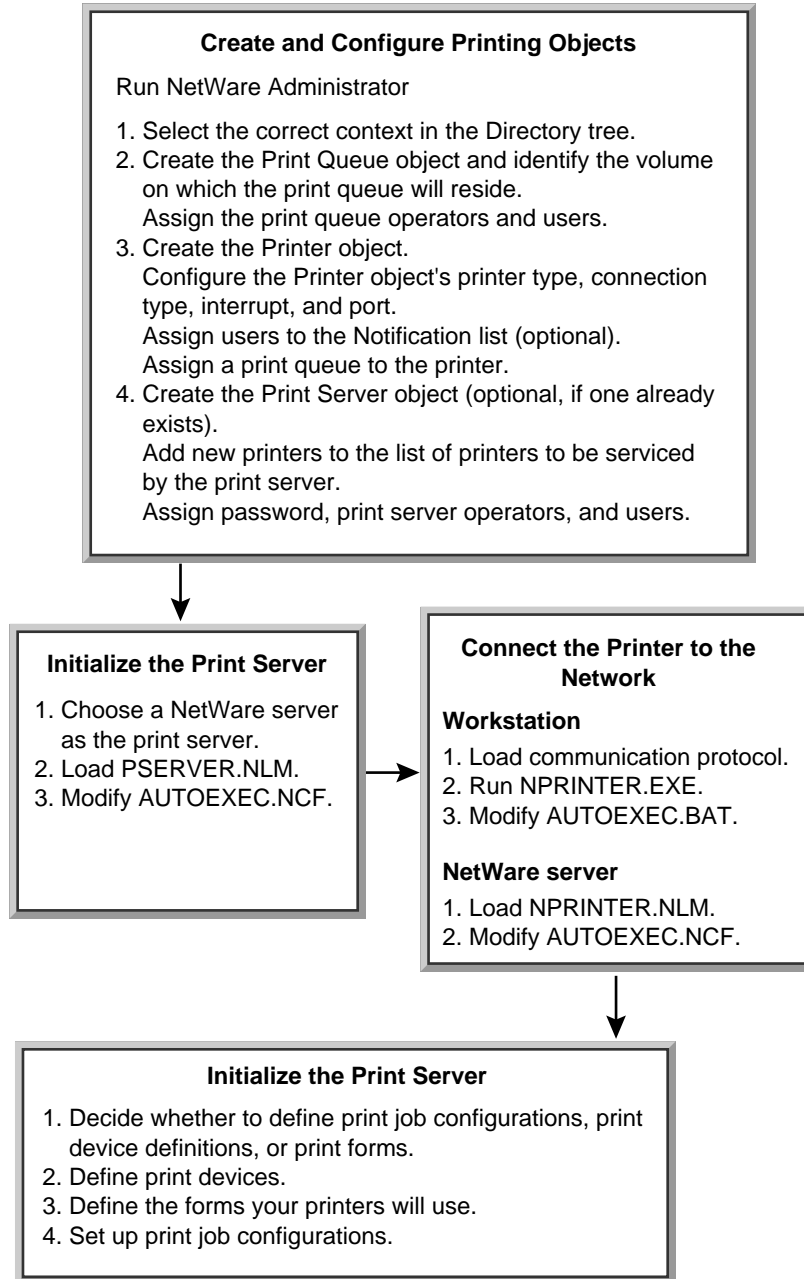


Figure 3-9: Printing Setup Flowchart

Summary of the Print Services Setup Tasks



3-9 (Figure 3-9: Printing Setup Flowchart)

- Review the flowchart with the students.

Summary

NetWare provides a complete set of queue-based print services. You can define the print services to meet your organization's needs.

The basic steps you follow to set up the queue-based print services include these:

- Create and configure print services objects.
- Set up the print server.
- Set up the network printer.
- Customize the print services environment.

The queue-based print services elements include print queue, printer, and print server objects. Each of these NDS objects is a logical representation of the corresponding physical device.

The print server is a NetWare server running PSERVER.NLM. The printers can be attached to NetWare servers or workstations. Printers can also be directly connected to the network cable. NPRINTSERV is used to activate the network printer.

Using NetWare Administrator, you can manage network printing through the print queue, printer, and print server objects and their properties.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Set up a network printing environment by creating and configuring related print queue, printer, and print server objects.
2. Set up network printing hardware by bringing up a print server on a NetWare 5 server and connecting a printer to the network through a NetWare server or workstation.
3. Regulate who can do any of the following: print to a print queue, manage print jobs in the print queue, be notified by a printer when a problem occurs, view the status of the print server, or manage the print server.
4. Manage the flow of print jobs into and out of a print queue by managing the status of the print queue.
5. Manage print jobs in a print queue by pausing, rushing, delaying, and deleting print jobs in the print queue.

Notes

SECTION 4 Setting Up the Network File System

Duration 02:00

Preparation

None

SECTION 4 Setting Up the Network File System

In this section, you learn how to design and set up a network file system.

In addition, you learn how to design and set up a volume using Novell Storage Services™ (NSS), an optional file system in NetWare 5.

Objectives

Upon completing this section, you should be able to

1. Explain guidelines for planning and creating custom volumes in the network file system.
2. List the system-created directories; describe their contents and function.
3. List suggested directories for organizing the file system.
4. Identify the strengths and weaknesses of sample directory structures.
5. Design and create a directory structure based on a given scenario.
6. Describe the advantages, disadvantages, and storage concepts of the Novell Storage Services (NSS) file system.
7. Create an NSS volume on your server.

Presentation

Notes

Setting Up the Network File System

- Briefly introduce the section.

Objectives

- Introduce the objectives.

Planning and Creating a Customized Network File System

A network file system allows users to share file storage devices. As a result, users can share applications and data through the network file system; they can also store their personal files. Network file systems are usually faster and have a larger capacity than local storage systems.

The NetWare file system is composed of volumes and directories (see Figure 4-1).

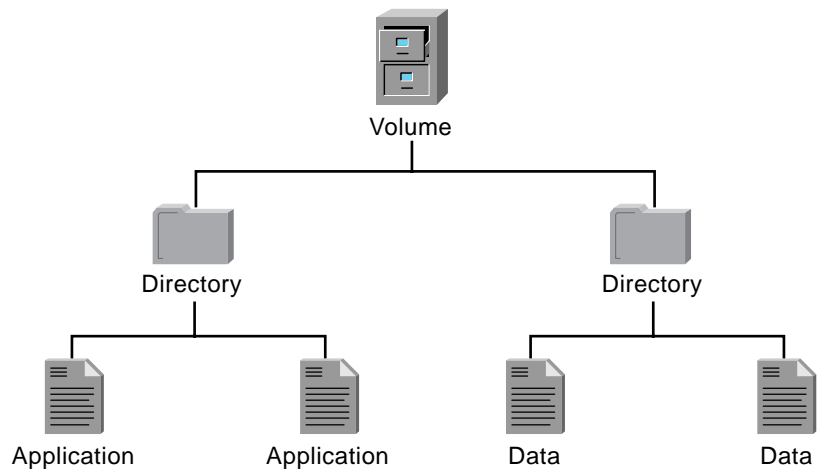


Figure 4-1: NetWare File System

In NetWare, some volumes and directories are created automatically. Others must be planned and created by the network administrator.

Your system needs and capabilities will determine how you use the system-created directories and what other directories you will create.

In general, you should plan your file system based on these three goals:

- Ease of use
- Ease of administration
- Ease of enforcing file system security

Planning and Creating a Customized Network File System

- Stress the importance of file systems.
- Introduce Novell Storage Services (NSS).



4-1 (Figure 4-1: NetWare File System)

- Review the file system structure, as illustrated in Figure 4-1.
- Ensure that students know that NetWare directories appear as “folders” in Windows and Macintosh workstations.
- Point out the benefits of creating a directory structure that is easy to use, administer, and keep secure.

The file system should not be overly complex or nonintuitive for you or your network users to follow. In addition, the layout of the file system and the names of directories and volumes should suggest who within the organization is likely to have access rights.

This section provides the following information and guidelines for planning and implementing a network file system:

- Suggestions on creating volumes
- Information on system-created directories
- Suggestions on creating directories
- Possible directory structures



For more information on planning the file system, see “File System Information” in the NetWare 5 online documentation.

Planning and Creating a Customized Network File System *(continued)*

- ❑ Point out that file system security can affect a directory structure.

Suggestions on Creating Volumes

The volume is the basic component of the NetWare file system and should be planned first. Volumes are created during server installation. Additional volumes can be created as needed after installation.

Follow these guidelines when planning NetWare volumes:

- Reserve volume SYS for the NetWare files and create one or more additional volumes for application and data files.

If your network includes workstations using an operating system (such as Windows 95 or Macintosh) that allows long filenames, you might create separate volumes to store each operating system's type of files.

This is especially useful if, for example, your Macintosh users do not need to share files with your DOS users or OS/2 users. If those users do share files, however, you might want to load the Macintosh name space on all volumes shared by the users. This would eliminate the need to create separate volumes.

- Enable name space capability on NetWare volumes used by workstations requiring long filenames.
- If fault tolerance is more important than performance, create one volume per disk.
- If both performance and fault tolerance are important, you can have the volume span multiple hard disks, but you should duplex each hard disk.
- Consider naming volumes with descriptive names. For example, if a volume will primarily hold applications, that volume could be named APPS.

Planning and creating NetWare volumes is outside the scope of this course; more details are provided in Course 580, Service and Support.

Presentation**Notes****Suggestions on Creating Volumes**

- Discuss the importance of planning volumes.
- Briefly discuss the guidelines.
- Provide more detail about using separate volumes for different operating systems.

If asked about fault tolerance, respond while avoiding detailed explanations.

System-Created Directories

During installation, NetWare automatically creates several directories and files on volume SYS, such as the ones shown in Figure 4-2.

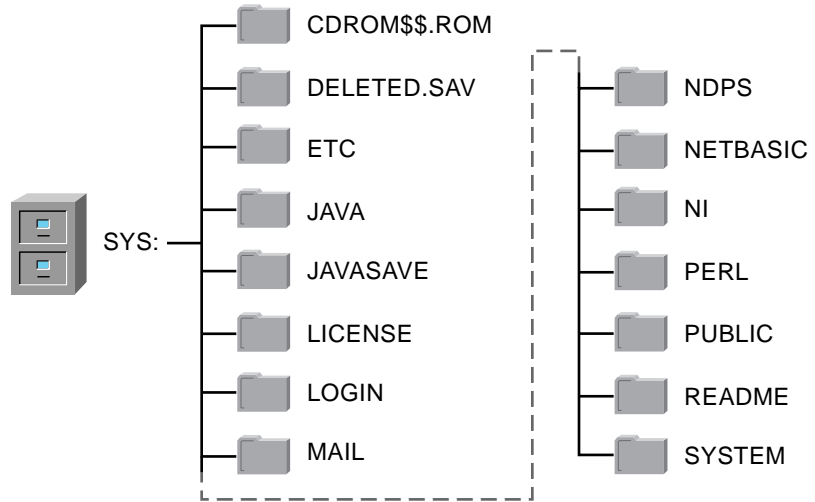


Figure 4-2: System-Created Directories

Directories created by NetWare are used to maintain normal server and network operations. These directories should not be deleted, moved, or renamed.



If you delete a system-created directory, you could have severe operational problems with NetWare.

System-Created Directories



4-2 (Figure 4-2:
System-Created Directories)

- Emphasize that system-created directories should never be deleted.

- Discuss the system-created directories and their contents, as shown in the figure.

The graphic emphasizes that during installation NetWare creates specific directories that are important to the functioning of the server.

List the contents of these directories as you discuss them.

The **LOGIN** directory is a directory available to a user before the login process occurs.

The **PUBLIC** directory contains all the NetWare commands executed by network users. These commands are covered throughout this course. Examples include NWADMN32 and NWBACKUP32.

The **SYSTEM** directory contains the NLMs necessary for server startup and supervisory commands for network administrators.

Note: Students tend to confuse volume SYS with the SYSTEM directory.

Table 4-1 gives a description of each directory shown in the graphic.

Directory	Description
CDROM\$.ROM	Contains index for mounted CD-ROM.
DELETED.SAV	Contains deleted files which have not been purged from directories that have been removed.
ETC	Contains sample files to help configure the server for TCP/IP protocols.
JAVA	Stores Java support-related files.
JAVASAVE	Contains Java-related files.
LICENCE	Contains license-related files.
LOGIN	Contains the programs necessary for logging in.
MAIL	May or may not contain subdirectories or files.
NDPS	Contains Novell Distributed Print Services.
NETBASIC	Contains NetBasic [®] support files.
NI	Contains NetWare installation files.
PERL	Stores PERL script-related files.
PUBLIC	Holds the NetWare commands and utilities available to network users.
README	Holds README files.
SYSTEM	Stores files used by the NetWare operating system or by the network administrator. The SYSTEM directory holds NLMs and files specific to the NetWare server.

Table 4-1: System-Created Directories

System-Created Directories

(continued)

- Continue discussing system-created directories and their contents.

The **DELETED.SAV** directory is created by the system during installation. Deleted files from a directory that has been removed are stored in DELETED.SAV until the files are purged or salvaged.

Deleted files of existing directories are stored in their respective directories until the files are purged or salvaged.

The **ETC** directory is created during installation and contains sample files to assist the network administrator in configuring the server.

The **MAIL** directory might be empty. If the network administrator upgrades his or her server from a previous version of the NetWare operating system, existing users will still have subdirectories here for their login scripts and print job configuration files.

Login scripts and print job configuration information become properties of the new user object during server upgrade.

If the network administrator creates new users after upgrading, the new users will not have directories in the MAIL directory.

Students might also see a **TEMP** directory which holds temporary files used by NetWare.

No corresponding page in student manual

Presentation**Notes****System-Created Directories***(continued)*

- Summarize and review system-created directories.

- Point out that students should never move system-created directories such as PUBLIC, LOGIN, and SYSTEM.

This warning is repeated several times because network administrators must be aware of the consequences of deleting (or moving) these directories.

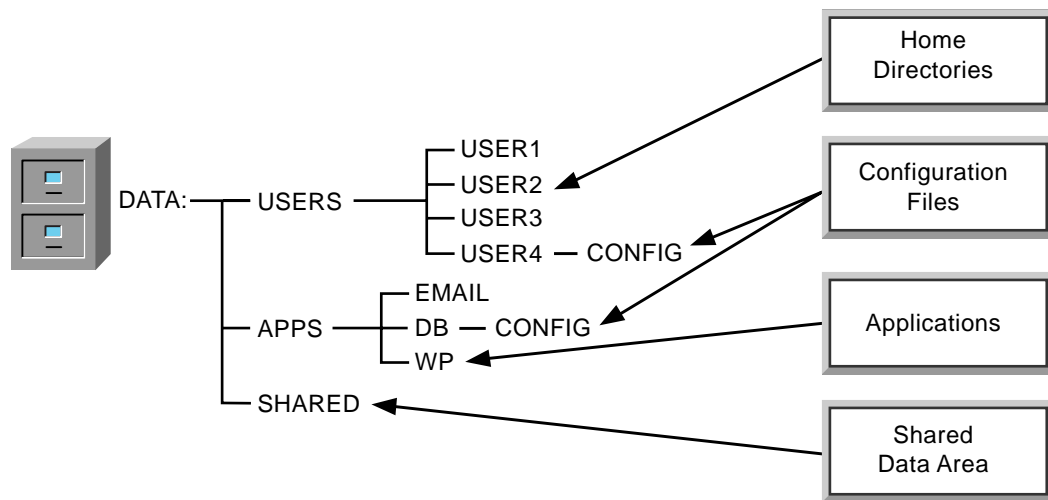


Figure 4-3: Suggested Directories

Suggestions on Creating Directories to Organize the File System

As network administrator, you need to create efficient directory structures for your network environment. We recommend that you use the following types of directories to organize individual files in the directory structure:

- Home directories
- Z.E.N.works™ profile directories
- Application directories
- Shared data directories

Consider using descriptive names for directories so that their purpose and content are easy to determine.

Suggestions on Creating Directories to Organize the File System



4-3 (Figure 4-3: Suggested Directories)

- Discuss the directory structure shown in Figure 4-3.

- Introduce the suggested directories:
 - Home directories
 - Z.E.N.works profile directories
 - Application directories
 - Shared data directories

Suggested directories are defined on the next page.

Home Directories

You should provide each user with a *home* directory in which to store individual user-created files. The home directory is often named after the user's login name for uniformity and ease in creating login scripts.

Usually, individual users are given full access to their own directories so that they can manage (create, delete, modify, move, and copy) their own files.

You can create a *parent* directory, such as the USERS directory in the Figure 4-3, to hold all the user home directories.

Application Directories

Application directories contain the application program files (.EXE, .BAT, and .COM files) and establish security over the application files. No user-created data files should be stored here.

You can create a *parent* directory, such as the APPS directory, to hold all the subdirectories containing individual applications.

A user must be given access to an application directory to use the application. User-created data files generated using the applications are usually *not* kept here.

Home directories can be used to store user-created files. The network administrator could also create various data directories for data files. (This is an important distinction to draw for the students; many times they are not aware that application and data files are separate entities.)

Shared Data Directories

You can create shared data directories so that groups of users can share information. You can also use these directories to ensure data security; you can grant or restrict users' rights to these directories.

Presentation**Notes****Home Directories**

- Define *home* directories.
- Point out the naming convention.
- Remind students that home directories can be created automatically when users are created.

Application Directories

- Define *application* directories.

Shared Data Directories

- Discuss *shared data* directories.
- Summarize reasons for creating the suggested directories.

A shared data directory allows groups of users to share information.

Possible Directory Structures

Directory structures vary depending on individual and organizational needs. There are few absolute right or wrong directory structures. Instead, directory structures

- Are either well adapted or poorly adapted to the current data storage needs of the organization
- Represent or do not represent an optimal mix of trade-offs in the areas of
 - Ease of use
 - Ease of administration
 - Ease of maintaining file system security

In addition, a directory structure often mirrors the type of information kept on the system. You should create each level of the directory structure after considering what information users need.

We recommend that you evaluate several potential directory structure designs before creating one for your organization.

Possible directory structures are illustrated on the following pages.

Possible Directory Structures

- Explain that directory structures reflect an organization's network needs.

- Ask students to think about and interpret the sample directory structures they see in this section as if they were professional file system consultants.

One-Volume Directory Structure

The figure below illustrates one possible directory structure for a company. Note that all these directories are organized under one volume.

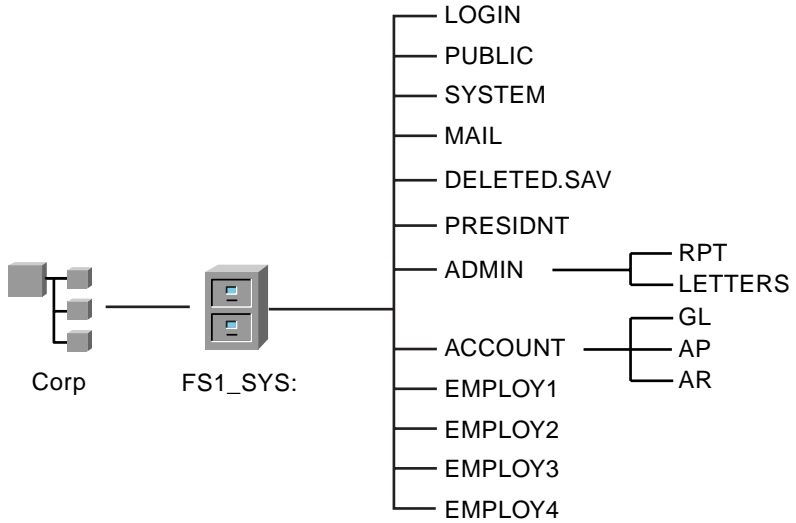


Figure 4-4: Sample One-Volume Structure

List the advantages and disadvantages of this structure in the table below.

Advantages	Disadvantages

Table 4-2: Advantages and Disadvantages of a One-Volume Directory Structure

Presentation**Notes****One-Volume Directory Structure**

4-4 (Figure 4-4: Sample One-Volume Structure)

- Ask a student what this directory structure indicates about the company.

- Ask students which directory is not shown in the structure.

- Discuss what determines whether a directory structure is good or bad.

- Have the students list advantages and disadvantages of this directory structure in the table provided.

This directory structure could be used for a small accounting firm. The structure implies that the company consists of a president, an administrator, and four employees.

All the directories are listed directly under volume SYS; therefore, there is no limit to the size of a directory except the size of the hard disk.

Each employee of the company has a directory for personal files. The administrator seems to have defined responsibilities; specific subdirectories (RPT and LETTERS) were created under the ADMIN directory.

Configuration file directories

Advantages:

- File storage has no limitations except for physical size of hard disk.
- Path names are short.
- Application data files are in a separate directory from application program files.

Disadvantages:

- User subdirectories are directly off volume SYS.
- No shared data directories are provided.
- Volume SYS should be reserved for NetWare files.

Multiple-Volume Directory Structure

Figure 4-5 illustrates a multiple-volume directory structure. Notice that the system-created directories and the applications directory are in volume SYS.

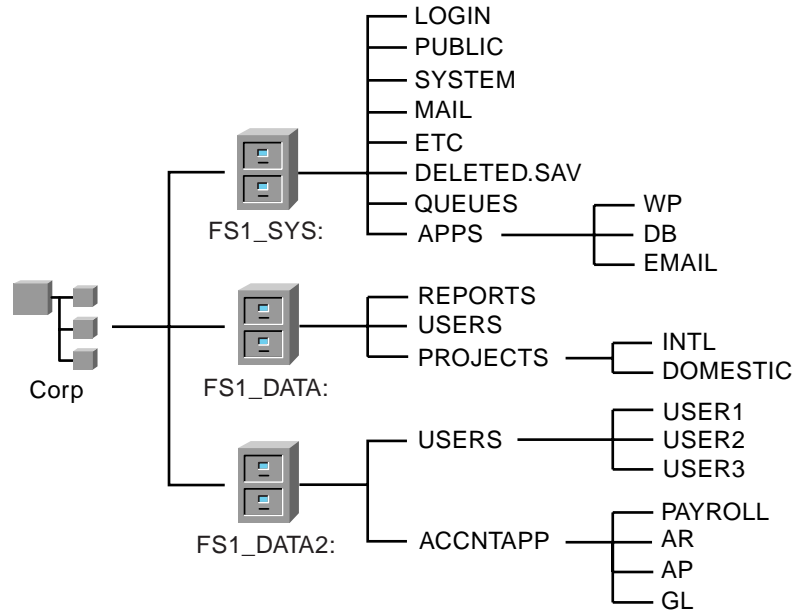


Figure 4-5: Sample Multiple-Volume Structure

List the advantages and disadvantages of this structure in the table below.

Advantages	Disadvantages

Table 4-3: Advantages and Disadvantages of a Multiple-Volume Directory Structure

Presentation**Notes****Multiple-Volume Directory Structure**

4-5 (Figure 4-5: Sample Multiple-Volume Structure)

- Have students describe this company based on the directory structure.

- Analyze the strengths and weaknesses of the directory structure with the class.

- Have the students list advantages and disadvantages of this directory structure in the table provided.

The three volumes might indicate that the system has three hard disks.

You might want to ask the following:

- Where are the users? (Point out users' directories.)
- Where do accounting people do their work? (Point out the USERS directory)
- How might this directory structure be improved?

Advantages:

- A different administrator can manage each section.
- Application program files are secure because they are located in a separate directory on volume SYS.
- Volume SYS is less volatile than the others. Volume space usage is minimal because few files are added or deleted. This creates a more stable volume.

Disadvantages:

- No well-defined shared data area has been created.
- Users are spread across the system, making security maintenance a more time-consuming task.
- Inheritance problems may exist.

Written Exercise 4-1: Designing a Directory Structure

In this exercise, you design and create a directory structure based on a given scenario.

You are the network administrator for EMA. Design and present a directory structure for the EMA Company network based on the EMA organizational chart shown in Figure 4-6.

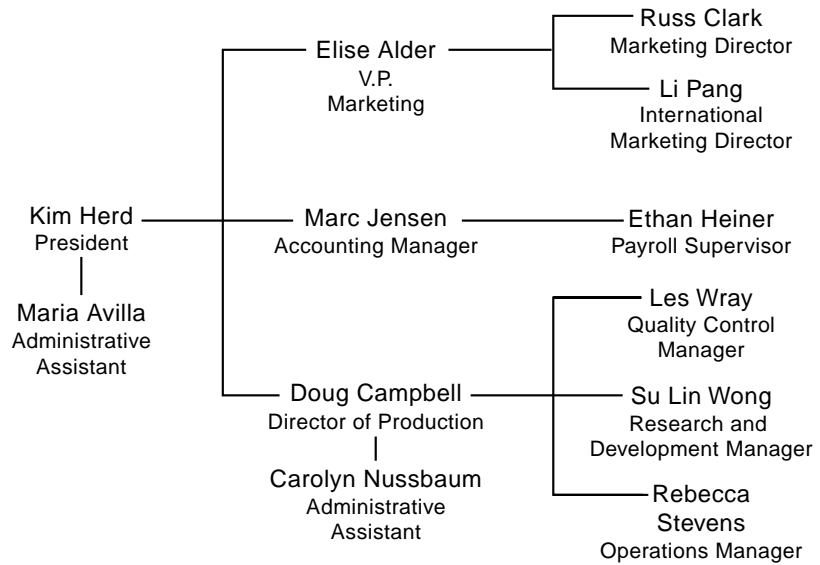


Figure 4-6: EMA Organization Chart

Determine the types of generic application software (such as database, word processing, accounting, and inventory) that employees in your company need to perform their duties efficiently.

Written Exercise 4-1: Designing a Directory Structure

- Introduce the exercise.

Talk through the steps with the class and determine if the students have any questions. Ask students how familiar they are with designing a directory to determine whether they need to perform this exercise.



- Have students create a directory structure for the EMA company.

Work through this exercise on your own before class to ensure you have reviewed the difficulties students might have in trying to construct a directory structure that provides the optimum shared area.

Assemble the class into small groups and allow them 20 minutes to complete the exercise. Working in groups is important to the success of this exercise.

- Point out the EMA organization chart and the EMA directory structure template at the end of the exercise.

File system security can have significant impact on a directory structure plan. Tell the students to complete the exercise based on the material in this section, but indicate to the students that more factors exist for deciding on a directory structure than have been mentioned in this section.

- Discuss structural implications of file system security.

- Point out that an organizational chart and a directory structure are not the same thing.

Consider the following guidelines prior to drawing the structure on paper.

- How will EMA's two hard disks of 2 GB each affect your design?
- How will your design reflect EMA's needs for a shared area that can be used to store common information?
- Should applications and data reside in the same volume or directory?
- Should more than one application reside in a given directory?
- How will you deal with applications that are shared by all users? Applications to be used by only a few users?

Create a file system that best suits the needs of the EMA Company. Note the key EMA Company data and file system guidelines that influenced the layout of your file system.

Create your design on the EMA File Structure Template found on the following page.

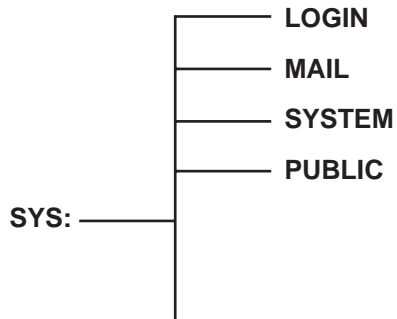


Be prepared to present your solution before the class.

**Written Exercise 4-1:
Designing a Directory
Structure** *(continued)*

- Continue with the exercise.

EMA Directory Structure Template



(End of Exercise)

Presentation**Notes****Written Exercise 4-1:
Designing a Directory
Structure** *(continued)*

- Tell students how you want them to use this template.

Have students plan their structures using the template, and then ask them to draw the finished structure on the whiteboard.

Divide the board area into the number of groups you assign. After all groups have drawn their structures and explained their methods, you can make comparisons to summarize the activity.

If you prefer to use transparencies, student groups should do one of the following:

1. Draw the directory structure they arrive at on this template so you can photocopy it onto a blank transparency before the group makes its presentation (allow the class to take a brief break while you do this).
2. Draw the directory structure on a blank transparency, using the template as a guide to lettering size and orientation of the structure. (Students typically write too small for the structure to be used effectively as a transparency.)

Also, if all groups orient their structures the same way on the transparency, fellow class members can more easily assess the structure during the group presentations.

- Review several solutions.

Have a representative from each group display solutions and discuss what the group did and why. Ask for feedback from the class. Emphasize the strengths of each solution and provide positive feedback to each group.

You might want to have your own solution to share with the class.

Understanding the NSS File System

Novell Storage Services (NSS) is an optional file system available in NetWare 5. It operates independently of, yet is fully compatible with, the default NetWare file system.

NSS is a powerful new high-performance file storage and access system that greatly expands the capabilities of NetWare 5. NSS was developed to meet the anticipated storage needs of the next decade.

Advantages of NSS

The traditional NetWare 5 file system has the following limitations:

- User files have a maximum of 2 GB available.
- Only 16 million directory entries are allowed.
- Large traditional volumes might take several minutes to mount and to repair.
- Only eight volumes are allowed per NetWare partition.

Key NSS improvements over the traditional NetWare file system include the following:

- The ability to store very large files, up to 8 terabytes (8 terabytes equals 8,192 gigabytes).
- The ability to create, access, and store trillions of files in a single directory.
- Rapid access to data, regardless of file size.
- Faster volume mounting and repair than in previous versions of the file system.
- Low server memory requirements. (A server with as little as 32 MB of RAM can mount an NSS volume of any size.)
- The ability to eventually support almost every kind of storage device.
- The ability to treat free space on multiple storage devices as a single volume.

Presentation**Notes****Understanding the NSS File System**

- Explain the function and purpose of NSS.

NSS is new and optional. Administrators are not required to use NSS.

Advantages of NSS

- Point out some situations when the default file system might be limiting to an administrator or network application.
- List the advantages of NSS.

- Enhanced CD-ROM support. (CDs are recognized and mounted automatically as read-only volumes.)
- Up to four NetWare partitions allowed per disk.
- Unlimited volumes allowed per NetWare partition.

These advantages serve the needs of large, high-performance databases, very large numbers of files, or rapidly growing numbers of users and files.



NSS still creates and uses volumes, file structures, and files.

Limitations of NSS

NSS cannot fully replace the traditional file system due to the following limitations:

- NSS cannot create its own volume SYS.
- NSS does not support the following:
 - Transaction Tracking System™ (TTS)
 - Disk striping
 - Disk mirroring
 - Hierarchical storage management (HSM)
 - Real-Time Data Migration (RTDM)
- NSS does not support file compression.
- NSS uses REBUILD and VERIFY instead of VREPAIR.

Despite these current limitations, you might want to create one or more NSS volumes on your server to gain the advantages NSS provides.

Presentation**Notes****Advantages of NSS** *(continued)*

- Describe a scenario to show how these advantages would be useful.

- Mention the note.

Limitations of NSS

- Explain that NSS cannot fully replace the default file system.

- Describe a scenario in which NSS would not be helpful.

NSS Storage Concepts

NSS was designed to make use of most storage space regardless of location. Using NSS requires familiarity with the following terms:

- Provider
- Consumer
- Storage group

Each term is represented in Figure 4-7 and discussed on the following page.

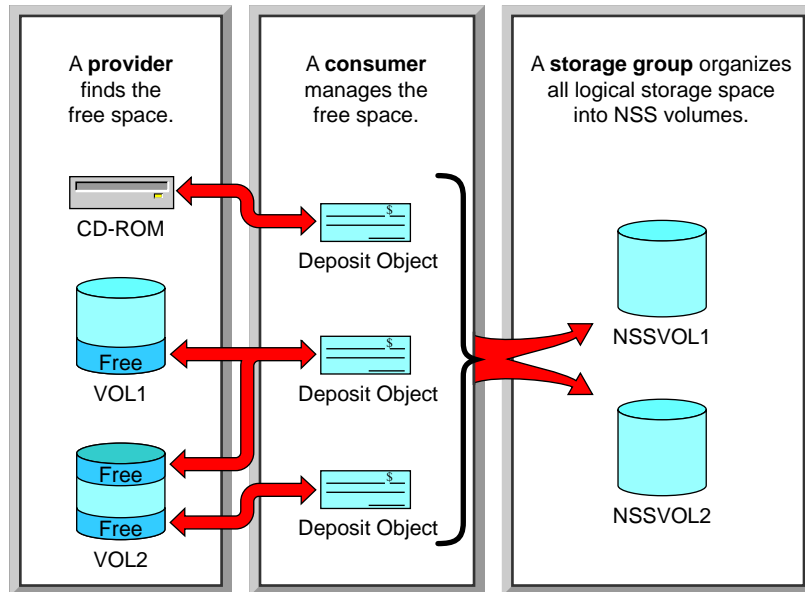


Figure 4-7: NSS Concepts

NSS Storage Concepts

- Introduce the NSS terms.



4-6 (Figure 4-7: NSS Concepts)

Provider

An NSS *provider* scans a server's storage devices, such as hard disks and CD drives, to identify and register usable free space.

A server's hard disk might provide free storage space

- Inside a previously defined NetWare partition
- On IBM-formatted (non-NetWare partitioned) free space

Two providers are included in NetWare 5:

- NSS Media Manager (MMPRV), which is designed for IBM-formatted partitions and file systems
- NSS File Provider (NWPRV), which is designed for use with existing NetWare volumes

Consumer

An internal NSS component called a *consumer* manages registered free space by doing the following:

- It creates a *deposit object* that represents a store of free space.
- It builds logical, internal file input and output paths to help NSS find stored data.
- It registers itself in the free space to prevent other consumers and the traditional file system from accessing the same space.

Administrators can form deposit objects into an NSS *storage group*.

Storage Group

An NSS *storage group* is a single object representing all the logical storage space residing on one or more storage devices as organized by providers and consumers.

An NSS storage group is organized into NSS volumes. NSS volumes mount and function as traditional volumes do.

Presentation**Notes****Provider**

- Explain that an NSS provider finds and registers free space.
- Explain that a provider finds space on NetWare volumes and on IBM-formatted free space.
- List the two providers included in NetWare 5.

Consumer

- Discuss how a consumer manages registered free space.

Storage Group

- Introduce a *storage group* as an object representing all logical storage space.
- Explain that an NSS storage group is divided into NSS volumes that mount and function like traditional volumes.

Setting Up NSS

To set up NSS, do the following:

1. Design an NSS volume by identifying its intended purpose.
2. Create an NSS volume.

Designing an NSS Volume

Most NSS storage groups and volumes you create will use physical hard disk space. Physical hard disk space might already be allocated to existing DOS partitions or NetWare partitions.

If your server's hard disks are already fully partitioned, you have several options:

1. You can use the NSS In-Place Upgrade Utility to convert existing traditional NetWare file system volumes (except SYS) to NSS-controlled volumes.



Do not convert volumes that contain files, such as TTS enabled files, that NSS cannot manage.

2. You can use NetWare partitioned space not being used by a volume or free volume space.
3. You can re-partition your server's hard disk to allow for free space. This free space will become part or all of an NSS storage group and NSS volume.
4. You can install a new hard disk on the server and devote the disk to NSS.

In your design, consider the advantages of NSS:

- Support for exceptionally large files
- Virtually unlimited numbers of files
- Rapid mounting and repair of volumes
- Low server memory requirements



For more information on designing NSS volumes, see NetWare 5 online documentation.

Setting Up NSS

- Provide an overview of the design and creation tasks for NSS volumes.

Designing an NSS Volume

- List the options for designing NSS when the server's hard disks are already fully partitioned:
 - Use the NSS In-Place Upgrade Utility.
 - Re-partition the server's hard disk.
 - Install a new hard disk.
- Reiterate the strengths the administrator should consider when designing NSS.
- Refer students to the online documentation for more information about NSS.

Creating NSS Components

To create NSS components, complete the following:

1. Ensure that sufficient free space exists on the server's storage devices.
2. Load NSS.NLM.
3. Select NSS providers and consumers.
4. Create an NSS storage group.
5. Create an NSS volume.

NSS provides several utilities, such as the NSS Advanced Configuration utility, to assist you in these tasks.

Presentation

Notes

Creating NSS Components



Demonstrate how to create an NSS volume.

- Mention that NetWare 5 includes several NSS utilities.

Hands-On Exercise 4-2: Creating an NSS Volume

In this exercise you use the NSS Advanced Configuration utility to create an NSS volume.

Complete the following:

1. At the server console prompt, enter **LOAD NWCONFIG**.
2. Select **NSS Disk Options**.
3. Select **Storage**.
4. Select **Update Provider Information**.
5. Select **NWPRV Traditional NW Volume**.
6. To continue, press **Enter**.
7. Select **Assign Ownership**.
8. Select the last **NW Volume** in the list. This is free space on the MAIL volume.
9. Enter **100 MB** as the file size for this consumer.



This size can be, but does not have to be, the intended size of the NSS volume you want to create.

10. To confirm, select **Yes**.
11. Select **Return to the previous menu**.
12. Select **NSS Volume Options**.
13. Log in to the tree as your **admin**.
14. Select **Create**.
15. Select **Storage Group**.
16. Select the **NW Volume** and press **Enter**.
17. To confirm, select **Yes**.
18. Select **NSS Volume**.
19. To select the NW Volume, press **Enter**.
20. To save the size, press **Enter**.

Presentation**Notes**

Hands-On Exercise 4-2: Creating an NSS Volume

- Introduce the exercise.



:15

- Conduct the exercise.

- Assist the students as necessary.

Be sure to work through this exercise before class to ensure you have reviewed the difficulties students might have in trying to construct a directory structure that provides the optimum shared area.

21. Enter **NSSVOL** as the volume name.
22. To confirm the name, select **Yes**.
23. To continue, press **Enter**.
24. Select **Return to the previous menu**.
25. Select **Return to the previous menu**.
26. Select **Return to the previous menu**.
27. To leave NWCONFIG, select **Exit**.
28. At the server console, enter **MOUNT NSSVOL**.
29. At the server console prompt, confirm the creation of this new volume by typing **VOLUMES**.

(End of Exercise)

Hands-On Exercise 4-2: Creating an NSS Volume

(continued)



(Optional) If needed, demonstrate how to add an NDS volume object using NetWare Administrator.

- Review the exercise.

Summary

This section discussed the methods and importance of creating directories and using them to organize the file system directories on the network. Just as folders organize information in a file cabinet, directories in a NetWare volume help keep information organized and easy to find.

Some directories on the NetWare volume are created by the installation process and are necessary for the proper functioning of the network. These include the SYSTEM, PUBLIC, MAIL, and LOGIN directories.

As network administrator, you are responsible for creating most of the directories on your network. You should set up the directories in the systematic manner shown in this section.

This section also discussed the optional NSS file system. NSS cannot fully replace the traditional NetWare 5 file system yet, but NSS can deliver powerful new capabilities to networks that otherwise might run into the file limits of the traditional file system.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Explain guidelines for planning and creating custom volumes in the network file system.
2. List the system-created directories; describe their contents and function.
3. List suggested directories for organizing the file system.
4. Identify the strengths and weaknesses of sample directory structures.
5. Design and create a directory structure based on a given scenario.
6. Describe the advantages, disadvantages, and storage concepts of the Novell Storage Services (NSS) file system.
7. Create a NSS volume on your server.

Notes

SECTION 5 **Optimizing the Network and Server**

Duration 02:30

Preparation

Determine which demonstrations and exercises you will be able to perform.

SECTION 5

Optimizing the Network and Server

In this section, you learn how to optimize the server by monitoring server statistics and using SET commands and server utilities to make changes.

Objectives

Upon completing this section, you should be able to

1. Describe NetWare 5 memory allocation and configure the server for memory deallocation and garbage collection.
2. Define virtual memory and configure a NetWare 5 server to use virtual memory.
3. Create an application and adjust the CPU time allocated to it.
4. Describe memory protection and configure a NetWare 5 server to use protected memory.
5. Interpret the MONITOR Statistics screen.
6. Monitor and modify file and directory cache performance.
7. View and modify server buffer and packet parameters.
8. Define and enable block suballocation.
9. List the steps used to enable file compression.
10. Enable and manage the Packet Burst™ protocol.
11. Enable and manage Large Internet Packets (LIPs).

Presentation

Notes

Optimizing the Network and Server

- Introduce the section.

Objectives

- Present the objectives.

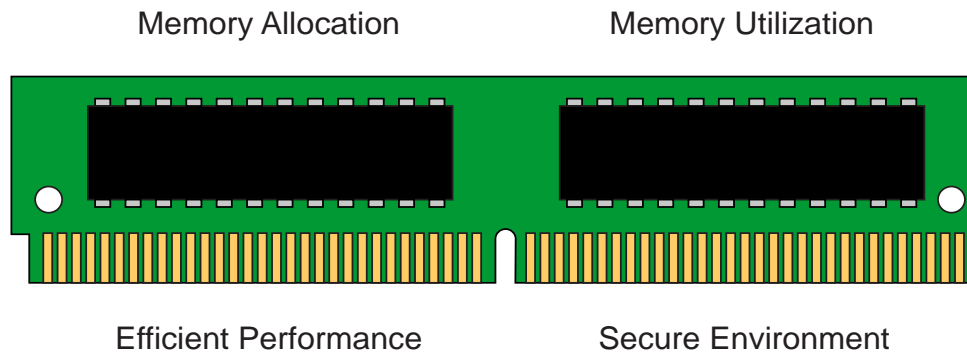


Figure 5-1: Memory Management Goals

NetWare 5 Memory Management

As network administrator, you need to be familiar with memory management.

Most memory management tasks are handled by the NetWare memory management architecture. It has the following goals:

- Memory Allocation
- Memory Utilization
- Efficient Performance
- Secure Environment

NetWare 5 has enhanced memory allocation and memory management features that provide efficient performance and provide a simple and straightforward environment for NLM developers.

NetWare 5 Memory Management



5-1 (Figure 5-1: Memory Management Goals)

- Introduce memory management.
- Point out that memory management is the automatic management of memory in the network operating system.

Some students might have knowledge of memory management in previous versions of NetWare and might want to discuss the differences. Be sure to limit the time spent on this topic.

Memory Allocation

When you manage the network, you need to be aware of memory allocation and how it affects NetWare server performance.

NetWare uses paging to allocate all memory resources in the system. A page is a 4 KB block of RAM. The system can assign physically discontinuous pages of memory in a logically contiguous (adjacent) range, resulting in efficient memory utilization.

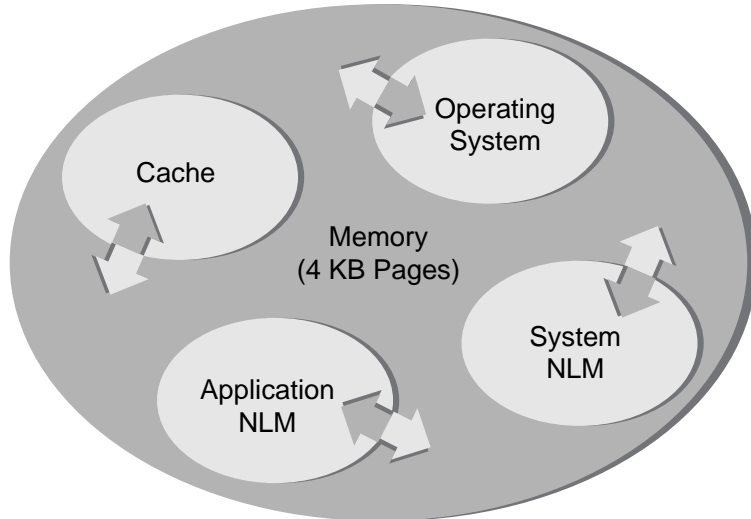


Figure 5-2: Memory Allocation

Memory allocation reserves a specific memory location in RAM for processes, instructions, and data. In the NetWare memory architecture, the network operating system (NOS) gives each process its own allocation pool.

Each process requests memory from its allocation pool and returns memory to the same pool; this minimizes fragmentation and maximizes efficiency.

Efficient NetWare memory allocation also allows third-party developers to expediently create and optimize applications.

Presentation**Notes****Memory Allocation**

5-2 (Figure 5-2: Memory Allocation)

- Describe the memory allocation process.

- Emphasize that third-party developers can easily write NLMs because of efficient memory allocation routines.

Most of this information is very important to application developers, but will be of limited use to most students.

Memory Deallocation and Garbage Collection

NetWare uses memory deallocation and garbage collection to collect unused segments of memory and return them to a common memory pool.

Garbage collection is triggered by demand on the virtual memory system. The virtual memory system is checked every 10 seconds. If virtual memory is being used heavily, then garbage collection happens immediately.

If virtual memory usage is low, then garbage collection happens according to the following process. First, an API named Free labels the memory as deallocated. The garbage collection process then recovers the pieces of deallocated memory and returns them to the memory pool.

The garbage collection routine is interruptible, can run in the background, and should run frequently.

You can use the **SET GARBAGE COLLECTION INTERVAL** command to optimize garbage collection. This parameter sets the interval for collection. The range is from 1 to 60 minutes; the default is 5 minutes.

Presentation**Notes****Memory Deallocation and Garbage Collection**

- Discuss memory deallocation and garbage collection.

- Emphasize that periodic garbage collection is necessary to ensure that deallocated memory is recovered.



- Demonstrate how to set garbage collection parameters with MONITOR.
- Emphasize that the demand on virtual memory overrides the values in the garbage collection parameters.
- Point out that the processes run in the background.

Virtual Memory

NetWare provides a virtual memory system that can move data out of memory and into a file on disk if the data is not used frequently. The virtual memory system ensures that RAM is used more efficiently. It also lessens the likelihood that low memory conditions will cause an abend.

Understanding Virtual Memory

NetWare 5 assesses available memory to see which data has been used less recently than the rest. Data that has not been used for some time can be moved from memory to disk, thus freeing memory for other uses.

When the data on disk is needed again, it is moved back into available memory. Because data is swapped on and off the disk, the available memory can be used for a larger amount of data than its actual physical capacity would allow.

When data is moved from memory to disk, it is stored in a *swap file*. A swap file is a file created on a NetWare volume to hold data moved out of memory and stored on disk.

A swap file is created on the SYS volume by default whenever the server is started. Swap files can be added to other NetWare volumes as well. Each volume can have only one swap file.

Swapping the data between memory and disk requires additional system resources, but it increases the memory available for use. The availability of the additional memory improves overall server performance.

Presentation**Notes****Virtual Memory**

- Discuss virtual memory.

- Explain the difference between virtual memory and physical memory.

Understanding Virtual Memory

- Explain how data is moved from physical memory into virtual memory.

- Define *swap file*.

- Discuss the benefits of virtual memory.

Data use is determined by a bit in each field of the translation table. This bit indicates whether the address translation has been used since the last time it was checked.

Considerations for Using Virtual Memory

When using virtual memory, keep the following in mind:

- You can create one swap file per volume.

The swap file on the SYS volume is created by default. You can delete this swap file and move it to another volume if necessary.

To avoid running out of space on the SYS volume, you should consider moving the swap file to a different volume. You should place a swap file on the fastest volume or on the volume with the most available space.

- Data moved to virtual memory will be stored in any available swap file on any volume.

- You can add a swap file to a volume even if the volume is not mounted.

Once you have added the swap file, the file will be created when you mount the volume.

- When you unmount a volume, the swap file is deleted.

To keep a swap file on a volume that will be dismounted, you must recreate the swap file when the volume is remounted. The exception is the SYS volume swap file, which is created by default.

You should place the commands to create swap files in the AUTOEXEC.NCF file so that the files are created each time the server is started.

- Swap files are dynamic. They change in size as data is swapped in and out of memory.

Presentation**Notes****Considerations for Using Virtual Memory**

- Discuss the considerations for using virtual memory.

- Emphasize that the swap file should be moved to a volume other than SYS, if possible.

- Emphasize that swap files are dynamic.

To do this, commands will have to be added to AUTOEXEC.NCF to remove the default swap file from SYS and then create a new swap file on a different volume.

When first created, swap files are usually about 2 MB in size. They will increase and decrease in size as needed.

Avoiding Disk Thrashing with Virtual Memory

If the overall supply of memory is running low, then swapping will occur more often. If memory is extremely low, the system might spend all its time swapping memory in and out of disk and have no time to accomplish useful work. This is called *disk thrashing*.

In extremely low memory conditions, NetWare 5 will move all the data from a protected address space into the disk swap file, temporarily stopping the modules within the protected address space.

After a period of time, NetWare will move the data back into the memory space and shut down another space, moving its data to disk. Without virtual memory, these extremely low memory conditions would cause processes to fail. With virtual memory, the server keeps running, although very slowly.

When disk thrashing occurs, you should add more RAM. Virtual memory cannot compensate for an overall lack of server memory, although it can prevent processes from failing and allow a server to continue to function.

The real value of virtual memory is in using a sufficient supply of memory more efficiently, thus improving server performance. Running server applications in virtual memory protects the application and improves server reliability.

Presentation**Notes****Avoiding Disk Thrashing with Virtual Memory**

- Define *disk thrashing*.
- Discuss what occurs in virtual memory when physical memory gets low.
- Explain how to fix disk thrashing.

Managing Virtual Memory

You can manage virtual memory by controlling the parameters of the swap files.

Use the following commands to monitor, create, delete, and manage swap files. For more information about the commands and parameters, enter HELP SWAP at the server console.

To do this	Enter this at the server console
Display information about swap files currently in use.	SWAP Alternatively, from the MONITOR Available Options menu, select Virtual Memory and then Swap Files .
Create a swap file on a designated volume.	SWAP ADD <i>volume_name</i> [<i>parameter=value</i>] Optional parameters are MIN=, MAX=, and MIN FREE=. These parameters specify the minimum and maximum size of the swap file and the minimum free space that must be left on the volume. Values are in millions of bytes. If parameters are not included, the following default values are used: <ul style="list-style-type: none"> ■ MIN = 2 ■ MAX = Free volume space ■ MIN FREE = 5
Delete a swap file from a designated volume.	SWAP DEL <i>volume_name</i> If the swap file is being used when it is deleted, then the swapped data is moved to another swap file.
Change the parameter values for a swap file on a designated volume.	SWAP PARAMETER <i>volume_name</i> <i>parameter=value</i> Parameters are MIN=, MAX=, and MIN FREE=.

Table 5-1: Managing Virtual Memory

Presentation**Notes****Managing Virtual Memory**

- Explain how to manage virtual memory with the SWAP command.



Demonstrate how to manage virtual memory with the SWAP command.

Demonstrate how to:

- Display virtual memory information
- Create a swap file on a volume other than SYS
- Delete a swap file from a volume
- Change the parameters of an existing swap file

Hands-On Exercise 5-1: Managing Virtual Memory

In this exercise, you manage virtual memory on your server.

Complete the following tasks. Write your observations in the space provided and be prepared to discuss them.

1. If ConsoleOne is running on your server, exit out of it.
2. Display virtual memory information.
 - a. At your server console, enter **SWAP**.
 - b. Note the information for the swap file on your server.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

3. Observe swap file dynamics.
 - a. At your server console, enter **MONITOR**.
 - b. In the Available Options menu, select **Virtual memory**.
 - c. Select **Swap files**.
 - d. Select the swap file for the SYS volume and press **Tab**.
 - e. Record the information for the swap file in the space below.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

Hands-On Exercise 5-1: Managing Virtual Memory

- Introduce the exercise.



- :10 Conduct the exercise.

- Assist students as needed.

- f. Return to the server console by pressing **Alt+Esc**.
- g. Start ConsoleOne on your server.
- h. Press **Alt+Esc** until you return to the MONITOR screen.
- i. Record the difference in the swap file parameters in the space below.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

- 4. Create a swap file on the DATA volume of your server.
 - a. At the server console, enter **SWAP ADD DATA**.
 - b. At the server console, enter **SWAP**.
 - c. Note the information for the swap files now on the server.

Volume Name		
Size		
Used		
Minimum		
Maximum		
Minimum Free		

**Hands-On Exercise 5-1:
Managing Virtual Memory**
(continued)

- Continue the exercise.

5. Delete the swap file from your SYS volume.
 - a. At the server console, enter **SWAP DEL SYS**.
 - b. At the server console, enter **SWAP**.
 - c. Note the information for the swap file now on the server.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

6. Increase the minimum size of the swap file on your DATA volume to 10 MB.
 - a. At the server console, enter **SWAP PARAMETER DATA MIN=10**.
 - b. At the server console, enter **SWAP**.
 - c. Note the information for the swap file now on the server.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

**Hands-On Exercise 5-1:
Managing Virtual Memory**
(continued)

- Continue the exercise.

7. On your DATA volume, increase the amount of disk space that cannot be used for a swap file to 50 MB.
 - a. At the server console, enter **SWAP PARAMETER DATA MIN FREE=50**.
 - b. At the server console, enter **SWAP**.
 - c. Note the information for the swap file now on the server.

Volume Name	
Size	
Used	
Minimum	
Maximum	
Minimum Free	

(End of Exercise)

**Hands-On Exercise 5-1:
Managing Virtual Memory**
(continued)

- Discuss students' observations.

- Review the exercise.

Using Applications

In addition to providing virtual memory, NetWare 5 allows you to allocate shares of CPU time to each application running on your server. Before doing so, you need to understand the following concepts:

- Threads
- Applications

Understanding Threads

The code that makes up an NLM is itself composed of routines that have a beginning and an end with multiple potential paths. When an NLM is running, it executes these routines and, based on the task involved, chooses a particular path. Each path that runs is called a *thread*.

If one thread encounters a delay of some sort, such as in reading from a disk, other threads from other programs or processes are forced to wait their turn to access the CPU. The thread causing the delay is said to have “gone to sleep” or to be a “CPU hog.” Although the “sleep time” is short (measured in microseconds), it can impact system performance.

To avoid these delays, NetWare can suspend a thread that is hogging the CPU and then reactivate it at a later time at the exact point where the thread went to sleep. NetWare can then give CPU time to another thread while the first thread is suspended.

Other threads in other NLMs and other threads in the sleeping thread’s NLM can still run.

Understanding Applications

In the context of this discussion, an *application* (sometimes referred to as a *virtual machine*) consists of a group of threads, defined by a group of modules loaded in an application space, that are treated as a unit when processing resources are assigned. The physical resources in the computer can be used to share the CPU and make each application appear to have its own processor.

The benefit derived from applications is that you can specify the amount of CPU time that threads in the application are allowed to use when competing with other applications.

For example, if you have a NetWare server on your network whose primary job is to be a Web server, you can create an application for the Web server program and allocate a higher proportion of CPU time to it.

Presentation**Notes****Using Applications**

- Introduce applications.

Understanding Threads

- Define *threads*.
- Discuss threads that have “gone to sleep.”
- Discuss the impact of a sleeping thread on other threads trying to use the CPU.
- Explain how NetWare handles sleeping threads.

Understanding Applications

- Define *application*.

Configuring Applications

When your NetWare server is started, one application is created by default, the NetWare Application. All the traditional NetWare services are provided by the NetWare Application. All the threads run by the NLMs loaded during server startup are assigned to this application.

Some programs can create their own applications when their NLMs are loaded. Programs that cannot create their own applications are assigned to the NetWare Application by default.

However, you can manually define an application. To do this, use the following syntax when loading NLMs at the server console:

LOAD -A=*user_defined_name* NLM_name

For example, if you want to load the NetBasic[®] NLM and create a application named FS1NetBasic for it, you would enter the following command at the server console:

LOAD -A=FS1NetBasic NETBASIC.NLM

Once an application is loaded, you can adjust the *share value* assigned to it. Share value is the proportional amount of CPU time that threads in the application are allowed to use when competing with other applications on the server.

For example, if you assign one application 70 shares and another application 10 shares, the first application will receive 7 times more CPU time than the second.

To adjust the share value assigned to an application, do the following:

1. At the server console, enter **MONITOR**.
2. In the Available Options menu, select **Kernel**.
3. In the Kernel Options menu, select **Applications**.
4. In the Applications menu, scroll down to the application whose share value you want to adjust.
5. Press **F3**.
6. In the New share value window, enter the *value* you want.

Presentation**Notes****Configuring Applications**

- Discuss the NetWare Application.

- Explain that NLMs which cannot create their own applications are loaded into the NetWare Application.



Show students the threads running in the NetWare Application.

- Define *share value*.



Demonstrate how to adjust an application's share value.

The NetWare Application is loaded with a default share value of 100.

Do the following:

1. Load **MONITOR**.
2. Select **Kernel**.
3. Select **Applications**.
4. Scroll down to **NetWare application** and press **Enter**.
5. Scroll down through the list of threads, stopping to discuss some of the more familiar ones.

Be sure to point out the thread's parent module and its current state.

The actual number used as the share value is irrelevant. The ratio between it and the other share values for other applications on the server determines the CPU time allocation.

Hands-On Exercise 5-2: Managing Applications

In this exercise, you configure applications on your server.

Part I: Create an Application

Complete the following steps at the server:

1. If MONITOR is running on your server, enter the following at the server console:
UNLOAD MONITOR
2. At your server console, enter the following:
LOAD -A=MyMonitor MONITOR.NLM
3. Press **Alt+Esc** until you return to the server console prompt.
You will see a message that states that MONITOR.NLM has been loaded into the newly created application MyMonitor.
4. Press **Alt+Esc** until you return to MONITOR.
5. In the Available Options menu, select **Kernel**.
6. In the Kernel Options menu, select **Applications**.
7. In the Applications menu, select **MyMonitor**.
8. In the Application Share Group 'MyMonitor' Threads menu, scroll down to **MONITOR main**. Note the parent module and current state of the thread.
9. In the Application Share Group 'My Monitor' Threads menu, scroll down to **MONITOR updates**. Note the parent module and current state of the thread.
10. In the Application Share Group 'My Monitor' Threads menu, press **F4**. Note the busiest threads.
11. Press **Esc** until you return to the General Information screen in MONITOR.

Hands-On Exercise 5-2: Managing Applications

- Introduce the exercise.



:10

- Conduct the exercise.

- Assist students as needed.

Part II: Configure the Application

Complete the following steps:

1. In the Available Options menu, select **Kernel**.
2. In the Kernel Options menu, select **Applications**.
3. In the Applications menu, highlight **MyMonitor**.
4. In the Applications menu, press **F3** to edit the share value.
5. In the New Share Value window, enter **50**.

Because the NetWare Application is loaded with a default share value of 100, the MyMonitor application will now receive half as much CPU time as the NetWare Application.

6. Exit MONITOR.

(End of Exercise)

Hands-On Exercise 5-2: Managing Applications *(continued)*

- Review the exercise.

Protected Memory

With NetWare 5, portions of memory can be set aside as *protected memory* or *protected address spaces*.

A protected address space is a portion of memory that has carefully controlled communication with the server operating system. The operating system creates a boundary around the protected address space. Any programs running in the protected address space are prohibited from referencing areas of memory outside the boundary.

In older operating systems, a program that attempted to read or write to a memory location outside its boundary would cause the entire system to crash. With NetWare 5, however, an offending program can be closed without affecting any other running programs.

The protected address space provides a safe place to run programs. Modules loaded into a protected address space can't corrupt the operating system or cause server abends. You can use protected address spaces to run untried or ill-behaved NLMs.

The NetWare operating system itself cannot run in a protected address space. The operating system address space is called the *OS address space* or the *kernel address space*.

SYSCALLS.NLM, in conjunction with the memory protection subsystem, prevents modules in a protected address space from having direct access to anything outside the address space.

SYSCALLS.NLM and the memory protection subsystem serve as the interface between the protected address spaces and the server operating system. They prevent NLM programs in protected spaces from passing calls to the operating system address space that would corrupt or fault the core operating system.

Modules that are loaded into protected address spaces use virtual memory. Both the module and the data it accesses can be swapped to disk.

Modules that are not loaded into protected address spaces can still use virtual memory. However, the modules themselves cannot be swapped to disk.

You can create a protected address space, load modules into a protected address space, unload modules from a protected address space, remove a protected address space, or kill a protected address space.

Presentation**Notes****Protected Memory**

- Introduce protected memory.
- Define *protected memory*.
- Explain how protected address spaces work.
- Discuss uses for protected memory.
- Explain the relationship between protected address spaces and virtual memory.

Considerations for Using Protected Address Spaces

When using protected address spaces, keep the following in mind:

- Because modules loaded into a protected address space have controlled communication with the operating system, all modules that must communicate with each other should be loaded into the same protected address space.
- If you load an NLM that depends upon another module into an address space, the other module will be loaded automatically into the same address space.
- If the same module is loaded into more than one address space, the module's code will be shared among the address spaces. Therefore, loading the module into multiple address spaces does not require additional memory for the module itself. Only data for the required module is unique for each address space.
- Even if an NLM is designed to be loaded only once, you can load multiple copies of the NLM if you load them into different protected spaces.
- When you load modules into a protected address space, NetWare assigns whatever amount of memory the loaded modules need, up to a maximum size of 512 MB.

The maximum size of a protected address space is fixed, but within that maximum limit, the memory size of the space grows and shrinks as needed by the modules in the space.

- If you want the server to clean up address spaces that abend, enter the following at the server console

SET Memory Protection Fault Cleanup=On

If an address space abends, the server removes the space and its modules and returns the resources to the system.

If the Memory Protection Fault Cleanup parameter is set to Off, the situation is left to the abend recovery mechanism.

Considerations for Using Protected Address Spaces

- Discuss the considerations for using protected address spaces.

Managing Protected Address Spaces

You can create a protected address space and load one or more modules by using the following commands:

To do this	Enter this command at the server console
Display a list of loaded modules with their address space names.	MODULES This command displays each loaded NLM name and the name of the address space it resides in.
Display a list of all address spaces.	PROTECTION This command displays each address space on the system and a list of modules in that space.
Load one module into a new protected address space.	LOAD PROTECTED <i>Module_Name</i> A new address space, named ADDRESS_SPACE n (where n is a number), is created and the module is loaded into it.
Load one module into a new protected space with <i>restart</i> enabled.	RESTART <i>Module_Name</i> A new address space, named ADDRESS_SPACE n (where n is a number), is created and the module is loaded into it. If the module in the protected space abends, the system shuts down and restarts the space, and reloads the module into it.
Load more than one module into the same protected space.	LOAD ADDRESS SPACE=<i>Address_Space_Name Module_Name</i> The specified module is loaded into the specified address space.
Load multiple modules into a new protected space.	PROTECT <i>NCF_File_Name</i> A new protected space, named the same as the .NCF file name, is created and all the modules listed in the .NCF file are loaded into the address space.
Unload a module from an address space.	UNLOAD ADDRESS SPACE=<i>Address_Space_Name Module_Name</i> The specified module is unloaded from the specified address space, but the address space itself remains intact.
Unload all modules from an address space and remove the address space.	UNLOAD ADDRESS SPACE=<i>Address_Space_Name</i> All the modules are unloaded from the specified address space, the address space is closed, and the resources are returned to the system.
Remove the address space without unloading modules.	UNLOAD KILL ADDRESS SPACE=<i>Address_Space_Name</i> The specified address space is removed, but the modules in it are not unloaded first. The resources are then returned to the system.

Table 5-2: Managing Protected Address Spaces

Presentation

Notes

Managing Protected Address Spaces

- Discuss the protected address space commands.



Demonstrate how to create and remove a protected address space.

NETBASIC.NLM works well for this demonstration.

Hands-On Exercise 5-3: Managing Protected Memory

In this exercise, you

- Create a protected address space and load NetBasic into it
- Remove a protected address space

Part I: Creating a Protected Address Space

To create a protected address space and load NetBasic into it, complete the following:

1. At your server console, enter
LOAD PROTECTED NETBASIC
2. View protected address space information from the server console.
 - a. At your server console, enter
PROTECTION
 - b. What is the name of the protected address space?
 - c. What NLMs are loaded in the protected address space?
 - d. Are there any other protected address spaces on your server? If so, what are their names?

Presentation**Notes****Hands-On Exercise 5-3:
Managing Protected Memory**

- Introduce the exercise.



:05

- Conduct the exercise.

- Assist students as needed.

Remind students that, in Step 2d, the OS address space is not a protected address space.

Part II: Removing a Protected Address Space

To remove a protected address space, complete the following:

1. At your server console, enter
UNLOAD KILL ADDRESS SPACE=*Address_Space_Name*
Substitute *Address_Space_Name* with the name of the address space identified in Step 2b of Part I.
2. Verify that the protected address space was removed.
 - a. At your server console, enter
PROTECTION
 - b. Verify that the protected address space as been removed.

(End of Exercise)

Hands-On Exercise 5-3: Managing Protected Memory *(continued)*

- Review the exercise.

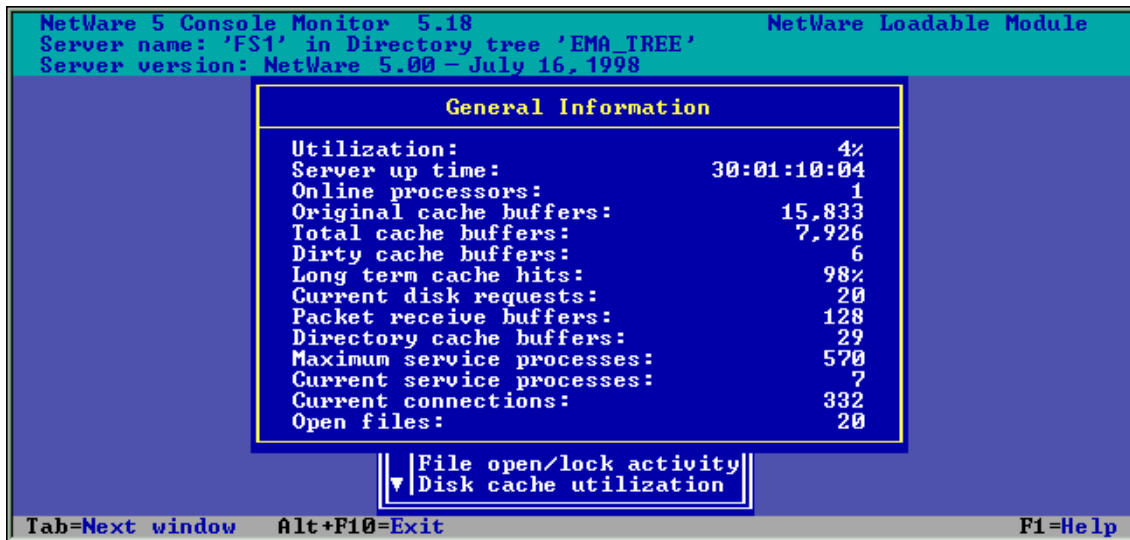


Figure 5-3: MONITOR General Information

MONITOR Statistics

You can use the MONITOR utility to monitor your server's performance.

The main MONITOR screen, General Information, displays information about the status of the network. This information appears a few seconds after you load MONITOR.NLM.

You can track much of your server's performance from the main MONITOR screen without having to look at specific displays. You can expand and contract the General Information screen by pressing **Tab**.

MONITOR Statistics



5-3 (Figure 5-3: MONITOR General Information)

- Discuss the MONITOR General Information screen.

The following table lists the statistics available on the MONITOR General Information screen.

Statistic	Explanation
Server information	Name of the NetWare server and current NDS tree.
Operating system version and date	Version and release date of the operating system (upper-left corner of the screen).
Utilization	Percentage of time the processor is being used.
Server up time	Length of time the NetWare server has been running since it was last booted.
Online processors	The number of enabled processors.
Original cache buffers	Number of cache buffers available when the server is first booted. The figure represents the number of blocks installed as memory in your server less the OS kernel and DOS.
Total cache buffers	Number of buffers currently available for file caching. This number decreases as modules are loaded into memory.
Dirty cache buffers	Number of cache buffers containing information that needs to be written to disk.
Long term cache hits	Number of times the server found requested data in RAM rather than having to go to disk.
Current disk requests	Number of disk requests in a queue that the server is waiting to service.
Packet receive buffers	Number of buffers available to receive station requests.
Directory cache buffers	Number of buffers allocated for directory caching.
Service processes (maximum and current)	Number of task handlers allocated for station requests. When the number of station requests exceeds what is currently allocated, the operating system uses extra task handlers to execute the requests. Once memory is allocated for a service process, it remains allocated. The only way to remove this memory allocation is to bring down the server.
Current connections	Number of licensed and unlicensed connections currently attached to the NetWare server.
Open files	Number of files being accessed by the NetWare server and by workstations.

Table 5-3: MONITOR Statistics

Presentation**Notes****MONITOR Statistics** *(continued)*

- Discuss the statistics in Table 5-3.

Explain only those statistics that apply to performance. Some of these statistics are discussed in detail in this section.

The first two items in the table are general information and do not relate to performance.

Discuss the remaining items, which relate to performance:

- Utilization
- Original cache buffers
- Total cache buffers
- Dirty cache buffers
- Long-term cache hits
- Current disk requests
- Packet receive buffers
- Directory cache buffers
- Service processes (maximum and current)
- Current connections
- Open files

Cache Utilization

NetWare uses caching to speed up reads and writes on server hardware. A *cache* is a temporary, quickly accessible area in RAM that stores frequently used information from the hard disk. As long as a block of data stays in RAM, NetWare can access it much faster than accessing data on the disk.

In essence, caching is the converse of virtual memory. Virtual memory moves infrequently used data out of RAM and into a file on disk. Caching, on the other hand, holds frequently used data from disk in memory for fast access.

A *cache hit* means that the server found the data in RAM, rather than having to go to the disk. This represents a large performance increase.

Having sufficient RAM to cache disk data results in a high percentage of cache hits. The more NLMs and other services you load, the less RAM the server has available for caching data. This lowers your cache hit percentage and slows network performance.

To view long-term cache hits, select Disk Cache Utilization from the MONITOR Available Options menu.

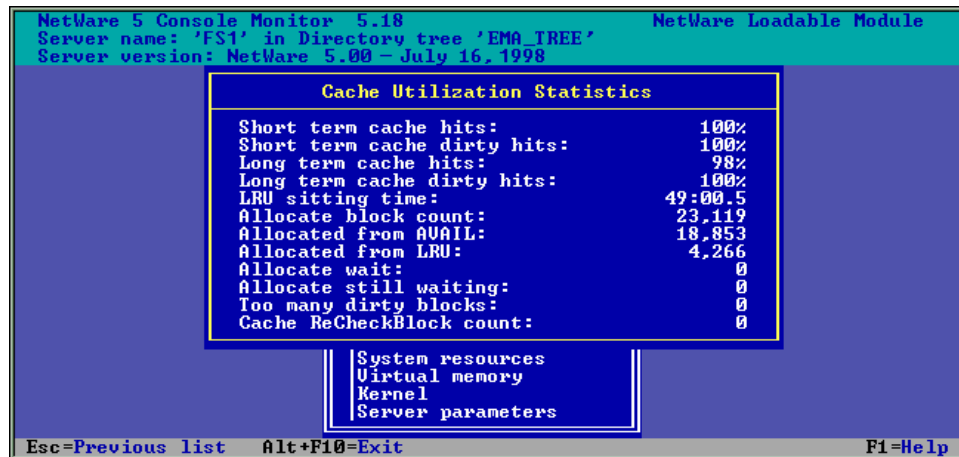


Figure 5-4: Cache Utilization Information



If the long-term cache hits statistic falls below 90%, you should add more RAM. A short-term solution would be to unload NLMs that are not critical.

Presentation**Notes****Cache Utilization**

- Define *cache*.
- Explain the relationship between virtual memory and caching.



Demonstrate how to access cache utilization information.

- Explain how using caching can improve performance.

- Define *cache hit*.



Demonstrate how to view long-term cache hits.



5-4 (Figure 5-4: Cache Utilization Information)

- Explain how to improve the percentage of cache hits.

Discuss cache utilization concepts and statistics as you proceed.

NetWare can access information in RAM faster than it can access data from a hard disk.

A cache hit is a successful search for data in a memory cache.

In the MONITOR Available Options menu, select **Disk Cache Utilization**.

To improve cache hits, the network administrator can do each of the following as needed:

- Add RAM (large impact).
- Unload NLMs (varied impact).

Setting Cache Read and Write Parameters

You can improve server performance by increasing the speed of reads and writes. You can adjust the performance of both read and write operations by following the guidelines in the tables below. (The guidelines will differ slightly from system to system.)

Setting the Write Cache

If network users frequently make many small write requests, consider using the following settings:

Parameter	Setting	Default
Dirty Disk Cache Delay Time	7 sec	3.3 sec
Maximum Concurrent Directory Cache Writes	25	10
Dirty Directory Cache Delay Time	2 sec	0.5 sec
Maximum Concurrent Disk Cache Writes	200	200

Setting the Read Cache

If your server responds slowly to read requests, use the following settings:

Parameter	Setting	Default
Maximum Concurrent Directory Cache Writes	5	10
Maximum Concurrent Disk Cache Writes	40	200
Directory Cache Buffer NonReferenced Delay	60 sec	5.5 sec

Setting read and write cache performance levels might offset each other. For example, if the write cache is set too high, the read cache might be affected.

These parameters can be changed using either MONITOR or SET. You can access the context-sensitive help in MONITOR to find ranges for the parameters and to help you understand the reasons for setting particular values.

To make changes permanent, put the appropriate SET commands in your AUTOEXEC.NCF file. If you don't, the server will use the default values when it is restarted.

Setting Cache Read and Write Parameters

- Explain the effect of adjusting cache read and write parameters.



- Demonstrate how to set cache read and write parameters using MONITOR.
- Point out that read and write cache settings can offset each other.

A server has a finite set of processor resources—every increase in the read performance naturally affects the write performance and vice versa.

Processor Utilization

Another critical factor in network performance is the CPU. Network performance can be dramatically affected by a heavy load on the CPU caused by one or more processes.

High processor utilization alone is not always a problem. Processes that make efficient use of the processor can cause utilization to stay at 100% for short periods of time.

For example, processes such as compression and decompression make efficient use of the processor but can still cause 100% utilization.

This type of utilization is entirely appropriate. It just means the process is using the processor efficiently. It might stay at 100% for two or three minutes without affecting performance. However, if connections are dropped or server performance is severely impaired during the 100% utilization, problems exist.

Memory Utilization

NLMs immediately return memory when they are unloaded. The NLM loading and unloading process provides flexibility in managing memory to ensure high performance.

Available memory is a factor in performance because it affects the number of cache buffers.

Keep the following points in mind:

- Many NLMs rely on prerequisite NLMs. Memory needed for loading an NLM is approximately the same as the file size of the NLM, plus the file sizes of any prerequisite NLMs.
- Some NLMs allocate additional memory as they are running.

You can use the System Resource information screen in MONITOR to check memory before and after loading an NLM. The difference indicates the approximate size of the NLM.

You should test new NLMs and monitor changes in server performance. Intermittent problems might indicate that the NLM grows as it runs and then returns memory after completing a task.

Presentation**Notes****Processor Utilization**

- ❑ Point out that a 100% processor utilization figure does not always mean that performance will decrease.

Memory Utilization

Demonstrate how to access memory utilization information.

Discuss memory utilization concepts and statistics as you proceed.

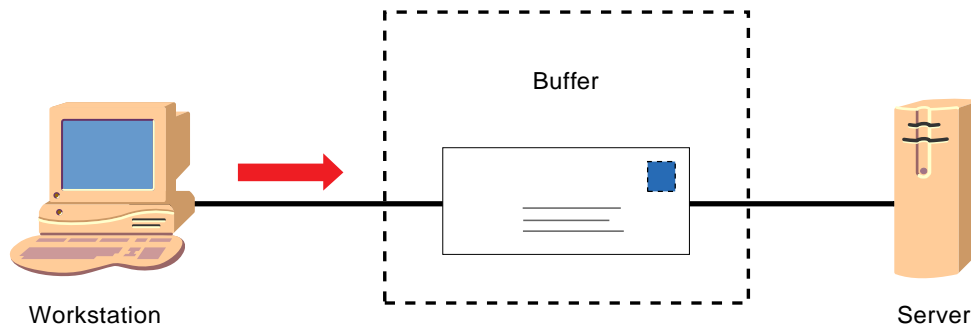


Figure 5-5: Server Packets and Buffers

Server Packets and Buffers

Server packet and buffer parameters are critical factors in server performance. You might need to modify them to enhance performance.

Packets

A packet is a unit of information used in network communication, transmitted as a whole from one device to another.

Messages sent between network devices are formed into packets at the source device. The packets are reassembled into complete messages when they reach their destination.

A packet might contain a request for service, information on how to handle the request, and the data to be serviced. An individual packet consists of headers and a data portion. The different headers are appended to the data portion as the packet travels through the communication layers.

Packet size is determined by the NetWare server and the workstation. The default packet size depends on the capacity of the LAN driver being loaded. The allowable range for a workstation is 576 to 6500 bytes, depending on the LAN driver.

Servers and workstations negotiate the largest packet size possible. If the server can handle a 4 KB packet and the workstation can handle only a 1 KB packet, they will exchange 1 KB packets.

Server Packets and Buffers



5-5 (Figure 5-5: Server Packets and Buffers)

Packets

- Define *packet* (if necessary).
- Discuss the default packet size.
- Discuss how maximum packet size is negotiated.

Packets are not always contiguous, meaning that they are not always sent in proper order (1, 2, 3, 4...). Sometimes they are sent in random order, depending on which ones can be accessed fastest. The receiving server or workstation knows how to reassemble the packets in the proper order.

If the server and workstation are both configured to handle 4 KB packets, they can exchange 4 KB packets as long as any intermediate routers are also configured to handle 4 KB or larger packets.

Maximum Physical Receive Packet Size

You can use MONITOR to increase the Maximum Physical Receive Packet Size parameter to the largest client packet size actually in use on the network.

The network board driver should specify the maximum packet size it can handle. This parameter cannot be modified with SET commands at the console prompt. It must be defined in the STARTUP.NCF file.

Ideally, you should use the largest possible packet size, unless the client and server are configured for different packet sizes or the packet must cross a router to get to the server.

Topology	Default Maximum Packet Size
Token ring (16 Mbps)	4202
Token ring (4 Mbps)	4202
Ethernet	1514

Table 5-4: Default Maximum Packet Size by Topology

Packet Receive Buffers

Packet receive buffers are areas in the NetWare server memory set aside to hold data packets.

Use MONITOR to check current settings. If necessary, you can change the settings associated with the following parameters.

Maximum Packet Receive Buffers

The Maximum Packet Receive Buffers parameter determines the maximum number of packet receive buffers that the operating system can allocate.

Often, the default setting (500) is too low for busy servers. A setting between 700 and 1000 might be better for such servers.

Presentation**Notes****Packets** *(continued)*

- Continue discussing how maximum packet size is negotiated.

Maximum Physical Receive Packet Size

- Discuss the SET parameter for the Maximum Physical Receive Packet Size.
- Emphasize that a router might have a packet size limitation.

Packet Receive Buffers

- Define and discuss *packet receive buffers*.
- Discuss the SET parameter for the Maximum Packet Receive Buffers.



Use MONITOR or SET to demonstrate how to view and set Maximum Packet Receive Buffers.

In MONITOR, select **Server parameters** and then **Communications**.

Minimum Packet Receive Buffers

The Minimum Packet Receive Buffers parameter determines the minimum number of packet receive buffers that the operating system can allocate.

Rather than waiting for requests to come in, the operating system allocates the minimum number of buffers as soon as the NetWare server boots.

If the server is slow in responding immediately after it has been booted, you can increase this number. The default is 128.

This parameter must be set in the STARTUP.NCF file.

Maximum Service Processes

Maximum Service Processes is a related parameter. Be sure to check this number at the MONITOR General Information screen. If the number of allocated service processes is at its maximum, you can increase the maximum to decrease the need for more packet receive buffers.

The range for Maximum Service Processes is 5 to 1,000. This range accommodates networks with a large number of users.

Minimum Service Processes

The Minimum Service Processes parameter determines the minimum number of service processes handled in a group. If a large number of users are requesting processes, this number can be increased to handle the requests more quickly.

The range for Minimum Service Processes is 10 to 500. In a network with a large number of users, this range allows for more requests to be processed in a group.

Presentation**Notes****Packet Receive Buffers** *(continued)*

- Discuss the SET parameter for Minimum Packet Receive Buffers.



Demonstrate how to view and set Minimum Packet Receive Buffers in MONITOR.

- Discuss the SET parameter for Maximum Service Processes.

- Discuss the SET parameter for Minimum Service Processes.



Demonstrate how to view and set Maximum and Minimum Service Processes.

Select **Server parameters** and then **Communications**.

Use MONITOR or SET. In MONITOR, select **Server parameters** and then **Miscellaneous**.

Network Board Statistics

The network board handles traffic between the workstation and the server. You need to review network board statistics whenever you monitor the performance of the network.

These statistics reveal trends in communication or problem areas that need to be addressed. Most network board drivers can provide many different statistics, including general error entries and total packets sent and received.

```

NetWare 5 Console Monitor 5.18                               NetWare Loadable Module
Server name: 'FS1' in Directory tree 'EMA_TREE'
Server version: NetWare 5.00 - July 16, 1998

3C90X_1_EII [3C90X port=DC80 int=A frame=ETHERNET_III]

Generic counters
Total packets transmitted:                               97,805
Total packets received:                                 133,766
Receive discarded, no available buffers:                 0
Transmit failed, packet too big:                         0
Transmit failed, packet too small:                       0
Receive failed, adapter overflow condition:              Not supported
Receive failed, packet too big:                         0
Receive failed, packet too small:                       Not supported
Transmit failed, miscellaneous error:                   0
Receive failed, miscellaneous error:                    0
Transmit failed, retried:                               0
Receive failed, checksum error:                         0
Receive failed, packet length mismatch:                 63
Bytes transmitted modulo 4GB:                           22,410,902
Bytes transmitted rollover (<times 4GB>):               0
Bytes received modulo 4GB:                              61,697,692

Tab=Next window  Alt+F10=Exit                               F1=Help
    
```

Figure 5-6: Network Board Statistics

The “Receive discarded, no available buffers” statistic shows the number of packets dropped because no packet receive buffers were available. If the number is high (over 2% of total packets received), the server is not handling processes fast enough for the board.

If the count is high, you can increase the maximum and minimum packet receive buffer settings. The server might also need to be upgraded.

If the “Packets queued for transmission” statistic is high, the board might not be fast enough for the server.

Additional custom statistics might be available, depending on your network board, and can be useful in monitoring and troubleshooting network performance.

Presentation**Notes****Network Board Statistics**

- Discuss the role of the network board in network performance.



5-6 (Figure 5-6: Network Board Statistics)

- Discuss generic and custom counters.
- Discuss issues relating to network board performance problems.
- Discuss how to identify network board performance problems.
- Discuss how to correct network board performance problems.

Previous versions of NetWare used the term "No ECB available count" for "Receive discarded, no available buffers."

Disk Drivers and Controllers

NetWare server performance is affected by the disk drivers and controllers it uses. A *disk driver* is the software that interfaces with a host bus adapter or disk controller.

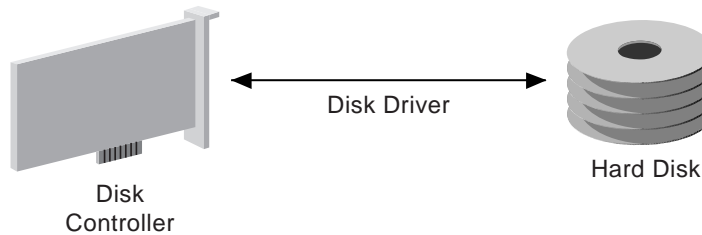


Figure 5-7: Disk Drivers and Controllers

Different types of disk drivers and controllers can be used in NetWare servers, as long as they meet Novell standards. Significant improvements in file read and write times are possible with high-end device driver/controller configurations.

High-end servers using Small Computer Systems Interface (SCSI) boards use an intelligent device driver, usually supplied by the drive manufacturer.

Some devices can service multiple drives connected to the same controller.

Some advanced disk controllers employ bus-mastering and 32-bit technologies to optimize the transfer of data to and from the disk.

Presentation**Notes****Disk Drivers and Controllers**

- Define *disk drivers* and *controllers*.



5-7 (Figure 5-7: Disk Drivers and Controllers)

- Discuss the role of the disk drivers and controllers in network performance.

The disk controller might need to be upgraded if disk reads and writes are too slow.

Hands-On Exercise 5-4: Monitoring and Maintaining Network Performance

In this exercise, you monitor and maintain network performance.

Use the MONITOR screens to track key performance parameters. Press **F1** at any time for context-sensitive help explaining particular screens and statistics.

Write your observations in the space provided and be prepared to discuss them.

1. At the server console, enter **MONITOR**.
2. Observe the Utilization number in the General Information panel at the top of the main screen. Record this number as you perform the activities in the following steps.
3. At the Monitor General Information screen, note the processor utilization value.
4. From your workstation, log in to your server and run NetWare Administrator. Record the peak processor utilization value shown on your server console.

Presentation**Notes**

Hands-On Exercise 5-4: Monitoring and Maintaining Network Performance

- Introduce the exercise.



:15

- Conduct the exercise.

- Assist students as needed.

The students should complete this exercise in pairs. Have one student perform tasks at the server console while the other student performs tasks at the workstation.

5. At the server console, select **Disk Cache Utilization** from the Available Options menu. Record the percentage of Long-Term Cache Hits.

6. At the workstation, open Windows Explorer and copy the contents of SYS:\PUBLIC to your workstation hard disk.
 - a. Click **Start**.
 - b. Click **Programs**.
 - c. Click **Windows Explorer**.
 - d. Browse to the root of your SYS volume.
 - e. Right-click the **PUBLIC** directory.
 - f. Click **Copy**.
 - g. Right-click your **C:** drive.
 - h. Click **Paste**.

7. Note the percentage of Long-Term Cache Hits.

8. At the server console, press **F1**; then press **Page Down** until you see an explanation of Short Term Cache Dirty Hits.

9. At the client workstation, create a user object with NetWare Administrator. Note the statistics on the console during the creation of the user object.

(End of Exercise)

Hand-On Exercise 5-4: Monitoring and Maintaining Network Performance

(continued)

- Discuss students' observations.

- Review the exercise.

Observations might include the following:

- The utilization value changes, based on the activities performed in Step 4.
- Running NetWare Administrator causes a load on the processor and should result in an increase in the processor utilization value.
- The Long-Term Cache Hits value might not change drastically based on this one activity; the Long-Term Cache Hits value is affected only by excessive activity.
- Step 8 demonstrates the context-sensitive Help feature.

Written Exercise 5-5: Interpreting MONITOR Information

In this exercise, you practice interpreting MONITOR information.

The following screens show a variety of situations you might encounter on your network. Assess each screen to evaluate the potential impact on system performance, consider what actions you might take, and answer the accompanying questions. Be prepared to discuss your answers.

The following figure is an example of a MONITOR Statistics screen. Evaluate the statistics and answer the questions that follow the figure.

```

NetWare 5 Console Monitor 5.18                               NetWare Loadable Module
Server name: 'FS1' in Directory tree 'EMA_TREE'
Server version: NetWare 5.00 - July 16, 1998

  General Information
  Utilization:                               100%
  Server up time:                             30:01:10:04
  Online processors:                           1
  Original cache buffers:                       15,833
  Total cache buffers:                          7,926
  Dirty cache buffers:                          6
  Long term cache hits:                         98%
  Current disk requests:                        60
  Packet receive buffers:                       128
  Directory cache buffers:                       29
  Maximum service processes:                    570
  Current service processes:                     7
  Current connections:                          102
  Open files:                                   1020

  File open/lock activity
  Disk cache utilization

Tab=Next window  Alt+F10=Exit                               F1=Help
    
```

1. Which items on the information screen above need attention?

2. Suggest actions to take for each item.

Presentation**Notes****Written Exercise 5-5:
Interpreting MONITOR
Information**

- Introduce the exercise.



:10

- Conduct the exercise.

- Discuss students' solutions for MONITOR Information.

Students should use the information in the graphics to answer the questions that correspond to each figure.

Answers for MONITOR Information:

1. Utilization is 100%.
2. Determine if the network board is performing adequately or if an ill-behaved NLM exists.

Action is only required if utilization remains at 100% for an extended period and workstation performance is noticeably degraded.

The following figure is an example of a Cache Utilization screen. Evaluate the statistics; then answer the questions that follow the figure.

Cache Utilization Statistics	
Short term cache hits:	100%
Short term cache dirty hits:	100%
Long term cache hits:	86%
Long term cache dirty hits:	99%
LRU sitting time:	10:41:59.4
Allocate block count:	53,872
Allocated from AVAIL:	20,670
Allocated from LRU:	33,202
Allocate wait:	0
Allocate still waiting:	0
Too many dirty blocks:	0
Cache ReCheckBlock count:	0

1. What items on the information screen above need attention?

2. Suggest actions to take for each item.

Presentation**Notes****Written Exercise 5-5:
Interpreting MONITOR
Information** *(continued)*

- Discuss students' solutions for Cache Utilization.

Answers for Cache Utilization:

1. The Long-Term Cache Hits percentage is below 90%.
2. Add more RAM (most effective), unload noncritical NLMs (less effective), or remove DOS (least effective) to free memory.

The following figure is an example of network board statistics. Evaluate the network board statistics; then answer the questions that follow the figure.

```

3C90X_1_EII [3C90X port=DC80 int=A frame=ETHERNET_II]
Generic counters
Total packets transmitted:          150,549
Total packets received:             195,802
Receive discarded, no available buffers: 17,756
Transmit failed, packet too big:      0
Transmit failed, packet too small:    Not supported
Receive failed, adapter overflow condition: Not supported
Receive failed, packet too big:      0
Receive failed, packet too small:    Not supported
Transmit failed, miscellaneous error:  0
Receive failed, miscellaneous error:  23
Transmit failed, retried:              0
Receive failed, checksum error:       32
Receive failed, packet length mismatch: 1,421
Bytes transmitted modulo 4GB:         191,617
Bytes transmitted rollover (times 4GB): 0
Bytes received modulo 4GB:            40,540,575
    
```

1. What items on the information screen above need attention?

2. Suggest actions to take for each item.

(End of Exercise)

Presentation**Notes****Written Exercise 5-5:
Interpreting MONITOR
Information** *(continued)*

- Discuss students' evaluation of the network board statistics.

- Review the exercise.

Answers for network board statistics:

1. The "Receive discarded, no available buffers" count is high, in relationship to the "Total packets received" count.

2. Increase the packet receive buffer settings. The server might also need to be upgraded with a faster CPU or additional RAM.

```
NetWare 5 Console Monitor 5.18                               NetWare Loadable Module
Server name: 'FS1' in Directory tree 'EMA_TREE'
Server version: NetWare 5.00 - July 16, 1998

Volume SYS Information

Volume is mounted:                                           Yes
File system name:                                           NW 5 Traditional File Sys.
Loaded name spaces:                                         DOS, LONG
Read only:                                                  Off
Compression status:                                         On
Sub-allocation:                                             On
Sub-allocation unit size:                                   512
Migration status:                                           Off
Migrated files:                                             0
Block size:                                                 32
Sectors per block:                                          64
Total blocks:                                               13,467
Free blocks:                                                2,629
FAT blocks:                                                 8
Freeable blocks in salvage system:                          2,318
Non-freeable blocks in salvage system:                       0
Directory size, in blocks:                                  126

Tab=Next window  Alt+F10=Exit                               F1=Help
```

Figure 5-8: Disk Space Management

Optimizing Disk Space

The memory management schemes discussed so far deal with RAM. As a network administrator, you also need to optimize disk space in your file system.

NetWare provides the following features to help you optimize your hard disk storage space:

- Block suballocation
- File compression

Optimizing Disk Space



5-8 (Figure 5-8: Disk Space Management)

- Contrast memory management with disk space management.

The following subsections deal with methods for managing disk space.

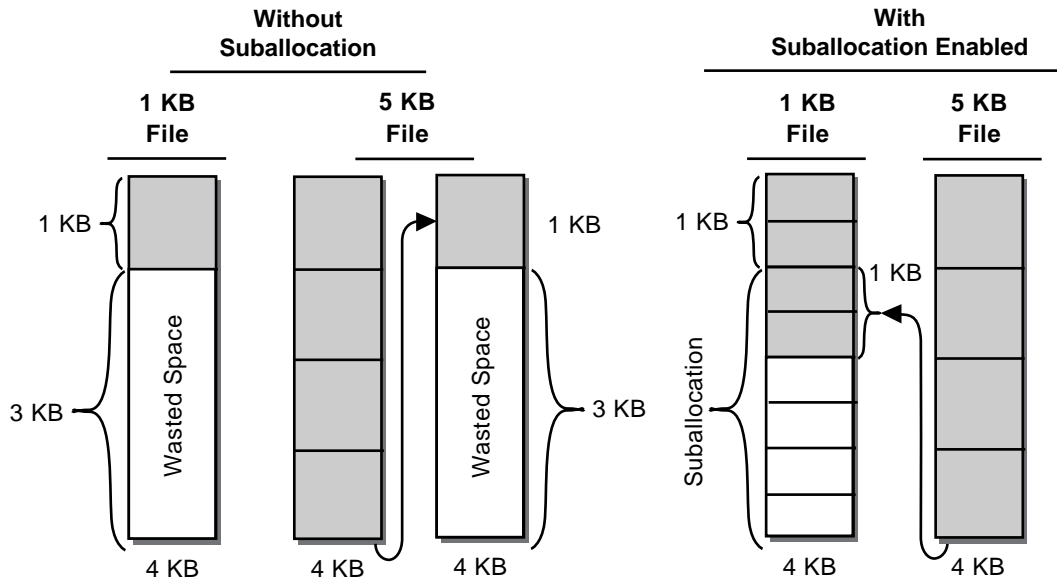


Figure 5-9: Block Suballocation

Block Suballocation

Block suballocation is a method NetWare uses to save hard disk space. With block suballocation, several files can share one disk block.

Files are stored in allocation blocks. Without block suballocation, a full block is allocated to store a file, even if the file is smaller than the block size.

For example, a 1 KB file on a volume with a 4 KB block size would still require one 4 KB block for storage. The remaining 3 KB of that 4 KB block would be unused and unavailable for storage.

To ensure more efficient memory usage, NetWare allows blocks to be broken into 512-byte increments (suballocation blocks). These smaller increments allow smaller files and file fragments to be stored together, filling the block (see Figure 5-9).

When a file is larger than the allocated block size, the excess is stored in the suballocation blocks (if suballocation is enabled). The beginning of every file is stored at the beginning of a block. If the file exceeds the allocated block size, the remainder of the file is placed in suballocation blocks.

Block Suballocation

- Discuss normal block allocation.



5-9 (Figure 5-9: Block Suballocation)

- Draw a similar example on the board, explaining the process as the drawing takes shape.

With suballocation, blocks are set aside to store files that are less than the block size and fragments of files that are larger than the block size.

- The beginning of every file is stored at the beginning of an allocated block, with and without suballocation.
 - The 1 KB file is stored at the beginning of a 4 KB allocated block.
 - The 5 KB file is stored at the beginning of another 4 KB allocated block.
 - Files smaller than the block size will be moved to a suballocated block sometime after file creation.
- Without suballocation, block space not filled by one file is wasted.
 - The 1 KB file takes up 1 KB of the 4 KB allocated block; the remaining 3 KB of that block are wasted.
- The 5 KB file takes up an entire 4 KB allocated block, plus the first 1 KB of a second 4 KB allocated block. The remaining 3 KB of the second allocated block are wasted.

For example, suppose you have an allocated block size of 4 KB and a 1 KB file. With suballocation, the system stores the 1 KB file at the beginning of a 4 KB block and uses the remaining 3 KB of that block for suballocation.

If a 5 KB file is subsequently created, the system stores the first 4 KB of that file in a 4 KB block and places the remainder in suballocation blocks.

Block suballocation saves small amounts of disk space per file, which, when multiplied by thousands of files on a large NetWare server, saves large amounts of disk space.

Enabling Block Suballocation

Block suballocation is enabled as a default during NetWare installation. Once block suballocation has been enabled, you cannot disable it without recreating the volume.

Presentation**Notes****Block Suballocation** *(continued)*

- Continue discussing block suballocation.

Enabling Block Suballocation

- Explain how block suballocation is enabled.

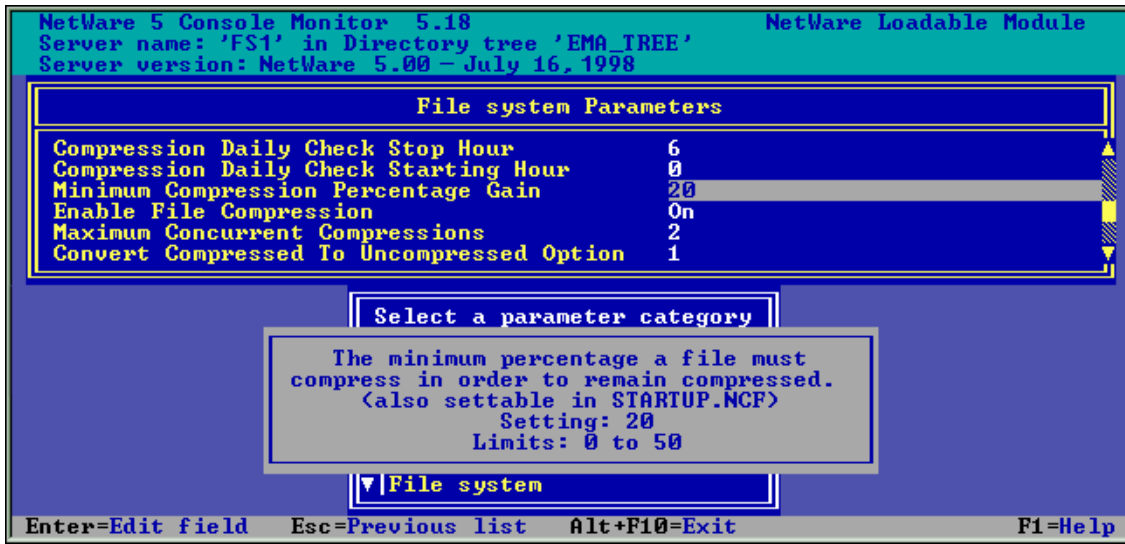


Figure 5-10: File Compression Options in MONITOR

File Compression

File compression helps you optimize hard disk space by allowing you to store more information on a hard disk.

File Compression Process

File compression is managed internally by NetWare. During file compression, the NetWare operating system does the following:

- Reads and analyzes the file.
- Builds a temporary file describing the original file.
- Determines if any disk sectors can be saved by compressing the file. A gain of at least 20% is required before a file is compressed.
- Begins creation of the compressed files.
- Replaces the original files with the compressed files after an error-free compressed version of each file is built.

If a disk error or power failure occurs during compression, NetWare retains the original uncompressed file.

File Compression



5-10 (Figure 5-10: File Compression Options in MONITOR)

- Define *file compression*.

File Compression Process

- Discuss the file compression process.

The system creates a temporary file describing the original file so that the original file is not at risk if the data becomes corrupted during the compression process.

Compression Ratio

The *compression ratio* is the difference in file size before and after compression. The average compression ratio in a volume is approximately 63 percent. For example, a volume holding 144 MB of data can be compressed to 54 MB.

Compression ratio per file varies based on the file type. For example, text files achieve a greater compression ratio than do executable files or graphic files.

The file compression/decompression subsystem sacrifices speed to optimize the file compression ratio. It assumes that compression ratio has priority over speed because compression can run during off hours when speed is usually not critical.

Rather than compressing every file, the system only compresses files that have not been accessed for a specified amount of time.

File decompression happens very quickly and with minimal overhead. Decompression has no noticeable effect on system performance.

Managing File Compression

During installation, file compression on each volume is turned on by default. Once file compression is turned on, it cannot be turned off unless you recreate the volume.

However, file compression can be disabled. You can disable file compression at the directory and file level. You can also use the following command at your server console to disable compression on all volumes for an entire server:

SET ENABLE FILE COMPRESSION=OFF

You will receive maximum disk space savings when you use the following options:

- Compression enabled
- Suballocation enabled
- Large disk allocation blocks (16 KB or larger)

Presentation

Notes

Compression Ratio

- Discuss file compression ratio.

- Emphasize that the network administrator can designate off-peak hours for file compression.

Managing File Compression

- Discuss considerations for managing file compression.

File Compression Options

Although file compression is set at the volume level, you can control file compression with SET commands or MONITOR. The settings are stored in the AUTOEXEC.NCF file.

The following table shows the SET commands that can be used to manage file compression. These settings affect all files and directories on the server.

SET Parameter	Explanation
Compression Daily Check Starting Hour	This option specifies when the server should start searching for unopened files to compress. Hours are specified in military time. Default is 0 (midnight).
Compression Daily Check Stop Hour	This option specifies when the system should stop looking for unopened files to compress. The default is 6 (6:00 a.m.). Automatic searching for unopened files stops until the starting hour on the next day.
Minimum Compression Percentage Gain	A file must be at least this specified percentage smaller after compression; otherwise, the system leaves it uncompressed. The default is 20%.
Enable File Compression	If you enter SET ENABLE FILE COMPRESSION=OFF, file compression is still enabled for the volume, but files will not be compressed. The setting applies to the entire server. Default is ON.
Maximum Concurrent Compressions	This option specifies the number of volumes that can be compressing files on a server at the same time. The default is 2. Novell recommends not changing this setting because increasing the number slows compression down considerably.
Convert Compressed to Uncompressed Option	This option specifies what to do to the uncompressed version of a file after it is decompressed. Option 0 always leaves the compressed version, 1 (default) leaves it compressed after a single access (within the "untouched" period), and 2 always changes to an uncompressed version.
Decompress Percent Disk Space Free To Allow Commit	This option specifies the percentage of free disk space required on a volume before an uncompressed file can be committed to disk. The default is 10 percent. This prevents newly uncompressed files from filling up the volume.
Decompress Free Space Warning Interval	This number specifies the interval for displaying warning alerts when the volume has insufficient free disk space for uncompressed files. To turn off the alerts, set it to 0. The default is 31 minutes 18.5 seconds.

Table 5-5: SET Parameters for File Compression

Presentation**Notes****File Compression Options**

- Discuss the parameters in Table 5-5.



Demonstrate how to set file compression options.

- Emphasize that the Maximum Concurrent Compressions setting should not be changed.

Use MONITOR to show the options. The compression parameters are in **Server parameters | File system**.

Use the context-sensitive help to explain the options. If time is running short, explain and demonstrate only the most important options.

This might be a good time to remind students that the default backup start time for both delayed file compression and delayed backups is midnight. Advise students to avoid conflicts by changing the start times.

Increasing the number slows compression considerably.

SET Parameter	Explanation
Deleted File Compression Option	This option specifies how the server should handle compression of unpurged deleted files: 0=DON'T, 1=Compress next day, or 2=Compress immediately. The default is 1.
Days Untouched Before Compression	This option specifies when an unmodified file should be compressed. The system automatically compresses files that have not been accessed for the number of days specified. The default is 14 days.

Table 5-5: SET Parameters for File Compression (continued)

Setting File Compression Attributes

You can set attributes for specific files and directories with NetWare Administrator, FILER, or Windows Explorer. The attributes are Immediate Compress (IC) and Don't Compress (DC).

The Immediate Compress (IC) attribute starts compression of the selected files immediately, regardless of the time set for daily compression.

If the SET parameter ENABLE FILE COMPRESSION has been set to OFF, compression on these files will be queued until the parameter is reset to ON. You might notice an extremely high processor utilization rate when compression occurs.

The Don't Compress (DC) attribute prevents compression of a particular file or of all the files in a subdirectory.

If you group files you want compressed on one volume and files you do not want compressed on another volume, you will not have to control compression at the file level.

Presentation**Notes****File Compression Options** *(continued)*

- Continue discussing file compression options.

Setting File Compression Attributes

- Discuss file compression attributes.
- Emphasize that setting compression attributes on files can be a time-consuming method for controlling file compression.



- Demonstrate how to set file compression attributes.

Controlling file compression at the volume level is preferable.

Viewing Compression Statistics

You can view file compression statistics using NetWare Administrator or Windows Explorer.

You can also use the NDIR and FILER utilities.

NetWare Administrator

Complete the following steps to view statistics with NetWare Administrator:

1. Click the **volume object**.
2. From the Object menu, click **Details**.
3. Click **Statistics**.

Windows Explorer

Complete the following steps to view statistics with Windows Explorer:

1. Right-click a drive mapped to the volume.
2. Click **Properties**.
3. Click the **NetWare Volume Statistics** tab.

Presentation

Notes

Viewing Compression Statistics

- Explain how the file compression statistics can be viewed.

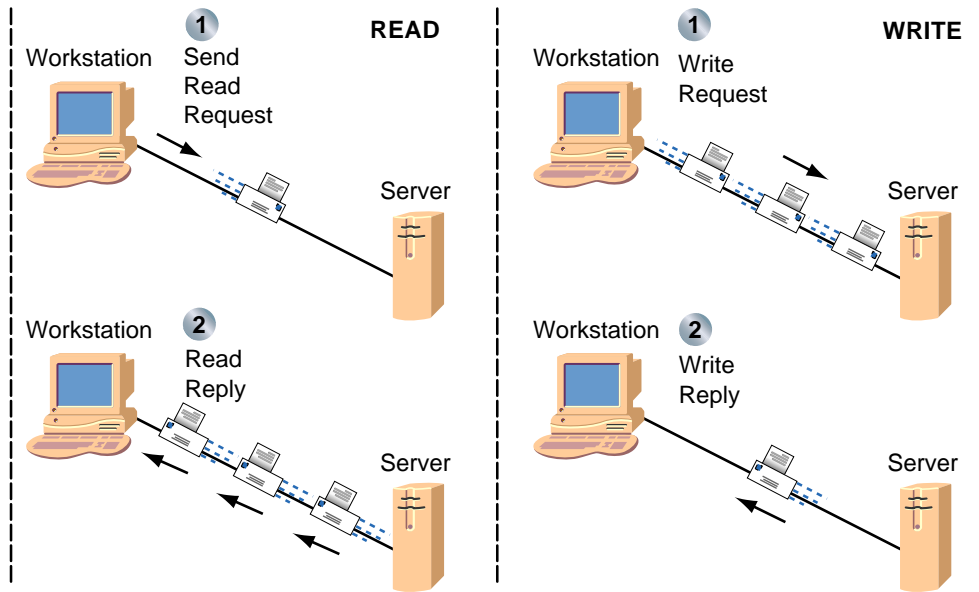


Figure 5-11: Packet Burst Protocol

Packet Burst Protocol

The Packet Burst™ protocol is a NetWare Core Protocol™ (NCP™) technology that expedites large file reads and writes. The Packet Burst protocol increases the efficiency of client/server communications by allowing workstations to submit a single file read or write request and receive up to 64 KB of data without submitting another request.

Over WAN links, standard NCP requests and responses can result in performance degradation due to the “ping pong” effect. As each station waits for a corresponding acknowledgment, the line is tied up and no other traffic is transmitted.

The delay is further compounded when large files are transmitted one packet at a time. Even small files require the exchange of numerous packets to fulfill a request.

The Packet Burst protocol can boost performance 10 to 300%, depending on factors such as memory, bandwidth, and file sizes.



In NetWare 5, Packet Burst is automatically enabled at both the workstation and the server.

Packet Burst Protocol



5-11 (Figure 5-11: Packet Burst Protocol)

- Define *Packet Burst protocol*.
- Explain how normal reads and writes occur.
- Discuss the performance gains that are possible when using the Packet Burst protocol.
- Explain that Packet Burst is automatically enabled.

In NetWare 4.11 and higher, the workstation client installation program automatically enables Packet Burst and the PBURST.NLM is now included in SERVER.EXE.

In prior versions of NetWare, the network administrator had to change parameters in the NET.CFG file on the workstation and load an NLM at the server to enable Packet Burst.

How the Packet Burst Protocol Works

The Packet Burst protocol allows a client to issue a single read or write request for blocks of data up to 64 KB in size. The data is partitioned into packets and these packets are transmitted back-to-back without requiring individual acknowledgment.

Burst Gap Time and Burst Window Size

The Packet Burst protocol uses a *burst gap time* and a *burst window size* to determine how much data is exchanged per *burst* transaction.

The *burst gap time* is a time delay requested by the client before individual packets are placed back-to-back on the media. This *gap time* is used to prevent fast servers from overrunning the client's buffers.

The *burst window size* refers to the number of frames or packets contained in a single burst.

With the Packet Burst protocol, the number of packets in the window is variable, up to a theoretical maximum value of 128 (64 KB divided by 512-byte packets).

The window size is also variable by workstation, depending on how many buffers the workstation has available, and by the constant monitoring of the line capacity by the Novell Client. The client renegotiates the parameters without user intervention.

Dropped Packets Recovery

When network traffic is heavy enough that packets are dropped in transmission, the Novell Client decreases the window size to minimize packet loss. Any packets that are lost are retransmitted individually; the entire *burst* does not need to be retransmitted.

The Packet Burst protocol monitors dropped packets and retransmits only the missing packets. When Packet Burst-enabled servers or clients transfer data to servers or clients that do not have Packet Burst enabled, the data defaults to normal NCP (one-request/one-response) mode.

Presentation**Notes****How the Packet Burst Protocol Works**

- Discuss burst gap time and burst window size.

This is one area in which the Packet Burst protocol's window technology differs from traditional sliding window protocols such as SDLC.

The window size for the Packet Burst protocol can be negotiated between the server and the workstation without user intervention.

- Discuss dropped packet recovery.

This is another deviation from standard windowing protocols. In standard windowing protocols, every packet including and after the bad packet must be retransmitted.

The Packet Burst Connection

A workstation sets up a Packet Burst connection with a NetWare server at attach/login time. Once established, the connection remains for the duration of the attachment.

If the Novell Client fails to make a Packet Burst connection during attach/login, it uses normal NCPs. By default, Packet Burst is enabled for all workstations.

Packet Burst is established individually for each connection to different servers. As a result, a workstation running the Novell Client can be attached to a NetWare 5 server using Packet Burst and to a NetWare 3.12 server using a standard NCP connection.

When Packet Burst is loaded, the Novell Client first determines whether the workstation has enough memory for the requested number of Packet Burst buffers. If sufficient memory is available, the client initiates a Packet Burst connection to the server.

During this connection process, the Novell Client negotiates maximum burst sizes, just as it negotiates packet size, with each connected server.

Once a Packet Burst connection is established between a workstation and a server, the NetWare workstation automatically uses the Packet Burst service whenever an application makes a read or write involving more than 512 bytes of data. Applications do not have to be Packet Burst aware.

Modifying Packet Burst Protocol Performance

In previous versions of NetWare, Packet Burst had to be enabled both at the workstation and at the server. In NetWare 5, Packet Burst is automatically enabled. It cannot be disabled at the server, but it can be disabled on individual workstations.

Presentation**Notes****How the Packet Burst Protocol Works** *(continued)*

- Explain that the Packet Burst connection occurs automatically.

- Discuss how to modify Packet Burst protocol performance.

The network administrator can disable Packet Burst or modify some Packet Burst parameters at the workstation.

To enable Packet Burst and set Packet Burst parameters in Windows 95 or Windows NT, do the following:

1. Right-click **Network Neighborhood**.
2. Click **Properties**.
3. Under the Configuration tab, click **Novell NetWare Client**.
4. Click **Properties**.
5. Click the **Advanced Settings** tab.
6. Scroll down and view the Packet Burst, Packet Burst Read Window Size, and Packet Burst Write Window Size parameters.

Large Internet Packets (LIPs)

Some network architectures, such as Ethernet and token ring, allow larger packets to be sent over the network. The Large Internet Packet (LIP) feature enhances throughput on networks with routers by allowing you to specify a large packet size.

On networks without LIP, the workstation and server negotiate the maximum packet size they will exchange. The maximum packet size depends on the packet receive buffer sizes set on both the workstation and the server.

You can increase the size on both, but if the server detects routers on the network, the negotiated packet size defaults to a 512-byte data packet size.

When LIP is enabled, the server ignores the router check during packet size negotiation. This allows data packets larger than 512 bytes to be exchanged, as long as the routers are configured to allow data packets larger than 512 bytes.



Just as with Packet Burst, LIP is automatically enabled at both the workstation and the server.

Presentation**Notes****How the Packet Burst Protocol Works** *(continued)*

- Continue discussing how to modify Packet Burst protocol performance.

Large Internet Packets (LIPs)

- Introduce LIP.
- Discuss the LIP process.

Enabling Routers for Larger Packets

Before LIP can allow larger packets to be exchanged through routers, you must configure the routers to handle larger packet sizes. To configure NetWare routers for larger packet sizes, use the following SET parameter:

SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE = *packet_size*

You can only use this parameter in the STARTUP.NCF file. The change takes effect when the server is restarted. The default value is 4202.

The maximum packet sizes supported by NetWare are listed below.

Topology	Packet Size
Token Ring (16 Mbps)	4202
Token Ring (4 Mbps)	4202
Ethernet	1514

Table 5-6: Maximum Packet Sizes

The Maximum Packet Size parameter must be set in all routers on your internetwork. Setting the routers to handle larger packet sizes allows servers and workstations to negotiate the largest packet sizes possible (the smaller of the workstation or server packet sizes).

ARCnet[®] segments will not handle LIPs because of their inherent size limitation.

Using LIP and Packet Burst Protocol

When LIP is used in conjunction with the Packet Burst protocol, several large packets can be sent consecutively without having to wait for the standard request/response dialogue of normal packet exchanges. This increases data transmission speed while reducing the number of packets exchanged.

Presentation

Notes

Enabling Routers for Larger Packets

- Discuss the procedures for enabling LIP at a router.

Using LIP and Packet Burst Protocol

- Discuss how implementing LIP and Packet Burst can greatly improve performance.

Written Exercise 5-6: Optimizing Network Performance

In this exercise, you optimize network performance.

Scenario: The Research department is writing an increasing number of small files to disk for a large database on your server. Users from other divisions within the organization are accessing this database and are causing additional traffic across the network.

The following questions are based on the scenario. Write your answers in the space provided and be prepared to discuss them.

1. What impact might a high-end disk driver/controller combination have on this situation?
2. Would implementing the Packet Burst protocol have a positive effect on network performance for this scenario? Why?
3. Would implementing LIP have a positive effect on network performance for this scenario? Why?

(End of Exercise)

Written Exercise 5-6: Optimizing Network Performance

- Introduce the exercise.



- Conduct the exercise.

- Discuss students' answers.

Answers:

1. Increased throughput; therefore, increased performance.
2. Yes. Increased throughput might be significant because of the reduction of the large number of reads and writes occurring with small files.
3. Yes, if the files are larger than 512 bytes.

Summary

One of the most challenging and rewarding responsibilities of a network administrator is optimizing performance on the network.

You should look at several areas when you assess the efficiency of your network or encounter a performance problem:

- Review performance statistics provided through MONITOR to determine the efficiency of your network.
- Modify parameters such as server packets and buffers, Packet Burst, and LIP to enhance server performance.
- Consider upgrading key components, such as network boards, disk drivers, and disk controllers.

Presentation**Notes****Summary**

- Summarize this section.

Review the objectives and answer questions:

1. Describe NetWare 5 memory allocation and configure the server for memory deallocation and garbage collection.
2. Define virtual memory and configure a NetWare 5 server to use virtual memory.
3. Create an application and adjust the CPU time allocated to it.
4. Describe memory protection and configure a NetWare 5 server to use protected memory.
5. Interpret the MONITOR Statistics screen.
6. Monitor and modify file and directory cache performance.
7. View and modify server buffer and packet parameters.
8. Define and enable block suballocation.
9. List the steps used to enable file compression.
10. Enable and manage the Packet BurstTM protocol.
11. Enable and manage Large Internet Packets (LIPs).

Notes

SECTION 6 Backing Up Servers and Workstations

Duration 02:00

Preparation

Complete the following:

- Make sure long name space has been added to all the volumes on the student servers.
- Copy the SMS backup emulator files (TPEMU.HAM and associated files) from your instructor CD to SYS:\SYSTEM\ on each student server.
- Load and configure the emulator on FS1.
- Perform a file system backup and restore to test the configuration in preparation for demonstrating and using NetWare Backup/Restore in class.
- Mount your Windows 95 installation CD as a NetWare volume and grant students access to it. Alternatively, you can copy the Windows 95 .CAB files to individual workstations.
- Mount your Novell Client CD as a NetWare volume and grant students access to it. Alternatively, you can copy the client installation files to an existing server volume.

SECTION 6

Backing Up Servers and Workstations

In this section, you learn how to back up and restore NetWare file systems, NDS directories, and workstation file systems.

Objectives

Upon completing this section, you should be able to

1. Explain backup strategies.
2. Back up a NetWare server's Directory and file system and a workstation's file system with NWBACK32.
3. Restore a NetWare server's Directory and file system and a workstation's file system with NWBACK32.

Presentation

Notes

Backing Up Servers and Workstations

- Introduce the section.

Objectives

- Discuss the objectives.

Introduction to Storage Management Services

NetWare 5 provides backup and restore functionality for complex networks through Storage Management Services™ (SMS™), a package of related services that allow data to be stored and retrieved.

The SMS backup process involves a *host server* (the NetWare server on which the backup program resides), a *target* (the NetWare server or workstation that contains the data to be backed up), and a workstation that is used to configure backup sessions and submit them to the host server.

SMS uses an application on the host server to communicate with modules on target devices. The application reads the information from the target device and sends it to a storage medium. Figure 6-1 illustrates this process.

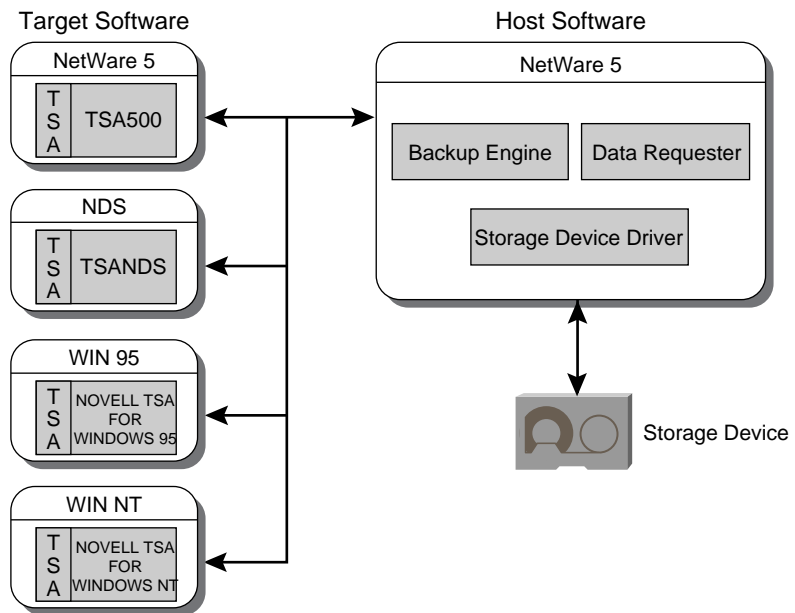


Figure 6-1: SMS Architecture

Presentation**Notes****Introduction to Storage Management Services**

- ❑ Discuss the importance of backing up data in a complex network environment.

- ❑ Emphasize that the network administrator is responsible for developing a backup strategy.

- ❑ Discuss the purpose of SMS.



6-1 (Figure 6-1: SMS Architecture)

A Target Service Agent (TSA) is a program which runs on a server or workstation. In conjunction with an SMS-compliant backup engine such as NetWare Backup/Restore, it allows data from a specific workstation or server to be backed up and restored.

Through specific software components, SMS allows you to back up the following types of information:

- NetWare server file system
- NetWare server DOS partition
- NDS database
- Windows 95 and Windows NT workstation file systems
- GroupWise® databases

Choosing a Backup Strategy

You can use three types of backups. Table 6-1 describes each strategy.

Type of Backup	Data That Will Be Backed Up	State of Archive Bit
Full	All data, regardless of when or if it has previously been backed up	Cleared
Incremental	Files that have been created or modified since the last full or incremental backup	Cleared
Differential	All data that has been modified since the last full backup	Not Cleared

Table 6-1: Backup Types

You can use these backup types in one of three backup strategies:

- Full backup at every backup session
- Full backup combined with incremental backups
- Full backup combined with differential backups



Do not combine differential and incremental backups. If you do, the differential backup will not contain all the changes that have been made since the last full backup.

When you are choosing a backup strategy, consider the time each method requires to back up data and the time each method requires to restore data.

Presentation**Notes****Introduction to Storage Management Services***(continued)*

- Briefly describe the SMS backup process.

- Mention the types of target devices that can be backed up using SMS.

Choosing a Backup Strategy

- Briefly explain each backup type.

- Describe the differences between the three suggested backup methods.

- Explain the rationale for choosing a strategy that combines backup types.

Focus on full server, full server incremental, and full server differential backups. These backups are the most common and complete types of backup. Used properly, they efficiently back up everything that needs to be backed up.

More customized types of backup can differ greatly in what they back up (files, directories, bindery, attributes, and so on). Those types of backups are not taught in this course.

This section provides an overview of SMS and presents a simple backup and restore. The CUSTOM type is not covered in this course.

Time Requirements for Completing a Backup

Figure 6-2 shows the relative amount of data backed up for each type of backup.

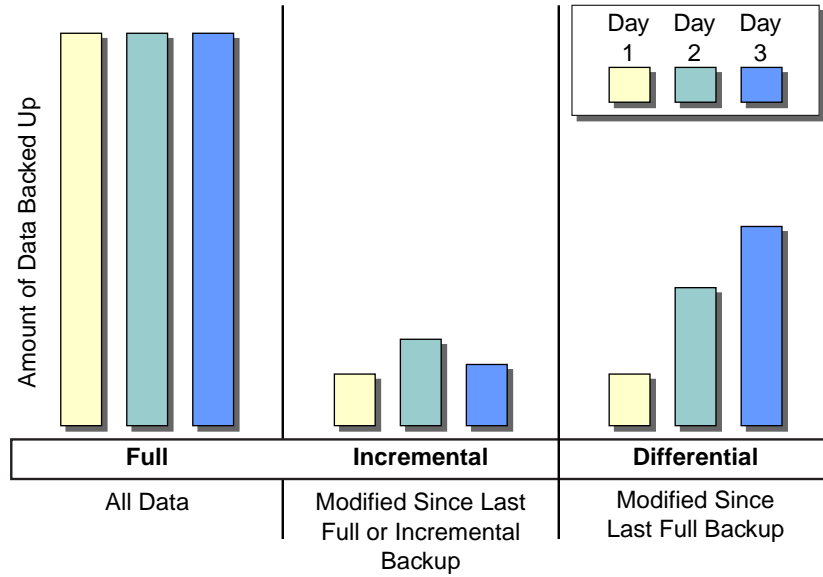


Figure 6-2: Backup Amounts

Time Requirements for Completing a Backup



6-2 (Figure 6-2: Backup Amounts)

- Explain how each backup strategy differs in the amount of data it backs up.

Based on the information from Figure 6-2, Figure 6-3 illustrates the relative amount of time each backup strategy might take.

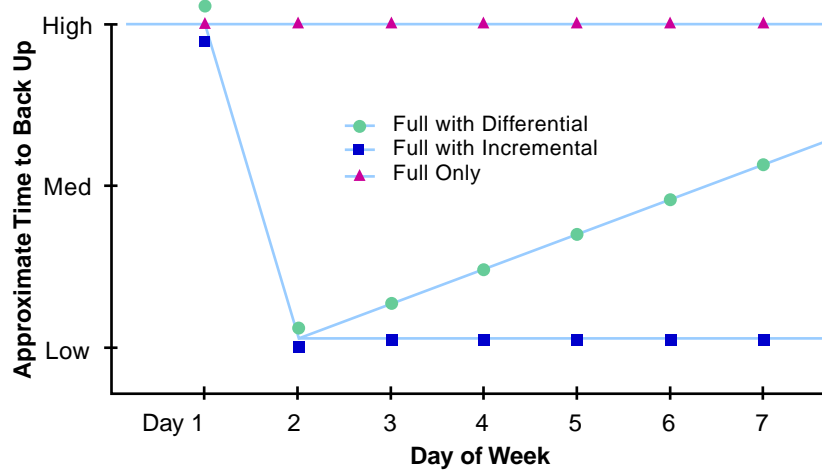


Figure 6-3: Time Requirements

Completing a full backup every time will require the most time. A full backup followed by incremental backups will require the least amount of time.

A full backup followed by differential backups will require increasingly longer amounts of time with each backup, but will require less time overall than performing a full backup.

Time Requirements for Completing a Backup *(continued)*

6-3 (Figure 6-3: Time Requirements)

- Explain how each backup strategy differs in the amount of time it requires to back up data.

Time Requirements for Restoring a Backup

Figure 6-4 shows the relative amount of time needed to perform a complete restoration based on each backup strategy.

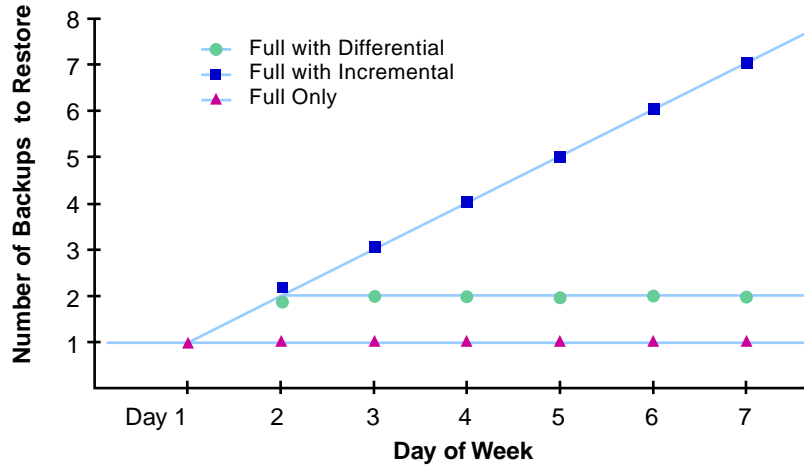


Figure 6-4: Time Required to Restore Backups

A full backup would be the fastest to restore because you need to restore only the most recent backup.

Full backups combined with incremental would be the slowest to restore because you need to first restore the most recent full backup and then each incremental backup since the full backup.

Full backups combined with differential backups fall somewhere in the middle, because you would need to first restore the most recent full backup and then the most recent differential backup.

Time Requirements for Restoring a Backup



6-4 (Figure 6-4: Time Required to Restore Backups)

- Explain how much time is required by each method to restore data.

- Summarize the differences between the three suggested strategies.

Use the following suggestions to help students decide which method should be used on a particular network:

- Daily full backup only. This strategy works well for a small network. A combination with another method would be more efficient.
- Weekly full backup with daily differential backup. This method is popular because restoring the data is easy.
- Weekly full backup with daily incremental backup. This method requires very little time to back up data.

Assigning Backup Responsibility

The user you assign to back up your network must have the following rights and knowledge:

- To work with NetWare server file systems, this user needs Read and File Scan rights to the files.
- To work with NDS, this user needs the Browse object and Read property rights to the whole tree.



These rights are sufficient for performing a full backup. To restore the file system or NDS tree, the user must also have Create rights.

- The user must know the passwords on the servers that act as hosts and targets.
- The user must know the password to the workstation if a password has been used with the target software.

Presentation

Notes

Assigning Backup Responsibility

- Discuss the rights required to perform backups.

This responsibility is usually given to the network administrator, who already has rights to all volumes and directories.

Written Exercise 6-1: Choosing a Backup Strategy

In this exercise, you recall facts related to backing up data.

1. What can be backed up using SMS?
2. Briefly describe the difference between a full backup combined with an incremental backup and a full backup combined with a differential backup.
3. Which backup method requires the greatest amount of time to restore data on day 7?
4. What are the minimum rights a user would need to back up NDS? The NetWare file system?

(End of Exercise)

Written Exercise 6-1: Choosing a Backup Strategy

- Introduce the exercise.



:5

- Have the students complete the exercise.

- Review the students' responses.

- Review the exercise.

Answers:

- Windows 95 and Windows NT workstation file systems
NetWare file systems
NetWare DOS partitions
NDS
GroupWise databases
- A full backup combined with incremental backups will back up only modified data from day to day. A full backup combined with differential backups will back up all data changed since the last full backup.
- The full backup combined with incremental backups.
- Browse object and Read property rights to the container being backed up. Read and File Scan rights to the directories and files being backed up.

Backing Up Servers and Workstations

You can use the SMS architecture to back up data from and restore data to servers and clients on your network. To back up servers and workstations, you need to use two utilities:

- NetWare Backup/Restore
- NWBACK32

NetWare Backup/Restore is a series of NLMs that run on the NetWare server. NWBACK32 is a client-based utility. Both are included with the NetWare 5 operating system.

NWBACK32 configures and submits backup or restore jobs to NetWare Backup/Restore, running on the host server. NetWare Backup/Restore processes the job, creates a session, establishes communication with the target, and conducts the backup or restoration.

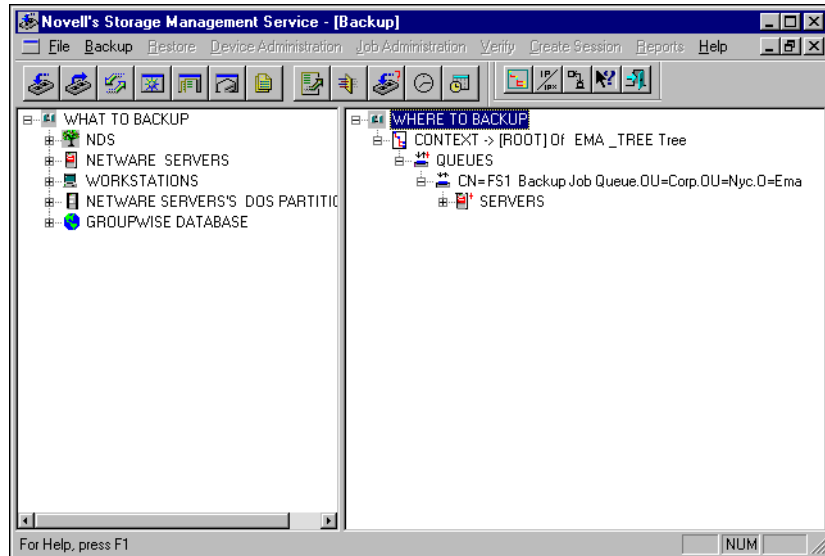


Figure 6-5: NWBACK32

Backing Up Servers and Workstations



6-5 (Figure 6-5: NWBACK32)

- Emphasize that NWBACK32 and NetWare Backup/Restore come with NetWare 5.

- Explain the roles of NWBACK32 and NetWare Backup/Restore.

Understanding Backup Terminology

You need to be familiar with the following terms:

- Host
- Target
- TSA
- Parent
- Child

Host

The *host* is the NetWare server running NetWare Backup/Restore to back up network resources. A backup device is attached to this server.



A tape device is attached to the host server, not to a workstation.

Target

The *target* is any NetWare server, workstation, or service which has a Target Service Agent (TSA) loaded. The TSA allows the target to be backed up by the host.

TSA

The *Target Service Agent (TSA)* is a program that processes data moving between a specific target and NetWare Backup/Restore.

Parent

A *parent* is a data set that can have subordinate data sets (other parents or children). In NetWare 5, for example, a parent would be a directory, a subdirectory, or a container.

Child

A *child* is a data set that has no subordinates. In the NetWare file system, for example, a child would be a file.

Presentation

Notes

Understanding Backup Terminology

- Discuss the terms presented on the student page.

- Emphasize that the tape device must be attached to the NetWare server (host).

NetWare Backup/Restore Guidelines

When you use NetWare Backup/Restore, keep the following guidelines in mind:

- Load NetWare Backup/Restore on the NetWare server to which your backup device is attached.
- Make sure you have enough disk space on the host server's SYS volume for temporary files and log files (1 MB should be sufficient).
- Make sure the designated media has enough storage space.

Be aware that security can be compromised if the scheduled backup session does not fit on the media.

In this case, you are prompted to insert another tape. If another tape is not inserted, the backup does not finish and the program does not exit.

To reduce this risk, set append to No, attend the backup so you can insert the next tape, or use a tape loader backup device.

- Limit access to the NetWare Backup/Restore NLMs to maintain the security of your NetWare server and to ensure data integrity.
- The error and backup log files display both the DOS-equivalent name and the name space (such as long, Macintosh[®], NFS[®], or OS/2[®]) used to create the directory or file.
- Monitor the size of NetWare Backup/Restore temporary files. NetWare Backup/Restore creates temporary files on the target server. These temporary files store information during backup. The files might become quite large if you have extended attributes or linked UNIX[®] files.
- Do not mount or dismount volumes or unload drivers during a backup session. You might corrupt data or abend the host server.

Presentation

Notes

NetWare Backup/Restore Guidelines

- Discuss the NetWare Backup/Restore guidelines.

- Explain that all file-specific information is backed up regardless of the filename format.

Backing Up a NetWare Server

You must load several software files and complete several tasks before you begin a backup session. The files differ depending on whether the information to be backed up is on the host server, the target server, or the workstation.

To back up NDS and file system information with NetWare Backup/Restore, complete the following tasks:

1. Load your tape device driver or driver interface.
2. Make sure a print queue object exists that is dedicated to and configured for backup operations.
3. Load the TSAs.

To Back Up	At This Console	Enter This Command
NetWare 5 host server	NetWare 5 host server	TSA500
NetWare 5 target server	NetWare 5 target server	TSA500
NDS	NetWare 5 server with a replica	TSANDS

Table 6-2: Commands for Backing Up a NetWare Server or NDS Database

4. Load the NetWare Backup/Restore NLMs on the host server.
5. On your workstation, run NWBACK32.EXE (located in SYS:\PUBLIC).
6. Specify the information to be backed up on the target.
7. Specify the location to which the information will be backed up.
8. Select the type of backup.
9. Set the schedule and rerun interval.
10. Provide a description of the session.
11. Submit the job.
12. Insert the media.
13. Proceed with the backup.
14. Add tapes as requested.

Presentation**Notes****Backing Up a NetWare Server**

- Discuss backing up a NetWare server.
- Emphasize that the files to be loaded differ depending on the target.
- Discuss the general steps for loading NetWare Backup/Restore.
- Emphasize the order in which TSAs must be loaded.



Demonstrate how to back up NDS and the file system.

- Re-emphasize the importance of testing backups.

If memory is in short supply, TSAs can be loaded and unloaded as needed. Otherwise, the TSAs can remain on the system. If the TSAs remain on the system, SMDR is loaded when NetWare Backup/Restore is loaded.

Load the TSA before you begin the demonstration.

Use presentation software to demonstrate how to back up data with NetWare Backup/Restore. Discuss the purpose of each step as you proceed.

Network administrators need to test both the backup software and the backup device. If using third-party software, they must make sure the software backs up the trustee assignments and extended NetWare file attributes.

Network administrators can test third-party backup software by creating a bogus directory structure with text files, backing up the files, deleting the files from the volume, and then restoring the files.

Backing Up Windows 95 or Windows NT Workstations

NetWare Backup/Restore can also be used to back up workstations on your network.

You can back up and restore information on the local hard disks of Windows workstations. You can back up specified directories or the entire workstation hard disk.

1. At the server, load TSAPROXY.
2. Add the Novell Target Service Agent for Windows 95 or the Novell Target Service Agent for Windows NT to the workstation.
3. Load the NetWare Backup/Restore NLMs on the host server.
4. On your workstation, run NWBACK32.EXE (located in the SYS:\PUBLIC directory).
5. Specify what information will be backed up on the target.
6. Specify the location to which the information will be backed up.
7. Select the type of backup.
8. Set the schedule and rerun interval.
9. Provide a description of the session.
10. Submit the job.
11. Insert the media.
12. Proceed with the backup.
13. Add tapes as requested.

Presentation

Notes

Backing Up Windows 95 or Windows NT Workstations

- Introduce workstation backups.

- Discuss the steps in backing up a Windows 95 or Windows NT Workstation.



(Optional) Demonstrate how to back up a Windows 95 or Windows NT Workstation.

Hands-On Exercise 6-2: Backing Up NDS and File System Information

In this exercise, you use NetWare Backup/Restore to back up NDS and file system information from another server in the classroom.

Part I: Loading the Client for Microsoft NetWorks, Backup Engine, and Tape Device Emulator

1. If you are using Windows 95 on your workstation, add the Client for Microsoft Networks. If you are using Windows NT Workstation, ignore this step.
 - a. On your Windows 95 workstation desktop, right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. In the Network window, make sure the **TCP/IP protocol** has been installed.
 - d. Click **Add**.
 - e. In the Select Network Component Type, double-click **Client**.
 - f. In the Select Network Client window, click **Microsoft** (under Manufacturers).
 - g. In the Select Network Client window, click **Client for Microsoft Networks**; then click **OK**.
 - h. In the Network window, make sure **Novell NetWare Client** is in the Primary Network Logon field.
 - i. In the Network window, click **TCP/IP**.
 - j. Click **Properties**.
 - k. In the TCP/IP Properties window, click the **Bindings** tab.

Hands-On Exercise 6-2: Backing Up NDS and File System Information

- Introduce the exercise.
- Introduce the tape device emulator.



Demonstrate how to use the tape device emulator.



:20

Have the students complete the exercise.

In order for the students to use NWBACK32.EXE, the students' workstations must have a DNS hostname assigned.

The tape device emulator is a HAM driver written by Novell that allows students to back up information to a file on a NetWare volume. The emulator emulates a tape drive attached to the host server.

The tape device emulator is not included in the NetWare server software. It is only available through Novell Education classes.

The tape device emulator is provided as a convenience for Novell Authorized Education Centers™ (NAECs™). Students will not be tested on how to use the backup emulator.

Demonstrate how to:

- Start the emulator
- Create a new virtual tape device file
- Mount an existing backup file
- Exit the emulator

- l. Make sure both **Client for Microsoft Networks** and **Novell Netware Client** are checked.
 - m. In the TCP/IP Properties window, click **OK**.
 - n. In the Network window, click **OK**.
 - o. If prompted, provide the **path** to the Windows 95 installation CD (provided by your instructor.)
 - p. When prompted, restart your workstation.
 - q. Login again as your Admin user.
 2. Create practice content to backup.
 - a. Using Windows Explorer, create a directory called **BACKUP** and a directory called **EXERCISE** at the root of your DATA volume.
 - b. Using Windows Explorer, copy the contents of the SYS:\JAVA directory on your server to DATA:\EXERCISE.
 3. Load the backup engine.
 - a. At your server console prompt, enter **TSA500**.
 4. Load the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUP\FILESYS.BCK**

Presentation**Notes****Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

- Provide students with the path to the Windows 95 installation files.

- Provide the tree name.

Part II: Configuring NDS

1. Verify that the backup queue was created correctly.
 - a. At your client workstation, run NetWare Administrator.
 - b. Browse to your **container**.
 - c. Verify that the backup queue exists.

Part III: Backing Up the File System

1. Load NetWare Backup/Restore.
 - a. At your server console, enter **QMAN**.
 - b. At the server console, enter **SBSC**.
 - c. At the server console, enter **SBCON**.
2. Make sure TSA500.NLM has been loaded on your target server.

If your server is	Your target server is
FS2	FS3
FS3	FS4
FS4	FS5
FS5	FS6
FS6	FS7
FS7	FS2

Table 6-3: Assigning Target Servers

Presentation**Notes****Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

- Make sure students understand which server they are to back up.

3. Configure NWBACK32.
 - a. On your workstation, run **NWBACK32.EXE** (located in the SYS:\PUBLIC directory).
 - b. In the SMDR Configuration window, select the **name** of your tree from the Tree Name drop-down list.
 - c. In the SMDR Context field, type the **typefull fully distinguished name** of your container.
 - d. In the SMDR Group Context field, type the **typefull fully distinguished name** of your container.
 - e. Make sure the Use SAP for Name Resolution box is marked.
 - f. Click **OK**.
 - g. Shut down and restart NWBACK32.
4. Configure your tape device emulator.
 - a. Click **Device Administration**.
 - b. Click **File**; then click **Change Context**.
 - c. In the Enter New Tree Name field, type the **name** of your tree.
 - d. In the Enter User's Name field, type the **fully distinguished name** of your Admin user.
 - e. In the Enter Password field, type the **password** for your Admin user.
 - f. In the Enter New Context field, type **[ROOT]**; then click **OK**.
 - g. In the left window pane, browse to the **Unidentified Media** in your tape backup device emulator.
 - h. Right-click **Unidentified Media**.
 - i. Click **New Label**.
 - j. In the Enter the New Label field, type **Virtual Cassette**.
 - k. Click **OK**.
 - l. When notified that the label has been changed, click **OK**.

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

5. Create the backup job.
 - a. Click **File**, then **New Session**, and then **Backup**.
 - b. In the left pane, double-click **WHAT TO BACKUP**.
 - c. In the left pane, double-click **NETWARE SERVERS**.
 - d. In the left pane, double-click your *target server*.
 - e. In the Authentication Required window, log in as your *Admin user*; then click **OK**.
 - f. In the left pane, double-click **DATA:**.
 - g. In the left pane, mark the box next to **EXERCISE** (under **DATA:**).
 - h. In the right pane, double-click **WHERE TO BACKUP**.
 - i. In the right pane, double-click **CONTEXT**.
 - j. In the right pane, double-click **QUEUES**.
 - k. In the right pane, right-click your *print queue*.
 - l. Click **Submit the Job**.
 - m. In the Enter the Type of Backup Job window, click **Full**; then click **Next**.
 - n. In the Subset of What You Are Backing Up window, click **Next**.
 - o. In the Filtering Options window, click **Next**.
 - p. In the Scheduling window, set the *value* in the Time field to two or three minutes later than the current time; then click **Next**.
 - q. In the Rerun Interval window, click **Next**.
 - r. In the Description of the Job You Are Submitting field, type **File System Backup *your_name***
 - s. Click **Finish**.
 - t. When asked if you want to submit the job now, click **Yes**.
 - u. When prompted that the job has been successfully submitted, click **OK**.

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

6. Observe the progress of the backup job.
 - a. In the NetWare Backup/Restore main screen on your server console, select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the backup Run Status to change to **Running**.
 - d. In the Queue Jobs window, scroll down to your **backup job** and press **Ins**.
 - e. Wait for the backup to be completed.
 - f. When notified that the session has been completed, press **Enter**.
 - g. At your server console, press **Esc** until you return to the NetWare Backup/Restore Main Menu.
7. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.
8. Delete the contents of DATA:\EXERCISE. This will help you verify that the files are restored properly in a later exercise.

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

Part IV: Backing Up NDS

1. Load the backup engine.
 - a. At the host server console, enter **TSANDS**.
 - b. At the host server console, enter **SMSDI**.
 - c. At the host server console, enter **SME**.
2. Configure the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUP\NDS.BCK**
3. Load NetWare Backup/Restore.
 - a. At the host server console, enter **QMAN**.
 - b. At the host server console, enter **SBSC**.
 - c. At the host server console, enter **SBCON**.
4. Make sure TSANDS.NLM has been loaded on your target server.

If your server is	Your target server is
FS2	FS3
FS3	FS4
FS4	FS5
FS5	FS6
FS6	FS7
FS7	FS2

Table 6-4: Assigning Target Servers

5. Configure the tape device emulator.
 - a. On your workstation, run **NWBACK32.EXE** (located in SYS:\PUBLIC).
 - b. Click **Device Administration**.
 - c. Click **File**; then click **Change Context**.
 - d. In the Enter New Tree Name field, type the **name** of your tree.

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

- e. In the Enter User's Name field, type the **fully distinguished name** of your Admin user.
 - f. In the Enter Password field, type the **password** for your Admin user.
 - g. In the Enter New Context field, type **[ROOT]**; then click **OK**.
 - h. In the left window pane, browse to the **Unidentified Media** in your tape backup device emulator.
 - i. Right-click **Unidentified Media**.
 - j. Click **New Label**.
 - k. In the Enter the New Label field, type **Virtual Cassette**
 - l. Click **OK**.
 - m. When notified that the label has been changed, click **OK**.
6. Create the backup job.
- a. Click **File**, then **New Session**, and then **Backup**.
 - b. In the left pane, double-click **WHAT TO BACKUP**.
 - c. In the left pane, double-click **NDS**.
 - d. In the left pane, double-click the **server** whose NDS replica you are supposed to back up.
 - e. In the left pane, double-click **EMA_TREE**.
 - f. In the Authentication Required window, log in as your **Admin user**; then click **OK**.
 - g. In the left pane, mark the box next to **Full Directory Backup** (under **EMA_TREE**).
 - h. In the right pane, double-click **WHERE TO BACKUP**.
 - i. In the right pane, double-click **CONTEXT**.
 - j. In the right pane, double-click **QUEUES**.
 - k. In the right pane, right-click your **print queue**.
 - l. Click **Submit the Job**.
 - m. In the Type of Backup Job window, click **Full**; then click **Next**.
 - n. In the Subset of What You Are Backing Up window, click **Next**.

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Continue the exercise.

- o. In the Filtering Options window, click **Next**.
 - p. In the Scheduling window, set the **value** in the Time field to two or three minutes later than the current time; then click **Next**.
 - q. In the Rerun Interval window, click **Next**.
 - r. In the Description of the Job You Are Submitting field, type **NDS Backup your_name**
 - s. Click **Finish**.
 - t. When asked if you want to submit the job now, click **Yes**.
 - u. When notified that the job has been successfully submitted, click **OK**.
 7. Observe the progress of the backup job.
 - a. In the NetWare Backup/Restore main screen, select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the backup Run Status to change to **Running**.
 - d. In the Queue Jobs window, scroll down to your **backup job** and press **Ins**.
 - e. Wait for the backup to be completed.
 - f. When notified that the session has been completed, press **Enter**.
 - g. Press **Esc** until you return to the NetWare Backup/Restore Main Menu.
 8. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.

(End of Exercise)

**Hands-On Exercise 6-2:
Backing Up NDS and File
System Information** *(continued)*

- Review the exercise.

Hands-On Exercise 6-3: Backing Up Workstations

In this exercise, you use NetWare Backup/Restore to back up your workstation's hard disk.

Part I: Load the Tape Device Emulator and Backup Engine

1. Load the backup engine.
 - a. At the host server console, enter **TSAPROXY**.
 - b. At the host server console, enter **SMSDI**.
 - c. At the host server console, enter **SME**.
2. Configure the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUPWORKSTAT.BCK**
3. Load NetWare Backup/Restore.
 - a. At the host server console, enter **QMAN**.
 - b. At the host server console, enter **SBSC**.
 - c. At the host server console, enter **SBCON**.
4. Create practice content to backup.
 - a. Using Windows Explorer, create a directory called **EXERCISE** at the root of your C:\ drive on your workstation.
 - b. Using Windows Explorer, copy the contents of the SYS:\JAVA directory on your server to C:\EXERCISE.

Hands-On Exercise 6-3: Backing Up Workstations



Introduce the exercise.



:20

Have the students complete the exercise.

Part II: Backing Up a Windows Workstation

1. If you are using Windows 95 or 98, add the Novell Target Service Agent for Windows 95/98 to your workstation.
 - a. Right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. In the Network window, click **Add**.
 - d. In the Select Network Component Type, click **Service**.
 - e. Click **Add**.
 - f. In the Select Network Service window, click **Novell**.
 - g. Click **Novell Target Services Agent for Windows 95/98**.
 - h. Click **OK**.
 - i. In the Network window, click **Novell Target Services Agent for Windows 95/98**.
 - j. Click **Properties**.
 - k. In the Username field, type **Admin**.
 - l. In the Password field, type **Novell**.
 - m. In the Protocol field, click **TCP/IP**.
 - n. In the Server Name field, type the name of your **server**.
 - o. In the Resources Available to TSA field, mark the **C** box.
 - p. Make sure **Auto Register on Reboot** and **Show TSA Icon on Taskbar** are marked.
 - q. Click **OK**.
 - r. Click **OK**.
 - s. If prompted, provide the path to the NetWare Client installation files (provided by your instructor).
 - t. Click **Yes** to restart the workstation.
 - u. Wait for your workstation to restart.
 - v. Log in as your **Admin user**.

**Hands-On Exercise 6-3:
Backing Up Workstations**
(continued)

- Continue the exercise.

- Provide the path to the NetWare Client installation files.

2. If you are using Windows NT, add the Novell Target Service Agent for Windows NT to your workstation.
 - a. Right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. Click the **Services** tab.
 - d. Click **Add**.
 - e. In the Select Network Service window, click **Novell Target Service Agent**.
 - f. Click **OK**.
 - g. In the Network Service window, click **Novell**.
 - h. In the Network window, click **Novell Target Service Agent**.
 - i. Click **OK**.
 - j. In the Network window, click **Novell Target Service Agent**.
 - k. Click **Properties**.
 - l. In the Preferred Server drop-down list, click your **server**.
 - m. In the Protocol drop-down list, click **TCP/IP**.
 - n. In the Drives Available field, mark the **C** box.
 - o. Make sure **Auto Register on Reboot** and **Allow backup user** are marked.
 - p. Click **OK**.
 - q. Click **Close**.
 - r. Click **Yes** to restart.
 - s. Wait for your workstation to restart.
 - t. Login in to your server as your **Admin user**.
3. Configure the tape emulator device.
 - a. On your workstation, run **NWBACK32.EXE** (located in the SYS:\PUBLIC directory).
 - b. Click **Device Administration**.
 - c. Click **File**; then click **Change Context**.
 - d. In the Enter New Tree Name field, type the **name** of your tree.

**Hands-On Exercise 6-3:
Backing Up Workstations**
(continued)

- Continue the exercise.

- e. In the Enter User's Name field, type the **full distinguished name** of your Admin user.
 - f. In the Enter Password field, type the **password** for your Admin user.
 - g. In the Enter New Context field, type **[ROOT]**; then click **OK**.
 - h. In the left window pane, browse to the **Unidentified Media** in your tape backup device emulator.
 - i. Right-click **Unidentified Media**.
 - j. Click **New Label**.
 - k. In the Enter the New Label field, type **Virtual Cassette**
 - l. Click **OK**.
 - m. When notified that the label has been changed, click **OK**.
4. Create the backup job.
- a. Click **File**, then **New Session**, and then **Backup**.
 - b. In the left pane, double-click **WHAT TO BACKUP**.
 - c. In the left pane, double-click **WORKSTATIONS**.
 - d. In the left pane, double-click your **server**.
 - e. Double-click your **workstation**.
 - f. In the Authentication Required window, type **Admin** in the User Name field and **Novell** in the Password field; then click **OK**.
 - g. In the left pane, double-click **C:** (under your **workstation**).
 - h. In the left pane, mark the box next to **Exercise**.
 - i. In the right pane, double-click **WHERE TO BACKUP**.
 - j. In the right pane, double-click **CONTEXT**.
 - k. In the right pane, double-click **QUEUES**.
 - l. In the right pane, right-click your **print queue**.
 - m. Click **Submit the Job**.
 - n. In the Enter the Type of Backup Job window, click **Full**; then click **Next**.
 - o. In the Subset of What You Are Backing Up window, click **Next**.

**Hands-On Exercise 6-3:
Backing Up Workstations**
(continued)

- Continue the exercise.

- p. In the Filtering Options window, click **Next**.
 - q. In the Scheduling window, set the **time** in the Time field to two or three minutes later than the current time; then click **Next**.
 - r. In the Rerun Interval window, click **Next**.
 - s. In the Description of the Job You Are Submitting field, type **Workstation Backup your_name**
 - t. Click **Finish**.
 - u. When asked if you want to submit the job now, click **Yes**.
 - v. When prompted that the job has been successfully submitted, click **OK**.
5. Observe the progress of the backup job.
 - a. In the NetWare Backup/Restore main screen, select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the backup Run Status to change to **Running**.
 - d. In the Queue Jobs window, scroll down to your **backup job** and press **Ins**.
 - e. Wait for the backup to be completed.
 - f. When notified that the session has been completed, press **Enter**.
 - g. Press **Esc** until you return to the NetWare Backup/Restore main screen.
 6. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.
 7. At your workstation, delete the C:\EXERCISE directory using Windows Explorer. This will help you verify that the files are restored properly in a later exercise.

(End of Exercise)

**Hands-On Exercise 6-3:
Backing Up Workstations**
(continued)

- Review the exercise.

Restoring Data

The SMS restore function allows you to restore data to the host server and any target, such as another server or a workstation.

To restore data, complete the following tasks:

1. Load your tape device driver or driver interface.
2. Load the TSAs.
3. Load NetWare Backup/Restore on the host server.
4. Run NWBACK32.EXE.
5. Select a target to which you want the files restored.
6. If required, log in as a user with necessary rights to restore the data.
7. Insert the media.
8. Select a restore device.
9. Select the session to be restored.
10. Specify what to restore from the backup.
11. Specify a schedule and rerun interval for the backup.
12. Submit the job.



If you are restoring both NDS and the file system, NDS must be restored first.

Presentation**Notes**

Restoring Data

- Discuss the general steps used to restore data.



Perform a restoration.

Delete several files which you backed up previously in class.

Restore the session containing the deleted files. Do not allow the data being restored to overwrite the existing data. This will restore only the missing files.

Hands-On Exercise 6-4: Restoring NDS and File System Information

In this exercise, you restore the NDS and file system information that you backed up in Exercise 6-3.

Part I: Restoring NDS.

1. Load the backup engine.
 - a. At the host server console, enter **TSANDS**.
 - b. At the host server console, enter **SMSDI**.
 - c. At the host server console, enter **SME**.
2. Configure the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUP\NDS.BCK**
3. Load NetWare Backup/Restore.
 - a. At the host server console, enter **QMAN**.
 - b. At the host server console, enter **SBSC**.
 - c. At the host server console, enter **SBCON**.
4. Make sure TSANDS.NLM has been loaded on your target server.

If your server is	Your target server is
FS2	FS3
FS3	FS4
FS4	FS5
FS5	FS6
FS6	FS7
FS7	FS2

Table 6-5: Assigning Target Servers

Hands-On Exercise 6-4: Restoring NDS and File System Information



Introduce the activity.



:20

Have the students complete
the exercise.

5. Create the restore job.
 - a. On your workstation, run **NWBACK32.EXE**.
 - b. Click **Restore**.
 - c. In the right pane, double-click **WHERE TO RESTORE**.
 - d. In the right pane, double-click **NDS**.
 - e. In the right pane, double-click your *target server*.
 - f. In the right pane, double-click your *target tree*.
 - g. In the Authentication Required window, login as your Admin user; then click **OK**.
 - h. Click **File**; then click **Change Context**.
 - i. In the Enter New Tree Name field, type the *name* of your tree.
 - j. In the Enter User's Name field, type the *full distinguished name* of your Admin user.
 - k. In the Enter Password field, type the *password* for your Admin user.
 - l. In the Enter New Context field, type **[ROOT]**; then click **OK**.
 - m. In the left pane, double-click **WHAT TO RESTORE**.
 - n. In the left pane, double-click **CONTEXT**.
 - o. In the left pane, double-click **QUEUES**.
 - p. In the left pane, double-click your *print queue*.
 - q. In the left pane, double-click **SERVERS**.
 - r. In the left pane, double-click your *server*.
 - s. In the left pane, double-click **DEVICES**.
 - t. In the left pane, double-click your *device*.
 - u. In the left pane, right-click on **Virtual Cassette**.
 - v. Click **Submit the Job**.
 - w. In the Select a Session window, click **NDS Backup your_name**; then click **Next**.
 - x. In the Subset of What You Are Restoring window, click **Next**.
 - y. In the Filtering Options window, click **Next**.
 - z. In the Another Location to Be Restored To and Overwriting Options window, click **Next**.

**Hands-On Exercise 6-4:
Restoring NDS and File
System Information** *(continued)*

- Continue the exercise.

- aa. In the Scheduling window, set the **value** in the Time field to two or three minutes later than the current time; then click **Next**.
 - ab. In the Rerun Interval window, click **Next**.
 - ac. Click **Finish**.
 - ad. When asked if you want to submit the job now, click **Yes**.
 - ae. When prompted that the job has been successfully submitted, click **OK**.
6. Observe the progress of the restore job.
 - a. In the NetWare Backup/Restore main screen, select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the Run Status to change to **Running**.
 - d. In the Queue Jobs window, scroll down to your backup job and press **Ins**.
 - e. Wait for the restore to be completed.
 - f. When notified that the session has been completed, press **Enter**.
 - g. Press **Esc** until you return to the NetWare Backup/Restore main screen.
 7. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.

**Hands-On Exercise 6-4:
Restoring NDS and File
System Information** *(continued)*

- Continue the exercise.

Part II: Restoring the File System

1. Load the backup engine.
 - a. At the host server console, enter **TSA500**.
 - b. At the host server console, enter **SMSDI**.
 - c. At the host server console, enter **SME**.
2. Configure the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUP\FILESYS.BCK**
3. Load NetWare Backup/Restore.
 - a. At the host server console, enter **QMAN**.
 - b. At the host server console, enter **SBSC**.
 - c. At the host server console, enter **SBCON**.
4. Make sure TSA500.NLM has been loaded on your target server.

If your server is	Your target server is
FS2	FS3
FS3	FS4
FS4	FS5
FS5	FS6
FS6	FS7
FS7	FS2

Table 6-6: Assigning Target Servers

5. Create the restore job.
 - a. On your workstation, run **NWBACK32.EXE**.
 - b. In the Quick Access window, click **Restore**.
 - c. In the right pane, double-click **WHERE TO RESTORE**.
 - d. In the right pane, double-click **NETWARE SERVERS**.
 - e. In the right pane, double-click your *target server*.

**Hands-On Exercise 6-4:
Restoring NDS and File
System Information** *(continued)*

- Continue the exercise.

- f. In the Authentication Required window, login as your Admin user; then click **OK**.
- g. Click **File**; then click **Change Context**.
- h. In the Enter New Tree Name field, type the *name* of your tree.
- i. In the Enter User's Name field, type the *full distinguished name* of your Admin user.
- j. In the Enter Password field, type the *password* for your Admin user.
- k. In the Enter New Context field, type **[ROOT]**; then click **OK**.
- l. In the left pane, double-click **WHAT TO RESTORE**.
- m. In the left pane, double-click **CONTEXT**.
- n. In the left pane, double-click **QUEUES**.
- o. In the left pane, double-click your *print queue*.
- p. In the left pane, double-click **SERVERS**.
- q. In the left pane, double-click your *server*.
- r. In the left pane, double-click **DEVICES**.
- s. In the left pane, double-click your *device*.
- t. In the left pane, right-click your *media*.
- u. Click **Submit the Job**.
- v. In the Select a Session window, click **File System Backup your_name**; then click Next.
- w. In the Subset of What You Are Restoring window, click **Next**.
- x. In the Filtering Options window, click **Next**.
- y. In the Another Location to Be Restored To and Overwriting Options window, click **Next**.
- z. In the Scheduling window, set the *value* in the Time field to two or three minutes later than the current time; then click **Next**.
- aa. In the Rerun Interval window, click **Next**.
- ab. Click **Finish**.
- ac. When asked if you want to submit the job now, click **Yes**.
- ad. When notified that the job has been successfully submitted, click **OK**.

**Hands-On Exercise 6-4:
Restoring NDS and File
System Information** *(continued)*

- Continue the exercise.

6. Observe the progress of the restore job.
 - a. In the NetWare Backup/Restore main screen, Select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the Run Status to change to **Active**.
 - d. In the Queue Jobs window, scroll down to your **restore job** and press **Ins**.
 - e. Wait for the restore job to be completed.
 - f. When notified that the session has been completed, press **Enter**.
 - g. At your server console, press **Esc** until you return to the NetWare Backup Restore main screen.
7. Using Windows Explorer, browse to the **EXERCISE** directory on your DATA volume and ensure that the files were restored.
8. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.

(End of Exercise)

**Hands-On Exercise 6-4:
Restoring NDS and File
System Information** *(continued)*

- Review the exercise.

Hands-On Exercise 6-5: Restoring Workstations

In this exercise, you restore the workstation file system information that you backed up previously.

Complete the following:

1. Load the backup engine.
 - a. At the host server console, enter **TSAPROXY**.
 - b. At the host server console, enter **SMSDI**.
 - c. At the host server console, enter **SME**.
2. Configure the tape device emulator.
 - a. At your server console prompt, enter **TPEMU**.
 - b. When prompted to specify an IO stream file, enter **DATA:\BACKUPWORKSTAT.BCK**
3. Load NetWare Backup/Restore.
 - a. At the host server console, enter **QMAN**.
 - b. At the host server console, enter **SBSC**.
 - c. At the host server console, enter **SBCON**.
4. Make sure Novell Target Services is running on your workstation and has been registered with your server.
5. Create the restore job.
 - a. On your workstation, run **NWBACK32.EXE**.
 - b. In the Quick Access window, click **Restore**.
 - c. In the right pane, double-click **WHERE TO RESTORE**.
 - d. In the right pane, double-click **WORKSTATIONS**.
 - e. In the right pane, double-click the **server** to which your workstation TSA is registered.
 - f. Double-click your **workstation**.
 - g. In the Authentication Required window, type **Admin** in the User Name field, and **Novell** in the Password field; then click **OK**.
 - h. Click **File**; then click **Change Context**.

Hands-On Exercise 6-5: Restoring Workstations



Introduce the exercise.



:20

Have the students complete
the exercise.

- i. In the Enter New Tree Name field, type the **name** of your tree.
- j. In the Enter User's Name field, type the **full distinguished name** of your Admin user.
- k. In the Enter Password field, type the **password** for your Admin user.
- l. In the Enter New Context field, type **[ROOT]**; then click **OK**.
- m. In the left pane, double-click **WHAT TO RESTORE**.
- n. In the left pane, double-click **CONTEXT**.
- o. In the left pane, double-click **QUEUES**.
- p. In the left pane, double-click your **print queue**.
- q. In the left pane, double-click **SERVERS**.
- r. In the left pane, double-click your **server**.
- s. In the left pane, double-click **DEVICES**.
- t. In the left pane, double-click your **device**.
- u. In the left pane, right-click your **media**.
- v. Click **Submit the Job**.
- w. In the Select a Session window, click **Workstation Backup your_name**; then click **Next**.
- x. In the Subset of What You Are Backing Up window, click **Next**.
- y. In the Filtering Options window, click **Next**.
- z. In the Another Location to Be Restored To and Overwriting Options window, click **Next**.
- aa. In the Scheduling window, set the **value** in the Time field to two or three minutes later than the current time; then click **Next**.
- ab. In the Rerun Interval window, click **Next**.
- ac. Click **Finish**.
- ad. When asked if you want to submit the job now, click **Yes**.
- ae. When notified that the job has been successfully submitted, click **OK**.

**Hands-On Exercise 6-5:
Restoring Workstations**
(continued)

- Continue the exercise.

6. Observe the progress of the restore job.
 - a. In the NetWare Backup/Restore main screen, select **Job Administration**.
 - b. In the Select Job window, select **Current Job List**.
 - c. Wait for the restore job to begin.
 - d. In the Queue Jobs window, scroll down to your **restore job** and press **Ins**.
 - e. Wait for the restore job to be completed.
 - f. When notified that the session completed, press **Enter**.
 - g. Press **Esc** until you return to the NetWare Backup/Restore main screen.

7. Unload the backup engine and tape emulator.
 - a. At the server console, enter **UNLOAD SBCON**.
 - b. At the server console, enter **UNLOAD SBSC**.
 - c. At the server console, enter **UNLOAD QMAN**.
 - d. At the server console, enter **UNLOAD SMSDI**.
 - e. At the server console, enter **UNLOAD TPEMU**.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 6-5:
Restoring Workstations**
(continued)

- Review the exercise.

Summary

SMS is a group of related services that allow you to back up and restore data. SMS comprises several software modules, including device drivers, SDI, SMDR, and TSAs, which allow data to be backed up and restored independently of the operating system.

NetWare 5 includes the NWBACK32 and the NetWare Backup/Restore utilities. Together, they allow you to use SMS to back up and restore data located on various targets, both workstations and NetWare servers.

SMS also creates backup session log and error files that help you manage the backup and restore process.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions:

1. Explain backup strategies.
2. Back up a NetWare server's Directory and file system and a workstation's file system with NWBACK32.
3. Restore a NetWare server's Directory and file system and a workstation's file system with NWBACK32.

Notes

SECTION 7 Using DNS/DHCP Services

Duration 03:00

Preparation

Make the .Container_Admns.CORP.NYC.EMA group object a trustee of the CORP.NYC.EMA container with Write [W] right.

SECTION 7 Using DNS/DHCP Services

In this section you learn how to install and configure Novell DNS/DHCP services.

Objectives

Upon completing this section, you should be able to

1. Describe Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services.
2. Install DNS and DHCP services.
3. Configure and start DHCP services.
4. Configure DHCP options to deliver configuration information to TCP/IP hosts on the network.
5. Import a DHCP database.
6. Configure and start DNS services.
7. Import a DNS database.

Presentation

Notes

Using DNS/DHCP Services

- Introduce the section.

Objectives

- Present the section objectives.

DNS/DHCP Overview

In the past, NetWare has only supported the NetWare Core Protocol™ (NCP™) natively over the IPX™ protocol. The IPX protocol requires very little user intervention to configure and administer.

With the release of NetWare 5, NetWare adds native NCP support for the TCP/IP protocol, eliminating the need to encapsulate. However, the overhead required to configure and administer the TCP/IP protocol can be very time-consuming.

To alleviate the administration requirements of the TCP/IP protocol, NetWare 5 includes a product called Novell DNS/DHCP Services. This product integrates the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) into the NDS database.

Integration of these services into NDS offers centralized administration, replication, and enterprise-wide management of Internet Protocol (IP) network addresses and hostnames.

This section provides a brief overview of DHCP and DNS, and explains how to install and configure these services on the NetWare platform.

DNS

Domain Name Services (DNS) is a distributed database system that provides hostname-to-IP address mapping for computers on an internetwork. Internet Protocol (IP) requires every machine on the network to have a unique IP address such as 137.65.1.79.

Unlike computers, users identify things more easily by names than by addresses. DNS was created to help users find other computers on the network by name rather than by IP address.

DNS services are offered to networks through a DNS server. Any computer on the Internet can use a DNS server to locate any other computer on the Internet.

DNS is made up of two distinct components, the hierarchy and the name service. The *DNS hierarchy* specifies the structure, naming conventions, and delegation of authority used in the DNS service. The *DNS name service* provides the actual name-to-address mapping mechanism.

Presentation**Notes****DNS/DHCP Overview**

- Contrast the administration overhead required for IPX and IP.
- Explain that DHCP and DNS have been integrated with NDS.

DNS

- Define *DNS*.

DHCP

DHCP, which is built on a client-server model, provides configuration parameters to Internet hosts. Both servers and clients are hosts. The DHCP server provides initialization parameters through DHCP. The client requests parameters from the server.

The DHCP protocol consists of two components: a protocol used to deliver host-specific configuration parameters from a DHCP server to a host and a protocol for assigning network addresses to hosts.

IP address assignments are supported by DHCP in one of three ways:

- **Automatic Allocation:** DHCP assigns a permanent IP address to a host.
- **Dynamic Allocation:** An IP address is assigned to a host for a limited period of time (or until the host relinquishes the address).
- **Manual Allocation:** This method requires that you assign the address. DHCP simply delivers the address to the host.

DHCP is designed to provide all the necessary name and address information required to automatically locate hosts on the network.

Presentation

Notes

DHCP

- Define *DHCP*.

- Introduce and describe DHCP.

For more information, refer to RFC 1531.

Snap-Ins for NetWare Administrator

To manage DNS/DHCP within NDS, you must extend the schema of the NDS tree. Whenever you extend the schema of an NDS tree, you must also install the appropriate snap-in files to manage those new objects from within NetWare Administrator. NetWare 5 includes the appropriate snap-in files for DNS/DHCP Services.

Most NetWare Administrator snap-in files allow you to configure new objects in an extended NDS tree. The DNS/DHCP snap-in files do not provide this functionality.

The DNS/DHCP snap-in files do allow you to see DNS/DHCP objects as known objects. You cannot view or configure the details of these objects in NetWare Administrator, but you can perform other NDS operations, such as deleting and moving these objects.

You must configure the new objects through a utility called DNS/DHCP Management Console.

DNS/DHCP Management Console

The DNS/DHCP Management Console, a Java application that provides a graphical user interface, allows you to configure and manage IP addresses and name services through NDS-based DHCP and DNS objects.

The DNS/DHCP Management Console can be launched from within NetWare Administrator or as a standalone utility on a Windows 95 or Windows NT client.

Because the DNS/DHCP Management Console requires access to the DNS and DHCP objects that are stored in the NDS database, you must run the utility on a workstation that has the Novell Client loaded.

Your workstation must have a minimum of 48 MB of RAM to run the DNS/DHCP Management Console. The recommended amount of RAM is at least 64 MB.

The DNS/DHCP Management Console consumes 8.5 MB of disk space on the workstation on which it is installed.

Presentation**Notes****Snap-Ins for NetWare Administrator**

- Explain that if the DNS/DHCP snap-in files are not installed, the DNS/DHCP objects appear as unknown objects in NetWare Administrator.

- Point out that the DNS/DHCP snap-in files do not allow the network administrator to configure DNS/DHCP objects in NetWare Administrator.

DNS/DHCP Management Console

- Discuss the purpose of the DNS/DHCP Management Console.

- Discuss the requirements for running the DNS/DHCP Management Console.

DNS/DHCP Objects

Novell integrates DNS and DHCP into NDS by extending the NDS schema to support new NDS objects. The extended schema supports various objects specific to DNS and DHCP. Integrating these new objects into NDS simplifies the administration and configuration of DNS and DHCP services.

At the time the schema is extended, three NDS objects are created: a DNSDHCP-GROUP group object, a DNS-DHCP locator object, and a RootServerInfo zone object. Only one instance of these object types can exist in an NDS tree.

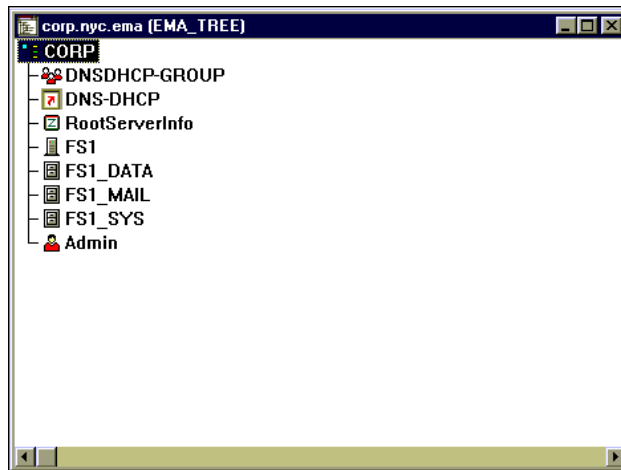


Figure 7-1: DNS/DHCP Group and Locator Objects in NetWare Administrator



In this course, the new NDS objects that support DNS and DHCP services are referred to as *DNS objects* and *DHCP objects*.

Other DNS and DHCP objects can be created manually as needed.

Presentation**Notes****DNS/DHCP Objects**

- Introduce the new DNS/DHCP objects supported when the schema is extended:
 - DNSDHCP-GROUP group object
 - DNS-DHCP locator object
 - RootServerInfo zone object

You might need to explain schema extension to students who are not familiar with the term.

DNSDHCP-GROUP Group Object

The DNSDHCP-GROUP group object is a standard NDS group object.

When a DNS or DHCP object is created, the DNSDHCP-GROUP group object is always automatically made a trustee. Access to information contained in DNS and DHCP objects can then be obtained by any NDS object by making that object a member of the DNSDHCP-GROUP group object.

NetWare servers that you designate as DNS and DHCP servers are automatically made members of the DNSDHCP-GROUP group object. This provides the designated NetWare servers with rights to the DNS and DHCP configuration information contained in NDS.

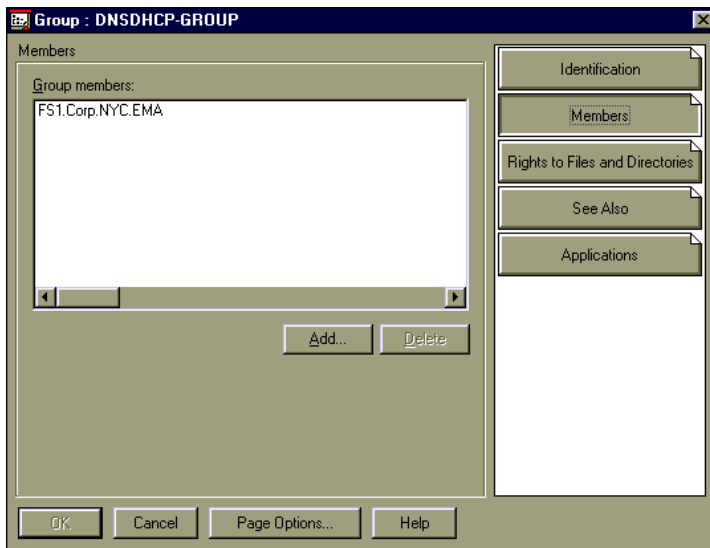


Figure 7-2: Members of the DNSDHCP-GROUP Group Object

Presentation

Notes

DNSDHCP-GROUP Group Object

- Discuss the DNSDHCP-GROUP group object.

DNS-DHCP Locator Object

The DNS-DHCP locator object contains global defaults, DHCP options, and lists of all DHCP and DNS servers, subnets, and zones in the NDS tree.

The DNS/DHCP Management Console can display DNS/DHCP objects without having to search the tree. The DNS-DHCP locator object is an unconfigurable object; therefore, it is not displayed in the DNS/DHCP Management Console.

RootServerInfo Zone Object

On the Internet, domain names are reserved by organizations to ensure that a particular name will resolve to the IP address used by the organization.

The domain names reserved by these organizations usually fit under an existing root of a domain. For example, some common domain roots are .COM, .ORG, .GOV, and .EDU.

Root name servers are domain name servers that are maintained on the Internet. These servers contain configuration information for the starting of a domain.

The RootServerInfo zone object points to root servers on the Internet. This object allows you to resolve domain names that belong to domains that you do not maintain in your NDS tree.

For example, suppose you maintain a domain in your tree for the domain XYZ.ORG. and you need to resolve the name WWW.NOVELL.COM. Since the NOVELL.COM zone is not in your tree, the RootServerInfo zone object points you to a root name server on the Internet that could resolve that name into an IP address for you.

Presentation

Notes

DNS-DHCP Locator Object

- Discuss the DNS-DHCP locator object.

RootServerInfo Zone Object

- Discuss the RootServerInfo zone object.

DHCP Objects

Five new DHCP objects (see Figure 7-3) are available once the schema has been extended. They are described in greater detail later in this section.

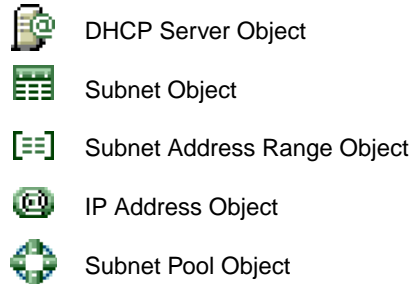


Figure 7-3: The DHCP Objects

DNS Objects

Four new DNS objects (see Figure 7-4) are available after the schema has been extended. They are described in greater detail later in this section.

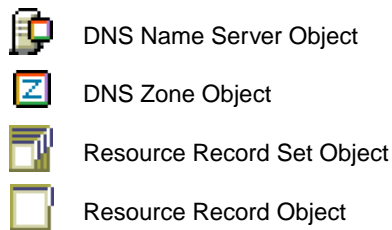


Figure 7-4: The DNS Objects

Presentation**Notes****DHCP Objects**

7-1 (Figure 7-3: The DHCP Objects)

- Introduce the DHCP objects.

DNS Objects

7-2 (Figure 7-4: The DNS Objects)

- Introduce the DNS objects.

Installing DNS/DHCP Services

When you install NetWare 5, the files to run Novell DNS/DHCP services are copied to the SYS volume on your server. These files include NLMs, which are copied to SYS:SYSTEM, and the Management Console setup files, which are copied to SYS:SYSTEM\PUBLIC\DNSDHCP.

To complete the installation of DNS/DHCP, you must complete the following tasks:

1. Extend the NDS schema and create default DNS/DHCP objects.
2. Install the Novell Client on the machine that will run the DNS/DHCP Management Console.
3. Install the DNS/DHCP Management Console and NetWare Administrator snap-in files.

Extending the NDS Schema and Creating Default DNS/DHCP Objects

The schema of NDS must be extended so that DNS and DHCP objects can be entered and stored in the NDS database.

You can extend the NDS schema and create the three DNS/DHCP default objects in one of three ways:

- Install Novell DNS/DHCP Services during the initial NetWare installation.
- Install Novell DNS/DHCP Services by running the NetWare installation program from the NetWare GUI.
- Run DNIPINST.NLM.

Presentation**Notes****Installing DNS/DHCP Services**

- Briefly discuss the additional tasks required to complete the installation of DNS/DHCP.

Extending the NDS Schema and Creating Default DNS/DHCP Objects

- Point out the three ways to extend the NDS schema and create the default DNS/DHCP objects.

To extend the NDS schema and create the three default DNS/DHCP objects using the NetWare installation program, do the following:

1. Launch the NetWare installation program.
 - a. In the NetWare GUI, click **Novell**.
 - b. Click **Install**.
 - c. In the Installed Products window, click **New Product**.
 - d. In the Source Path window, provide the **path** to the INSTALL directory of the NetWare 5 installation files.

You can use the Browse button to the right of the Path field to navigate to the source directory.

If the source files are located on another server, you will be prompted to authenticate to that server.
 - e. When the path has been provided, click **OK**.
 - f. In the Additional Products and Services window, mark the **Novell DNS/DHCP Services** box.
 - g. Click **Next**.
2. Authenticate yourself to NDS as a user that has rights to extend the schema. This user object must have Supervisor object rights to the [Root] of the tree.
 - a. In the Username field, type in the **fully distinguished name** of a user that has Supervisor rights to the [Root] of your NDS tree.
 - b. In the Password Field, enter the **password**.
 - c. Click **OK**.
3. Provide the NDS context in which you want to create the DNS-DHCP locator, DNSDHCP-GROUP group, and RootServerInfo zone objects.
 - a. To change the context in which to create any one of the default objects, browse to or type in the **desired context**.
 - b. When the contexts are set, click **Next**.
4. In the Summary Window, click **Finish**.
5. In the Installation Complete window, click **Yes** to reboot.

Presentation**Notes****Extending the NDS Schema and
Creating Default DNS/DHCP
Objects** *(continued)*

Demonstrate how to extend the NDS schema to run DNS/DHCP services.

Note: You can use either the DNIPINST.NLM, or the NetWare installation program in the NetWare GUI.

This demonstration must take place before Exercise 7-1 so that the schema will be extended for students.

To extend the NDS schema and create the three default DNS/DHCP objects using the DNIPINST.NLM, do the following:

1. At your NetWare server console prompt, enter
DNIPINST
2. Authenticate yourself to NDS as a user that has rights to extend the schema. This user object must have Supervisor object rights to the [Root] of the NDS tree.
 - a. In the Username field, type in the **fully distinguished name** of a user that has Supervisor rights to the [Root] of your NDS tree.
 - b. In the Password Field, enter the **password**.
 - c. Select **Press ENTER to Login to NDS**.
3. Provide the NDS context in which you want to create the DNS/DHCP locator, DNSDHCP-GROUP group, and RootServerInfo zone objects.
 - a. To change the context in which to create any one of the default objects, highlight the **context** field.
 - b. Enter the **context** in which you want to create the object.
 - c. When the desired contexts are set, select **Press ENTER to Create Objects**.
4. Once the DNS/DHCP schema extensions have been added, press **Enter** to terminate DNIPINST.NLM.

Presentation

Notes

**Extending the NDS Schema and
Creating Default DNS/DHCP
Objects** *(continued)*



Continue the demonstration.

Installing the Novell Client

Because the DNS/DHCP Management Console must be able to configure DNS and DHCP objects in the NDS tree, the DNS/DHCP Management Console must be installed and executed on a workstation that has the Novell Client installed.

Installing the DNS/DHCP Management Console

To configure DNS and DHCP services and see the new DNS/DHCP objects within NetWare Administrator, you must install the DNS/DHCP Management Console and the NetWare Administrator snap-in files.

To install the DNS/DHCP Management Console and NetWare Administrator snap-in files, complete the following:

1. Log in to your NetWare server.
2. Run the DNS/DHCP installation utility. This utility allows you to
 - Execute **SYS:\PUBLIC\DNSDHCP\SETUP.EXE**
 - Install the DNS/DHCP Management Console on the local hard disk
 - Install the snap-in files to the same directory as the NetWare Administrator tool
 - Reboot the computer

Presentation**Notes****Installing the Novell Client**

- Explain that the workstation running the DNS/DHCP Management Console requires the Novell Client.
- Point out that the Novell Client has already been installed as part of classroom setup.

Installing the DNS/DHCP Management Console

- Point out that the new objects in the NDS tree can only be viewed in NetWare Administrator using the snap-in files.
- Point out that DNS/DHCP objects can only be configured using the DNS/DHCP Management Console.



Demonstrate how to install the DNS/DHCP Management Console and the NetWare Administrator snap-in files.

Note: Students perform this task in the next exercise. If you want, you can have the students perform this task as you demonstrate it.

Hands-On Exercise 7-1: Installing Novell DNS/DHCP Services

In this exercise you install the DNS/DHCP Management Console and the NetWare Administrator snap-in files needed to administer DNS and DHCP services through NDS.

Complete the following from your workstation:

1. Log in to your NetWare server as your **Admin** user.
2. Run the DNS/DHCP Administration installation utility.
 - a. Click **Start**.
 - b. Click **Run**.
 - c. Click **Browse**.
 - d. Navigate to and double-click **SYS:\PUBLIC\DNSDHCP\SETUP.EXE**.
 - e. Click **OK**.
 - f. After reading the welcome screen, click **Next**.
 - g. To accept the default destination path, click **Next**.
 - h. When files are done copying, make sure **Copy the snap-in files** is marked.
 - i. Click **Next**.
 - j. When prompted to select a directory in which to place the snap-in files, click **Browse**.
 - k. Navigate to the **SYS:\PUBLIC\WIN32** directory.
 - l. Click **OK**.
 - m. Click **Next**.
 - n. When asked to view the readme file, click **No**.
 - o. Click **OK** to finish.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 7-1:
Installing Novell DNS/DHCP
Services**

- Introduce the exercise.



:10

- Conduct the exercise.

- Review the exercise.

Point out that the NDS schema has already been extended during the instructor demonstration.

Assist the students as necessary.

Configuring and Starting DHCP Services

To use DHCP services on your network, you must

- Assign a NetWare server as a DHCP server
- Configure the IP information that you want DHCP to assign to the workstations
- Start the DHCP service

The DNS/DHCP Management Console is the only utility you can use to configure DHCP objects that reside in the NDS tree.

Running the DNS/DHCP Management Console

You can start the DNS/DHCP Management Console from the Tools menu in NetWare Administrator or from the DNSDHCP shortcut created on your desktop during installation.

If you launch the DNS/DHCP Management Console from within NetWare Administrator, the NDS tree you are currently browsing will be set as the target NDS tree.

If you launch the DNS/DHCP Management Console from a Windows 95 or Windows NT desktop, you will be prompted for the target NDS tree.

Because the DNS/DHCP Management Console allows you to configure DNS and DHCP services in multiple trees, you must specify which NDS tree you want to configure.

To specify the NDS tree you want to administer, enter the tree name in the Enter NDS Tree Name field and click Launch.

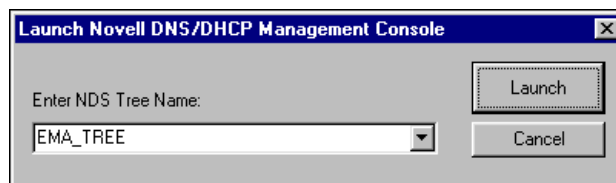


Figure 7-5: Selecting a Target NDS Tree to Manage DNS/DHCP Services

Configuring and Starting DHCP Services

- Discuss the two ways to launch the DNS/DHCP Management Console.

Running the DNS/DHCP Management Console



Demonstrate how to launch the DNS/DHCP Management Console.

Note: By default, the DNS/DHCP Management Console is installed in the following directory:

C:\Program Files\Novell\DNSDHCP\

The executable is DNSDHCP.EXE.

When the main console screen appears, it includes two tabs—a DNS Service tab and a DHCP Service tab.

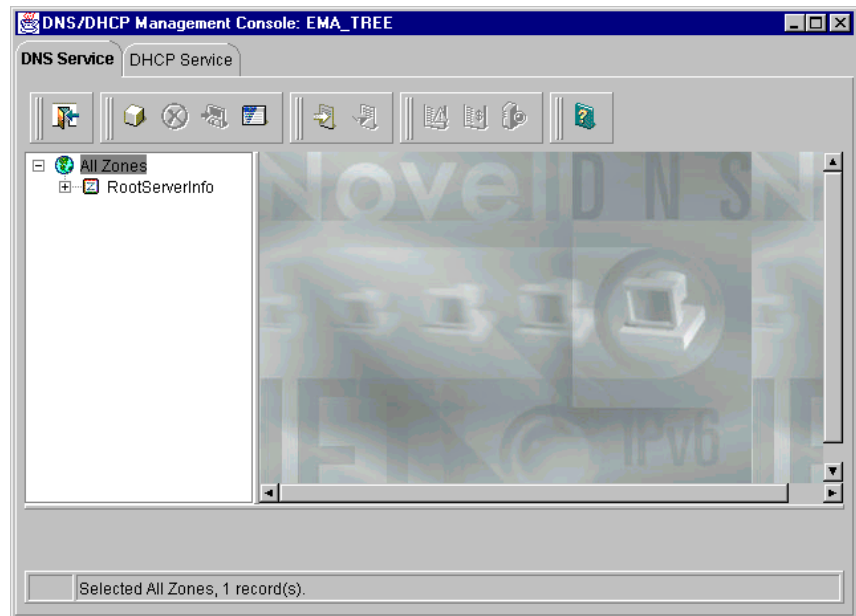


Figure 7-6: The DNS/DHCP Management Console

Each tab page has three panes. The left pane displays the managed objects (either IP addresses or DNS zones) in the tree. The right pane displays detailed information about the highlighted object in the left or bottom pane. The bottom pane lists either the DHCP servers or the DNS servers that exist in the NDS tree that is being managed.

You use the toolbar below the DHCP Service and DNS Service tabs to manage the highlighted items.

Each button on the tool bar has an identification screen associated with it. The identification screen appears when you rest the cursor on top of the button.

The status bar at the bottom of the DNS/DHCP Management Console shows the selected object, the current database access operation status, or the server interface status.

Presentation**Notes****Running the DNS/DHCP Management Console** *(continued)*

Demonstrate the different parts of the DNS/DHCP Management Console main screen.

Configuring a DHCP Server Object

The DHCP server object represents a DHCP server. It contains a listing of subnet ranges that the DHCP server is servicing. The DHCP server object also contains all server-specific configuration and policy information.

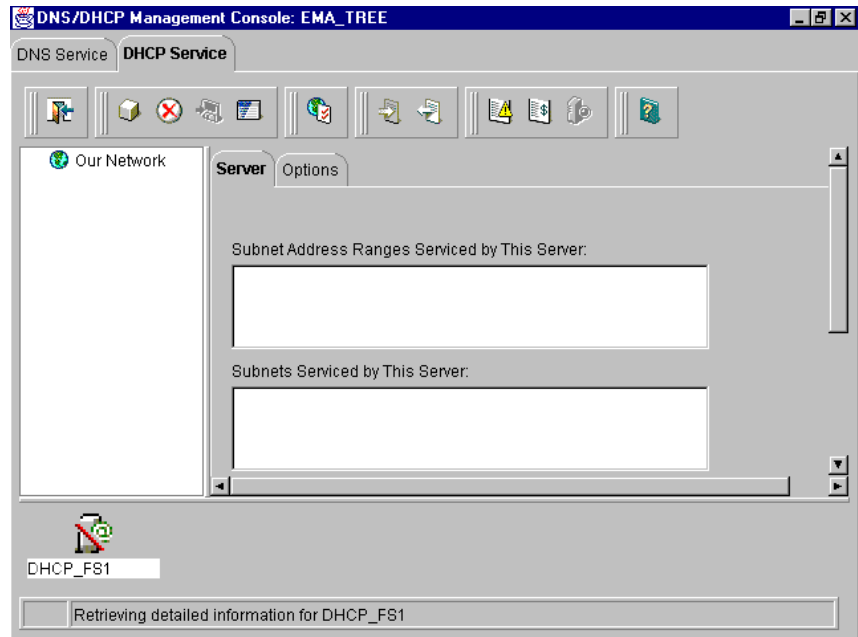


Figure 7-7: Configurable DHCP Server Options

You can create a DHCP server object in any of the following container objects:

- Organization (O)
- Organizational Unit (OU)
- Country (C)
- Locality (L)

Presentation

Notes

Configuring a DHCP Server Object

- Describe the DHCP server object.

- Point out which containers can hold a DHCP server object.

To create a DHCP server object, do the following:

1. Start the DNS/DHCP Management Console.
2. Click the **DHCP Service** tab.
3. Create a DHCP server object.
 - a. Click the **Create** button.
 - b. Click **DHCP Server**.
 - c. Click **OK**.
4. Select the NetWare server you want to specify as a DHCP server.
 - a. Browse to the container where your NetWare server resides.
 - b. Click your *server object*.
 - c. Click **OK**.

The NDS server object you choose sets the context of the to-be-created DHCP server object. The default DHCP server name will be the same as the selected NDS server object with the DHCP_ prefix.

You can modify the name of the DHCP server later from within NetWare Administrator.

5. Click **Create**.
6. In the bottom pane of the DHCP Service tab windows, click the DHCP server you just created. The details window appears.

From the DHCP server object details window, you can configure SNMP traps, audit trails, audit logs, audit alerts, mobile user options, and synchronization wait time.

You can also configure the DHCP server to verify that an IP address is not in use by having it ping first for the address.



The DHCP server object you just created will have a line through it until the DHCP service is actually running on the server.

Presentation**Notes****Configuring a DHCP Server Object***(continued)*

Demonstrate how to create a DHCP server object.

- Discuss the DHCP server options.

Be sure to mark **Define Additional Properties**.

Configuring a DHCP Subnet Object

The DHCP subnet object represents an IP network address that is assigned to a physical network segment. The subnet object is a container object that holds IP address configuration information that can be assigned to nodes that reside on that IP network segment.

The configuration information that is contained in the DHCP subnet object is represented in NDS as the IP address and address range objects.

You can create a DHCP subnet object in the following container objects:

- Organization (O)
- Organizational Unit (OU)
- Country (C)
- Locality (L)

To create a DHCP subnet object, do the following:

1. In the toolbar, click the **Create** button.
2. In the Create New DHCP Record dialog, double-click **Subnet**.

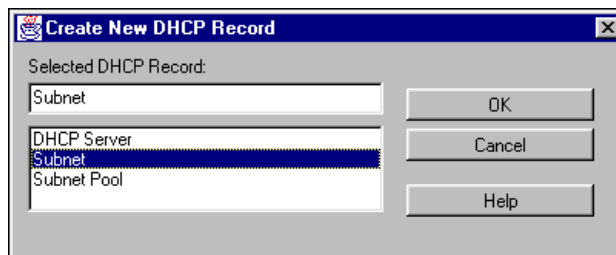


Figure 7-8: The Create New DHCP Record Dialog

Presentation**Notes****Configuring a DHCP Subnet Object**

- Introduce the DHCP subnet object.
- Explain that the DHCP subnet object is a container object.



Demonstrate how to create a DHCP subnet object.

Note: In Exercise 7-2, “Configuring and Starting DHCP Services,” students configure their workstations to request IP addresses from a DHCP server.

You should only have one valid DHCP server configured for use on your classroom network segment. If you configure more than one DHCP server to service the same network segment, you will have the following problems:

- You cannot guarantee which DHCP server will service the requests.
- The DHCP servers do not know which IP addresses have already been assigned by other DHCP servers.

If a DHCP server is already in use in your classroom, create a subnet object that uses an IP subnet address other than the one in use in your classroom.

If a DHCP server is not already in use in your classroom, create a subnet object that uses the IP subnet address appropriate for your classroom. Student workstations can then receive addresses from your DHCP server during the exercise.

3. Provide the subnet object with the following:

- Subnet Name
- NDS Context
- Subnet Address
- Subnet Mask
- Default DHCP Server

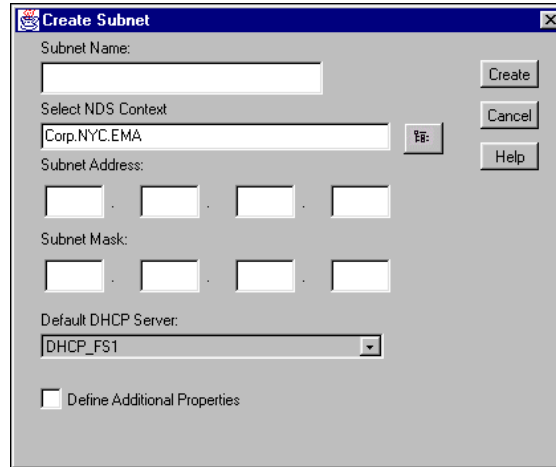


Figure 7-9: The Create Subnet Dialog

Each subnet object must have a unique NDS name. Individual subnet addresses can only exist once in the NDS tree. The following will cause the subnet creation process to fail:

- Giving a subnet object the same name as another NDS object in the same container
- Using a subnet address that has already been assigned to another subnet object anywhere in the tree

Presentation**Notes****Configuring a DHCP Subnet Object***(continued)*

- Continue demonstrating how to create a subnet object.

- Explain that the subnet object follows NDS naming conventions.

4. When you have entered the required information, click **Create**.
5. In the left pane of the DHCP Service tab window, click the **subnet object** you just created. The details window appears.

You can also configure the following:

- DNS zone for dynamic update
- Domain name
- Subnet pool reference
- Default DHCP server

In addition, you can record comments about the subnet.



For more information, see “Configuring DHCP” in the *Novell DNS/DHCP Administrator’s Guide*.

Configuring a Subnet Address Range Object

The Subnet Address Range (SAR) object identifies a range of IP addresses available for dynamic address assignment. It can also be configured to exclude a range of addresses from address assignment. The SAR object can also store the start of a hostname that can be assigned to clients when addresses are assigned.

The SAR object must be contained within a subnet object. You can create multiple SAR objects under a single subnet object. For example, you could create separate SAR objects to provide multiple ranges of IP addresses for dynamic assignment, BOOTP clients, and exclusions.

To create a new SAR object, do the following:

1. Click the **subnet object** in which the range will be contained.
2. Click the **Create** button.

The Create New DHCP Record dialog appears.

Because the subnet object is a container object, the Create DHCP Objects dialog contains two more DHCP objects—the subnet address range object and the IP address object.

3. Double-click **Subnet Address Range**.

Presentation**Notes****Configuring a DHCP Subnet Object**

(continued)



Demonstrate how to expand and close the subnet object using the (+) and (-) icons.

Configuring a Subnet Address Range Object

- Introduce the subnet address range (SAR) object.



Demonstrate how to create a SAR object.

4. Provide the SAR object with required configuration information.

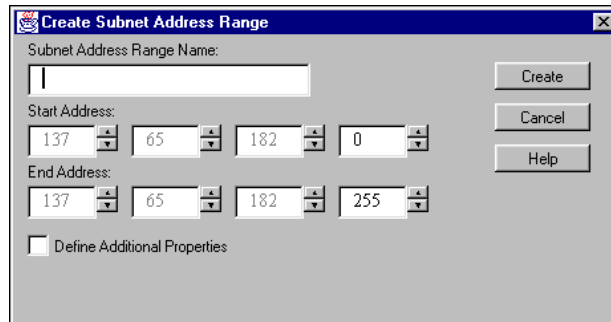


Figure 7-10: The Create Subnet Address Range Dialog

The address ranges of SAR objects cannot overlap. When you change the starting or ending addresses of a SAR object, you must use continuous unspecified and unassigned network addresses within the associated subnet; otherwise, the creation of that object will fail and you will get an error.

5. To configure additional SAR parameters, mark the **Define Additional Properties** box.
6. Click **Create**.
7. In the left pane of the Name Services tab window, click the **SAR object** you just created. To see the SAR object, you might need to expand the subnet object. When you select the SAR object, the details window appears.

You can also configure the following:

- Range type
- DNS update option
- DHCP server assignment

In addition, you can record comments about the SAR object.

Presentation

Notes

Configuring a Subnet Address Range Object *(continued)*



Continue demonstrating how to create a SAR object.

Configuring an IP Address Object

To manually assign an IP address to a specific machine on the network or to specifically exclude the assignment of an IP address to a machine on the network, you can create an IP address object.

The IP address object represents a single IP address. IP address objects can only be created in subnet object containers.

To create an IP address object, do the following:

1. Click the **subnet object** in which you want the IP address object placed.
2. Click the **Create** button.
3. Click **IP Address**.
4. Click **OK**.

The IP address object must include an address number and an assignment type.

5. Click **Create.x**

If you chose to manually assign an IP address, the Define Additional Properties box is automatically selected for you. You must provide additional information to configure the IP address object.

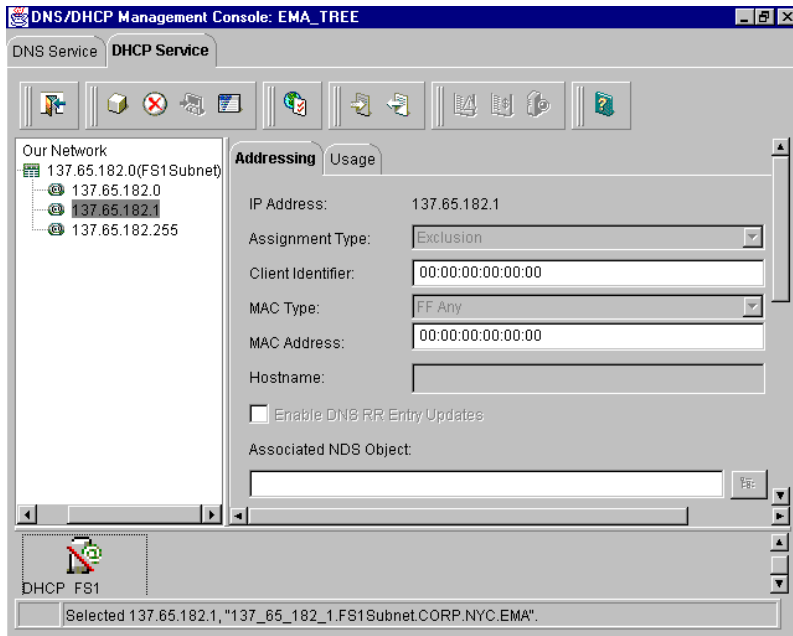


Figure 7-11: The IP Address Details Window

Presentation

Notes

Configuring an IP Address Object

- Define *IP address object*.



Demonstrate how to configure an IP address object.

If you chose to exclude an IP address, the IP address object is configured and the exclusion is in effect.

Use a manual IP address assignment to make sure a particular machine is always assigned the same IP address. Use an exclusion to make sure that a particular IP address is never assigned.

For every subnet object that is created, two IP address objects are automatically created. The two IP address objects are exclusions for the IP addresses of 0 and 255. These exclusions are created because some TCP/IP stacks do not support the assignment of 0 and 255 to nodes on the network.

Configuring a Subnet Pool Object

In the past, a physical network segment could only be configured with one IP subnet address. Now, however, many TCP/IP protocol stacks, including Novell's, support the configuration of multiple IP subnet addresses for a particular physical network segment.

The subnet pool object in NDS allows you to assign multiple subnet objects to service DHCP requests for a network segment that has more than one IP subnet address configured on it.

You can create a subnet pool object in the following container objects:

- Organization (O)
- Organizational Unit (OU)
- Country (C)
- Locality (L)

Presentation**Notes****Configuring an IP Address Object***(continued)*

Continue demonstrating how to configure an IP address object.

Configuring a Subnet Pool Object

- Introduce the subnet pool object.

To assign multiple subnet objects to service the same physical network segment, do the following:

1. Create a subnet pool object.
 - a. In the toolbar, click the **Create** button.
 - b. Click **Subnet Pool**.
 - c. Click **OK**.
 - d. In the Subnet Pool Name field, provide a **name** for the new subnet pool object.
 - e. In the Select NDS Context field, enter or browse to the **container** in which you want to create the new object.
 - f. Click **Create**.
2. Assign subnet objects to the subnet pool object.
 - a. In the left window pane, click the **subnet pool object** you just created.
 - b. In the subnet pool details window, click **Add**.
 - c. In the Select Subnet dialog, select the subnet objects that you want to assign to the subnet pool object; then click **OK**.
 - d. When all the subnet objects you want to service a particular physical network segment are assigned to the subnet pool object, click the **Save Data to NDS** button.
 - e. When asked to verify the save, click **Yes**.

Presentation

Notes

Configuring a Subnet Pool Object

(continued)



Demonstrate how to create a subnet pool object.

Starting the DHCP Server

After you have created a DHCP server object and assigned it IP addresses to service, you can load the DHCP software on the NetWare server. Enter the following command at the server console prompt:

DHCP SRVR

When DHCP SRVR.NLM is loaded, it reads IP address configuration information from NDS and loads the information into the DHCP server's cache.

Configuring the Workstation for DHCP

After the DHCP server is running, you must configure your workstation so that it will make a request for an IP address from the DHCP server.

To configure a workstation to obtain an IP address, complete the following at your workstation:

1. Configure the TCP/IP protocol stack for DHCP services.
 - a. On your desktop, right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. If you are on a Windows NT machine, click the **Protocols** tab.
 - d. Click the **TCP/IP** protocol.
 - e. Click **Properties**.
 - f. If you are on a Windows NT machine, click **Obtain an IP address from a DHCP server**.
 - g. If you are on a Windows 95 machine, click **Obtain an IP address automatically**.
 - h. If you previously had an IP address that was configured manually and you are asked if you want to enable DHCP, click **Yes**.
 - i. To close the TCP/IP Properties window, click **OK**.
 - j. To close the NetWork Properties window, click **OK**.
2. Reboot the workstation. It will obtain an IP address from a DHCP server.

Presentation

Notes

Starting the DHCP Server



Demonstrate how to start the DHCP server.

Configuring the Workstation for DHCP



Demonstrate how to configure a workstation to request an IP address from a DHCP server.

Configuring DHCP Options

You can configure two types of DHCP options in the DNS/DHCP Management Console.

The first type of DHCP option is used to configure administration features provided as part of Novell's implementation of DHCP. These features are provided by Novell to ease the administration of DHCP. Administrative options are configurable as part of the DHCP Server and DHCP subnet objects in the DNS/DHCP Management Console.

For example, you can configure the DHCP server to ping an IP address it is about to assign to make sure that the address is not already in use.

The other type of DHCP option is used to deliver configuration information to workstations on your network. DHCP specifications provide a framework for delivering configuration parameters, other than IP addresses, to hosts on your network.

For example, you can use DHCP options to provide your workstations with Domain Name Server, Router, Preferred Server, and NDS context information. You can even define your own DHCP options to deliver custom parameters to your clients.



For more information regarding DHCP options, see "DHCP Options" in the *Novell DNS/DHCP Services Administrator's Guide*.

DHCP options that deliver parameters to workstations can be configured so that they apply globally or only to a particular subnet. If the same DHCP option is set for both levels, the value set at the lower level will be the value assigned to the workstation.

For example, if you define the global Domain Name Server option as 137.65.1.1 and make another Domain Name Server option assignment of 137.65.10.1 for the subnet 137.65.10.0, workstations on the 137.65.10.0 subnet will have their Domain Name Server parameter set to 137.65.10.1.

Presentation**Notes**

Configuring DHCP Options

- Explain that DHCP administration and parameter options are configurable in the DNS/DHCP Management Console.

- Point out that DHCP options can be set on the global and subnet levels.

- Explain that if a DHCP option is set at more than one level, the client will use the value assigned to the lower level.

Setting Global DHCP Options

By selecting the Global Preferences button in the tool bar, you can set DHCP options that apply globally to all DHCP configurations in your NDS tree.

Global DHCP Options Tab

The Global DHCP Options tab allows you to configure parameters to be delivered to all workstations when they receive their IP address assignments. The options that appear in this list will be delivered globally by all DHCP servers in your NDS tree.

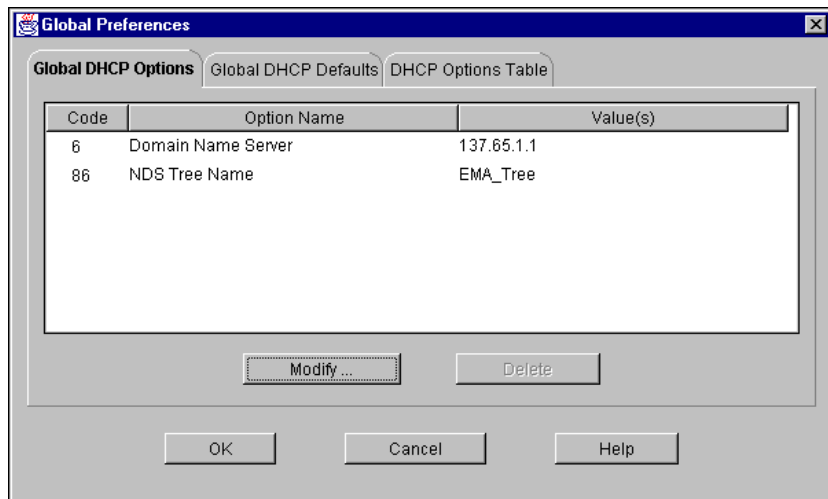


Figure 7-12: The Global Preferences Window

Presentation

Notes

Setting Global DHCP Options



Demonstrate configurable items in the Global Preferences window.

Global DHCP Defaults Tab

The Global DHCP Defaults tab allows you to define specific hardware addresses that you want to exclude from receiving IP addresses from DHCP servers. These exclusions apply to all DHCP servers in the NDS tree.

DHCP Options Table Tab

The DHCP Options Table tab displays all the DHCP options that have been defined. You can add new DHCP options by defining your own DHCP option types. You can make any existing DHCP option unavailable for configuration by removing it from this list.

Presentation

Notes

Setting Global DHCP Options

(continued)



Continue the demonstration.

Setting DHCP Options at the Subnet Level

When you select a subnet object in the DNS/DHCP Management Console, you can set DHCP options through the Subnet Options and Other DHCP Options tabs.

Subnet Options Tab

The Subnet Options tab allows you to configure administrative preferences for the IP addresses contained in the selected DHCP subnet object.

By default, DHCP is configured to lease IP addresses to workstations for three days. In this tab, you can change the amount of time an address in the subnet is leased by making the assignment permanent or changing the amount of time the address is leased.

The Novell DHCP service also supports the BOOTP protocol. You can configure DHCP to provide a BOOTP client with the address and name of a server the client can contact for a boot image, and a boot filename.

Other DHCP Options Tab

The Other DHCP Options tab allows you to configure parameters to be delivered only to workstations that reside on a particular subnet when they receive their IP address assignment. You configure the subnet level DHCP options in the same manner you configure the global DHCP options.

Presentation**Notes****Setting DHCP Options at the Subnet Level**

Demonstrate how to set DHCP administration options through the Subnet Options tab.



Demonstrate how to configure parameters through the Other DHCP Options tab.

Setting DHCP Server Options

The Novell DHCP server implementation provides several administrative features configurable as options on the DHCP server object.

To configure administrative options on the DHCP server, do the following:

1. Click a **DHCP server object**.
2. Click the **Options** tab.

You can configure the DHCP server object with Simple Network Management Protocol (SNMP) traps, alert and audit logging, mobile user options, and pinging to determine if an IP address is already in use.

SNMP Traps

SNMP traps determine the types of information about the DHCP server that can be monitored by network management software such as ManageWise®.

Audit Trails and Alerts

Audit trails and alerts control the level of event and audit logging the DHCP server will generate. The auditing and alert logs can be viewed by selecting the View Events/Alerts and View Audit Trail Log buttons on the toolbar.

Mobile Users

The Mobile Users options allow you to configure how the DHCP server will treat a workstation that moves from one subnet to another.

Ping Enabled

If you mark the Ping Enabled box, the DHCP server will ping an IP address before making an IP assignment. If something responds to the ping, the server does not assign the IP address, thus preventing an IP conflict on the network.

Presentation

Notes

Setting DHCP Server Options



Demonstrate the administrative options that can be set at the DHCP server object.

Hands-On Exercise 7-2: Configuring and Starting DHCP Services

In this exercise, you

- Configure DHCP using the DNS/DHCP Management Console
- Start DHCP services on your NetWare server
- Configure your workstation to obtain an IP address from a DHCP server

Part I: Configuring DHCP Using the DNS/DHCP Management Console

From your workstation, do the following:

1. Log in to the EMA_TREE as your **Admin** user.
2. Start the DNS/DHCP Management Console.
 - a. Double-click the **DNSDHCP** shortcut on your desktop.
 - b. In the Enter NDS Tree Name field, type **EMA_TREE**.
 - c. Click **Launch**.
3. Click the **DHCP Service** tab.
4. Create a DHCP server object.
 - a. Click the **Create** button.
 - b. Click **DHCP Server**.
 - c. Click **OK**.
 - d. Browse to your **container**.
 - e. Click your **server object**.
 - f. Click **OK**.
 - g. Click **Create**.

Presentation

Notes

Hands-On Exercise 7-2: Configuring and Starting DHCP Services



Introduce the exercise.



:20

Conduct the exercise.

Assist the students as necessary.

5. Create a subnet object.
 - a. Click the **Create** button.
 - b. Click **Subnet**.
 - c. Click **OK**.
 - d. In the Subnet Name field, type **yourservernameSUBNET**.
For example, if your server is FS1, you would type FS1SUBNET.
 - e. In the Select NDS Context field, type in or browse to and select your **context**.
 - f. In the Subnet Address field, type the **subnet address** that corresponds to your server. (Refer to Table 7-1 below.)

Server	Subnet Address	Subnet Mask
FS2	192.168.2.0	255.255.255.0
FS3	192.168.3.0	255.255.255.0
FS4	192.168.4.0	255.255.255.0
FS5	192.168.5.0	255.255.255.0
FS6	192.168.6.0	255.255.255.0
FS7	192.168.7.0	255.255.255.0
FS8	192.168.8.0	255.255.255.0
FS9	192.168.9.0	255.255.255.0
FS10	192.168.10.0	255.255.255.0
FS11	192.168.11.0	255.255.255.0
FS12	192.168.12.0	255.255.255.0
FS13	192.168.13.0	255.255.255.0

Table 7-1: DHCP Subnet Configuration Information

- g. In the Subnet Mask field, type the **subnet mask** for your subnet (as specified in the table above).
- h. In the Default DHCP Server field, select the DHCP server called **DHCP_ yourservername**.
- i. Click **Create**.

Presentation**Notes****Hands-On Exercise 7-2:
Configuring and Starting
DHCP Services** *(continued)*

- Assist students as needed.

Note: The subnet addresses students use for this exercise should not be valid subnet addresses for your classroom network segment.

The subnet addresses are provided in the exercise to help students learn how to configure DHCP only. Having a student configure DHCP services using a subnet address that is valid for use in your classroom will cause problems.

If the subnet addresses provided in the exercise are valid for your classroom network segment, you will need to provide your students with subnet addresses that are not valid for your classroom network segment.

6. Configure your subnet to lease IP addresses on a permanent basis.
 - a. Click your **subnet object**.
 - b. Click the **Subnet Options** tab.
 - c. In the Lease Type box, click **Permanent**.
7. Configure a router address to deliver to the workstations on your subnet.
 - a. Click the **Other DHCP Options** tab.
 - b. Click **Modify**.
 - c. In the Available DHCP Options list, click **Router**.
 - d. Click **Add**.
 - e. In the Selected DHCP Options list, click **Router**.
 - f. In the Router Box, click **Add**.
 - g. For the router IP address, type **your_subnet.254**. For example, if your subnet is 192.168.20.0, you would type 192.168.20.254.
 - h. Click **OK**.
8. Configure a Domain Name Server address to be delivered to the workstations on your subnet.
 - a. In the Available DHCP Options list, click **Domain Name Server**.
 - b. Click **Add**.
 - c. In the Selected DHCP Options list, click **Domain Name Server**.
 - d. In the Domain Name Server Box, click **Add**.
 - e. For the Domain Name Server IP address, type **your_subnet.1**. For example, if your subnet is 192.168.20.0, you would type 192.168.20.1.
 - f. Click **OK**.
 - g. To close the Modify DHCP Options window, click **OK**.
 - h. To save the configurations on your subnet object, click the **Save Data to NDS** button.
 - i. When prompted about saving changes, click **Yes**.

Presentation

Notes

**Hands-On Exercise 7-2:
Configuring and Starting
DHCP Services** *(continued)*

- Assist students as needed.

9. Create a subnet address range object that will assign the IP address range of 50 to 100.
 - a. Click your **subnet object**.
 - b. Click the **Create** button.
 - c. Click **Subnet Address Range**.
 - d. Click **OK**.
 - e. In the Subnet Address Range Name field, type **Available Addresses**.
 - f. In the fourth octet field of the starting IP address, type **50**.
 - g. In the fourth octet field of the ending IP address, type **100**.
 - h. Click **Create**.
10. Configure your DHCP Server to exclude the IP address of 10 on your subnet.
 - a. Double-click your **subnet object**.

Notice the two default IP address exclusions for addresses 0 and 255 for your subnet.
 - b. Click your **subnet object**.
 - c. Click the **Create** button.
 - d. Click **IP Address**.
 - e. Click **OK**.
 - f. Use the Up-arrow button to set the IP address to **10**.
 - g. Make sure the Assignment Type field says **Exclusion**.
 - h. Click **Create**.
11. Exit the DNS/DHCP Management Console.
 - a. Click the **Exit** button.
 - b. When asked if you are sure you want to exit, click **Yes**.

Part II: Starting the DHCP Server

Load the DHCP server. At your NetWare server, enter
DHCPSRVR

Presentation

Notes

**Hands-On Exercise 7-2:
Configuring and Starting
DHCP Services** *(continued)*

- Assist students as needed.

Part III: Configuring the Workstation to Use DHCP Services

Configure a workstation to obtain an IP address from a DHCP server.



The focus of this exercise is to configure a workstation so that it will make a DHCP request. Your DHCP server is not configured for the classroom network segment and will not respond to your workstation's DHCP request.

Do the following at the workstation:

1. Configure the TCP/IP protocol stack for DHCP services.
 - a. On your desktop, right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. If you are on a Windows NT machine, click the **Protocols** tab.
 - d. Click the **TCP/IP protocol** that is installed.
 - e. Click **Properties**.
 - f. If you are on a Windows NT machine, click **Obtain an IP address from a DHCP server**.
 - g. If you are on a Windows 95 machine, click **Obtain an IP address automatically**.
 - h. If you previously had an IP address that was configured manually and you are asked if you want to enable DHCP, click **Yes**.
 - i. To close the TCP/IP Properties window, click **OK**.
 - j. To close the NetWork Properties window, click **OK**.
2. To allow the workstation to obtain an IP address from a DHCP server, **reboot** the workstation.

Presentation**Notes****Hands-On Exercise 7-2:
Configuring and Starting
DHCP Services** *(continued)*

- Assist students as needed.

If the workstations in your classroom have two TCP/IP protocol stacks installed, Step 1d (Part III) will require you to help students identify the correct TCP/IP protocol stack to select.

Note: The objective of this exercise is to teach students how to configure workstations to use DHCP.

This part of the exercise assumes you have a DHCP server, configured for your classroom network segment, that can respond to the DHCP requests made from the student workstations.

To have student workstations receive a response from the DHCP server they configured, you must configure your classroom with seven network segments. Each segment should have one workstation and one server.

3. Verify that your workstation obtained IP address configuration information from a DHCP server.

On a Windows 95 machine, do the following:

- a. Click **Start**.
- b. Click **Run**.
- c. In the Open field, type **WINIPCFG**.
- d. Click **OK**.
- e. Click **More Info**.

IP address information obtained from a DHCP server should be displayed.

On a Windows NT machine, do the following:

- a. Click **Start**.
- b. Click **Programs**.
- c. Click **Command Prompt**.
- d. Enter the following command:

IPCONFIG /ALL

IP address information obtained from a DHCP server should be displayed.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 7-2:
Configuring and Starting
DHCP Services** *(continued)*

- Assist students as needed.

- Review the exercise.

Note: If your students are using Windows NT and are unable to run IPCONFIG successfully, have them execute it from the SYSTEM32 directory.

Importing DHCP Databases

You can use the DNS/DHCP Management Console to import DHCP configuration information. This is useful for Novell customers with Novell DHCP Services 2.0 who are going to use DHCP Services 3.0. When you import DHCP Services 2.0 configurations, you do not need to re-create them in NDS.



Because a subnet address can only be defined once in NDS, you cannot import a subnet address that is already defined in NDS.

The Novell DHCP information that you import must be in DHCP 2.0 or 3.0 file format.

To import existing DHCP information, do the following from within the DNS/DHCP Management Console:

1. Click the **Import DHCP Database** button.
2. In the DHCP file field, type in or browse to the **location of the DHCP information file**.
3. If you are importing DHCP 2.0 information and you have a MAC address configuration file, type in or browse to the **location of the MAC address configuration file**.

The Import DHCP - Subnet List window appears, listing each subnet found in the configuration file.

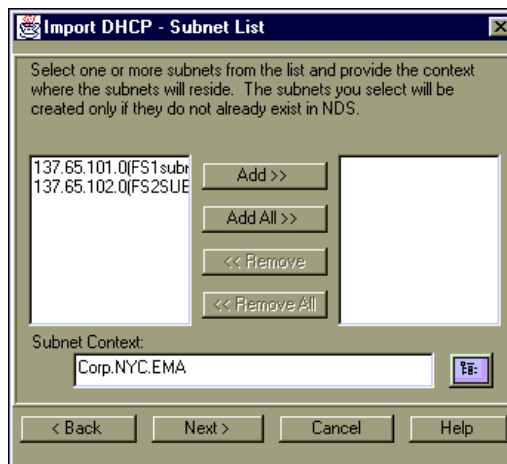


Figure 7-13: The Import DHCP Subnet Dialog

Presentation**Notes**

Importing DHCP Databases

- Explain the DHCP configuration files needed to import existing DHCP information.



Demonstrate how to import existing DHCP information.

Import the FS1SUBNET101 subnet from the FS1\DATA:SETUP\DHCP3TAB backup file.

4. Add the desired subnet or subnets to the import list.
5. Type in or browse to the **NDS context** you want to place the subnet objects in.
6. Click **Next**
7. Click **Import**.
8. For each DHCP object, select a **DHCP Server** to manage the configuration you are importing and click **OK**.
9. Click **Finish**.

Importing DHCP Databases (continued)



Continue the demonstration.

Hands-On Exercise 7-3: Importing DHCP Databases

In this exercise, you import DHCP configuration information from a DHCPTAB file and place it in NDS.

To import your DHCP 3.0 database file, do the following from within the DNS/DHCP Management Console:

1. Map a drive to FS1\DATA.
2. Click the **DHCP Service** tab.
3. Click the **Import DHCP Database** button.
4. In the DHCP File field, browse to and select the **FS1\DATA:\SETUP\DHCP3TAB** file using the drive you mapped in Step 1.
5. Click **Next**.
6. Click the **subnet** that has the same name as your server. For example, if your server is FS3, click the FS3Subnet103 subnet.
7. Click **Add**.
8. In the Subnet Context field, browse to and select the **context** assigned to you by your instructor.
9. Click **Next**.
10. Click **Import**.
Every DHCP object that is imported must be assigned to a DHCP server.
11. When the Server Input dialog appears, select your **DHCP server object** and click **OK**.
12. When the status says "Transfer Complete," click **Finish**.

(End of Exercise)

Presentation

Notes

Hands-On Exercise 7-3: Importing DHCP Databases

Introduce the exercise.



:10 Conduct the exercise.

Review the exercise.

Configuring and Starting DNS Services

In traditional DNS, the administrator makes all configuration changes to a single *master name server* (also called *primary name server*). The master name server stores DNS configuration information locally in a file.

This file is in Berkeley Internet Name Domain (BIND) format. The master name server can then use this file to resolve domain names into IP addresses.

To distribute the workload of name resolution and eliminate a single point of failure, DNS information can be replicated to replica name servers.

A *replica name server* (also called *secondary name server*) keeps its replica of the BIND master file current by querying the master name server for configuration changes.

When changes occur, replica name servers request configuration updates from the master name server and save that DNS information locally. Configuration updates to replica name servers are called *zone transfers*.

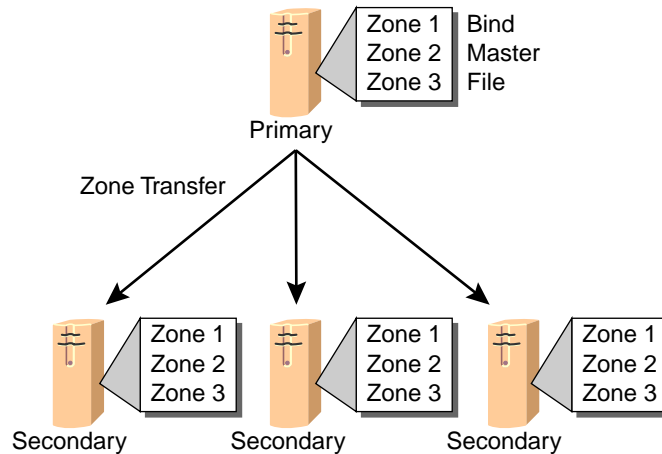


Figure 7-14: Traditional DNS Structure

Configuring and Starting DNS Services



7-3 (Figure 7-14: Traditional DNS Structure)

- Discuss the traditional method used to configure and distribute DNS data.

Note: Changes to the BIND master file are recorded by updating the serial number in the Start of Authority (SOA) record on the master name server.

A replica name server knows that a change in the BIND master file has occurred when its SOA serial number is lower than the master SOA serial number.

DNS Zones in NDS

In NetWare 5, all DNS information is stored in NDS and replicated throughout the network. DNS information can then be updated and retrieved by NetWare servers designated as *domain name servers*.

DNS information is defined in NDS using zones. A *zone* contains all information about some part of the domain name space. A zone also contains the domain names and data for a particular domain.

Zone data is stored within NDS and is replicated just like any other data in the tree. All NetWare servers can access DNS data from the NDS tree. This provides fault tolerance and load balancing for the DNS information. Using NDS, you can make changes to DNS zones from anywhere in the network.

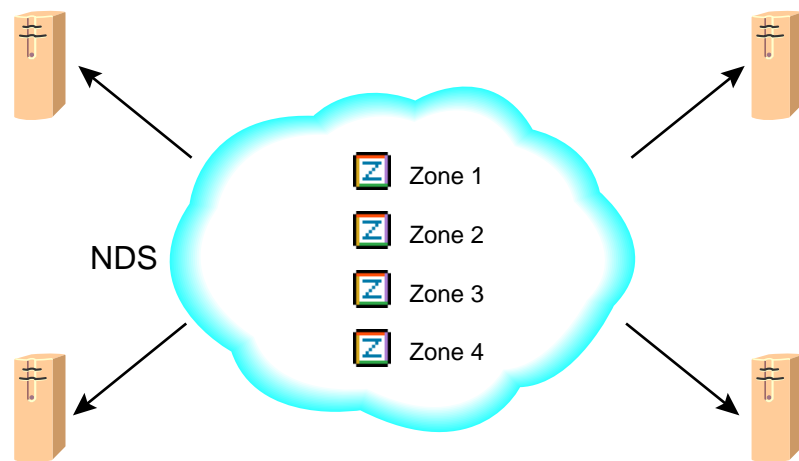


Figure 7-15: DNS Zone Information Available throughout the Network from NDS

The DNS zone object in NDS can represent three kinds of zones. The DNS zone object can be a standard DNS Zone, an IN-ADDR.ARPA zone, or an IP6.INT zone.

All DNS zone objects must be configured as one of two types: a primary DNS zone or a secondary DNS zone.

Presentation**Notes****DNS Zones in NDS**

- Discuss the ability of NDS to store and replicate DNS information.
- Discuss Novell's concept of a DNS zone.
- Discuss the advantages of using NDS to hold DNS zone configurations.



7-4 (Figure 7-15: DNS Zone Information Available throughout the Network from NDS)

- Discuss the three kinds of DNS zone objects the network administrator can create in NDS.
- Explain that a DNS zone object must be configured as either a primary DNS zone or a secondary DNS zone.

Designated Servers

If you want a NetWare server to obtain and update DNS data in the NDS tree, you must make the server a designated server. A *designated server* is a NetWare server that is assigned to service a DNS zone object.

The DNS tasks that a designated server performs depend on the type of DNS zone object that it is servicing.

If the server is servicing a primary DNS zone object, it performs the task of a master name server. If it is servicing a secondary DNS zone object, then the designated server performs the tasks of a replica name server.

Designated Server Tasks for a Primary Zone Object

If a NetWare server is designated to service a primary DNS zone object, some of its tasks include

- Querying NDS to resolve names into IP addresses
- Adding and deleting Resource Records
- Updating the zone serial number

Presentation**Notes****Designated Servers**

- Define *designated server*.

- Discuss the tasks of a designated server that is assigned to service a primary DNS zone object.

Designated Server Tasks for a Secondary Zone Object

If a NetWare server is designated to service a secondary DNS zone object, its responsibility is to receive zone transfers from a traditional master name server whose DNS information is not stored in NDS. The designated server then places that information in NDS.

NDS replicates the information throughout the network. Designated servers can then retrieve that DNS information to resolve names into IP addresses.

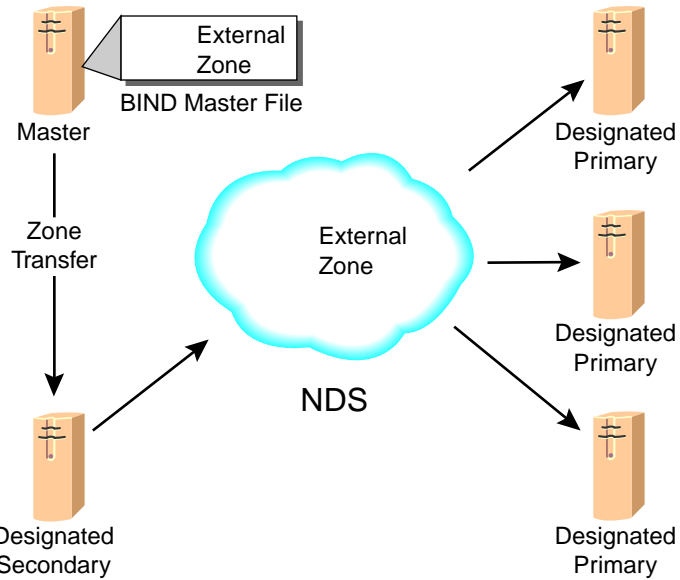


Figure 7-16: Adding External Domain Information to NDS through Zone Transfers

For example, if your company resolves domain names from a master name server provided by an Internet Service Provider (ISP), you could speed up that name resolution by creating a DNS zone object that would act as a secondary to your ISP's master name server.

The NetWare server you designate to service that secondary DNS zone object would receive zone transfers from the master name server and place that information in your NDS tree.

This DNS information would then be replicated by NDS throughout your network, and it would be available to your network users for quicker name resolution.

Presentation**Notes****Designated Servers** *(continued)*

- 7-5 (Figure 7-16: Adding External Domain Information to NDS through Zone Transfers)

- Discuss the tasks of a designated server that is assigned to service a secondary DNS zone object.

Configuring a DNS Server Object

When you create a DNS server object, you are designating a server that can respond to queries about the DNS zone. (The DNS server object is a separate entity from the NCP server object.)

To create a DNS server object, do the following from within the DNS/DHCP Management Console:

1. Click the **DNS Service** tab.
2. Click the **Create** button.
3. Click **DNS Server**.
4. Click **OK**.
5. Browse to and select the **NDS server object** that you want to designate as a DNS server object.
6. In the Host Name field, type a **name** for the DNS server.
Use the name that the DNS server will have in its domain.
7. In the Domain field, type the **domain** that the DNS server will be in.
The domain that you specify in the Domain field may or may not already exist in your NDS tree.
8. Click **Create**.

To view the details window for the DNS server object you just created, click your **DNS server object**, which appears in the bottom pane of the DNS Service tab window.

From the DNS server object detail window, you can view zones for the server, configure the forwarding list, configure the no-forwarding list, and enable event logging for the server. You can also make comments about the DNS server object.



When a DNS server object is created, it will have a line through it until the DNS service is actually running on the server.

Presentation

Notes

Configuring a DNS Server Object



Demonstrate how to create a DNS server object.

- Discuss the configuration tabs in the DNS server object detail window.

Configuring a DNS Zone Object

A DNS zone object is a container object that contains all the data for a single DNS zone. This data includes resource record set objects and resource record objects.

You can represent multiple DNS domains within NDS by having separate, independent DNS zone objects. You can support multiple DNS domains on a single NetWare server by creating multiple DNS zone objects and assigning a server to service those zones.

The DNS zone object correlates to a DNS Start of Authority (SOA) resource record and includes a member list of all NDS-based DNS servers that support the zone.



The DNS name space hierarchy is not represented within the NDS hierarchy. A domain and its subdomain can appear as peers within the NDS hierarchy, even though they actually have a parent/child relationship within the DNS hierarchy.

To create a new DNS zone object, do the following:

1. Click the **DNS Service** tab.
2. In the left pane, click the **All Zones** virtual object.
3. Click the **Create** button.
4. Click **Zone**.
5. Click **OK**.

Presentation

Notes

Configuring a DNS Zone Object

- Define *DNS zone object*.



Demonstrate how to create a DNS zone object.

6. Specify the kind of DNS zone you want to create.

You can create three kinds of DNS zones using the Create Zone window. You must specify one of the following:

- Standard DNS zone
- IN-ADDR.ARPA zone
- IP6.INT zone



You can create only one IP6.INT zone object in a tree. All IP Version 6 addresses must be grouped under this object. If an IP6.INT Zone already exists, the Create IP6.INT box will not be displayed.

7. Provide the NDS context in which you want the DNS zone object created.

8. Name the domain.

9. Specify the DNS zone object type.

By default, the primary zone type is selected. If you specify the secondary zone type, the domain name must match the name of the domain being replicated from the master name server. You must also provide the IP address of the master name server.

DNS information for a secondary DNS zone object will be replicated from the master name server to NDS at the time the DNS service is started on the designated server.

10. Assign a DNS server.

A DNS server must be designated to service the zone in order for the DNS zone object to be created. The DNS server can be a DNS server object that has already been defined in NDS or one that will be defined.

Presentation

Notes

Configuring a DNS Zone Object

(continued)



Continue demonstrating how to create a DNS zone object.

To assign a DNS server object that is already defined in NDS, select it from the Assign Authoritative DNS server list. If you still need to create the DNS server object, provide the hostname and domain in the Host Name and Domain fields.

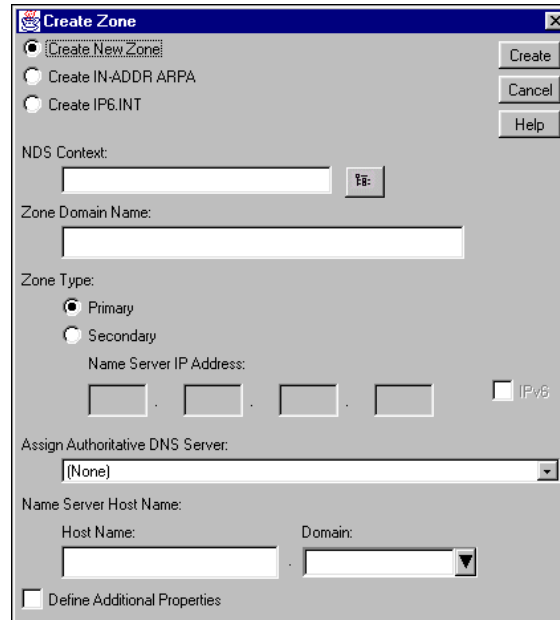


Figure 7-17: The Create Zone Dialog

11. When you have entered the information for the new zone, click **Create**.
12. A message appears reminding you that only the zone is being created and that you must create resource records for the zone. Click **OK**.
13. In the left pane of the DNS Service tab window, click the **zone** you just created. The details window appears.



You can also specify SOA information and make comments about the zone object in the DNS zone object details window.

Presentation

Notes

Configuring a DNS Zone Object

(continued)



Continue demonstrating how to create a DNS zone object.

Configuring a Resource Record Object

The resource record object is an NDS leaf object that contains the type and data of a single resource record. resource record objects are placed in resource record set objects. The resource record set object is created automatically when the resource record object is created.

The most commonly used resource record objects are listed below:

- **A records** map machine names to IP addresses.
- **CNAME records** map alias names to DNS names. (CNAME stands for canonical name.)
- **MX records** are Mail eXchange records. They map SMTP mail addresses to domain names.
- **NS records** are Name Server records. They map domain names to hostnames.
- **PTR records** are Pointer records. They map IP addresses to machine names within an IN-ADDR.ARPA zone.

To create a resource record object, do the following:

1. Click a **DNS zone object**.
2. Click the **Create** button.
3. Click **Resource Record**.
4. Click **OK**.
5. In the Domain Name field, type a **name** for the resource record object.
6. Select the **resource record type** and provide the necessary information to configure the resource record.
7. When you have entered all Resource Record information, click **Create**.

Once you have created a resource record object, you cannot modify it. If changes are required, you must delete the object and create a new one.

Presentation**Notes****Configuring a Resource Record Object**

- Define *resource record object*.
- Discuss the DNS resource record object.



Demonstrate how to create a resource record object.

Note: Questions might arise about other types of resource records that can be created. Only discuss the common resource records mentioned in the student manual.

If students request more information regarding DNS and resource records, refer them to <http://www.internic.net>.

Starting the DNS Server

After you have created and configured a DNS server and a DNS zone, you are ready to start the DNS server so that it can respond to queries about the zone.

To start the DNS server, enter the following at the server console prompt:

NAMED

Configuring the Workstation for DNS

Once a DNS server is running, you must configure your workstation to use your DNS server for name resolution.

To configure a workstation for DNS name resolution, do the following on your workstation:

1. Configure the TCP/IP protocol stack for DNS services.
 - a. On your desktop, right-click **Network Neighborhood**.
 - b. Click **Properties**.
 - c. If you are on a Windows NT machine, click the **Protocols** tab.
 - d. Click the **TCP/IP protocol**.
 - e. Click **Properties**.
 - f. Click the **DNS** tab.
 - g. If you are using Windows 95, click **Enable DNS**.
 - h. In the Host Name field, type the name of your **workstation**.
 - i. In the Domain Name field, type the **domain name** you configured in NDS.
 - j. Under the DNS Search Order window, click **Add**.
 - k. Enter your DNS server's **IP address**.
 - l. Click **Add**.
 - m. To close the TCP/IP Properties window, click **OK**.
 - n. To close the NetWork Properties window, click **OK**.

Presentation**Notes****Starting the DNS Server**

Demonstrate how to start DNS on a designated server.

If configuration changes to DNS occur after NAMED.NLM is loaded, they won't take effect until NAMED.NLM is unloaded and reloaded.

Configuring the Workstation for DNS

Demonstrate how to configure a workstation to use DNS services.

Hands-On Exercise 7-4: Configuring and Starting DNS Services

In this exercise, you

- Configure DNS services using the DNS/DHCP Management Console
- Start DNS services on your NetWare server
- Configure your workstation to use DNS services from your DNS server

Part I: Configuring DNS Using the DNS/DHCP Management Console

From your workstation, do the following:

1. Log in to the EMA_TREE as your **Admin** user.
2. Start the DNS/DHCP Management Console.
 - a. Double-click the **DNSDHCP** shortcut on your desktop.
 - b. In the Enter NDS Tree Name field, type **EMA_TREE**.
 - c. Click **Launch**.
3. Click the **DNS Service** tab.

Presentation**Notes****Hands-On Exercise 7-4:
Configuring and Starting DNS
Services**

- Introduce the exercise.



:20

- Conduct the exercise.

- Assist the students as necessary.

4. Create a DNS server object for your server.
 - a. Click the **Create** button.
 - b. Click **DNS Server**.
 - c. Click **OK**.
 - d. Navigate to your **container** using the button to the right of the Select Server Object field.
 - e. Click your **server object**.
 - f. Click **OK**.
 - g. In the Host Name field, type the **name** of your NetWare server.
 - h. In the Domain field, type
yourNDScontext.COM
For example, if you are assigned the ACCT.NYC.EMA context, you would type ACCT.NYC.EMA.COM as your domain name.
 - i. Click **Create**.
5. Create a DNS zone object.
 - a. In the left pane, click **All Zones**.
 - b. Click the **Create** button.
 - c. Click **Zone**.
 - d. Click **OK**.
 - e. In the NDS Context field, type in or browse to your **NDS context**.
 - f. In the Zone Domain Name field, type
yourNDScontext.COM
For example, if you are assigned the ACCT.NYC.EMA context, you would type ACCT.NYC.EMA.COM as your domain name.
 - g. In the Assign Authoritative DNS Server field, select your **DNS server**.
 - h. Click **Create**.
 - i. After reading the reminder to create proper resource records, click **OK**.

Presentation**Notes****Hands-On Exercise 7-4:
Configuring and Starting DNS
Services** *(continued)*

- Assist students as needed.

Note: The domain name typed in Steps 4h and 5f should not include a leading or trailing period.

6. Create an A resource record object type for your server in your DNS zone.
 - a. Click your **DNS zone object**.
 - b. Click the **Create** button.
 - c. Click **Resource Record**.
 - d. Click **OK**.
 - e. In the Host Name field, type **yourservername**.
For example, if you are assigned server FS1, you would type FS1 in the Host Name field.
 - f. In the IP Address field, type your **server IP address**.
 - g. Click **Create**.
7. Exit the DNS/DHCP Management Console.
 - a. Click the **Exit** button.
 - b. To confirm that you want to exit, click **Yes**.

Part II: Starting the DNS Server

1. To start your DNS server, enter the following at your NetWare server console prompt:
NAMED

Presentation

Notes

**Hands-On Exercise 7-4:
Configuring and Starting DNS
Services** *(continued)*

- Assist students as needed.

Part III: Configuring the Workstation to Use DNS Services

1. Configure your workstation to use your DNS server for name resolution.

On a Windows NT workstation, do the following:

- a. Right-click **Network Neighborhood**.
- b. Click **Properties**.
- c. Click the **Protocols** tab.
- d. Click **TCP/IP Protocol**.
- e. Click **Properties**.
- f. Click the **DNS** tab.
- g. In the Host Name field, type your **workstation name**.
- h. In the Domain Name field, type the **domain name** you configured in step 5f of Part I. For example, ACCT.NYC.EMA.COM.



If the DNS Search Order window already contains IP addresses, you must remove them prior to performing the next step.

- i. In the DNS Search Order window, click **Add**.
- j. Type your **server IP address**.
- k. Click **Add**.
- l. To close the TCP/IP Properties window, click **OK**.
- m. To close the NetWork Properties window, click **OK**.
- n. Click **Start**.
- o. Click **Shut Down**.
- p. Click **Restart the Computer**.
- q. Click **Yes**.
- r. Press **Ctrl+Alt+Del**.

Presentation

Notes

**Hands-On Exercise 7-4:
Configuring and Starting DNS
Services** *(continued)*

- Assist students as needed.

Provide students with names to enter in the Host Name field.

On a Windows 95 workstation, do the following:

- a. Right-click **Network Neighborhood**.
- b. Click **Properties**.
- c. Click the **TCP/IP protocol** that is installed.
- d. Click **Properties**.
- e. Click the **DNS Configuration** tab.
- f. If not already selected, mark the **Enable DNS** button.
- g. In the Host field, type your **workstation name**.
- h. In the Domain Name field, type the **domain name** you configured in step 5f of Part I. For example, ACCT.NYC.EMA.COM.



If the DNS Search Order window already contains IP addresses, you must remove them prior to performing the next step.

- i. In the DNS Search Order field, type your **server IP address**.
 - j. Click **Add**.
 - k. To close the TCP/IP Properties window, click **OK**.
 - l. To close the Network Configuration window, click **OK**.
 - m. When asked if you want to restart your computer, click **Yes**.
2. Test your DNS configuration by logging in to your NetWare server using its domain name.
- a. Enter your Admin **username** and **password**.
 - b. Click **Advanced**.
 - c. In the Server field, type your server's domain name.
For example, if your server is FS1, you would type
FS1.CORP.NYC.EMA.COM
 - d. To log in, click **OK**.
The login utility should have been able to find your server by its domain name.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 7-4:
Configuring and Starting DNS
Services** *(continued)*

- Assist students as needed.

Note: Students using Windows 95 might need you to identify the TCP/IP protocol stack they should select in Step 1c.

Provide students with names to enter in the Workstation Name field.

- Review the exercise.

Importing DNS Databases

You can use the DNS/DHCP Management Console to import DNS configuration information from a BIND master file.



You will get an error if you attempt to import a DNS zone that already exists in the NDS tree.

To import existing DNS information from a BIND master file to NDS, do the following from within the DNS/DHCP Management Console:

1. Click the **Import DNS Database** button.
2. Type in or browse to the **location** of the BIND master file.
3. Click **Next**.
4. In the Zone Context field, type in or browse to the **NDS context** in which you want to place the DNS zone.

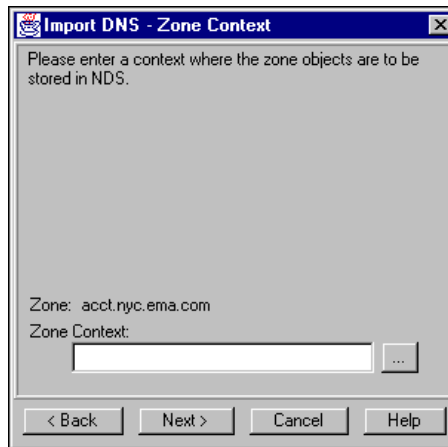


Figure 7-18: The Import DNS-Zone Dialog

5. Click **Next**.
6. In the list of existing DNS Servers, click the **designated server** you want to service this zone.
7. Click **Next**.
8. Click **Import**.
9. Click **Finish**.

Presentation

Notes

Importing DNS Databases



Demonstrate how to import DNS information from a BIND master file to NDS.

Note: Use the FS1\DATA\SETUP\DNSBIND file to demonstrate how to import a DNS zone.

Hands-On Exercise 7-5: Importing DNS Databases

In this exercise, you import a DNS zone into NDS.

Part I: Exporting DNS Configuration Information

To complete the exercise, you must first create a BIND master file from which to import DNS information. You create this file by exporting the DNS zone object you configured in the previous exercise.

Complete the following from within the DNS/DHCP Management Console:

1. Click the **DNS Service** tab.
2. If not already expanded, expand the **All Zones** object by double-clicking it.
3. Click your **zone object**.
4. Click the **Export DNS Database** button.
5. In the Export File Name field, type **C:\DNSBIND**.
6. Click **Export**.
7. When the status says "Transfer Complete," click **Finish**.

The BIND master file is now created.

Part II: Deleting a DNS Zone Object

You cannot import a DNS zone into NDS if that zone already exists. In Part III of this exercise, you import the DNS zone you exported in Part I. Therefore, you must first delete your DNS zone object.

Do the following from within the DNS/DHCP Management Console:

1. Click your **DNS zone object**.
2. Click the **Delete** button.
3. Click **Yes**.

Hands-On Exercise 7-5: Importing DNS Databases



Introduce the exercise.



:10

Conduct the exercise.

Part III: Importing DNS Configuration Information

To import DNS zone information from a BIND master file, do the following from within the DNS/DHCP Management Console:

1. Click the **DNS Service** tab.
2. Click the **Import DNS Database** button.
3. In the DNS File field, type **C:\DNSBIND**.
4. Click **Next**.
5. In the Zone Context field, type your **NDS context** as the context to which the DNS zone object will be imported.
6. Click **Next**.
7. In the list of DNS servers, click your **DNS server**.
8. Click **Next**.
9. Click **Import**.
10. When the status says "Transfer Complete," click **Finish**.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 7-5:
Importing DNS Databases**
(continued)

- Assist students as needed.
- Review the exercise.

Summary

In this section you learned how to install DNS and DHCP services by extending the NDS schema, installing NetWare Administrator snap-ins, and installing the DNS/DHCP Management Console.

DNS and DHCP services are configured using the DNS/DHCP Management Console utility.

DNS and DHCP objects are stored and managed within NDS.

DNS/DHCP services support the importing and exporting of DNS and DHCP configuration information to and from NDS.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Describe Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services.
2. Install DNS and DHCP services.
3. Configure and start DHCP services.
4. Configure DHCP options to deliver configuration information to TCP/IP hosts on the network.
5. Import a DHCP database.
6. Configure and start DNS services.
7. Import a DNS database.

Notes

SECTION 8 Installing a Web Server and an FTP Server

Duration 04:15

Preparation

Complete the following:

- Copy the Netscape FastTrack™ Server for NetWare installation files from the *NetWare 5 Operating System CD* (PRODUCTS\NOVONYX\SETUP.EXE) to each of the student workstations.
- Make the Novell FTP Services installation files available to students by mounting the *NetWare 5 Operating System CD* on the classroom server. Alternatively, you can also copy the NWUXPS directory on the CD to each of the classroom servers.

SECTION 8 **Installing a Web Server and an FTP Server**

In this section you learn how to install and configure the Netscape FastTrack™ Server for NetWare and the Novell FTP Server.

Objectives

Upon completing this section, you should be able to

1. Explain the services provided by the Netscape FastTrack Server for NetWare.
2. Install the Netscape FastTrack Server for NetWare.
3. Use the Administration Server to configure the Netscape FastTrack Server for NetWare.
4. Troubleshoot and tune the Netscape FastTrack Server for NetWare.
5. Explain the services provided by Novell FTP Services.
6. Install Novell FTP Services.
7. Configure Novell FTP Services.
8. Use Novell FTP Services to transfer binary and text files.
9. Troubleshoot basic Novell FTP Services problems.

Presentation

Notes

Installing a Web Server and an FTP Server

- Introduce the section.

Objectives

- Present the section objectives.

Overview of the Netscape FastTrack Server

This subsection introduces Web servers and the Netscape FastTrack Server for NetWare.

Understanding Web Servers

A Web server is an application that publishes documents as well as other types of files on the World Wide Web or on an intranet.

A Web server operates in a client/server relationship. A client program, such as a Web browser, requests information, and the Web server program supplies the information.

A Web server runs on a computer that is physically connected to a TCP/IP-based network. The Web server software receives requests and serves documents via the HyperText Transfer Protocol (HTTP). Web browsers submit HTTP requests; Web servers use HTTP to respond with the requested file.

A Web server uses a specified directory in the file system to store all the files it will serve to clients. All the files in the directories and subdirectories below that main content directory are also available to clients.

Web servers primarily publish documents created with the HyperText Markup Language (HTML). It is the language used to create the pages you've seen on the World Wide Web.

HTML uses ASCII text character combinations to tag blocks of text with various options. This feature allows an HTML file to be used on a variety of computer platforms. HTML coding can be used to format text, create lists, insert multimedia, create forms for collecting user input, and create links to other Web locations.

Web servers can also distribute many other types of files, including

- Executable (.EXE)
- Video (.MOV, .AVI)
- Audio (.AU, .WAV)
- Graphics (.GIF, .JPEG, etc.)
- Compressed (.ZIP)

Presentation**Notes**

Overview of the Netscape FastTrack Server

- Introduce the section.

Understanding Web Servers

- Define *Web server*, *World Wide Web*, and *intranet*, if necessary.

Web server: A server application that publishes HTML and other types of files on the World Wide Web. When a Web server receives an HTTP, FTP, or other type of request for a document from a Web browser, it responds by sending the document to the browser.

World Wide Web: A wide-area hypermedia information retrieval initiative on the Internet that provides universal access to a large body of documents.

Intranet: An internal network that employs Internet technology, especially Web servers and the TCP/IP protocol.

- Explain the function of Web servers.
- Discuss HTTP.
- Discuss HTML.

Gauge the experience level of your students. Spend some extra time discussing Web servers in general if students are unfamiliar with them.

**Introduction to the Netscape
FastTrack Server for NetWare**

The Netscape FastTrack Server, included with NetWare 5, is a Web server. It enables users to publish documents on internal corporate networks (intranets) and on the World Wide Web (the Internet).

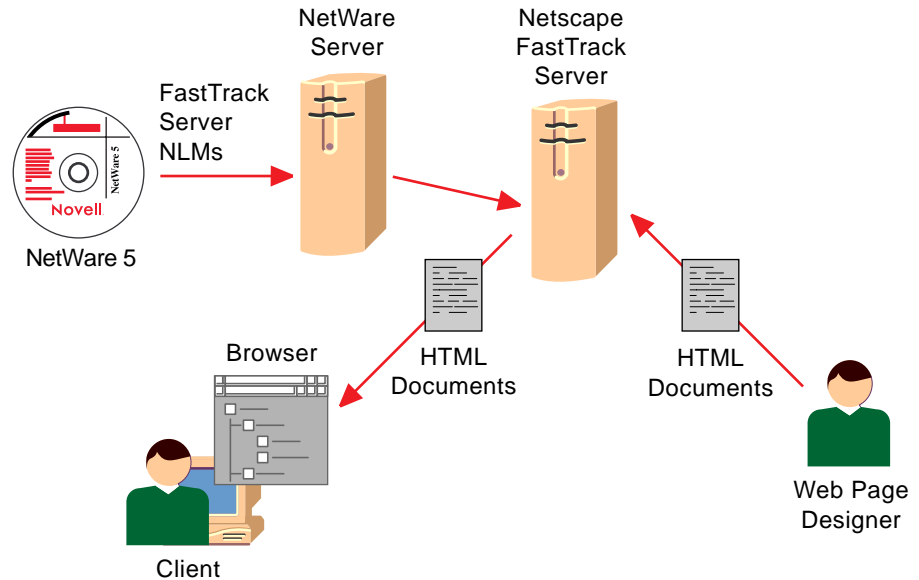


Figure 8-1: Adding Web Server Functionality to a NetWare 5 Server

FastTrack Server NLMs

The FastTrack Server comprises a set of NLMs that run on a NetWare 4.11 or NetWare 5 server. When you start the FastTrack Server, the following NLMs are initially loaded:

- CRON.NLM (NetWare scheduler NLM)
- NSHTTPD.NLM (Netscape FastTrack Server for NetWare NLM)
- NETDB.NLM (Network database access NLM)
- CSSYSMSG.NLM (System messages facility NLM)
- BTRIEVE.NLM (Btrieve® client/server database NLM)
- NSLCGI.NLM (LCGI support library NLM)
- ADMSERV.NLM (Netscape Administration Server NLM)

Presentation

Notes

**Introduction to the Netscape
FastTrack Server for NetWare**

- Introduce the Netscape FastTrack Server for NetWare.



8-1 (Figure 8-1: Adding Web Server Functionality to a NetWare 5 Server)

FastTrack Server NLMs

- Discuss the NLMs that are loaded when the FastTrack Server is started.

Installing the Netscape FastTrack Server

The following subsection explains how to install the Netscape FastTrack Server for NetWare.

System Requirements

The system requirements for installing the Netscape FastTrack Server are discussed below. Your system should also meet the basic NetWare 5 server requirements.

Hardware and Software

To install and configure the Netscape FastTrack Server, you need to use two computers, one as a NetWare client and the other as a NetWare server.

The client computer must have the following:

- Windows 95 or Windows NT
- NetWare Client software (installed and configured)
- Netscape 3.x or higher (installed and configured)
- A CD-ROM drive (if installing FastTrack from a CD)
- 100 MB of free hard disk space

The NetWare server must have the following:

- NetWare 4.11 or higher running
- A minimum of 64 MB of RAM
- 100 MB of free space on the SYS volume
- Long name space support added to SYS and any other volume that will hold Web server content



Long name space support is automatically added to NetWare 5 volumes when the server is installed. However, it is not added to volumes on a NetWare 5 server that has been upgraded from an earlier version of NetWare.

- TCP/IP bound and configured.

Presentation**Notes**

Installing the Netscape FastTrack Server

- ❑ Provide an overview of the installation steps.

System Requirements

- ❑ Emphasize that the server hardware must meet the minimum NetWare 5 requirements in addition to the FastTrack Server requirements.

Hardware and Software

- ❑ Discuss the hardware and software system requirements.
- ❑ Mention that the FastTrack installation program automatically loads and binds TCP/IP on the NetWare server, if necessary.

To add long name space support to a volume, enter the following at the server console:

LOAD LONG.NAM

ADD NAME SPACE LONG TO *volume_name*

Name space is loaded only once on a volume. Once loaded, the name space loads automatically each time the server boots.

Other Requirements

To install the FastTrack Server, you must also

- Have Supervisor rights to the SYS volume.
- Have a unique IP address for the NetWare server.
A registered IP address is mandatory for Internet access.
- (Optional) Know the DNS hostname that will be used for the NetWare server.

If DNS is not running, you will not be able to use hostnames. The FastTrack server will still function, but you will have to use IP addresses.

Installing the Netscape FastTrack Server

To install the Netscape FastTrack Server, complete the following:

1. From a client workstation, use Windows Explorer to map a drive to the root of the SYS volume on which you are going to install the FastTrack Server.
2. From the client workstation, run the Fast Track Server installation file. The installation wizard in Figure 8-2 will be displayed.

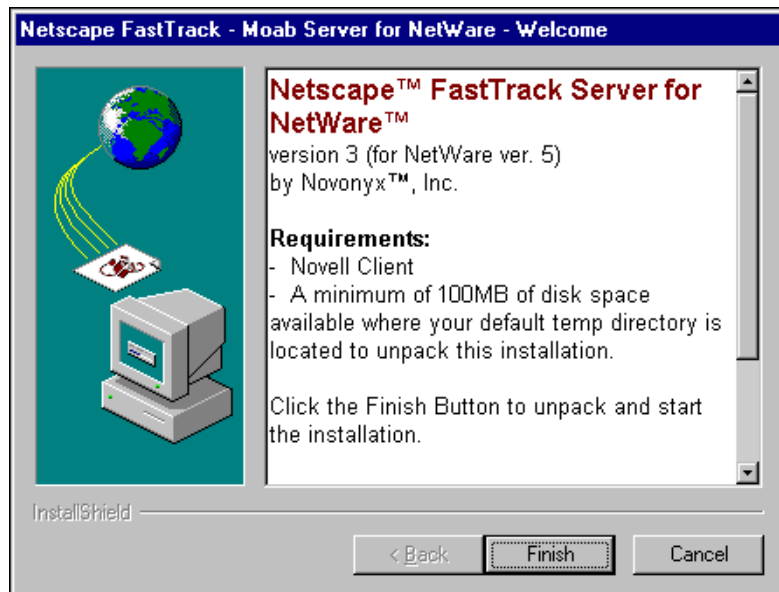


Figure 8-2: FastTrack Server Installation Wizard

Presentation**Notes****Other Requirements**

- Discuss the other system requirements for the FastTrack Server.

- Mention that DNS does not have to be running to use the FastTrack Server.

Installing the Netscape FastTrack Server

- Discuss the tasks associated with the installation process.



Demonstrate how to install the FastTrack Server for NetWare.



8-2 (Figure 8-2: FastTrack Server Installation Wizard)

3. Wait for the installation files to be unpacked.
4. Configure the IP address and hostname for the FastTrack Server.
5. Configure the port numbers for the FastTrack Server.
6. Specify a username and password for configuring the FastTrack Server.
7. Specify that the FastTrack Server be loaded when the NetWare server is started.
8. Wait for the FastTrack Server files to be copied to the NetWare server.
9. Start the FastTrack Server.
10. Test the installation by retrieving the FastTrack Server home page with a Web browser. If successful, the page in Figure 8-3 should be displayed.

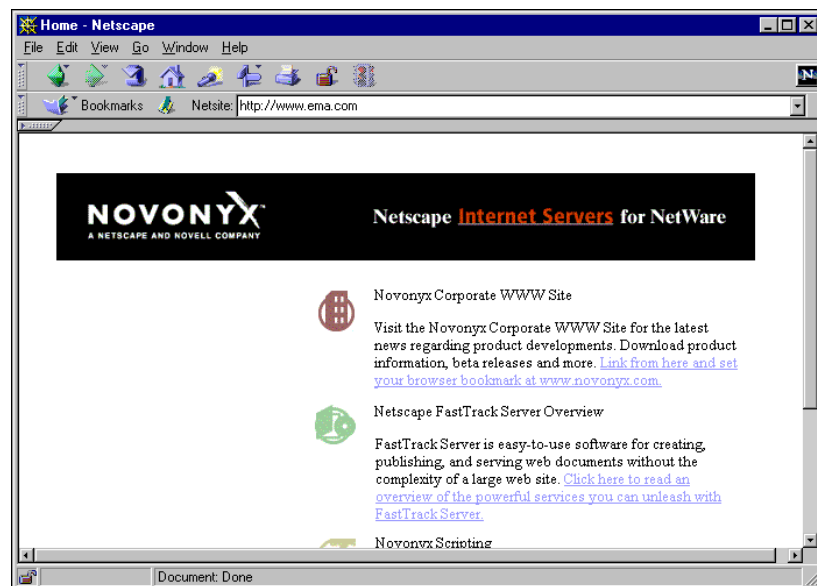


Figure 8-3: FastTrack Server Home Page

Presentation

Notes

Installing the Netscape FastTrack Server *(continued)*



Continue demonstrating how to install the FastTrack Server for NetWare.



8-3 (Figure 8-3: FastTrack Server Home Page)

Changes Made During Installation

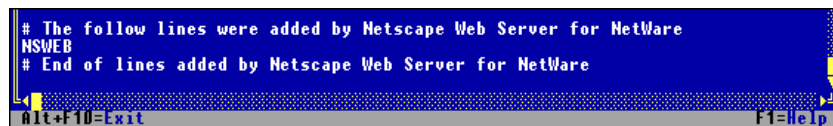
After the FastTrack Server has been installed, several changes are made to your NetWare server.

FastTrack Server Startup and Shutdown Files

When you install the FastTrack Server, a file named NSWEB.NCF is created. This file contains all the LOAD commands needed to start the FastTrack Server.

The NSWEBDN.NCF file is also created. This file contains all the commands needed to unload the FastTrack Server.

The following lines are added to the NetWare server's AUTOEXEC.NCF file during installation. These lines automatically load the FastTrack Server NLMs when the NetWare server is started.



```
# The follow lines were added by Netscape Web Server for NetWare
NSWEB
# End of lines added by Netscape Web Server for NetWare
```

Figure 8-4: AUTOEXEC.NCF Changes

Presentation**Notes****Changes Made During Installation**

- Discuss the changes made to the NetWare server during installation.

FastTrack Server Startup and Shutdown Files

- Point out that the NSWEB.NCF file can be run from the server console to start the FastTrack Server.
- Point out that the NSWEBDN.NCF file can be run from the server console to stop the FastTrack Server.
- Discuss the changes made to the NetWare server's AUTOEXEC.NCF file when the FastTrack Server is installed.



8-4 (Figure 8-4:
AUTOEXEC.NCF Changes)

FastTrack Server Directory Structure

When you install the FastTrack Server, the directory structure shown in Figure 8-5 is added to your NetWare server's file system.

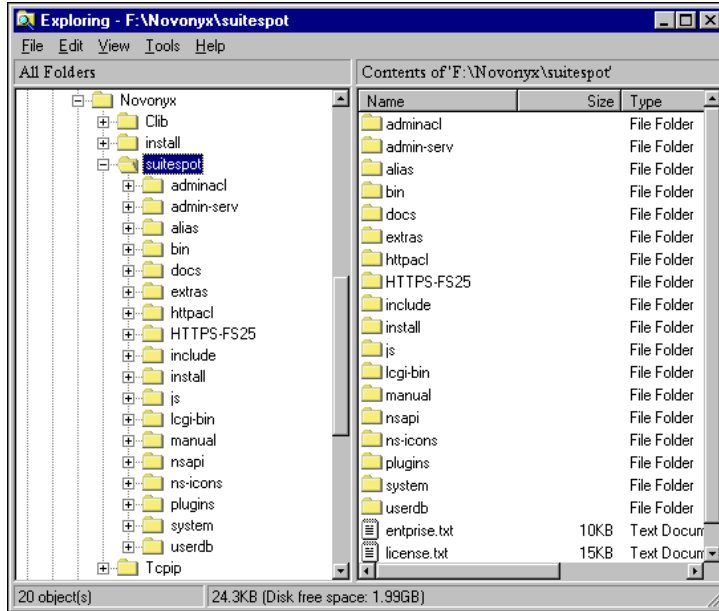


Figure 8-5: FastTrack Server Directory Structure

When you install the FastTrack Server, a document directory, SYS:\NOVONYX\SUITESPOT\DOCS, is created. This directory contains the files that the FastTrack Server serves to clients.

Any files in the subdirectories below this directory are also available to clients.

Presentation

Notes

FastTrack Server Directory Structure



8-5 (Figure 8-5: FastTrack Server Directory Structure)

- Discuss the FastTrack Server directory structure, emphasizing the role of the DOCS directory.

Product Documentation

You can use several sources of product documentation to learn more about the Netscape FastTrack Server:

- Netscape FastTrack Server Readme
http://server_hostname/readme/readme.htm
- Netscape Scripting Information
http://server_hostname/Netscape_scriptng.htm

You can also access extensive online documentation when you are configuring your FastTrack Server by clicking the context-sensitive HELP button located at the bottom of each administration page.

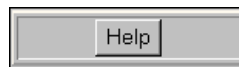


Figure 8-6: Context-Sensitive Help Button

Presentation

Notes

Product Documentation

- Discuss the sources of FastTrack Server documentation.



8-6 (Figure 8-6: Context-Sensitive Help Button)

Hands-On Exercise 8-1: Installing the Netscape FastTrack Server for NetWare

In this exercise, you install the Netscape FastTrack Server.

To install the Netscape FastTrack Server, complete the following:

1. Unpack the FastTrack Server installation files.
 - a. From your client workstation, click **Start**; then click **Run**.
 - b. In the Run dialog box, enter the following:
drive_letter:\path_to_FastTrack_install_file\SETUP.EXE
Your instructor will provide the path to the installation files.
 - c. Click **OK**.
 - d. Click **Finish**.
 - e. Wait for the installation files to be unpacked.
2. Configure and run the FastTrack Server installation.
 - a. In the Welcome screen, click **Next**.
 - b. In the Software License Agreement screen, click **Yes**.
 - c. In the Choose Destination Location screen, click **Browse**.
 - d. Browse to a ***drive*** mapped to the root of your server's SYS volume.
 - e. Click **Next**.
 - f. In the IP Address field of the Configure Server screen, type the ***IP address*** of your NetWare server (provided by your instructor).
 - g. In the Hostname field of the same screen, type the ***hostname*** of your NetWare server (provided by your instructor); then click **Next**.
 - h. In the Web Server Configuration screen, verify that **80** is in the Server Port field; then click **Next**.
 - i. From the Administration Server Port Configuration screen, write down the admin port number; then click **Next**.
 - j. When prompted to write down your Administration Server port number, click **OK**.

Hands-On Exercise 8-1: Installing the Netscape FastTrack Server for NetWare

- Introduce the exercise.

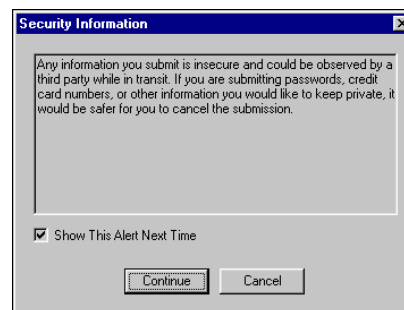


:30

- Conduct the exercise.
- Provide students with the path to the FastTrack installation files.
- Provide students with the IP addresses and associated hostnames (if applicable) for their NetWare servers.
- Inform students about the default security warning displayed by the Netscape browser.

Assist the students as necessary.

Any time students submit information to the FastTrack Server, the Netscape browser will display the security warning shown below.



Because the warning can be disabled by unmarking the Show This Alert Next Time box, steps have **not** been included in the exercises instructing students to click **Continue** each time the warning is displayed.

We recommend that you instruct students to unmark the previously mentioned box the first time the warning is displayed. Doing so will make the steps in the exercise more closely match what the students experience on the computer.

- k. In the Administration Server Authentication screen, enter **admin** as the username.
- l. In the Administration Server Authentication screen, enter the same **password** used by your Admin user object as the password to be used for your Administration Server; then click **Next**.



This step creates an Admin user in FastTrack's own directory, not in NDS. The username and password are case-sensitive.

- m. When notified that you can use LDAP with FastTrack, click **Next**.
 - n. In the Autoexec.ncf Options screen, mark the **Change the Autoexec.ncf file** box; then click **Next**.
 - o. In the Start Copying Files screen, click **Next**.
 - p. Wait for the installation to be completed.
 - q. In the Setup Complete screen, mark the **View the Read Me file** and **Launch Web server** boxes; then click **Finish**.
 - r. Wait for the installation to be completed.
 - s. Click **Finish**.
3. Verify that the FastTrack Server home page loads in your browser.

(End of Exercise)

Presentation**Notes****Hands-On Exercise 8-1:
Installing the Netscape
FastTrack Server for NetWare***(continued)*

- Emphasize that the Admin user created in Step 2k is created in FastTrack's own directory.

- Review the exercise.

The students **must** use the same password as the one specified for the Admin user object in their containers.

Using the Administration Server

You can configure and manage the FastTrack Server using the Administration Server and Server Manager.

Introduction to the Administration Server

The Administration Server, which comprises a series of NLMs running on the NetWare server, helps you manage the Netscape FastTrack Server from a single interface—the Administration Server home page.

You can access Server Manager from the Administration Server's home page. Server Manager is a collection of forms the Administration Server uses to configure and control your FastTrack Server.

Accessing the Administration Server

Before you can access the Administration Server, the Administration Server NLMs must be running on the NetWare server.



The commands to launch the Administration Server are added to the NetWare server's AUTOEXEC.NCF file during installation. If you need to manually launch the Administration Server, enter **ADMSEV** at the NetWare server console.

You can use any standard Web browser to access the Administration Server. Start your Web browser and enter the following URL in the Location field:

http://server_hostname:admin_port_number/

Substitute *admin_port_number* with the number you were assigned during the FastTrack Server installation.

Presentation**Notes****Using the Administration Server**

- Introduce the Administration Server and Server Manager.

- Clearly identify and differentiate between the different servers that will be discussed in the remainder of the section.

Introduction to the Administration Server

- Explain the function of the Administration Server.

Accessing the Administration Server

- Discuss how to start the Administration Server.

- Explain how to access the Administration Server from a Web browser.

Differentiate between the following:

- The FastTrack Server
- The Administration Server
- The NetWare Server
- The LDAP Server
- The Novell FTP Server (discussed later)

When you are prompted for a username and a password, enter the username and password you chose during installation and click OK.

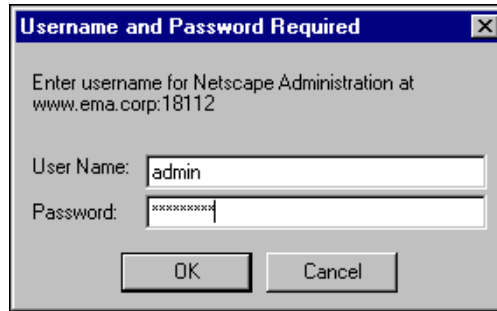


Figure 8-7: Authenticating to the Administration Server

When you have been authenticated, the Administration Server home page appears.



Figure 8-8: Administration Server Home Page

Presentation**Notes****Accessing the Administration Server** *(continued)*

8-7 (Figure 8-7:
Authenticating to the
Administration Server)



Explain the options
available on the
Administration Server page.



8-8 (Figure 8-8:
Administration Server Home
Page)



Demonstrate how to access
the Administration Server
with a Web browser.

Introduction to Server Manager

Server Manager is a collection of forms you use to configure and control your FastTrack Server. Server Manager can be accessed from the Administration Server home page.

The Administration Server home page lists all the Netscape servers installed on your system. To access Server Manager, click the button displaying the name of your NetWare server.

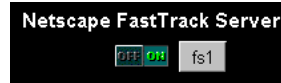


Figure 8-9: Accessing Server Manager

The Server Manager page appears.

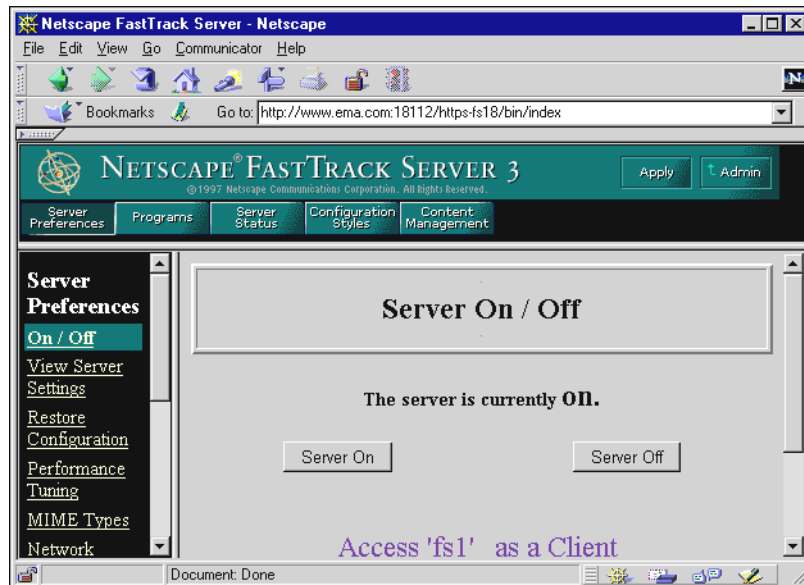


Figure 8-10: Server Manager

You can use the server configuration tabs in the top frame to configure the FastTrack Server. After clicking a tab, a list of links appears in the left-hand frame.

When you click one of these links, the corresponding form comes up in the main frame. If you need more information about a form, click Help for context-sensitive help.

Presentation**Notes****Introduction to Server Manager**

- Introduce students to Server Manager.
- Explain how to access Server Manager.



8-9 (Figure 8-9: Accessing Server Manager)

- Explain the location and function of the top, left, and main frames of Server Manager pages.



8-10 (Figure 8-10: Server Manager)



Demonstrate how to access Server Manager from the Administration Server.

Using the Resource Picker

Most of the Server Manager forms make changes that apply to the entire FastTrack Server. However, you can use some forms to configure either the entire FastTrack Server or specific resources on the server, such as files or directories.

You can use the resource picker, shown in Figure 8-11, to specify the resource you want to configure.



Figure 8-11: Resource Picker

Many of the forms in Server Manager allow you to specify wildcard patterns to represent one or more items. Wildcard patterns use special characters.

Pattern	Purpose
*	Match zero or more characters.
?	Match exactly one occurrence of any character.
	An <i>or</i> expression. The substrings used with this operator can contain other special characters such as * or \$. The substrings must be enclosed in parentheses, as in (a b c), but the parentheses cannot be nested.
\$	Match the end of the string. This is useful in <i>or</i> expressions.
[abc]	Match one occurrence of the characters <i>a</i> , <i>b</i> , or <i>c</i> .
[a-z]	Match one occurrence of a character between <i>a</i> and <i>z</i> .
[^az]	Match any character except <i>a</i> or <i>z</i> .
*~	This expression, followed by another expression, removes any pattern matching the second expression.

Table 8-1: Resource Picker Wildcard Patterns



If you want to use one of these characters without the special meaning, precede it with a backslash (\) character.

Presentation

Notes

Using the Resource Picker

- Discuss how to use the resource picker in Server Manager.



8-11 (Figure 8-11: Resource Picker)



Demonstrate how to use wildcards in the resource picker.

Saving and Applying Changes

After you submit a form, you are presented with a hypertext link that saves and applies your changes. When configuring your FastTrack Server, you must always save and apply your changes.

When you have finished making changes with Server Manager, you can return to the Administration Server home page by clicking the Admin button in the upper-right corner, as shown in Figure 8-12.



Figure 8-12: Return to the Administration Server Page Button

Presentation

Notes

Saving and Applying Changes

- Discuss saving and applying changes made with Server Manager.

- Discuss how to return to the Administration Server page.



8-12 (Figure 8-12: Return to the Administration Server Page Button)

Configuring the FastTrack Server

You can use Server Manager to configure your FastTrack Server to provide an Internet or intranet Web server. Although many configuration options are available, this course covers the following topics:

- Modifying basic server parameters
- Modifying directories in the document tree
- Configuring document preferences
- Restricting access

Modifying Basic Server Parameters

This subsection discusses how to configure the following basic server preferences:

- Starting and stopping the server
- Configuring the server port number

Starting and Stopping the Server

Once installed, the FastTrack Server runs constantly, listening for and accepting requests. If your FastTrack Server is running, you will see the On icon and its green light on the Administration Server home page, as shown in Figure 8-13.



Figure 8-13: Starting and Stopping the FastTrack Server

You can start and stop the FastTrack Server by clicking the Off and On buttons.

Configuring the FastTrack Server

- Introduce the topics to be covered.

Modifying Basic Server Parameters

- Introduce the parameters that will be presented.

Starting and Stopping the Server

- Discuss starting and stopping the FastTrack Server.



8-13 (Figure 8-13: Starting and Stopping the FastTrack Server)



Demonstrate how to start and stop the FastTrack Server from the Administration Server home page.

You can also start, stop, and restart the FastTrack Server from Server Manager:

1. In Server Manager, click **Server Preferences**.
2. Click **On/Off**.
3. Click **Server On** or **Server Off**.



After you shut down the FastTrack Server, the server might take a few seconds to complete its shut-down process and to change the status to "Off."

You can also shut down and restart the FastTrack Server from the NetWare server console. To do so, complete the following steps:

1. To shut down the server, at the server console enter
NSWEBDN
2. To restart the server, at the server console enter
NSWEB

Presentation

Notes

Starting and Stopping the Server

(continued)



Demonstrate how to start and stop the FastTrack Server from Server Manager.



Demonstrate how to start and stop the FastTrack Server from the NetWare server console.

Configuring the Server Port Number

Using the Server Manager, you can configure the FastTrack Server's server port number. The server port number specifies the TCP port that the FastTrack Server listens to for http requests.

The standard insecure Web server port number is 80; the standard secure Web server port number is 443. The port number can be any port from 1 to 65535.

The port number you choose can affect your users. If you use a nonstandard port, then anyone accessing your FastTrack server with a Web browser must specify a server name and port number in the URL.

For example, if your server has a DNS hostname of www.ema.com and you use port 8090, a user must specify the following URL to access your server:

http://www.ema.com:8090

Figure 8-14 shows the Server Manager form you can use to change the server port number.

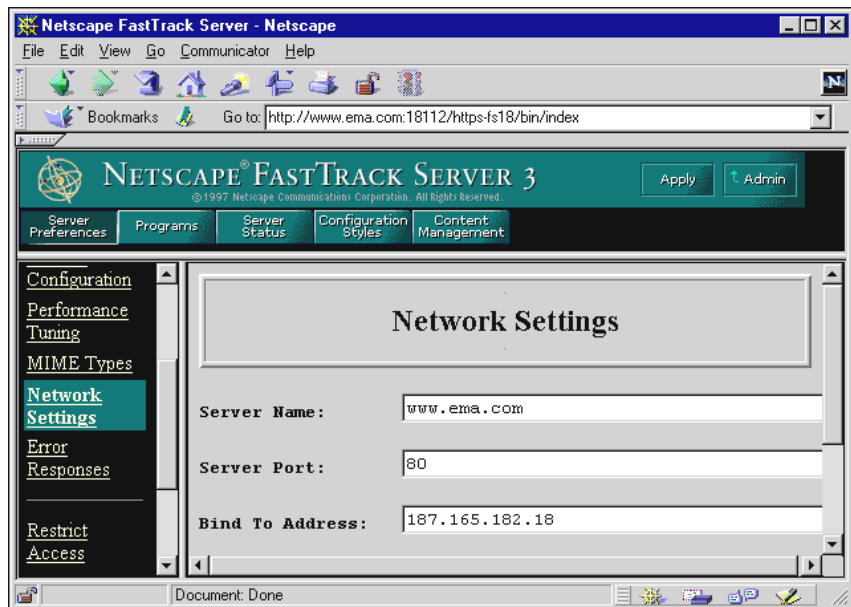


Figure 8-14: Configuring Network Settings with Server Manager

Presentation

Notes

Configuring the Server Port Number

- Explain how to configure the server port number with Server Manager.



8-14 (Figure 8-14: Configuring Network Settings with Server Manager)

To change the FastTrack Server server port number, do the following:

1. In Server Manager, click **Server Preferences**.
2. Click **Network Settings**.
3. In the Server Port field, type a new port number for your FastTrack Server.
4. Save and apply the changes.

Modifying Directories in the Document Tree

You can use Server Manager to manage your FastTrack Server's content.

Setting the Primary Document Directory

The FastTrack Server keeps its documents in a central location on the NetWare server. This location is known as the *document root* or *primary document directory*.

By default, the primary document directory for the FastTrack Server is SYS:\NOVONYX\SUITESPOT\DOCS. The URL for your FastTrack Server maps to this directory.

For example, suppose your primary document directory is SYS:\NOVONYX\SUITESPOT\DOCS and your FastTrack Server hostname is *www.ema.com*. A user makes an http request such as the following:

`http://www.ema.com/products/info.html`

The following file is retrieved:

`SYS:\NOVONYX\SUITESPOT\DOCS\PRODUCTS\INFO.HTML`

If you were to move all your Web content to a new directory on your NetWare server, you would only have to change the primary document directory that the FastTrack Server uses, instead of mapping all URLs to the new directory.

Presentation**Notes****Configuring the Server Port Number** *(continued)*

Demonstrate how to change the FastTrack Server port number.

Modifying Directories in the Document Tree

- Explain how to modify directories in the document tree.

Setting the Primary Document Directory

- Remind students of the default location of the primary document directory.
- Explain how the FastTrack Server's IP address maps to the primary document directory.

Server Manager provides the form you need to change the primary document directory, as shown in Figure 8-15 below.

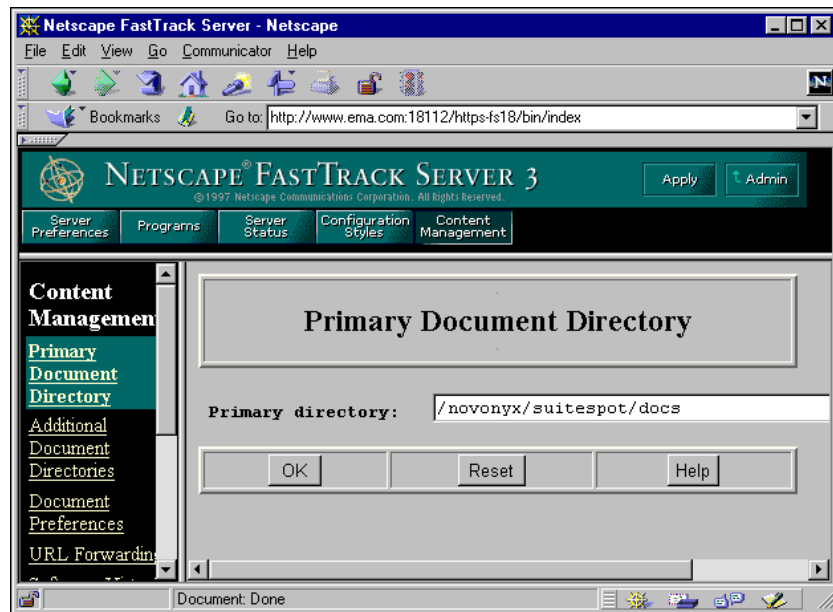


Figure 8-15: Setting the Primary Document Directory

To change your server's primary document directory, do the following:

1. In Server Manager, click **Content Management**.
2. Click **Primary Document Directory**.
3. In the Primary Directory field, type the full pathname of the directory that you want to make the primary document directory.
4. Save and apply the changes.

Setting Additional Document Directories

You can serve documents from a directory outside your primary document directory by configuring additional document directories.

To add a document directory, you first need to choose a URL. Next, you need to create and specify the directory to be mapped to that URL.

Presentation**Notes****Setting the Primary Document Directory** *(continued)*

8-15 (Figure 8-15: Setting the Primary Document Directory)



Demonstrate how to change the primary document directory.

Setting Additional Document Directories

- Explain how to set additional document directories.

You can then use the Server Manager form shown in Figure 8-16 to add a document directory.

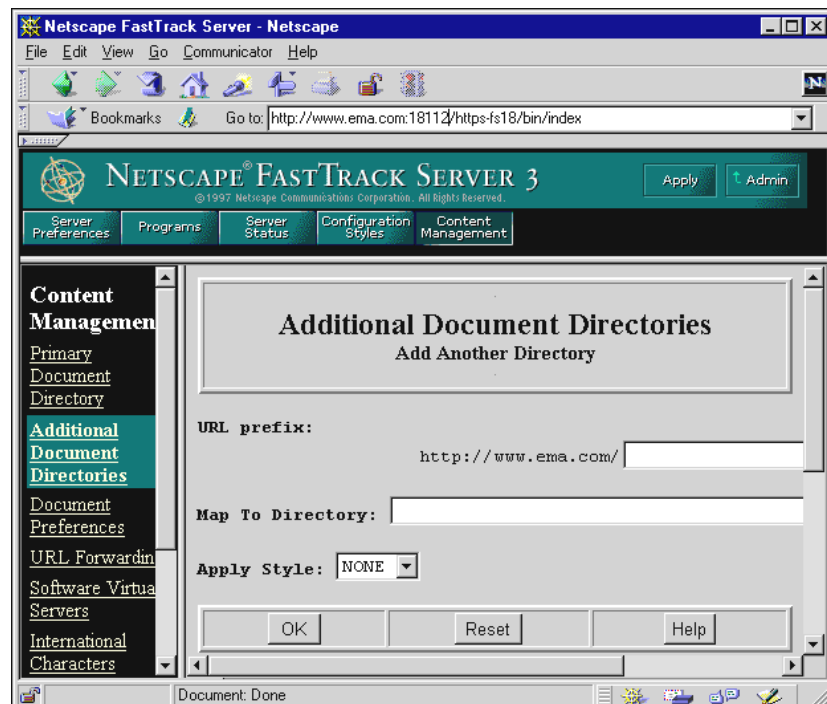


Figure 8-16: Setting Additional Document Directories

To add document directories, do the following:

1. In Server Manager, click **Content Management**.
2. Click **Additional Document Directories**.
3. In the URL Prefix field, type the **URL prefix** you want to map.
For example, if you type marketing in the URL Prefix field and your DNS hostname is www.ema.com, then users who access www.ema.com/marketing/ with a Web browser will retrieve documents from the directory you specify in Step 4 below.
4. In the Map to Directory field, type the **absolute path** of the directory you want the URL prefix to map to.
5. Save and apply the changes.

Presentation

Notes

Setting Additional Document Directories *(continued)*



8-16 (Figure 8-16: Setting Additional Document Directories)



Demonstrate how to add a document directory.

Configuring Document Preferences

The FastTrack Server allows you to configure how the FastTrack Server responds to document requests from Web browsers.



Figure 8-17: Configuring Document Preferences

You can configure the following preferences for FastTrack Server documents:

- Index filenames
- Directory indexing
- Server home page

Index Filenames

The Fast Track Server automatically displays the file you specify with this option when a filename is not explicitly requested in a URL.

The defaults are index.html and home.html. If more than one name is specified, the FastTrack Server looks in the order in which the names appear in this field until one of the specified names is found.

Presentation**Notes****Configuring Document Preferences**

- Explain how to configure document preferences.



8-17 (Figure 8-17:
Configuring Document
Preferences)

Index Filenames

- Discuss specifying index filenames.

If a document name is not explicitly specified in the URL and the FastTrack Server finds a file with the filename specified in this field, it assumes that this file is the index file.

If more than one filename is specified with this option, the FastTrack Server looks for the first filename specified. If it doesn't find the first filename, it looks for the second filename specified, and so on.

Directory Indexing

If your document directory has subdirectories, you can allow clients to access an index of the contents of these directories.

The FastTrack Server automatically indexes directories using the following process:

1. The FastTrack Server first searches the directory for the file you configured as the index file.
2. If the file is not found, the FastTrack Server generates an index file that lists all the files in the document root. The generated index has one of the following formats:
 - *Fancy directory indexing*, which includes a graphic that represents the type of file, the date the file was last modified, and the file size.
 - *Simple directory indexing*, which simply lists the files available. This format takes less time to generate.



You can also specify that no dynamic directory listing be generated.

Server Home Page

By default, the FastTrack Server finds the index file specified in the Index filename field and uses that for the home page.

However, you can also specify the file you want to be used as the home page. Simply mark the radio button next to Home page and enter the filename for the home page in the field next to the radio button.

Configuring Document Preferences

To configure document preferences, do the following:

1. In Server Manager, click **Content Management**.
2. Click **Document Preferences**.
3. Type a new index filename or add a file in the Index Filenames field.
4. Select the kind of directory indexing you want.
5. Specify whether you want users to see a particular home page or an index file when they access your FastTrack Server.
6. Save and apply the changes.

Presentation

Notes

Directory Indexing

- Discuss configuring directory indexing.

Server Home Page

- Discuss setting the server home page.

Configuring Document Preferences



Demonstrate how to configure document preferences.

Restricting Access

After installation, anyone accessing your FastTrack Server with a Web browser can access the documents in the SYS:\NOVONYX\SUITESPOT\DOCS directory or any of its subdirectories.

This scenario is appropriate for public-access Web servers. If you need to restrict access to your FastTrack Server content, complete the following tasks:

- Bind the FastTrack Server to NDS.
- Create access restrictions.

Bind the FastTrack Server to NDS

The FastTrack Server comes with its own scaled-down directory service, which is automatically installed. The FastTrack Server uses this by default until you redirect it to another directory service.

To provide a higher degree of security and centralized management, you can redirect the FastTrack Server to NDS. This allows FastTrack to leverage your existing directory information and use the exceptional security features of NDS.

When the FastTrack Server is bound to NDS, it can determine access based on NDS and NetWare file system trustee assignments.

To bind the FastTrack Server to NDS, complete the following:

1. Start the Administration Server.
2. Specify that the FastTrack Server use NDS.
3. Specify the NDS contexts to be searched.
4. Shut down and restart the Administration Server and the FastTrack Server.

Presentation

Notes

Restricting Access

- Discuss restricting access.

Bind the FastTrack Server to NDS

- Discuss the Netscape Directory that is installed with the FastTrack Server.



Demonstrate how to bind the FastTrack Server to NDS.

No corresponding page in student manual

Bind the FastTrack Server to NDS

(continued)



(Optional) Demonstrate how to bind the FastTrack Server to NDS using LDAP.

Complete the following:

1. Using NetWare Administrator, create a user with no password in your container.
The LDAP Server will use this object as a proxy to authenticate to NDS.
2. Give the LDAP proxy user Browse object rights and Read and Compare property rights to your container.
3. Configure the LDAP Group object.
 - a. Set the user object you just created as the proxy user.
 - b. Set the LDAP Group object to accept clear text passwords.
 - c. Shut down and restart the LDAP server.
4. Access the Administration Server.
5. Specify that the FastTrack Server use LDAP.
6. Specify the LDAP host server IP address and base distinguished name.
7. Shut down and restart the Administration Server and the FastTrack Server.
8. Test the bind with NDS.
 - a. In the Administration Server page, click **Users & Groups**.
 - b. In the Users and Groups frame, click **Manage Users**.
 - c. In the Find User field, type * and click **Find**.
 - d. Open NetWare Administrator and compare the list of users presented on the Administration Server page with those listed by NetWare Administrator.

If they are the same, NDS has been bound correctly.

Create Access Restrictions

With the FastTrack Server bound to NDS, you can restrict access to your Web server content by making trustee assignments for the desired NDS user, group, or container object to the file or directory you want to restrict.

When users attempt to access a restricted file or directory, the Web browser displays a dialog box asking the user to enter a username and password.

To restrict access using NDS authentication, do the following:

1. Determine which users will be given access to the resource (file or directory).
2. Run NetWare Administrator.
3. Create a group and assign the users (identified in Step 1) to it.
4. Make the group a trustee of the resource. You will need to give a minimum of Read and File Scan rights.



If all the users in a given container are to have access to the resource, you can make the trustee assignment for the container itself instead of creating a group.

Presentation**Notes****Create Access Restrictions**

- Discuss creating access restrictions.



- Demonstrate how to restrict access.

Complete the following:

1. Make a directory named **RESTRICTED** under `sys:\novonyx\suitespot\docs`.
2. Using a text editor, open a new file and enter the following lines:

```
<html><body><h1>This is a restricted file!</h1></body></html>
```
3. Save the file as **INDEX.HTML** in the `sys:\novonyx\suitespot\docs\restricted` directory.
4. Give `.EAlder.CORP.NYC.EMA` Read and File Scan rights to `sys:\novonyx\suitespot\docs\restricted`.
5. Block access for all other users to the directory by making an explicit rights assignment for `.CORP.NYC.EMA` and removing the check marks in the Read and File Scan boxes.
6. Try to access the directory with a Web browser. Show the authentication dialog box.
7. Try to authenticate as another user in the CORP container. Show the denied access message.
8. Authenticate correctly as EAlder.

Hands-On Exercise 8-2: Configuring the Netscape FastTrack Server for NetWare

In this exercise you do the following:

- Modify basic server parameters.
- Modify directories in the document tree.
- Restrict access.

Part I: Modifying Basic Server Parameters

Complete the following steps:

1. Start Netscape on your client workstation.
2. In the Location field, enter the **IP address** or **hostname** of your FastTrack Server and the Administration Server **port number**, as shown below:

`http://server's_hostname:admin_port_number`
3. In the Username and Password Required screen, enter **Admin** for the username; then enter your **password**.

Remember that the username and password are case-sensitive.
4. Click **OK**.

Stop and Start the FastTrack Server

1. To stop the FastTrack Server, click **Off** in the Administration Server home page.
2. To acknowledge that the server has been shut down, click **OK**.
3. To restart the server, click **On**.
4. To acknowledge that the server has been restarted, click **OK**.

Hands-On Exercise 8-2: Configuring the Netscape FastTrack Server for NetWare

- Introduce the exercise.
- Have students configure their Web browsers.



:30

Conduct the exercise.

Several of the steps in this exercise will fail if the students' Web browsers use a cached copy of a Web page instead of retrieving it off the Web server.

To prevent this, have the students do the following:

- Set the Web browser's memory and disk cache to **0**.
- Set the Web browser to verify documents every time.

Assist the students as necessary.

Configure Network Settings

1. Change the server port number from 80 to 2001.
 - a. Start Server Manager from the Administration Server home page by clicking the button displaying the **name** of your NetWare server.
 - b. Click **Server Preferences**.
 - c. Click **Network Settings**.
 - d. In the Server Port field, change the number from 80 to **2001**.
 - e. Click **OK**.
 - f. Click **Save and Apply**.
 - g. When notified that the changes have been applied, click **OK**.
2. Test the new configuration.
 - a. Exit and restart your Web browser.
 - b. In the Location field, enter
http://server_hostname/
Note the result.
 - c. In the Location field, enter
http://server_hostname:2001
Note the result.
3. Repeat all of Step 1, changing the Server Port number back to **80**.

**Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**
(continued)

- Continue the exercise.

Part II: Modifying Directories in the Document Tree

In Part II of the exercise, you:

- Set MYSTUFF as the primary document directory
- Set MYDOCS as an additional document directory
- Add MYSTUFF.HTML as an index filename

Set MYSTUFF as the Primary Document Directory

1. Create a new document directory and sample content.
 - a. From your client workstation, start Windows Explorer.
 - b. Under SYS:\NOVONYX\SUITESPOT\DOCS, create a new directory called **MYSTUFF**.
 - c. Create a sample web page by opening a new file in a text editor and entering the following lines:

```
<html><body><h1>This is the index file in  
sys:\novonyx\suitespot\docs\mystuff.</h1></body></html>
```
 - d. Save the file as **INDEX.HTML** in the
SYS:\NOVONYX\SUITESPOT\DOCS\MYSTUFF directory.
2. Set the primary document directory.
 - a. In Server Manager, click **Content Management**.
 - b. Click **Primary Document Directory**.
 - c. In the Primary Directory field, erase the existing entry and type
/novonyx/suitespot/docs/mystuff
 - d. Click **OK**; then click **Save and Apply**.
 - e. When notified that the changes have been applied, click **OK**.
3. Test the new configuration.
 - a. Exit and restart your Web browser.
 - b. In the Location field, enter
http://server_hostname/
Note the result.
4. Repeat Step 2, changing the primary document directory back to
/novonyx/suitespot/docs.

Hands-On Exercise 8-2: Configuring the Netscape FastTrack Server for NetWare *(continued)*

- Emphasize that the correct spelling needs to be used in Step 2.

If students misspell a directory or filename, the FastTrack Server will accept it anyway and generate an error when the mapping is accessed from a Web browser.

Set MYDOCS as an Additional Document Directory

1. Create a new document directory.
 - a. From your client workstation, start Windows Explorer (if it isn't already running).
 - b. At the root of SYS, create a new directory called **MYDOCS**.
 - c. Using a text editor, open a new file and enter the following lines:

```
<html><body><h1>This is the index file in  
sys:\mydocs.</h1></body></html>
```
 - d. Save the file as **INDEX.HTML** in the SYS:\MYDOCS directory.
2. Set an additional document directory.
 - a. In Server Manager, click **Content Management**.
 - b. Click **Additional Document Directories**.
 - c. In the URL Prefix field, type
extrathings
 - d. In the Map to Directory field, type
/mydocs
 - e. Click **OK**.
 - f. Click **Save and Apply**.
 - g. When notified that the changes have been saved and applied, click **OK**.
3. Test the new configuration.
 - a. Exit and restart your Web browser.
 - b. In the Location field, enter
http://server_hostname/extrathings/
Note the result.

**Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**
(continued)

- Continue the exercise.

Add MYSTUFF.HTML as and Index Filename

1. Rename the homepage file for SYS:\MYDOCS.
 - a. From your client workstation, start Windows Explorer.
 - b. Rename the INDEX.HTML file in SYS:\MYDOCS to **MYSTUFF.HTML**.
2. Test the configuration.
 - a. Exit and restart your Web browser.
 - b. In the Location field, enter
http://server_hostname/extrathings/
Note the result. Why did this occur?
3. Set the index filename to MYSTUFF.HTML.
 - a. In Server Manager, click **Content Management**.
 - b. Click **Document Preferences**.
 - c. In the Index Filenames field, type the following after the existing entries:
,mystuff.html
 - d. Click **OK**.
 - e. Click **Save and Apply**.
 - f. When notified that the changes have been saved and applied, click **OK**.
4. Test the configuration.
 - a. Exit and restart your Web browser.
 - b. In the Location field, enter
http://server_hostname/extrathings/
Note the result. Why did this occur?

Presentation

Notes

**Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**
(continued)

- Continue the exercise.

In step 3c, be sure students understand that they must type a **comma and mystuff.html** after index.html and home.html in the Index Filenames field.

Part III: Restricting Access

To restrict access to your Web server content, you must

- Bind the FastTrack Server to NDS
- Create access restrictions

Bind the FastTrack Server to NDS

To bind the FastTrack Server to NDS, complete the following:

1. Bind the FastTrack Server to NDS.
 - a. In Server Manager, click **Admin**.
 - b. On the Administration Server page, click **Global Settings**.
 - c. On the Obtain Directory Service From line in the Configure Directory Service frame, click **Novell Directory Services**.
 - d. When notified that FastTrack will switch to Novell Directory Services mode, click **OK**.
 - e. Verify that the name of your **NDS tree** is listed on the Treename line.
 - f. Click **Insert Context**.
 - g. In the New NDS Context field, type the **context of your container** without a leading period; then click **OK**.

For example, if your context were .OU=CORP.OU=NYC.O=EMA, you would type

CORP.NYC.EMA
 - h. Click **Save Changes**.
 - i. When prompted to shut down and restart the Administration Server and the FastTrack Server, click **OK**.
2. Shut down and restart the Administration Server and the FastTrack Server.
 - a. At the server console, enter
NSWEBDN
 - b. At the server console, enter
NSWEB

**Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**

(continued)

- Continue the exercise.

- Emphasize that the context entry in step 2g must not have a leading period.

Create Access Restrictions

To create an access restriction, do the following:

1. Create a directory for restricted documents.
 - a. From Windows Explorer, create a directory called **RESTRICTED** under SYS:\NOVONYX\SUITESPOT\DOCS on your server.
 - b. Using a text editor, open a new file and enter the following lines:

```
<html><body><h1>This is a restricted file!</h1></body></html>
```
2. Save the file as **INDEX.HTML** in the SYS:\NOVONYX\SUITESPOT\DOCS\RESTRICTED directory.
3. Run NetWare Administrator.
4. In your container, create a group called **RestrictedWebUsers**.
 - a. Click your *container*.
 - b. Press **Ins**.
 - c. Click **Group**; then click **OK**.
 - d. In the Create Group window, type **RestrictedWebUsers**.
 - e. Click **Define additional properties**; then click **Create**.
 - f. In the Group: RestrictedWebUsers window, click **Members**.
 - g. Click **Add**.
 - h. In the Select Object window, hold down the **Control** key and click **two user objects** in your container.
 - i. Click **OK**.
5. Give the RestrictedWebUsers group Read and File Scan rights to SYS:\NOVONYX\SUITESPOT\DOCS\RESTRICTED.
 - a. In the Group: RestrictedWebUsers window, click **Rights to Files and Directories**.
 - b. Click **Add**.
 - c. Under Browse Context, double-click on the **SYS volume** object for your server.
 - d. Under Browse Context, double-click **Novonyx**.
 - e. Under Browse Context, double-click **suitespot**.

Presentation**Notes****Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**

(continued)

- Continue the exercise.

- Remind students that they should *not* use a user object that occupies the Manager role in their container.

- f. Under Browse Context, double-click **docs**.
 - g. Under Available objects, double-click **RESTRICTED**.
 - h. Under Rights, make sure the **Read** and **File Scan** boxes are marked; then click **OK**.
6. Block access for all other users in your container to the **RESTRICTED** directory.
- a. In NetWare Administrator, double-click on the **SYS volume** object for your server in your container.
 - b. Double-click **Novonyx**.
 - c. Double-click **suitespot**.
 - d. Double-click **docs**.
 - e. Right-click **RESTRICTED**.
 - f. Click **Details**.
 - g. Click **Trustees of this Directory**.
 - h. Click **Add Trustee**.
 - i. Click your **container**; then click **OK**.
 - j. Under Access Rights, remove the check mark from the **Read** and **File Scan** boxes; then click **OK**.
7. Test the new configuration.
- a. Exit and restart your Web browser.
 - b. In the Location field enter
http://server_hostname/restricted/
 - c. Enter a user name and password for a user who is *not* a member of the RestrictedWebUsers group.
Note the result. Why did this happen?
Exit and restart your Web browser.
 - d. In the Location field enter
http://server_hostname/restricted/
 - e. Enter a user name and password for a user who *is* a member of the RestrictedWebUsers group.
 - f. Note the result. Why did this happen?

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 8-2:
Configuring the Netscape
FastTrack Server for NetWare**
(continued)

- Continue the exercise.

- Review the exercise.

Tuning and Troubleshooting the Netscape FastTrack Server

To troubleshoot and improve the performance of the Netscape FastTrack Server, you can

- Tune server performance
- Set the Maximum Packet Receive Buffers
- Regulate Web server content

Tuning Server Performance

You can improve the FastTrack Server's performance by configuring options to match the needs of your network. These options include:

- Number of maximum simultaneous requests
- Domain Name System lookups
- Listen-queue size
- HTTP persistent connection timeout

Configuring Maximum Simultaneous Requests

If your FastTrack Server is processing client requests slowly, you can change the Maximum Simultaneous Requests parameter (the number of active requests allowed for the server at one time) to improve performance. The default value is 48 requests.

To determine the number of simultaneous requests, the FastTrack Server counts the number of active requests, adding 1 to the number when a new request arrives, and subtracting 1 when the server fulfills the request.

When a new request arrives, the FastTrack Server checks to see if it is already processing the maximum number of requests. If the server has reached the limit, it defers processing new requests until the number of active requests drops below the maximum amount.

In theory, you could set the maximum simultaneous requests to 1 and still have a functional server. Setting this value to 1 would mean that the FastTrack Server could handle only one request at a time.

Tuning and Troubleshooting the Netscape FastTrack Server

- Introduce this subsection.

Tuning Server Performance

- Discuss tuning server performance.

Configuring Maximum Simultaneous Requests

- Discuss configuring maximum simultaneous requests.

For general purpose Internet or intranet use, most FastTrack Servers probably will not need to have the default value changed.

Because HTTP requests generally have a very short duration (response time can be as low as 5 milliseconds), processing one request at a time would still allow you to process up to 200 requests per second.

However, in reality, Internet clients frequently connect to the server and then do not complete their requests. In these cases, the FastTrack Server waits 30 seconds or more for the data before timing out. Also, some sites perform large transactions that take minutes, rather than seconds, to complete.

Both of these factors add to the maximum simultaneous requests that are required. If your site is processing a large number of requests that take several seconds to fulfill, you might need to increase the number of maximum simultaneous requests.

If you need to change the number of maximum simultaneous requests, set the number before starting the FastTrack Server. To reset the number, do the following:

1. In Server Manager, click **Server Preferences**.
2. Click **Performance Tuning**.
3. Type the number of requests.
4. Click **OK**.
5. Click **Save and Apply**.
6. When prompted that the changes have been saved and applied, click **OK**.

Disabling Domain Name System Lookups

If your FastTrack Server is running slowly, you can also check to see if it has been configured to use Domain Name System (DNS) lookups.

By default, DNS lookups are not enabled; if you enable DNS lookups, the FastTrack Server must look up the hostname for the IP address of every client making a request.

Although DNS lookups can be useful for administrators when looking at logs, they can adversely affect performance.



If you turn off DNS lookups, hostname restrictions will not work and hostnames will not appear in your log files. Instead, you will see IP addresses.

Presentation**Notes****Configuring Maximum Simultaneous Requests** *(continued)*

- Continue discussing maximum simultaneous requests.



Demonstrate how to configure Maximum Simultaneous Requests.

Disabling Domain Name System Lookups

- Discuss enabling DNS lookups.

To disable DNS lookups, do the following:

1. In Server Manager, click **Server Preferences**.
2. Click **Performance Tuning**.
3. Under Enable DNS, click **No**.
4. Click **OK**.
5. Click **Save and Apply**.
6. When prompted that the changes have been saved and applied, click **OK**.

You can also specify whether to cache the DNS entries. If you enable the DNS cache, the server can store hostname information after receiving it. If the server needs information about the client in the future, the information is cached and available without further querying.

You can specify the size of the DNS cache and an expiration time for DNS cache entries. The DNS cache can contain from 32 to 32768 entries; the default value is 1024 entries. Values for expiration time can range from 1 second to 1 year (specified in seconds); the default value is 1200 seconds (20 minutes).

Configuring Listen-Queue Size

The listen-queue size is a socket-level parameter that specifies the number of incoming connections the system will accept for that socket. The default setting is 100 incoming connections.

If you manage a heavily used Web site, you should make sure your system's listen-queue size is large enough to accommodate the listen-queue size setting from the Server Manager form.

If you change the listen-queue size, make sure your system supports the new size. You can use the listen-queue size in the Server Manager form to change the listen-queue size requested by the server.

If the server requests a listen-queue size larger than the system's maximum listen-queue size, the size defaults to the system's maximum.

Setting the listen-queue size too high can degrade server performance. The listen-queue size was designed to prevent the server from becoming overloaded with connections it cannot handle. If your server is overloaded and you increase the listen-queue size, the server will only fall further behind.

Presentation

Notes

Disabling Domain Name System Lookups *(continued)*

- Continue discussing DNS lookups.

Configuring Listen-Queue Size

- Discuss configuring listen-queue size.

Normally, the network administrator should not change the listen-queue size. The default setting is sufficient in most cases.

To configure the Listen-Queue Size, do the following:

1. In Server Manager, click **Server Preferences**.
2. Click **Performance Tuning**.
3. In the Listen Queue Size field, type the appropriate **value**.
4. Click **OK**.
5. Click **Save and Apply**.
6. When prompted that the changes have been saved and applied, click **OK**.

Configuring the HTTP Persistent Connection Timeout

With HTTP 1.1, a connection can be set to be persistent. However, even if a connection is persistent, it still needs to have a timeout setting; otherwise, it might consume system resources.

If you need to change the HTTP persistent connection timeout setting, do the following:

1. In Server Manager, click **Server Preferences**.
2. Click **Performance Tuning**.
3. In the HTTP Persistent Connection Timeout field, type a **number** in seconds.
4. Click **OK**.
5. Click **Save and Apply**.
6. When a dialog box appears stating that the changes have been saved and applied, click **OK**.

Presentation**Notes****Configuring Listen-Queue Size***(continued)*

- Discuss configuring listen-queue size.

Normally, the network administrator should not change the listen-queue size. The default setting is sufficient in most cases.

Configuring the HTTP Persistent Connection Timeout

- Discuss configuring HTTP persistent connection timeout.

Normally, the network administrator should not change the persistent connection timeout. The default setting is sufficient in most cases.



Demonstrate how to configure HTTP persistent connection timeout.

Setting the Maximum Packet Receive Buffers

When you are tuning the FastTrack Server, you also need to consider the following:

- Maximum Physical Receive Packet Size
- Maximum Packet Receive Buffers

Setting the Maximum Physical Receive Packet Size

You can increase or decrease the Maximum Physical Receive Packet Size parameter to match the largest client packet size in use on the network. The network board driver should specify the maximum packet size it can handle.

This parameter cannot be modified at the console prompt; you must include the parameter in the STARTUP.NCF file.

Ideally, you should use the largest possible packet size unless the client and server are configured for different packet sizes or if the packet must cross a router to get to the server.

Topology	Default Maximum Packet Size
Token Ring (16 Mbps)	4202
Token Ring (4 Mbps)	4202
Ethernet	1514

Table 8-2: Default Maximum Packet Sizes by Topology

To set the Maximum Physical Receive Packet Size, complete the following steps:

1. At the NetWare server console, enter **MONITOR**.
2. Select **Server Parameters**.
3. Select **Communications**.
4. Select **Maximum Physical Receive Packet Size**.
5. Enter the *packet size* for your network.
6. Press **Esc** twice.
7. Exit **MONITOR**.
8. Restart the NetWare server.

Presentation

Notes

Setting the Maximum Packet Receive Buffers

- Discuss the parameters presented on the student page.

Setting the Maximum Physical Receive Packet Size

- Discuss the effect of the Maximum Physical Receive Packet Size on Web server performance.



(Optional) Demonstrate how to set the Maximum Physical Receive Packet Size.

Setting the Maximum Packet Receive Buffers

The Maximum Packet Receive Buffers parameter determines the maximum amount of memory allocated to receive incoming packets. The default is 100 for a NetWare server.

The Maximum Packet Receive Buffers parameter can be set to any value between 50 and 4,294,967,295.

The Maximum Packet Receive Buffers value can be increased to accommodate a greater number of HTTP requests to the FastTrack Server. However, you should not change this value without first assessing how much server memory is being used by other server processes.

To calculate memory requirements, do the following:

1. Multiply the maximum physical receive packet size by the *current* maximum packet receive buffers. The answer equals A.
2. Multiply the maximum physical receive packet size by the *desired* maximum packet receive buffers. The answer equals B.
3. Subtract A from B to determine the memory requirement for the change.

Using MONITOR, check the available memory on your NetWare server. Adjust the Maximum Packet Receive Buffers setting only if you have enough memory available.

To set the Maximum Packet Receive Buffers parameter, complete the following steps:

1. At the server console, enter
MONITOR
2. Select **Server Parameters**.
3. Select **Communications**.
4. Select **Maximum Packet Receive Buffers**.
5. Enter the *number* you calculated for this parameter.
6. Press **Esc** twice.
7. Exit MONITOR.
8. Restart the server.

Presentation**Notes****Setting the Maximum Packet Receive Buffers**

- Discuss setting the Maximum Packet Receive buffers.

- Discuss the importance of calculating memory requirements before changing the Maximum Packet Receive Buffers value.



(Optional) Demonstrate how to set Maximum Packet Receive Buffers.

Regulating Web Server Content

Web server performance can be affected by file sizes and by HTML features, such as scripts and imagemaps, that require server processing.

You must understand how these issues affect server performance and must determine guidelines for Web server users.

File Sizes

You can set guidelines that limit the size and number of files that users store on the server.

The larger the file's size, the longer the file transfer will take. Text files are generally small, often less than 40 KB. Graphics cover a large size range, often ranging from 2 KB to 600 KB.

Audio clips vary in size, depending on file length, resolution, sampling rate, and compression rate.

A stereo, one-minute audio clip with CD-quality sampling is about 10 MB. Simple sounds, rather than complex music, might be as small as 10 KB.

Video clips can also vary greatly in size, from 100 or 200 KB to as much as 20 MB.

Each HTTP request uses a new thread. Large files tie up a thread for quite some time. If all your users store large audio and video clips on the FastTrack Server, some clients attempting to access your server might have packets dropped and be forced to attempt another connection to the server.

HTML Features

HTML features that require server processing, such as CGI scripts and imagemaps, can also affect FastTrack Server performance.

You should set guidelines for Web server users regarding HTML file and graphic file sizes.

If you do not limit the number of imagemaps and scripts on a Web server, you might find that they adversely affect server performance by slowing server response time or by causing client packets to be dropped.

Presentation**Notes****Regulating Web Server Content**

- Discuss the effect of Web server content on performance.
- Discuss file size restrictions.
- Describe HTML features.

Most Web server administrators do not restrict user file sizes. However, many administrators place restrictions on the size of audio or video clips.

Scripts can retrieve data, perform operations, and create HTML documents.

CGI scripts can be accessed with HTML forms. When data is input into an HTML form, the script communicates with a Web server by issuing a GET or POST function.

Each time a form is submitted, the server must process the request.

Overview of Novell FTP Services for NetWare

This subsection discusses FTP servers and Novell FTP Services for NetWare.

Understanding FTP Servers

The File Transfer Protocol (FTP) is a part of the TCP/IP suite of control procedures for transferring files between a remote host computer and a local computer on a TCP/IP network. FTP includes functions to log in to the network, list directories, and copy files.

An FTP server is an application that provides users with the ability to transfer files to and from the computer on which it is running via the FTP protocol.

An FTP server operates in a client/server relationship. When a client program requests a file, and the FTP server program supplies the file. Likewise, when the client sends a file, the FTP Server receives it.

An FTP server uses specified directories in the file system to store all the files it will send to and receive from clients.

The FTP protocol is supported by most Web browsers. FTP transfers are initiated from within a Web browser by entering the URL preceded with *ftp://* instead of *http://*.

Presentation

Notes

Overview of Novell FTP Services for NetWare

- Introduce the subsection

Understanding FTP Servers

- Discuss the FTP protocol.
- Discuss FTP Servers.

Introduction to Novell FTP Services for NetWare

Novell FTP Services for NetWare provides FTP clients with the ability to access and transfer files. The server allows up to 64 client sessions to be active at one time.

The FTP file transfer service consists of two modules:

- FTPSERV.NLM
- INETD.NLM

The FTP Server module (FTPSERV.NLM) is activated by the INETD NLM when an FTP client initiates a session with the NetWare server, as shown in Figure 8-18.

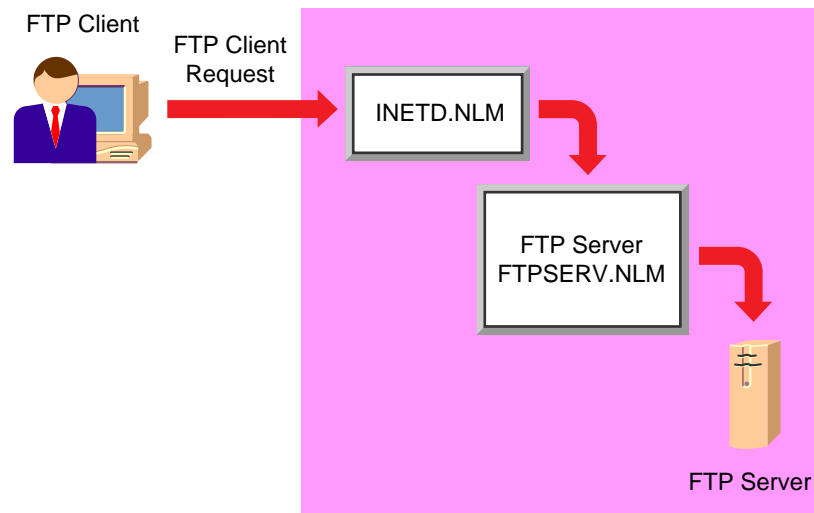


Figure 8-18: The Novell FTP Server

The agent module accepts the connection and loads FTPSERV to service the connection. To free up as much memory and as many resources as possible on the NetWare server, the FTPSERV module is unloaded when no active FTP sessions exist.

Presentation

Notes

Introduction to Novell FTP Services for NetWare

- Describe Novell FTP Services for NetWare.



8-18 (Figure 8-18: The Novell FTP Server)

Installing Novell FTP Services for NetWare

Before you install Novell FTP Services for NetWare, you must have NetWare installed. You must also have TCP/IP configured and loaded on the server.

System Requirements

The Novell FTP Server is installed as part of NetWare NFS Services. The following requirements must be met to install NetWare NFS Services:

- NetWare 4.1 or later.
- An additional 12 MB of RAM. This RAM requirement is in addition to the RAM requirement for the network operating system.
- 8 MB of free disk space on the SYS volume.
- TCP/IP configured on the server.

Installing the Server

Before installing the FTP Server, you must load the NFS name space (NFS.NAM) and add it to the volume the FTP Server will be using.

To load the NFS.NAM module, enter the following console command:

LOAD NFS.NAM

After the required name space support driver is loaded and you have verified that your server contains enough memory to support the name space, you must perform a one-time procedure to add the name space.

To add the NFS name space to a NetWare volume, enter the following command at the server console:

ADD NAME SPACE NFS TO *volume_name*

Replace *volume_name* with the name of the volume being configured for the NFS name space.



Do not place the ADD NAME SPACE command in the AUTOEXEC.NCF file. This command needs to be executed only once on a NetWare volume.

Installing Novell FTP Services for NetWare

- Explain the software requirements needed to run FTP Services for NetWare.

System Requirements

- Review the hardware requirements necessary to run the Novell FTP Server.

Installing the Server



- Demonstrate how to add the NFS name space.
- Remind students that a name space only needs to be loaded once.

Students should not put the ADD NAME SPACE command in the server's AUTOEXEC.NCF file.

After you have configured your volume for the NFS name space, use the following steps to install NetWare NFS Services:

1. Mount the NetWare CD-ROM as a NetWare volume.
2. Set the default NDS context to the container where your server object is located.
3. Load NWCONFIG.
4. Select **Product Options**.
5. Select **Install a product not listed**.
6. Press **F3** to enter a new path.
7. Enter **volumentame:\PRODUCTS\NWUXPS**.
8. Follow the screen prompts.

You are prompted to choose one of the following name services options during the installation:

- Local NIS
- Remote NIS

Network Information Services (NIS) is a distributed database that provides common information such as information about users and groups from a central location.

Presentation**Notes****Installing the Server** *(continued)*

Demonstrate how to install the FTP Server.

- Explain the NIS options.
- Discuss NIS.

Use the Local NIS option and the DATA volume.

Students should consult their ISPs before choosing which name service to provide on their FTP Servers.

Selecting *Local NIS* allows you to update and manage the NIS master database using the Unicon utility, shown in Figure 8-19.

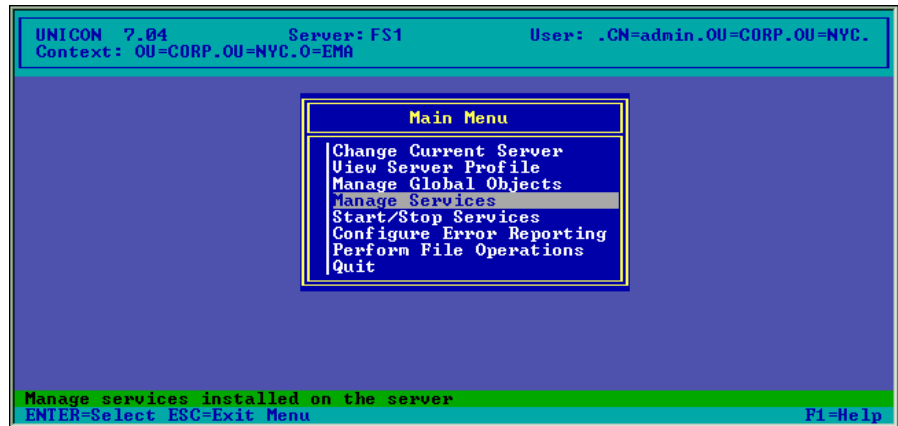


Figure 8-19: Unicon

Once you configure a NetWare server as the master, it can provide NIS information to any other NFS/NetWare Print Services servers on the network.

Selecting *Remote NIS* does not allow you to update or manage the NIS database using Unicon. You can view user, group, and host information stored on the master, but you can not make any modifications. All user, group, and host information must be managed on the master.

After Novell FTP Services is installed, you need to start the service before it can be used. Perform the following steps to start Novell FTP Services:

1. Load Unicon.
2. From the Running Services menu, press **Ins** and select **FTP Server**.
3. Exit the installation program and restart the server.

Presentation

Notes

Installing the Server *(continued)*

- Introduce Unicon.



8-19 (Figure 8-19: Unicon)

- Continue discussing NIS.



Demonstrate how to start the FTP Server.

Hands-On Exercise 8-3: Installing the Novell FTP Server

In this exercise you load the NFS name space and install Novell FTP Server.

Complete the following.

1. Load the NFS name space and add it to the SYS and DATA volumes.
 - a. At the server prompt, enter
LOAD NFS.NAM
 - b. At the server prompt, enter
ADD NAME SPACE NFS TO SYS
 - c. At the server prompt, enter
ADD NAME SPACE NFS TO DATA
2. Install the FTP Server.
 - a. Load **NWCONFIG.NLM**.
 - b. Select **Product Options**.
 - c. Select **Install a product not listed**.
 - d. Press **F3** to specify a path.
 - e. Enter the **path** provided by your instructor.
 - f. If you are installing over the network, log in as your **Admin user**.
 - g. If you are installing over the network, press **Enter** when informed that files are being copied temporarily to your server.
 - h. Read the message regarding the README file; then press **Enter**.
 - i. When asked if you want to read the README file, select **No**.
 - j. When prompted to enter the drive and/or path for booting NetWare, enter **C:\NWSERVER**.
 - k. If you are warned that the HOST.DB file does not exist, press **Enter**.
 - l. In the Server Login screen, log in as your **Admin user**.

Presentation

Notes

Hands-On Exercise 8-3: Installing the Novell FTP Server

- Introduce the exercise.



:20

- Have the students complete the exercise.

- Provide the path to the installation files.

- m. In the Available Name Service Options screen, select **Local NIS** or **Remote NIS**.
 - n. In the Setup Name Services screen, press **Esc** to keep the defaults.
 - o. When prompted to continue name services installation, select **Yes**.
 - p. Press **Esc** when prompted.
 - q. Press **Esc** when prompted.
 - r. In the Running Services screen, press **Ins**.
 - s. In the Available Services screen, select **FTP Server**.
 - t. Press **Esc** to complete the installation.
 - u. Press **Esc**.
 - v. Exit NWCONFIG.
3. Restart the server.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 8-3:
Installing the Novell FTP
Server** *(continued)*

- Review the exercise.

Configuring the Novell FTP Server

You need to complete two tasks to configure the Novell FTP Server:

- Configure server parameters.
- Set file system rights.

Configuring FTP Server Parameters

The Novell FTP Server is configured through Unicon. Follow the procedure below to configure the Novell FTP Server:

1. At the server console, load Unicon.
2. Select **Manage Services**.
3. Select **FTP Server**.
4. Select **Set Parameters**.

The various configuration options for the Novell FTP Server are described in Table 8-3.

Parameter	Description
Maximum Number of Sessions	Specifies the number of FTP client sessions that can be active concurrently. Range: 1 to 64, inclusive.
Maximum Session Length	Specifies the length of time a client can remain connected to the FTP Server. Range: 0 to 99,999 minutes, inclusive.
Idle Time Before FTP Server Unloads	Specifies the interval between no active client sessions and the FTPSERV module unloading. Range: -1 to 99,999 minutes, inclusive.
Anonymous User Access	Allows or prevents anonymous logins to the FTP Server.
Default User's Home Directory	Identifies the directory in which users will be placed upon logging in to the FTP Server.
Anonymous User's Home Directory	Identifies the directory anonymous users will be placed in upon logging in to the FTP Server if they do not have home directories.

Table 8-3: FTP Server Configuration Parameters

Presentation**Notes****Configuring the Novell FTP Server**

- Briefly outline the three tasks required to configure the Novell FTP Server.

Configuring FTP Server Parameters

- Describe the FTP Server configuration options.
- Explain the -1 option for "Idle Time Before FTP Server Unloads."

Setting this option to -1 means the FTP Server never unloads itself from server memory.

Parameter	Description
Default Name Space	Determines which name space (DOS or NFS) is active when a client initiates a session.
Intruder Detection	Enables or disables intruder detection.
Intruder Detection: Number of Unsuccessful Attempts	Specifies the number of unsuccessful login attempts allowed within the time period specified.
Intruder Detection: Detection Reset Interval	Specifies the time interval within which unsuccessful logins are counted.
Log Level	Determines what, if any, information is written to a log file maintained by the FTP Server. Options include <ul style="list-style-type: none"> ■ None. Nothing is written to the log file. ■ Statistics. Records file transfer data. ■ Logins. Records login information. ■ File. Records FTP transaction data. Only one of these options can be used at any given time.

Table 8-3: FTP Server Configuration Parameters (continued)

Enable Anonymous User Access

By default, the Novell FTP Server uses NDS authentication to determine access to the FTP Server. For example, suppose user .EAlder.CORP.NYC.EMA opens an FTP session with your FTP Server. Before she is allowed access, she must supply her NDS username and password.

However, the Novell FTP Server also provides the option of allowing anonymous user access. This allows non-NDS users to access your FTP Server.

Anonymous users are not required to supply a username and password to access the FTP Server. Because of this, anonymous users are usually restricted to a specified directory tree in the file system.

Presentation

Notes

Configuring FTP Server Parameters

(continued)



Demonstrate how to configure FTP Server parameters.

- Discuss enabling anonymous user access.

To enable anonymous user access on your FTP Server, complete the following:

1. At the server console, load Unicon.
2. Select **Manage Services**.
3. Select **FTP Server**.
4. Select **Set Parameters**.
5. Set Anonymous User Access to **Yes**.
6. Save the changes.

Set Default Directories for FTP Users

After installation, FTP users, including anonymous users, are placed by default at the root of the SYS volume when they access the FTP Server.

We recommend that you configure your FTP Server to redirect NDS and anonymous users to default home directories in the file system when they access the FTP Server.

For example, authenticated NDS users could be placed in a home directory named USERS while anonymous users could be placed in a home directory named ANON.

To set the default directory for FTP users, complete the following:

1. At the server console, load Unicon.
2. Select **Manage Services**.
3. Select **FTP Server**.
4. Select **Set Parameters**.
5. Select **Default User's Home Directory**.
6. Select a **volume**; then enter a **directory name**.
7. Select **Anonymous User's Home Directory**.
8. Select a **volume**; then enter a **directory name**.
9. Save the changes.

Presentation

Notes

Configuring FTP Server Parameters

(continued)



Demonstrate how to enable anonymous user access.



Discuss setting default directories for FTP users.



Demonstrate how to set default directories for FTP users.

Setting File System Rights

After you configure the FTP Server, you must make sure that the NDS user objects have the correct file system rights to the home directories you specified.

The following rights are necessary for users who need to download files:

- Read
- File Scan

The following rights are necessary for users who need to download and upload files:

- Read
- File Scan
- Write
- Create

The Erase right can be added for users who need to be able to delete files.

To set file system rights to FTP home directories, complete the following:

1. Run NetWare Administrator.
2. Browse to the desired **directory**.
3. Right-click the **directory**; then click **Details**.
4. Click **Trustees of this Directory**.
5. Add the appropriate NDS user objects to the list of trustees and assign them the appropriate rights.
6. To grant rights for anonymous users, add the Anonymous user object to the trustee list and grant the appropriate rights.

Presentation

Notes

Setting File System Rights

- Discuss setting file system rights for FTP users.



- Demonstrate how to set file system rights for FTP users.

Hands-On Exercise 8-4: Configuring the Novell FTP Server

Complete the following:

1. Create FTP directories and provide sample content.
 - a. At the root of the DATA volume, create two directories: **ANON** and **USERS**.
 - b. Copy some files and directories from your workstation's hard disk to the DATA:\ANON and DATA:\USERS directories.
 - c. In your container, create a new user. The default home directory for this user should be DATA:\USERS.
2. Configure FTP user home directories.
 - a. At the server prompt, enter
LOAD UNICON
 - b. Log in as your *Admin user*.
 - c. In the Main Menu, select **Manage Services**.
 - d. In the Manage Services menu, select **FTP Server**.
 - e. In the FTP Administration menu, select **Set Parameters**.
 - f. In the FTP Server Parameters screen, select **Anonymous User Access**.
 - g. In the Allow Anonymous User Access screen, select **Yes**.
 - h. In the FTP Server Parameters screen, select **Default User's Home Directory**.
 - i. In the Default User's Home Directory screen, select **Volume Name**.
 - j. In the Available NetWare Volumes screen, select **DATA**.
 - k. In the Default User's Home Directory screen, Select **Directory Name**.
 - l. Enter **USERS**.
 - m. Press **Esc** and save the changes.
 - n. In the FTP Server Parameters screen, select **Anonymous User's Home Directory**.
 - o. In the Anonymous User's Home Directory screen, select **Volume Name**.

Presentation

Notes

Hands-On Exercise 8-4: Configuring the Novell FTP Server



Introduce the exercise.



:15

Have the students complete the exercise.

- p. In the Available NetWare Volumes screen, select **DATA**.
 - q. In the Anonymous User's Home Directory window, select **Directory Name**.
 - r. Enter **ANON**.
 - s. Press **Esc** and save the changes.
 - t. In the FTP Server Parameters screen, select **Default Name Space**.
 - u. In the Default Name Space screen, select **NFS**.
 - v. Press **Esc** to exit.
 - w. Select **Yes** to save changes.
 - x. Press **Esc** until you return to the Main Menu.
3. Set file system rights for the ANON home directory to allow users to download files.
 - a. Start NetWare Administrator.
 - b. Browse to the **ANON** directory on your DATA volume.
 - c. Right-click **ANON**.
 - d. Click **Details**.
 - e. Click **Trustees of this Directory**.
 - f. Click **Add Trustee**.
 - g. Click **anonymous**; then click **OK**.
 - h. Verify that *only* the **Read** and **File Scan** boxes are marked.
 - i. Click **OK**.
 4. Set file system rights for the USERS home directory to allow users to upload and download files.
 - a. Browse to the **USERS** directory on your DATA volume.
 - b. Right-click **USERS**.
 - c. Click **Details**.
 - d. Click **Trustees of this Directory**.
 - e. Add your container as a trustee.
 - f. Give your container **Read**, **Write**, **Create**, and **File Scan** rights.
 - g. Click **OK**.

(End of Exercise)

**Hands-On Exercise 8-4:
Configuring the Novell FTP
Server** *(continued)*

- Review the exercise.

Using Novell FTP Services

You can use a standard Web browser to browse, download files from, and upload files to your FTP Server, as shown in Figure 8-20.

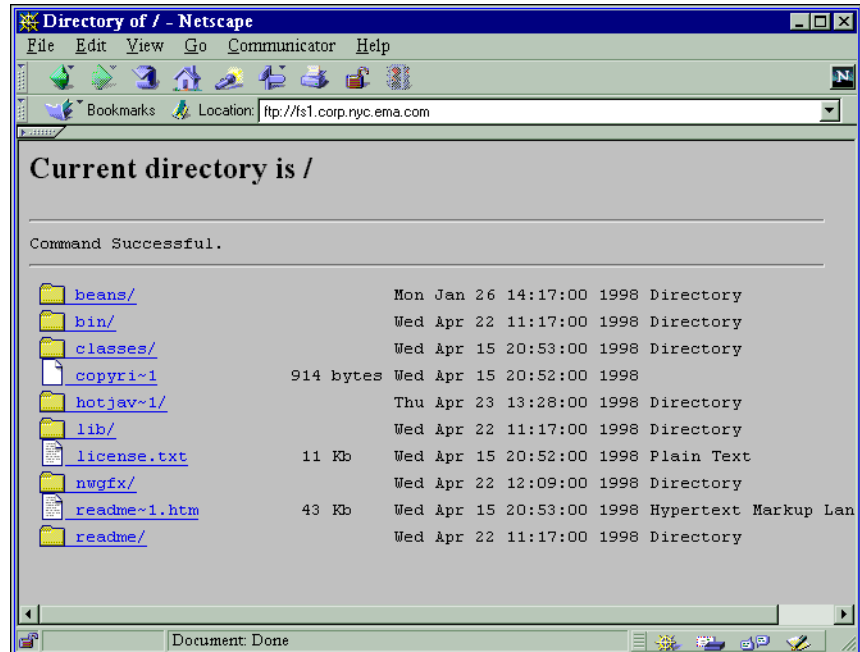


Figure 8-20: Using Netscape to Browse an FTP Site

To use the Netscape browser to access the FTP Server, enter the following in the Location field:

`ftp://FTP_server_hostname`

When you use a Web browser to download and upload files on a Novell FTP Server, the you are automatically logged in to the site as user Anonymous.

To specify an NDS user, enter the NDS username followed by the @ symbol followed by the FTP Server name or address. Use the following syntax:

`ftp://username@FTP_server_hostname`

If the user object has a password, you will be prompted to enter it.

Using Novell FTP Services



8-20 (Figure 8-20: Using Netscape to Browse an FTP Site)

- Describe how to use a Web browser to access the FTP Server.

Downloading Files

Netscape® can be configured to do different things when you click an FTP file. You can download the file to your hard disk or launch an application. To configure your browser to save files to disk, see Netscape's online documentation.

Uploading Files

To upload a file to an FTP site using Netscape, navigate to the FTP directory where you want to place the file. In the File menu, click Upload. Browse to the file you want to upload and double-click it.

Presentation

Notes

Downloading Files



Demonstrate how to use Netscape to transfer files from the FTP Server.

Uploading Files



Demonstrate how to use Netscape to transfer files to the FTP Server.

Hands-On Exercise 8-5: Transferring Files Using Netscape

In this exercise you use Novell FTP Services and Netscape to transfer binary and text files.

Complete the following:

1. As an anonymous user, download a file from your FTP Server.
 - a. On your workstation, launch Netscape.
 - b. In the File menu, click **Open Page**.
 - c. In the Open Page window, type
ftp://ftp_server_hostname
Replace *ftp_server_hostname* with the hostname for your FTP server.
 - d. Click **Open**.
 - e. Right-click a *file* listed on your FTP Server and click **Save Link As** from the pop-up menu.
 - f. Select a location on your hard disk to save the file to; then click **Save**.
2. As a user in your container, upload a file to your FTP Server.
 - a. In the File menu, click **Open Page**.
 - b. In the Open Page window, type
ftp://username@ftp_server_hostname
Replace *username* with the name of the user you created in Exercise 8-4 Step 1c. Replace *ftp_server_hostname* with the hostname for your FTP Server.
 - c. Click **Open**.
 - d. In the File menu, click **Upload File**.
 - e. Select a file to upload; then click **Open**.
You can change the type of file being displayed by specifying a different type in the **Files of type** field.
3. Exit Netscape.

(End of Exercise)

Presentation**Notes**

Hands-On Exercise 8-5: Transferring Files Using Netscape

- Introduce the exercise.



- Have the students complete the exercise.

- Assist students as needed.

- Review the exercise.

The following are frequently seen mistakes on the part of students:

- If students copy files with the Read Only attribute to their FTP Servers, they cannot download the files.
- The entries for the default user and anonymous user directory are case-sensitive. If students use the wrong case, they may see an error stating "*Username can't change directory to default_directory on server.*"

Troubleshooting FTP

Most FTP-related problems can be categorized as follows:

- Network failure
- FTP Server not running
- Overloaded FTP Server
- FTP client configuration errors
- FTP Server configuration errors
- User error

Network Failure

You can verify that apparent FTP problems are generated due to a network failure by attempting to PING the desired FTP Server. To do this, complete the following steps:

1. Open a DOS window on your workstation.
2. At the C: prompt, enter **PING FTP_Server_ip_address**.

If the PING test fails, the problem is likely network related.

FTP Server Not Running

If you determine you have no network problems, your FTP Server might not be running. To see if the server is running, perform the following steps from the server:

1. Load Unicon.
2. In the main menu, select **Start/Stop Services**.
3. Verify that the FTP Server is present in the Running Services list.

If it is missing, press **Ins**; then select **FTP Server** from the Available Services list.

Troubleshooting FTP

- Outline the basic problems discussed in this subsection.

Network Failure



Demonstrate how to use PING to determine if the network is down.

FTP Server Not Running



Demonstrate how to verify that the FTP Server is running.

Use Unicon's Running Services menu.

Overloaded FTP Server

You can impose a limit on the maximum number of concurrent client connections on your FTP Server. This maximizes FTP Server performance and minimizes the impact of FTP client sessions on a busy host.

If you attempt to connect to an FTP Server that does not have client sessions available, you will receive an error message. The error message that you receive depends on the FTP client application.

For example, when you try to connect to an FTP server that has no available sessions, the LAN Workplace for DOS FTP.EXE program returns the "I/O Error, Connection Lost" message.

Under these same circumstances, a Web browser's FTP client usually returns a more user-friendly message, which indicates that the server has no available connections and that you should attempt to connect at a later time.

Another typical indication of an overloaded FTP Server is extremely slow file transfers. This is common during peak network/server usage times and occurs most frequently when you attempt to transfer large files, such as those that exceed 1 MB.

FTP Client Configuration Errors

If a user cannot connect to the FTP Server, you might have an improperly configured client. If your client has the TCP/IP protocol loaded, check the following:

- Is the client TCP/IP protocol stack properly loaded?
- Is the client TCP/IP protocol stack configured with the proper IP address, subnet mask, and default router information?
- Is the client network interface board configured for the proper frame type?

You can verify these parameters by performing the PING test. The client TCP/IP protocol stack is functional if you can successfully PING the FTP Server from the client.

Presentation**Notes****Overloaded FTP Server**

- Discuss the types of messages returned by overloaded FTP Servers.



Demonstrate the overloaded FTP Server error message received when using Netscape.

Set the number of available connections on the classroom FTP Server to 1 and have two or more students attempt to access the site.

FTP Client Configuration Errors

- Discuss the types of errors that can occur on an improperly configured FTP client.

FTP Server Configuration Errors

If a user cannot connect to a specific FTP Server, the user account might be restricted from accessing the server. If a user cannot download a specific file, make sure the file is not flagged with the Read-Only file attribute.

User Error

Many problems can result from inexperienced or improperly trained FTP users. If you are contacted by a user for FTP-related problems, verify the following.

- Was the FTP Server name specified correctly?
- Was the proper account name specified when the user attempted to log in to the FTP Server?

In some cases, such as when the FTP Server is running on a NetWare server, the user might need to specify his or her distinguished NDS name to gain access to the server.

- Was the proper password specified when the user attempted to log in to the FTP Server?
- If a file transfer failed, did the user have the appropriate rights to create a file in the destination directory?

Presentation**Notes****FTP Server Configuration Errors**

- Discuss possible FTP Server configuration errors.



Demonstrate what happens when a user tries to download a Read-Only file using the Netscape browser.

These errors include improper user restrictions or user directory locations.

Flag one of the files in the Anonymous user directory as Read-Only and attempt to download it using the browser.

User Error

- Discuss typical problems related to user error.

Most network administrators are familiar with the problems discussed here.

The number of assumptions made by the administrator should be kept to a minimum and the fundamental procedures for troubleshooting should be adhered to.

Summary

In this section you learned that the FastTrack Server for NetWare provides a fast Web server for Internet or intranet use.

The FastTrack Server for NetWare is administered through the Administration Server via a Web browser.

The FastTrack Server can be bound to NDS to provide security for Web server content.

The Novell FTP Server provides FTP services to anonymous and authenticated NDS users.

The FTP Server is administered at the server console through the Unicon utility.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

1. Explain the services provided by the Netscape FastTrack Server for NetWare.
2. Install the Netscape FastTrack Server for NetWare.
3. Use the Administration Server to configure the Netscape FastTrack Server for NetWare.
4. Troubleshoot and tune the Netscape FastTrack Server for NetWare.
5. Explain the services provided by Novell FTP Services.
6. Install Novell FTP Services.
7. Configure Novell FTP Services.
8. Use Novell FTP Services to transfer binary and text files.
9. Troubleshoot basic Novell FTP Services problems.

Notes

SECTION 9 Securing the NDS Tree

Duration 02:30

Preparation

Do the following:

- Make each student a copy of the NDS Security Concepts List (page B-1) for Exercise 9-1.
- Make a single-sided copy of the NDS Security Concepts (pages B-2 through B-5) for Exercise 9-1. Cut out the concepts to create cards to hand to each student.

SECTION 9

Securing the NDS Tree

In this section you learn to distribute network administration by implementing NDS security.



This section begins with an exercise designed to review your knowledge of NDS security.

Objectives

Upon completing this section, you should be able to

1. List the default rights assigned when creating a Directory and objects.
2. Explain the guidelines and considerations for implementing NDS security in a multicontext environment.
3. Describe the differences between centralized and distributed NDS management.
4. Determine the administrative roles needed in your organization and identify the NDS objects and rights assignments that support those roles.

Presentation

Notes

Securing the NDS Tree

- Introduce the section.

Objectives

- Present the section objectives.

Group Exercise 9-1: NDS Security Review

In this exercise, you review the basic NDS security concepts learned in Course 560, NetWare 5 Administration. The concepts presented later in this section build on the basic NDS security concepts.

The exercise is divided into four phases:

- **Phase I**—Each student is assigned a concept and given time to review it.
- **Phase II**—The class is divided into two teams; each student shares with the team his or her insights about the assigned concept.
- **Phase III**—Each team writes questions about the other team's concepts and then selects the best questions to present in the review challenge match.
- **Phase IV**—The teams take turns asking each other questions about the concepts.

(End of Exercise)

Presentation**Notes****Group Exercise 9-1: NDS Security Review**

Introduce the exercise.



:45

Have the students complete the NDS security review exercise.

Pay close attention to the time of each phase as the activity progresses.

No corresponding page in student manual

Presentation**Notes****Group Exercise 9-1: NDS Security Review** *(continued)*

:10 Phase 1:
Individual Concept Review

1. Divide the class into two teams.
2. Distribute the concept cards to the students. Have the students on each team discuss the concepts and resolve any questions.
3. Give the students five minutes to review the concepts and prepare to teach the concepts to their team.



:15 Phase 2:
Group Concept Review

1. Have each student take a turn teaching his or her team a concept from the cards.
2. Give each student two minutes.
3. On the whiteboard, list the teams and the concepts that the team members are reviewing.
4. Keep track of the time and notify the teams when they should begin discussing the next concept.



:08 Phase 3:
Challenge Questions
Creation

1. Give each team member a copy of the NDS Security Concepts List.
2. Have each student create questions and expected answers for the other team's concepts. Give the students four minutes to create the questions and answers.
3. Give the teams four minutes to select six to eight of the best questions and answers.

No corresponding page in student manual

Presentation**Notes****Group Exercise 9-1: NDS Security Review** *(continued)*

:10

**Phase 4:
Review Challenge** Review the exercise.

1. Begin the challenge; each team asks the other team one of the questions.
2. The team answering the question must follow these rules:
 - a. A student who has not answered a question receives the question.
 - b. If the student can answer the question correctly without help from his or her team, his or her team scores two points.
 - c. If the student answers correctly with the help of his or her team, the team scores one point.
 - d. If the answer is incorrect, one point is subtracted from the team's total.
3. The team with the highest score wins.
4. Provide a reward for the winning team (optional).

Clear up any misconceptions about the NDS security concepts that were discussed during the exercise.

Understanding NDS Default Rights

To coordinate security with your overall network design, you should consider the default rights assigned to NDS objects. When you initiate the following events, rights are assigned by default:

- Create the initial tree ([Root])
- Create a container
- Install a server
- Create a user

These default rights allow new objects, representing network resources, to be accessed and administered by the appropriate users and network administrators.

Knowing the default rights assigned to objects provides you with a starting point for your security implementation; you can then make additional security assignments as needed.

Default Rights Granted at Initial Tree Creation

When you install NDS on the first server in a new NDS tree, two objects are automatically created: a [Root] object and an Admin object. The [Public] trustee is also created at this time.

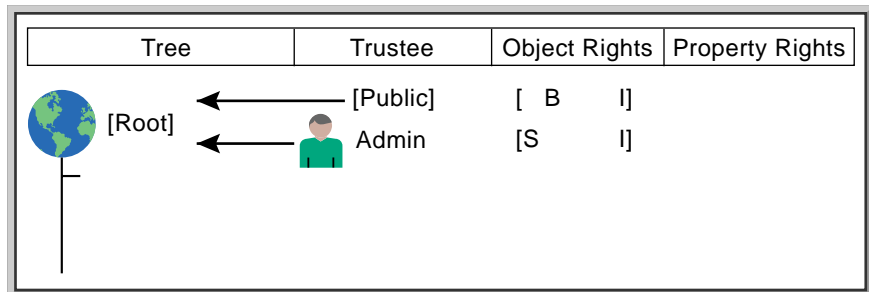


Figure 9-1: Default Objects and Rights Created in Initial Tree

Presentation**Notes****Understanding NDS Default Rights**

- Introduce NDS default rights.
- Explain that when a network administrator initiates certain events, NDS assigns default rights.
- Stress the default settings.

In most cases the default rights are sufficient for the network to work properly. Additional rights are usually assigned to users who will be responsible for network administration at one level or another.

Default Rights Granted at Initial Tree Creation

9-1 (Figure 9-1: Default Objects and Rights Created in Initial Tree)

[Public] and Admin are granted the following default rights when you install NDS.

Trustee	Default Rights	Reasons for Defaults
[Public]	[BI] - Browse and Inheritable object rights to [Root]	Allows users to see the NDS tree and all the objects in it
Admin	[SI] - Supervisor and Inheritable object rights to [Root]	Allows the first user object created (Admin) to administer the NDS tree

Table 9-1: NDS Rights Granted During NDS Installation

Default Rights Granted to New Containers

Any container you create in NDS receives default rights to itself. This rights assignment makes user objects in the container security equivalent to the container.

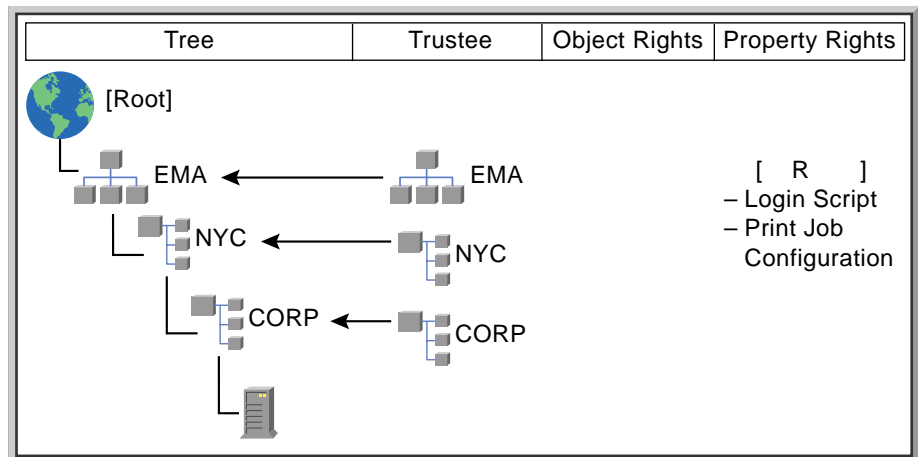


Figure 9-2: Default Rights Granted to a New Container

Presentation**Notes****Default Rights Granted at Initial Tree Creation** *(continued)*

- Discuss the default rights assignments that are made when NDS is installed.

- Discuss the reasons these defaults are created.

Default Rights Granted to New Containers

9-2 (Figure 9-2: Default Rights Granted to a New Container)

Reasons:

- The [Public] [BI] object rights are granted so that users can see the NDS tree and all the objects that will be placed in it.

- The Admin [SI] object rights are granted so that the first user object created (Admin) can administer the network.

The following default rights are assigned to a container when it is created:

Trustee	Default Rights	Reasons for Defaults
Container object	[R] - Read property right to Login Script property	Allows users in the container to read the container login script
	[R] - Read property right to Print Job Configuration (Non-NDPS) property	Allows users in the container to read the container's print job configurations

Table 9-2: NDS Rights Granted During NDS Installation

Default Rights Granted at Server Installation

When you install NDS on a NetWare server, default rights are given to the user who creates the server object and to the [Root] object and the [Public] trustee.

The user who creates the server object is usually the person associated with the network or container administrator's user object. The user object is typically identified in the NDS tree as the Admin user.

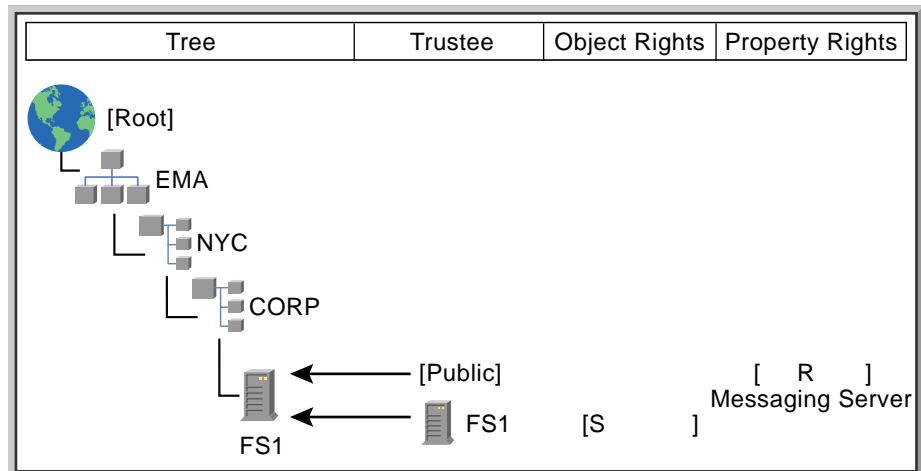


Figure 9-3: Default Rights Granted at Server Installation

Presentation**Notes****Default Rights Granted to New Containers** *(continued)*

- Explain the reasons for the default rights.

Information about login scripts is found in Section 7 of Course 560, NetWare 5 Administration.

Remind students that the container login script applies to all users in the container. Container scripts supply multiple users with the scripts they need without having to create individual scripts for each user.

Default Rights Granted at Server Installation

9-3 (Figure 9-3: Default Rights Granted at Server Installation)

A server installed in the NDS tree receives the following default rights.

Trustee	Default Rights	Reasons for Defaults
Server	[S] - Supervisor object right to itself	Allows the server to modify the parameters of its own object
[Public]	[R] - Read right to Messaging server property	Allows any network client to identify the messaging server assigned to this server

Table 9-3: NDS Rights Granted During Server Installation

Presentation**Notes****Default Rights Granted at Server Installation** *(continued)*

- Explain the reasons for the default rights.
- Provide an example of a server needing Supervisor rights to itself.
- Describe a messaging server.

When a new network board is installed in a server, the server needs Supervisor rights so that the new board parameters can be read automatically and stored as properties of the server object.

Messaging server objects can be created in the NDS tree to represent servers that handle mail services and broadcast messages on the network.

These servers provide messaging services through NetWare's Message Handling Services (MHS). The servers are useful in delivering email messages between dissimilar platforms.

Default Rights Granted to New User Objects

When you create a new user object in NDS, certain necessary rights are granted automatically. These rights are granted to provide the user with some degree of access to resources on the network.

The user object receives enough rights to modify its login script and its print job configurations. If you do not want the user to modify his or her login script, you must revoke the Login Script property right.

Similarly, you must revoke the Print Job Configuration property right if you do not want users to be able to modify their print job configurations in a non-NDPS environment.

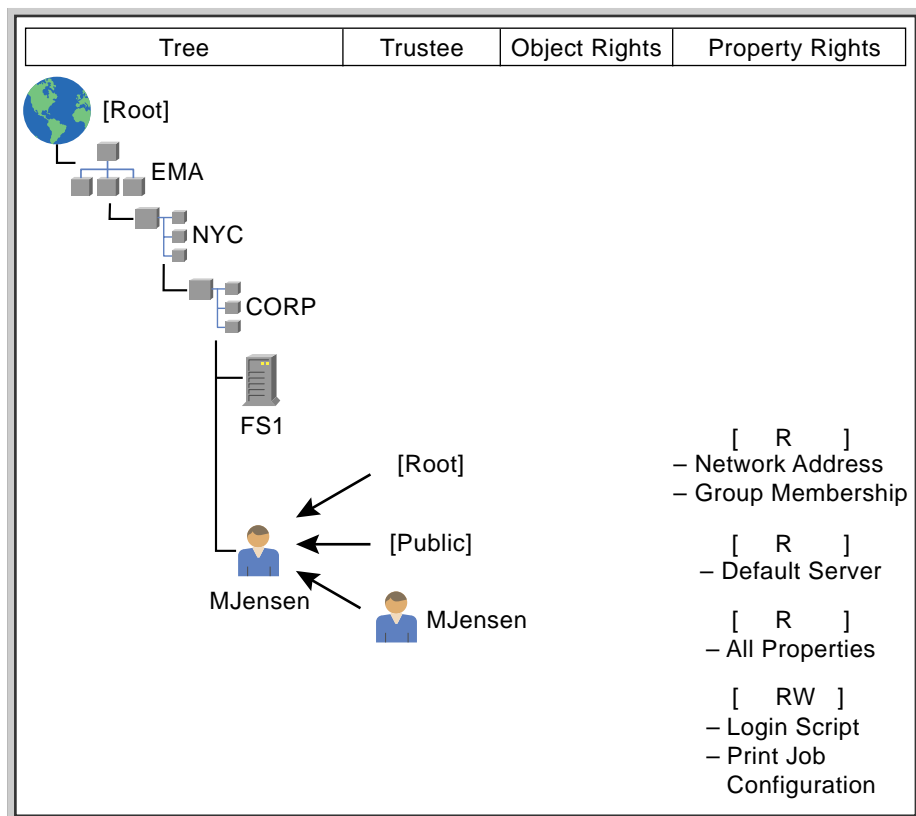


Figure 9-4: Default Rights Granted to New User Objects

Presentation**Notes****Default Rights Granted to New User Objects**

9-4 (Figure 9-4: Default Rights Granted to New User Objects)

- Discuss the default rights granted to new user objects.

- Explain that students can revoke default rights for new users by using a template object to create user objects.

Following is a list of the default rights granted to a new user object.

Trustee	Default Rights	Allows Trustee To
[Root]	[R] - Read property right to Network Address and Group Membership properties	Identify the network address and any group memberships
[Public]	[R] - Read property right to Default Server property	Determine the default server for the user object
User	[R] - Read right to All Property rights	Read the properties stored in the user object
	[RW] - Read and Write property rights to Login Script property	Execute and change his or her login script
	[RW] - Read and Write property rights to Print Job Configuration (Non-NDPS) property	Create print jobs and send them to the printer

Table 9-4: Default Rights Granted During User Object Creation

Presentation**Notes****Default Rights Granted to New User Objects** *(continued)*

- Discuss the default rights automatically assigned to a new user object.



Demonstrate how to find the default rights in NetWare Administrator.

Do the following:

1. Point out both the **All Properties** and **Selected Properties** default rights in the Trustee of Object window.
2. Click the **Selected Properties** and scroll through the Properties window to see how the selected properties are marked.
3. Indicate that the properties marked with an arrow are the properties that apply to this NDS object.
4. Click the **Login Script** property and show the change in the property rights.

Note: The default object rights are not marked in the Trustee of Object window because the rights are not assigned explicitly — they are assigned through security equivalences. Avoid discussing this in detail.

Guidelines for Implementing NDS Security

Within a multicontext environment, NDS rights should be granted for these reasons:

- To allow users to use network resources in one or more contexts
- To manage NDS objects and their properties
- To provide administrative security measures

Using Network Resources

For most users, the default NDS rights provide adequate access to necessary network resources. Users receive the Browse object right automatically through the [Public] trustee. This allows them to see the objects in the NDS tree.

In the following cases, you need to assign users additional NDS rights:

- To use a directory map object, the user object needs the Read property right to the Path property or to the All Properties option.
- To use a profile login script object that has been assigned to the user, the user object needs the Read property right to the Login Script property.

Presentation**Notes****Guidelines for Implementing NDS Security**

- Introduce the reasons for granting NDS rights.

Using Network Resources

- Explain that the network administrator will rarely need to grant a user rights in NDS.
- Discuss the two cases of granting a user NDS rights.

The guidelines presented here are identical to those presented in Section 8 of Course 560, NetWare 5 Administration. Review them as needed.

Managing NDS Objects and Properties

The defaults help you create, with very little effort, a secure environment that allows users to access needed network resources.

Only those users who need to manage NDS objects on a regular basis need additional rights. Most users do not need to create and delete objects or modify property values.

If you need to assign additional NDS rights, refer to the following table for guidelines and cautions.

Guideline	Explanation
1. Start with the default assignments.	Defaults give users access to the resources they need without giving them access to resources or information they do not need.
2. Avoid assigning rights through the All Properties option.	Avoiding All Properties protects private information about users and other resources on the network. When the All Properties option is used to assign rights, rights are granted to the Object Trustees (ACL) property. This could seriously compromise security in the NDS tree because this property controls the granting of rights to other objects.
3. Use Selected Properties to assign property rights.	Using Selected Properties allows you to assign more specific rights and helps you avoid future security problems.
4. Use caution when assigning the Write property right to the Object Trustees (ACL) property of any object.	This right effectively gives the trustee the ability to grant anyone, including himself or herself, all rights, including the Supervisor right. This is another reason to use extreme care when making rights assignments with All Properties.

Table 9-5: NDS Security Guidelines

Presentation**Notes****Managing NDS Objects and Properties**

- Introduce NDS security guidelines.

- Discuss the NDS security guidelines.

Security problems occur when network administrators begin to assign too many rights or particular rights without considering the implications.

Guideline	Explanation
<p>5. Use caution when granting rights to a server object.</p>	<p>Granting the Write property right to the Object Trustees (ACL) property of the server object gives the trustee Supervisor file system rights to all volumes linked to that particular server.</p> <p>Through inheritance, trustees can receive this right when given the Write right to All Properties of the server or the Supervisor right to the server.</p> <p>This object rights assignment should only be made after considering the implications of a network administrator having access to all files on all volumes linked to a particular server.</p>
<p>6. Granting the Supervisor object right implies granting the Supervisor right to all properties.</p>	<p>For some container administrators, you might want to grant all object rights except the Supervisor right, and then grant property rights through the Selected Properties option.</p>
<p>7. Use caution when filtering Supervisor rights with an IRF.</p>	<p>For example: A container administrator uses an IRF to filter the network administrator's rights to a particular branch of the NDS tree.</p> <p>If the network administrator (who has the Supervisor right to the container administrator's user object) deletes the container administrator's user object, that particular branch of the NDS tree can no longer be managed.</p>
<p>8. Revoking the Inheritable object right restricts a user's rights to objects in a container.</p>	<p>For example: A trustee assigned the Supervisor object right to a container who has the Inheritable object right revoked does not inherit the Supervisor object right to objects in the container.</p> <p>This is helpful when a user is assigned the duties of partition manager and should not have rights to objects in the container.</p>

Table 9-5: NDS Security Guidelines (continued)

Presentation**Notes****Managing NDS Objects and Properties** *(continued)*

- Continue presenting guidelines.

Additional Administrative Security

Because Admin users are granted Supervisor rights to [Root] by default, additional measures should be taken to protect the Admin users' access to objects in the NDS tree.

The following table includes guidelines that will provide additional security for the network.

Guideline	Explanation
1. Assign administrative user objects all object and property rights, not just Supervisor rights.	<p>For example: Assign administrative users the SBDR object rights and SCRWA property rights to a server object.</p> <p>This ensures the Admin user of being able to access the server object if Supervisor rights are blocked by an IRF placed on the server object.</p>
2. Rename the Admin user object.	<p>Renaming the Admin user object makes it more difficult for users to locate the Admin user object if they intend to usurp the rights granted to Admin.</p>
3. Avoid making other user objects security equivalent to administrative user objects.	<p>Security equivalence is risky because rights can be lost to security equivalent users when an administrative user object is deleted.</p> <p>For example: User MAVilla is granted SBCDRI object rights to a container as the container administrator, and user MJensen is given security equivalence to MAVilla as the backup container administrator.</p> <p>When MAVilla leaves the company, the Admin user deletes the MAVilla user object and MJensen loses rights to the container.</p>

Table 9-6: Additional Administrative Security Guidelines

Presentation

Notes

Additional Administrative Security

- Present the guidelines for providing additional network security.

When administrative roles are assigned to users other than Admin, security problems increase.

Guideline	Explanation
4. Change the administrative users' passwords regularly.	Configure the password parameters of the administrative user objects to require more frequent password changes. This will deter users from gaining access to the NDS tree with supervisory rights to objects if the administrative users' passwords become known.

Table 9-6: Additional Administrative Security Guidelines (*continued*)

Presentation

Notes

Additional Administrative Security

(continued)

- Continue presenting guidelines.

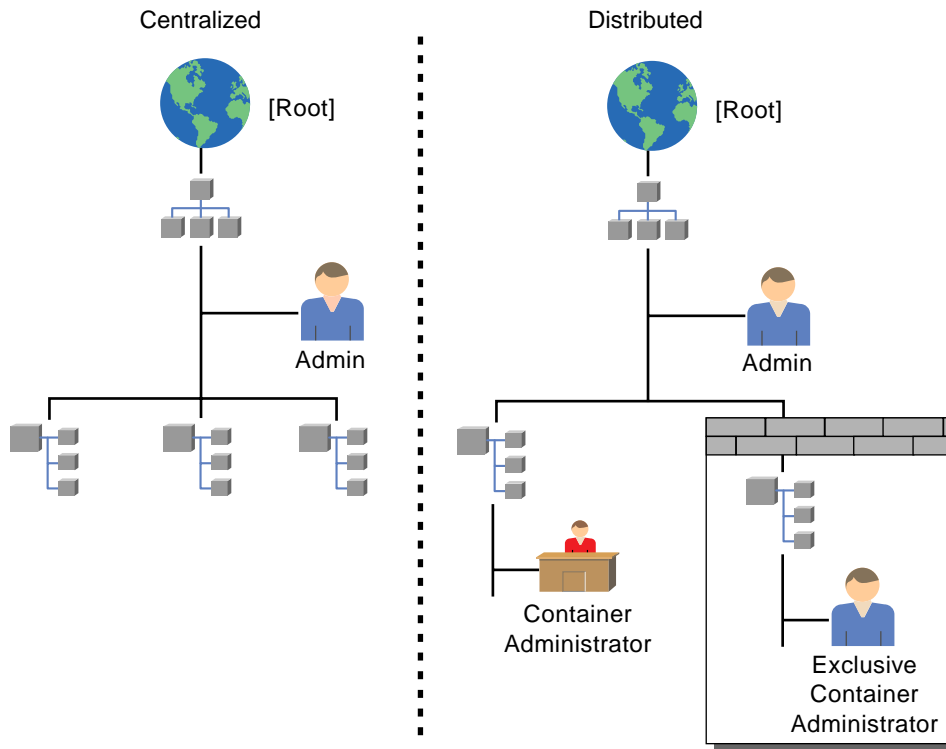


Figure 9-5: Centralized and Distributed Administration

Understanding Centralized and Distributed Administration

Because NetWare is flexible in its administration, you can design network security to meet your organization's specific needs.

NetWare allows for both centralized and distributed administration. A tree can have one administrator for the entire tree, administrators for branches of the tree, or a combination of one administrator over the entire tree and several container administrators managing branches.

Understanding Centralized and Distributed Administration



9-5 (Figure 9-5: Centralized and Distributed Administration)

- Discuss centralized and distributed administration.

NetWare allows for both centralized and distributed administration. It also allows for a combination of the two.

Certain tasks should be managed centrally; others can be distributed.

Compare NetWare 5 with NetWare 3.x. For example, in NetWare 3.x, the *Supervisor user* could share the responsibility with a *supervisor equivalent* or a *Workgroup Manager*.

These particular terms do not exist in NetWare 5, but users can be set up to perform similar tasks through the assignment of NDS rights.

Centralized Administration

In *centralized administration*, one or more users have rights to the entire NDS tree. This is the NetWare default.

The user object Admin is created during installation and has all rights to manage the NDS tree through an explicit assignment of the [SI] object rights to [Root]. User Admin consequently inherits rights to the rest of the tree unless an IRF is applied lower in the tree to block Admin's rights.

Centralized administration is appropriate for organizations with small NDS trees or organizations that want to retain a central administrator.

Some tasks should be centrally administered. These include the following:

- Renaming the NDS tree
- Creating the first levels of the NDS tree
- Managing partitioning and replication (discussed in Course 575, NDS Design and Implementation)
- Managing time synchronization (discussed in Course 575, NDS Design and Implementation)
- Assigning container administrators

Presentation**Notes****Centralized Administration**

- | | |
|---|---|
| <input type="checkbox"/> Define <i>centralized administration</i> . | Centralized administration means having one user or a central committee administer the entire NDS tree. This user or committee has unrestricted rights to administer all objects in the NDS tree. Any changes to the tree must be made by this user or committee. |
| <input type="checkbox"/> Describe the Admin user object. | The Admin user object is the first account created. It is automatically assigned all rights over the NDS tree so that other objects can be created.

This assignment is an explicit trustee assignment of the Supervisor and Inheritable object rights to the [Root] object. These rights are subsequently inherited throughout the tree. |
| <input type="checkbox"/> Suggest appropriate situations for centralized administration. | Centralized administration should generally be limited to organizations with small NDS trees or to departmental implementations of NetWare 5. |
| <input type="checkbox"/> Describe the tasks that should be administered centrally. | Some tasks should be centrally administered because of their impact on the entire NDS tree. These tasks are listed in the student manual. |

Distributed Administration

In *distributed administration*, designated users are given enough NDS rights to manage branches of the NDS tree. The user who is assigned the administrative tasks at the container level (a branch of the NDS tree) becomes the container administrator.

Distributed administration tends to allow administrators to respond to users' needs more quickly, especially in a large network, because control of the network does not reside with one person.

The following tasks can be distributed:

- Creating user accounts
- Managing user passwords
- Creating and configuring print services
- Backing up and restoring data
- Managing file system security
- Installing additional servers
- Creating workgroup managers

Setting Up the Container Administrator

Use the following guidelines to set up container administrators:

- If only one person will administer a container, then you only need to make the proper rights assignments to his or her user object.
- If more than one person will administer the container, then use an organizational role object as the container administrator.
- If you use the organizational role object, you should consider making an additional explicit Supervisor trustee assignment to a user object as a safety precaution. This ensures that container administration can continue if the organizational role object is deleted.
- For fault tolerance, always ensure that at least two trustees, such as an organizational role object (with multiple occupants) and a user object, are granted container administrator rights. With container administration responsibilities distributed to multiple trustees, network needs for the container can be addressed by a number of users rather than a few who might be unavailable.

Presentation**Notes****Distributed Administration**

- Define *distributed administration*.

- Describe the administrative tasks that can be distributed.

Distributed administration means that administrative tasks are divided among various administrators, enabling local administrators to better meet the needs of their users.

Setting Up the Container Administrator

- Identify the guidelines for creating container administrators.

- Discuss how to set up container administrators using user objects and organizational role objects.



Use extreme caution in using the Security Equal To property of a user object to create more than one container administrator (Novell does not recommend this approach).

If the user object is deleted and all other container administrator user objects are security equivalent to the deleted user object, all security equivalent objects will lose rights derived from the security equivalence.

In the case of the exclusive container administrator, this could mean being cut off from administering a branch or container of the NDS tree.

The organizational role object is an ideal object to use in setting up container administrators. The organizational role is designed to represent a particular position within an organization where the users who occupy the position might change, but the position's responsibilities do not change.

When a user object is made an occupant of an organizational role object, the organizational role object appears in the user object's Security Equal To property.

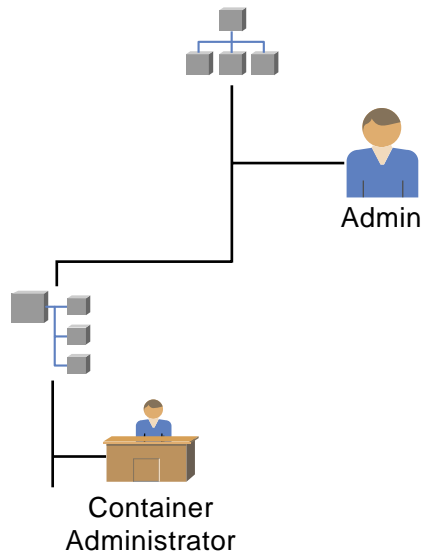


Figure 9-6: Setting Up the Container Administrator

Presentation**Notes****Setting Up the Container Administrator** *(continued)*

- Discuss the value of the organizational role object.



9-6 (Figure 9-6: Setting Up the Container Administrator)

To create container administrators using the organizational role object, do the following:

1. Create the organizational role object in the appropriate container.
2. Make the organizational role object a trustee of the container.
3. Assign the appropriate NDS rights to administer the container: [S I], [BCDRI], or all rights [SBCDRI].

The choice of NDS rights will vary based on the network administrator's plans to implement IRFs and the container administrator's need to manage the file system in addition to the NDS tree.



The Inheritable object right [I] must be assigned for the trustee assignment to be inherited to objects and containers below the container in the NDS tree. If the Inheritable object right is revoked, the assigned rights apply to only the container object.

Container objects are the only NDS objects which have the Inheritable object right [I]. All other NDS objects have the [SBCDR] object rights.

4. (Optional) Grant the organizational role object the Read property right to the Object Trustees (ACL) property.

Granting an object explicit Read property rights to the Object Trustees (ACL) property prevents that object from modifying the Object Trustees (ACL) property.

Many organizations use this procedure to prevent administrators from creating additional administrators or setting the container IRF, while still allowing the administrator to manage the objects in the container.



Always maintain at least one administrator who has either explicit or inherited rights to manage the Object Trustees (ACL) property of the container.

5. Assign any necessary rights to the file system that pertain to a container administrator.
6. Make the appropriate user objects occupants of the organizational role object.

Presentation**Notes****Setting Up the Container Administrator** *(continued)*

- Demonstrate how to set up container administrators using the organizational role object.

- Discuss the optional Step 4.

When performing this step, always maintain at least one administrator who has either explicit or inherited rights to manage the Object Trustees (ACL) property of the container.

Exclusive Container Administrator

Depending on the security requirements of your organization, you might want only one user or a small group of users to have administrative rights to a particular branch.

An *exclusive container administrator* is a container administrator who is the only one with Supervisor rights within a specified container. All rights to the exclusive container are then blocked from network administrators of parent containers.

For example, this assignment might be used in a government organization or in a department of a company with highly sensitive information. In this situation, you might need to cut off the rights inherited by the original Admin user.

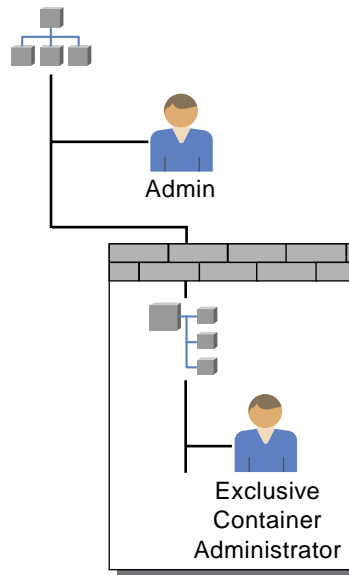


Figure 9-7: Exclusive Container Administrator



If you use the organizational role object to create exclusive container administrators, make an additional explicit trustee assignment to at least one of the container administrators' user objects. This will prevent a loss of administrative control of the container in the event the organizational role object is deleted.

Presentation**Notes****Exclusive Container Administrator**

9-7 (Figure 9-7: Exclusive Container Administrator)

- Define *exclusive container administrator*.

To create an exclusive container administrator, do the following:

1. Make the container administrator's user object a trustee of the container object with the following rights assignments:

[SBCDRI] object rights and [SCRWAI] property rights



Assign all rights, not just the Supervisor and Inheritable object rights. This will ensure that if the Supervisor right is filtered out by an IRF, total administration is still possible and the rights will flow down the NDS tree from the container.

2. Revoke inherited rights with an IRF at the workgroup container so that the original Admin does not inherit rights to the container.

Set the IRF to [B] object rights and [R] property rights.

Do not revoke the Browse object right; you might still want to allow other users to see that part of the tree.

3. Remove the original Admin user's trustee assignments to the container.
4. Ensure that the new container administrator has [S] object rights to himself or herself. Then remove any of the original Admin's trustee assignments to the new container administrator's user object. This prevents the original Admin from restricting the new administrator's rights.



Before using an IRF to revoke the [S] and [I] rights to the container object, you must make explicit trustee assignments that include the [S] and [I] rights for the container object.

If you attempt to revoke the [S] and [I] rights with the IRF without making any explicit trustee assignments that include the [S] and [I] rights, the utilities will prevent you from doing so.

However, you can still lose control over a branch of the tree if the only user with the [S] and [I] rights assigned to him or her through an explicit trustee assignment is deleted and the IRF for the container object blocks the [S] and [I] rights.

Presentation**Notes****Exclusive Container Administrator***(continued)*

Demonstrate how to set up an exclusive container administrator.

Some organizations will want to maintain a high level of security by centralizing NDS and file system management in the container. This is a typical government requirement.

Determining Suggested Administrative Roles and Rights Assignments

Administration in NetWare is extremely flexible; no fixed roles for administering the tree have been defined. However, the table below suggests some administrative roles that can be useful. The table also lists types of accounts you should create for these roles.

Role	Recommended Account	Functions
Enterprise NDS Administrator	Admin user object (default Admin user object)	Install the first server. Name the NDS tree. Create the upper levels of the NDS tree. Manage partitioning and replication. Manage time synchronization. Assign container administrators. Issue the initial auditor password. Upgrade servers, clients, and applications.
Container Administrator	Container administrator/ organizational role object (with individual user accounts as occupants)	Perform data backup and restoration. Create and configure print services. Write and maintain login scripts. Monitor file server performance. Track errors. Monitor disk space usage. Assign file system trustees. Upgrade server, client, and application software.

Table 9-7: NetWare 5 Administrative Roles

Determining Suggested Administrative Roles and Rights Assignments

- Explain the role of the enterprise NDS administrator.

- Remind the students to maintain separate accounts for the enterprise NDS administrator role and the user who fills that role.

- Explain the role of the container administrator.

The enterprise NDS administrator is responsible for those tasks that affect the entire NDS tree or NetWare network. These include tasks that affect parameters that are seldom changed and tasks that affect the entire network. These tasks are listed in Table 9-7.

The Admin user account is created for this purpose.

The user responsible for the enterprise NDS administrator role should have another account from which to perform his or her daily duties. This second account protects the network from inadvertent changes and increases network security.

Container administrators are used in distributed administration of the NDS tree. They perform day-to-day configuration tasks according to the needs of their groups.

The organizational role object is very convenient for assigning container administration rights. Users can be made administrators without their rights being reassigned.

Role	Recommended Account	Functions
Password Manager	Password Manager / organizational role object (with individual user accounts as occupants)	Reset user passwords to allow users to log in when they forget their passwords. Set password restrictions for user accounts. Set requirements for password length. Track user account intruders. Assign days between forced password changes. Manage user account reset time. Set password expiration date.
Print Server Operator (Queue-based)	PS Operator/ organizational role object (with individual user accounts as occupants)	Load the print server. Bring down the print server.
Print Queue Operator (Queue-based)	PQ Operator/ organizational role object (with individual user accounts as occupants)	Delete print jobs. Change the order of print jobs. Change queue status.
Print Job Operator (NDPS)	PJ Operator/ organizational role object (with individual user accounts as occupants)	View, delete, or modify print jobs. Change the order of print jobs. Copy or move print jobs.

Table 9-7: NetWare 5 Administrative Roles (continued)

Determining Suggested Administrative Roles and Rights Assignments *(continued)*

- | | |
|---|---|
| <ul style="list-style-type: none"><input type="checkbox"/> Explain the role of the password manager. | <p>The password manager acts as the administrator of user account passwords. The password manager primarily resets users' passwords when they forget their passwords.</p> <p>Other responsibilities can include setting up the requirements for passwords and regulating the timeframe for password expiration and changes. This role could be incorporated into the role of the container administrator.</p> <p>Note: This feature is available only with the version of NDS that ships with NetWare 5.</p> |
| <ul style="list-style-type: none"><input type="checkbox"/> Explain the role of the print server operator for queue-based printing. | <p>The print server operator is responsible for managing print services. This role is often incorporated into the role of the container administrator.</p> |
| <ul style="list-style-type: none"><input type="checkbox"/> Explain the role of the print queue operator for queue-based printing. | <p>The print queue operator can assist the print server operator or container administrator in the administration of print services by managing print jobs in a particular queue.</p> |
| <ul style="list-style-type: none"><input type="checkbox"/> Explain the role of the print job operator for NDPS printing environments. | <p>The print job operator can assist the container administrator in the administration of print jobs by managing print jobs through the printer objects in the NDS tree.</p> |

The Admin account should be used only for the enterprise NDS administration functions. The individual who assumes this role should have an individual user account to use regular network services.



Even if your organization does not want a central administrator, Novell recommends that you keep an account that has all rights to the [Root] for the sake of partitioning the Directory (discussed in Course 575, NDS Design and Implementation), performing NDS backups, and creating additional organization objects.

The container administrator can create additional administrators to help with creating and deleting user accounts. Creating a Password Manager role object enables the network administrator or container administrator of a large network to offload frequent password management tasks.



If you use IRFs to block the rights of the Admin user, ensure that each container has an administrator who can restore Admin's rights for the sake of partitioning the NDS tree.

Creating a Container Admin organizational role object makes this reassignment very easy because the task only involves adding Admin as a member of the organizational role object.

Presentation**Notes**

Determining Suggested Administrative Roles and Rights Assignments *(continued)*

- Emphasize the first note on the student page.

The network should always have an account with Supervisor rights to the [Root] and to the entire NDS tree.

Effective partitioning of the entire NDS tree and complete NDS backups are not possible if such an account does not exist.

If an administrator needs to merge partitions and such an account does not exist, temporary assignments for the purpose of partitioning must be made. (To merge partitions, a user needs the Supervisor object right to parent containers and servers on which the replicas will be stored.)

If students object to the existence of such a centralized account, suggest that multiple administrators hold the Admin account password or that an independent administrator hold that password.

- Explain the role of additional container administrators.

The container administrator can create additional container administrators for subcontainers created in his or her container, or add more user objects as members of the Container Admin organizational role object.

- Explain that a container administrator can serve as the Password Manager or other users can be assigned to the role.

The Password Manager role can be performed by a container administrator, or a separate organizational role object can be created for users who will perform password administration tasks.

Users assigned to the Password Manager organizational role are trustees over specific properties related to password management.

- Emphasize the second note on the student page.

Rights for Administrative Roles

You must assign the proper rights to the administrative roles you create for your network. Proper assignment of administrative rights will help you maintain control of network resources and minimize security breaches.

Assigning Rights

Following are the rights assignments required for the administrative roles described in the previous subsection.

Account	Assignment
Admin (user)	[S] and [I] object rights to [Root] at installation (by default)
Container Administrator (organizational role)	[SBCDRI] object rights to respective container
Password Manager (organizational role)	[RWI] property rights to the Password Management property of the container to be managed
Print Server Operator (organizational role)	Added to the Print Server Operator property of the respective print server
Print Queue Operator (organizational role)	Added to the Print Queue Operator property of the respective print queue
Print Job Operator (organizational role)	Added to the NDPS Job Configurations property of the respective NDPS printer

Table 9-8: Rights for Administrative Roles

Through the assignment above, the container administrator receives enough rights for NDS and file system management. The Supervisor object right is inherited for all objects, including server objects.

Users with the Supervisor right (or any object or property right that causes the Object Trustees (ACL) property to receive the [W] right) receive file system rights as well as NDS rights. This is the *only* instance in which NDS security affects file system security.

Presentation**Notes****Rights for Administrative Roles**

- Describe the importance of assigning the proper rights.

Assigning Rights

- Explain the rights assignments in Table 9-8.

The enterprise NDS administrator and container administrators receive their rights to the file system through inheritance of the Supervisor object right to the servers.

Considerations for Assigning Rights

Keep the following suggestions in mind when you assign rights:

- When you assign rights to a container administrator, consider assigning all rights, not just the [S] and [I] object rights. This ensures that the container administrator can still manage that branch if the [S] and [I] object rights are blocked by an IRF at a subsequent level.
- Because an IRF can ultimately restrict the Admin user, consider adding Admin as a trustee of the container with Supervisor object rights.

This helps prevent the loss of the Admin account's rights and ensures that the Admin user can perform all NDS functions, even if an IRF is in place.

- Decide whether this container administrator will manage the file system:
 - If yes, grant the container administrator the Supervisor right to the server object (if you assign the Supervisor object right at the container level, then the container administrator already has the Supervisor object right to all objects in the container).
 - If no, create an IRF that blocks the Supervisor right to the server object. Assign this responsibility and the appropriate file system rights to another user.



If the branch of the tree has not been created, consider giving the container administrator only the Create object right. The container administrator will then receive the [S] Supervisor and [I] Inheritable object rights to every object he or she creates.

Presentation**Notes****Considerations for Assigning Rights**

- Explain why *all* rights should be assigned to a container administrator.

- Explain why the Admin user object should be added to the container administrator's organizational role object.

- Discuss how to grant or block the container administrator's rights to manage the file system.

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator

In this exercise you grant the appropriate rights for a container administrator based on scenarios of centralized and distributed NDS management.

This exercise is divided into four parts:

- Part I: Setting Up Container Administration of an Organizational Unit
- Part II: Re-Assigning Rights to the File System
- Part III: Using an IRF to Block File System Management
- Part IV: Removing the IRF from the Server Object

Part I: Setting Up Container Administration of an Organizational Unit

In Part I, you use NetWare Administrator to determine how container administration has been set up for your container through the Manager organizational role object.

Next, you create a new user object and add it as an occupant of the organizational role. Then you create another new user and assign the user an explicit Supervisor object right to the organizational unit object.

1. Determine the rights that have been granted to the Manager organizational role object.
 - a. Click your **container**.
 - b. Select **Object | Trustees of this Object**.
 - c. Click the **Manager** organizational role object in the Trustees window.
 - d. What object rights does the Manager organizational role have?

Presentation**Notes**

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator

- Introduce the exercise.



:30

- Have the students complete the exercise.
- Review the answer to the exercise.

Part I Answers:

- 1d. Supervisor and Inheritable object rights.

- e. What advantage does the Inheritable object right give to occupants of the organizational role?
 - f. Since the server object FSx is in your organizational unit container object, what object rights does the Manager organizational role object have to the server object FSx? Why does the object receive these rights?
 - g. Does the answer to the previous question have any implications for file system security? If so, what are the implications?
-
- 2. Create a new user object named **PReynolds**. Use **Reynolds** as the last name.
 - 3. Make the PReynolds user object an occupant of the Manager organizational role object.
 - a. Right-click the **Manager** organizational role object.
 - b. Click **Details**.
 - c. Click the **Add Occupant** button to the right of the Occupant field.
 - d. Click **Add**.
 - e. Double-click the **PReynolds** user object.
 - f. To close the Occupant window, click **OK**.
 - g. To close the Organizational Role window, click **OK**.
 - 4. Create a new user object named **AMunro**. Use **Munro** as the last name.

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator (continued)

- Continue the exercise.

Part I Answers (continued):

- 1e. The users who are occupants of the organizational role object will have Supervisor object rights to all objects in the container and subcontainers (if any).
- 1f. Supervisor object right.
The Supervisor object right assigned to the organizational role at the organizational unit object flows down to the server object because the server object is in the organizational unit and the user has been granted the Inheritable object right. This right allows the user to inherit rights to objects in the container.
- 1g. Yes. The Supervisor object right to the server object gives the administrator Supervisor rights to the file system on all volumes attached to that server object.

5. Add the AMunro user object to the trustee list of your container.
 - a. Right-click your **container**.
 - b. Click **Trustees of this Object**.
 - c. Click **Add Trustee**.
 - d. In the Browse context field, double-click your **container object**.
 - e. In the Available objects field, double-click the **AMunro** user object.
6. Give the AMunro user object [SBCDRI] object rights and [SCRWAI] property rights to All Properties. This ensures that the container has at least one administrator with an explicit rights assignment.



Granting AMunro the Inheritable object and property right to a container grants the user the same object and property rights to any *subcontainers* in the NDS tree.

7. To save your changes and close the Trustees window, click **OK**.
8. Check the effective rights of the PReynolds occupant of the Manager organizational role and AMunro in the PUBLIC directory. These rights indicate if either user object has the Supervisor object right to the server object.
 - a. To see the directories in the file system, double-click the **FSx_SYS** volume object in your container.
 - b. Right-click the **PUBLIC** directory.
 - c. Click **Details**.
 - d. Click **Trustees of this Directory**.
 - e. Click **Effective Rights**.
 - f. Click the **Browse** button to the right of the Trustee field.
 - g. In the Available Objects field, click the **PReynolds** user object.
 - h. Click **OK**.
 - i. Repeat Steps 8f through 8h for AMunro.
 - j. What rights do PReynolds and AMunro have in this directory?
- k. After finding the effective rights, exit the windows relating to the PUBLIC directory.

Presentation**Notes****Hands-On Exercise 9-2:
Making Rights Assignments
for a Container Administrator**
(continued)

- Review answers with the students.

Part I Answers *(continued)*:

8j. All rights including Supervisor.

Part II: Reassigning Rights to the File System

In the following steps, you use a secondary trustee assignment and an IRF to prevent Manager from inheriting Supervisor rights to the file system. In this case, you prevent the flow of the Supervisor object right to the server object.

1. Make the Manager organizational role object a trustee of the server object.
2. Grant the Manager organizational role object Compare and Read [CR] property rights to the Object Trustees (ACL) property of the server object.
 - a. With the Manager organizational role object highlighted in the Trustees list, click **Selected Properties**.
 - b. Scroll through the list of selected properties to locate the Object Trustees (ACL) property.
 - c. Click the **Object Trustees (ACL)** property.
 - d. Mark the boxes for the **Compare** and **Read** properties.
 - e. Click **OK**.
3. What did this explicit rights assignment do to the container administrators' (members of Manager) rights in the file system?
4. Check the effective rights to your server object for PReynolds and AMunro.
 - a. Right-click your **server** object; then click **Trustees of this Object**.
 - b. Click **Effective Rights**.
 - c. Click the **Browse** button to the right of the Object Name field.
 - d. In the Available Objects field, click the **PReynolds** user object.
 - e. Click **OK**.
 - f. Repeat Steps 4d through 4f for AMunro.

What rights to the server object do PReynolds and AMunro have?

Why are their rights different?
 - g. Close the Effective Rights window.

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator (continued)

- Continue reviewing answers with the students.

Part II Answers (continued):

3. An explicit rights assignment of Compare and Read property rights [CR] to the Object Trustees (ACL) property removes the Supervisor file system right from the volumes connected to the server.

The explicit rights assignment also takes away the ability of the user object to create trustees for the server object or to assign Supervisor rights to himself or herself.

4. The PReynolds user has the Browse object right and AMunro has all object rights [SBRD].

PReynolds' rights come from the Manager object, which was made a trustee in Step 2. AMunro's rights come from the explicit assignment made in Part I, Step 6.

Note: The Inheritable object right does not appear in the list of object rights for the server object because only container objects have the Inheritable object right.

Part III: Using an IRF to Block File System Management

In the following steps, you prevent users from inheriting rights to the file system by setting an IRF on the server object. To see the effect of setting the IRF, you will first remove the Manager organizational role trustee assignment, and then set the IRF.

1. Remove the Manager organizational role trustee assignment.
 - a. With the Trustees window still open, click the **Manager** organizational role object in the Trustees list.
 - b. Click **Delete Trustee**.
 - c. In the dialog window that states "Delete trustee assignment," click **Yes**.
2. Place an IRF to block the flow of the Supervisor object right to the server object.
 - a. Click **Inherited Rights Filter**.
 - b. Unmark the box next to the Supervisor object right.



A message should appear stating, "You cannot filter the Supervisor right because no user has explicit Supervisor object rights to this object."

Without this warning, you could eliminate users who can manage the server object in the NDS tree.

- c. To close the dialog, click **OK**.
 - d. To close the IRF window, click **OK**.
 - e. To close the Trustees window and return to NetWare Administrator, click **OK**.
3. Make the Admin user object (that you logged in as) a trustee of the server object and grant the Admin user the [SBDR] object rights.

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator

(continued)

- Tell students they are giving Admin Supervisor object rights to the server in Step 3 so that at least one user can manage the server.

4. To prevent the Supervisor object right from flowing down to the server object, place an IRF at the server object.
 - a. In your container, click the **FSx** server object.
 - b. Select **Object | Trustees of this Object**.
 - c. Click **Inherited Rights Filter**.
 - d. Unmark the box next to the Supervisor object right.

A shorter arrow with a line under it will appear next to the box, indicating that the right is being blocked.
 - e. To close the window and save changes, click **OK**.
 - f. To close the Trustees window and apply the IRF, click **OK**.
5. Check PReynolds and AMunro's effective rights to your server object. What object rights does each user have to the server object?

Will this affect PReynolds' and AMunro's rights to the file system?

Part IV: Removing the IRF from the Server Object

In the following steps, you restore the container administrators' rights to the file system by removing the server object IRF.

1. To allow Supervisor rights to the file system, reset the blocked Supervisor right in the IRF placed on the server object.
 - a. Click **Inherited Rights Filter**.
 - b. Mark the box next to the Supervisor object right.

The short arrow with the line under it next to the box changes to a longer arrow without a line under it, indicating that the right is allowed.
 - c. To close the window and save changes, click **OK** twice.
2. Check PReynolds and AMunro's effective rights to your server object. What object rights does each user have to the server object?

How does this affect their rights to the file system?

(End of Exercise)

Hands-On Exercise 9-2: Making Rights Assignments for a Container Administrator (continued)

- Continue reviewing answers with the students.

Part III Answers (continued):

5. Neither user has the Supervisor object right. The PReynolds user has Browse object rights and AMunro has all object rights except Supervisor [BDR].

Yes. This will affect both users' file system rights. PReynolds and AMunro will no longer have Supervisor rights in the file system.

Part IV Answers:

2. All rights including Supervisor.
Both users will have all rights to the files and directories in the volumes on the server.

Summary

In this section, you learned how to plan additional NDS security needs to supplement the default rights assignments given to objects as you create those objects in the NDS tree.

You also learned how to create user objects and organizational role objects as container administrators, and implement NDS security to distribute network administration.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. List the default rights assigned when creating a Directory and objects.
2. Explain the guidelines and considerations for implementing NDS security in a multicontext environment.
3. Describe the differences between centralized and distributed NDS management.
4. Determine the administrative roles needed in your organization and identify the NDS objects and rights assignments that support those roles.

Notes

SECTION 10 Maintaining Novell Directory Services

Duration 02:30

Preparation

Complete the following:

- Prepare to demonstrate NDS troubleshooting procedures.
- Prepare to create an NDS error for Exercise 10-1. See instructor notes for detailed instructions.

SECTION 10

Maintaining Novell Directory Services

In this section, you learn how to maintain a consistent and stable NDS database by performing preventive maintenance, identifying inconsistencies in the database, finding information on how to correct these inconsistencies, and completing NDS database repairs.

You also learn how to prepare the server for downtime and how to recover from hardware failures, which can adversely affect NDS.

Objectives

Upon completing this section, you should be able to

1. Explain NDS replication.
2. Explain preventive maintenance procedures for the NDS database.
3. Troubleshoot NDS database inconsistencies.
4. Explain NDS database repair procedures that can be accomplished in NDS Manager, including creating a new master replica, repairing a local database, sending and receiving updates, repairing network addresses, and repairing server IDs.
5. Explain the procedure for recovering NDS from a failed server or volume.

Presentation

Notes

Maintaining Novell Directory Services

- Introduce the section.

Objectives

- Present the section objectives.

Understanding Replication and Synchronization

To understand replication and synchronization, you must first understand some concepts regarding the NDS database. In this subsection, we discuss the following concepts:

- The Directory
- Partitions
- Replicas
- Changing the Directory

The Directory

The Directory has the following characteristics:

- It is a database that contains data on all objects in the NDS tree, including object names, rights, and property values.
- NDS uses the Directory for access control (checking to see if an object has rights to perform an action).
- NDS uses the Directory for authentication.
- Except for the server and volume objects, the Directory does *not* contain information about the file system.

Partitions

Partitioning is the process of dividing the Directory. Because a large Directory can contain information on thousands of objects, partitioning allows the Directory to be distributed among multiple servers. Partitions are managed by the network administrator.

Replicas

Replicas contain the actual Directory data for objects within the boundaries of a partition. Replicas are stored on NetWare 5 servers around the network and are managed by the network administrator.

Presentation**Notes****Understanding Replication and Synchronization**

- Briefly outline this subsection.

Students need a basic understanding of the Directory and how changes are made.

The Directory

- Discuss the characteristics of the Directory.

Partitions

- Define *partition*.

Partitions are the logical divisions of the Directory which enable the network administrator to divide the database among servers.

Replicas

- Explain the purpose of replicas.

NDS uses four types of replicas. These replicas, listed below, have different functions in the Directory:

- Master replicas
- Read/write replicas
- Read-only replicas
- Subordinate references

Master Replicas

A *master replica* is a complete copy of the partition. Each partition can have only one master replica.

A master replica can perform original requests for partition and object changes.

Read/Write Replicas

A *read/write replica* is a complete copy of the partition. You can have multiple read/write replicas of a partition.

A read/write replica can fill original requests for object changes, but passes all partition change requests to the master replica.

Read-Only Replicas

A *read-only replica* is a complete copy of the partition. You can have multiple read-only replicas of a partition.

A read-only replica cannot handle original requests for changes to NDS. It forwards all original change requests to master or read/write replicas.

Subordinate References

Subordinate references are not complete copies of the partition. They do not contain object data; they point to the replicas that do contain the data.



More information on the Directory, partitions, and replicas is found in Course 575, NDS Design and Implementation.

Presentation**Notes****Master Replicas**

- Explain the importance of the master replica.

The master replica is the only replica from which partition management can be done.

Read/Write Replicas

- Explain the purpose of a read/write replica.

Read-Only Replicas

- Explain the purpose of a read-only replica.

Subordinate References

- Explain the purpose of a subordinate reference.

Changing the Directory

Because NDS is a distributed, replicated database, NetWare 5 servers must continuously share information and synchronize changes in the database.

The NDS database is loosely consistent and requires time to be replicated and synchronized when major network changes occur.

The amount of time required for a change to be replicated and synchronized depends on the type of change, the size of the partition, and the number of servers the partition is replicated on.

You should not assume that delays in replication and synchronization of changes indicate problems in the database.

Simple Changes

A change (such as changing the phone number) that affects only a single user object takes relatively little time to be replicated and synchronized. The change is sent only to the servers that contain a replica that includes this user object.

Creating a partition takes very little time as well. When you create a partition, the NDS tree uses partition attributes to “draw” the new partition boundary. The information needed is already replicated around the network.

Complex Changes

More complex changes take more time. For example, joining two partitions that exist on two different sets of servers will take time. Each server that has a piece of the original partitions will receive a replica of each partition before the join is performed.

In this example, NDS performs the following tasks:

1. NDS automatically determines where all the replicas of each partition exist.
2. NDS forces the servers to replicate the data of both partitions to the servers.
3. NDS completes the join; the servers have the composite information of both partitions.

Presentation**Notes****Changing the Directory**

- Discuss how changes are made in NDS.

Some changes performed in NDS take a few minutes to completely replicate across the network.



- Show the Object Changes animation.

Make sure the students understand that a time lag or an occasional unknown object in the NDS tree does not indicate that a replica is corrupted.

- Point out that a change occurs first on one replica.

This animation uses a simple model. In a more complex environment, each server might hold replicas from several partitions, and each server would synchronize on a regular basis, even if changes had not occurred.

The change is then sent to the other replicas through the synchronization process.

Simple Changes

- Define *simple changes*.

Simple changes are those that occur immediately because the information already exists on the necessary servers.

Complex Changes

- Define *complex changes*.

Complex changes involve NDS forcing the servers to replicate some portion of the Directory (more than a single property or object).

NDS Maintenance Utilities

The main tools for monitoring and maintaining the NDS database are

- NDS Manager (Windows utility)
- DSREPAIR (server NLM)
- SET NDS TRACE (server command)



This class focuses on maintenance tasks performed from NDS Manager.

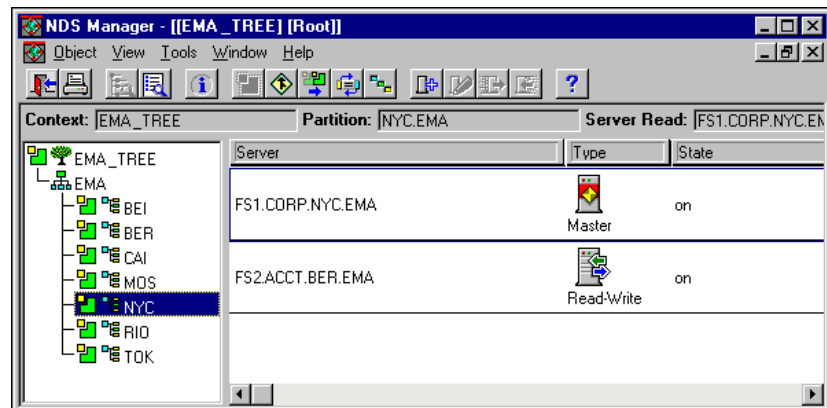


Figure 10-1: NDS Manager

Presentation**Notes****NDS Maintenance Utilities**

10-1 (Figure 10-1: NDS Manager)



Introduce and briefly demonstrate DSREPAIR and SET NDS TRACE TO SCREEN = ON.

- Point out that this course focuses on tasks performed within NDS Manager.

SET NDS TRACE is the documented version of SET DSTRACE, although SET DSTRACE and its command options are still functional.

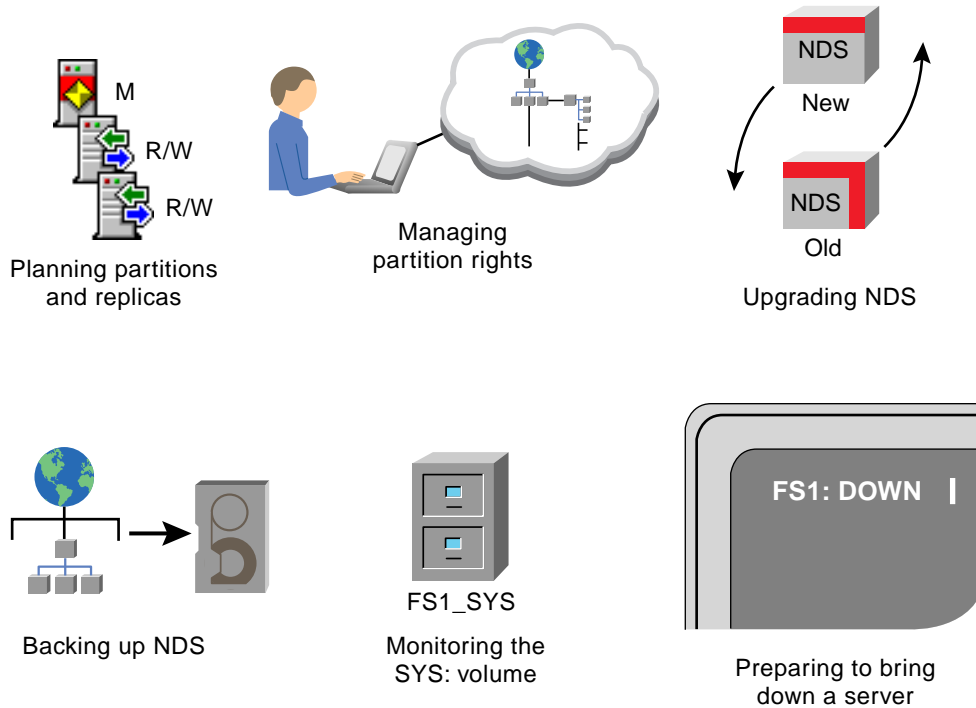


Figure 10-2: Preventive Maintenance Tasks

Understanding Preventive Maintenance

The following subsections discuss preventive maintenance techniques you can use to help prevent NDS database inconsistencies.

Planning Replica Placement Carefully

You should have enough replicas of a partition to facilitate user access to network resources. You should always have three replicas of every partition in the tree to ensure partition fault tolerance.

At the same time, too many replicas of a partition can cause excessive NDS synchronization traffic on the network and increase the risk of database inconsistencies.



For details, see Course 575, NDS Design and Implementation.

Presentation**Notes****Understanding Preventive Maintenance**

- Introduce this subsection.



10-2 (Figure 10-2: Preventive Maintenance Tasks)

- Remind the students that NDS is loosely consistent.

This subsection discusses preventive maintenance techniques that can help avoid problems in NDS.

NDS inconsistency is defined as dropped links to objects, unknown objects, and general unavailability of a particular replica. Following the preventative guidelines in this section will minimize inconsistency problems.

Tell the students that they might never experience NDS inconsistencies. Do not make the students unnecessarily concerned about inconsistencies in NDS.

Planning Replica Placement Carefully

- Explain how the defaults help provide fault tolerance for the Directory.

Accepting the defaults and the guidelines discussed in this course will provide fault tolerance for the students' Directories.

Regulating Partition Management Rights

Partition changes affect the database much more than simple, nonpartition-related changes. You should use caution in performing partition management procedures.

Limit Who Can Manage Partitions

One method of regulating partition actions is to limit who can perform these kinds of tasks.

If you want container administrators to manage partitions, grant them the Supervisor object right to the partition root object. Grant fewer NDS administrative rights to container administrators you do not want to manage partitions.

For example, granting the container administrator Create, Delete, Rename, and Browse object rights would allow the container administrator to manage a container, but not the partition.

Manage Partitions from One Workstation

You should create or merge partitions from only one workstation at a time. This helps you better regulate partition actions.

In NetWare 5, a partition locks while you change its boundaries. Therefore, two simultaneous operations are impossible.



When a partition is being moved, merged, or created, the affected partition can remain locked for partition operations from a few minutes up to several hours. However, users can still use the partition to access objects.

Presentation

Notes

Regulating Partition Management Rights

- Discuss which administrative rights allow partition management rights.

- Tell the students to perform partition operations at a single workstation.

- Point out the note on the student page.

Partitions lock as they are created or merged so that only one operation can be performed at one time.

Once the network administrator has allocated the administration of the NDS tree, he or she should try to centralize management of partitions, assigning one or two people to each unit of administration. This helps the network administrator track which units are managed by whom.

Backing Up the Directory

Backing up the file system does not back up the NDS tree.

You should back up the Directory according to the backup strategy you have chosen and keep the backup as a second protection for restoring the Directory. You should also back up the Directory before you create or merge a partition.

You should restore a directory backup only when all other options for restoring the information, such as resolving synchronization errors or recreating the replica from a valid replica, have failed.

If synchronization errors do occur, follow the troubleshooting techniques described later in this section and restore the backup when recommended by the documented help.



For more information, see Section 6, "Backing Up Servers and Workstations."

Presentation**Notes****Backing Up the Directory**

- ❑ Remind the students to back up the Directory on a regular basis.

Students will probably never need to restore the Directory from a backup because they will have replicas that protect the Directory.

However, we recommend that the network administrator always make a backup as protection against a catastrophic event. Backing up NDS is particularly important in small offices where a second server might not be available to hold replicas of a partition.

Note: Partition boundaries are not included in a Directory backup.

Maintaining a Standard NDS Version

NDS Manager is the NetWare utility used to manage and maintain NDS partitions and replicas.

NDS Manager has the ability to remotely update the NDS NLM (DS.NLM) on servers in the same NDS tree.

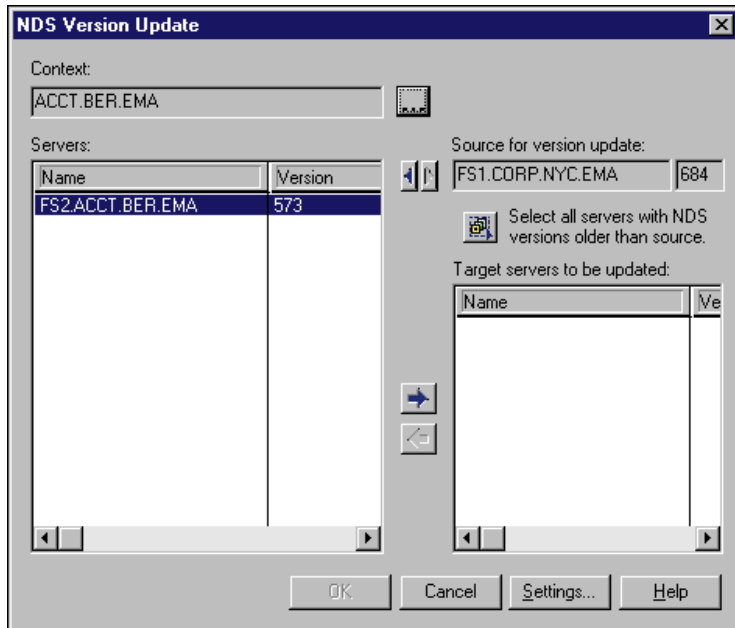


Figure 10-3: NDS Version Update Window

You should update the version of NDS on servers in your NDS tree whenever you receive an updated DS.NLM. Updated versions of the DS.NLM are periodically available on the Novell Support Connection Web page (<http://support.novell.com>).

Each update of NDS fixes problems and increases functionality. When a new version of NDS is released, the new features in NDS are not available unless all servers in a partition's replica list are running the new version.



Version update does not support updates across operating system releases. In other words, this feature will not update a NetWare 4.11 server's version of NDS to a NetWare 5 version of NDS.

Presentation**Notes****Maintaining a Standard NDS Version**

- Describe the importance of maintaining a single version of NDS.



10-3 (Figure 10-3: NDS Version Update Window)

- Point out the note on the student page.

Viewing NDS Version Numbers on Multiple Servers

You can use NDS Manager to view the version of NDS for all servers in a container:

1. Navigate the NDS tree and highlight the container containing the servers you want to view.
2. In the Object menu, click **NDS Version**.
3. In NDS Version, click **View**.



By default, NDS Manager will search only the current container. To search the entire subtree, select **Object | Preferences | NDS Update Options**; then click **Entire Subtree**.

Updating NDS Versions

You can use NDS Manager to update servers to a single version of NDS.

1. If known, locate and highlight the **server** with the version of NDS you want to distribute. This is called the *source server*.

If the source server is not known, locate and highlight any server you want to receive the update. This is called the *target server*.

2. In the Object menu, click **NDS Version**.
3. In the NDS Version menu, click **Update**.

A window appears, displaying the status of the search. When the search is completed, a window might appear informing you that servers listed in grey cannot be upgraded.

4. To close the window, click **OK**.

The NDS Version Update window appears and displays servers in the context of the server you selected in Step 1.

Presentation**Notes****Viewing NDS Version Numbers on Multiple Servers**

Demonstrate how to view the NDS version number on multiple servers.

Updating NDS Versions

Demonstrate how to update the NDS version on a server.

- Point out server names in grey.

Servers displayed in grey cannot be upgraded. They have a version of NDS that is newer than the source version, from a different release of NetWare, or an unknown version.

5. If your context is incorrect, use the **Browse** button located to the right of the Context field to change to the appropriate context.
If you want servers from multiple contexts, select the appropriate parent container.



By default, NDS Manager will search only the current container. To search the entire subtree, select **Object | Preferences | NDS Update Options**; then click **Entire Subtree**.

6. In the **Source for version update** field, place the source server with the version of NDS you want to distribute.



Ignore Step 6 if the source server listed already contains the version of NDS you want to distribute.

Normally, the most current version of NDS is the version you want to distribute; it is represented by the largest version number.

- a. To remove the current source server, click the left arrow to the left of the **Source for version update** field.
 - b. In the Server list, double-click the **new source server**.
7. Highlight all the servers you want to update.

Servers displayed in grey cannot be upgraded. They contain newer versions of NDS, versions of NDS from a previous NetWare OS, or unknown versions.

Hint: Use the **Select all servers with NDS version older than source** button to select all servers listed, use the Shift key to select a contiguous block of server names, or use the Control key to select noncontiguous server names.

8. To move the servers into the **Target servers to be updated** field, click the right arrow between the Servers list and the Target list.
9. To activate the update, click **OK**.

Updating NDS Versions *(continued)*



Continue demonstrating how to update the NDS version on a server.

Preventing the SYS Volume from Running Out of Space

The SYS volume contains the NDS database in a hidden directory. This directory is not viewable, even with the NDIR command. The NDS database is protected by the Transaction Tracking System™ (TTS™).

TTS automatically deletes any incomplete TTS transactions to prevent inconsistencies in the database and restores the database to a complete version. If the SYS volume becomes full, TTS shuts down and the Directory closes its files to any changes.

To avoid running out of disk space on the SYS volume, use the following guidelines:

- Set minimum space requirements so that you will receive a warning if the SYS volume is almost out of space. By default, this warning is set to occur when the volume has 256 blocks left.
- Store print queues on a volume other than the SYS volume.
- Store user files or other files on a volume other than the SYS volume.
- Do not add replicas to servers that are low on disk space.
- If you have CD-ROM drives attached to the server, they often create large index files on the SYS volume. Make sure the volume is large enough to accommodate these index files.

The NetWare CDROM.NLM creates a directory called SYS:CDROM\$\$\$.ROM. When a CD is mounted as a volume on the server, NetWare either copies a pre-built index into, or creates an index for, this directory.

This process ensures a fast mount the next time this CD is mounted. These files average 8 MB in size.

- Do not disable TTS on servers that contain active replicas. If TTS shuts down, unpredictable and possibly damaging results might occur to the replicas on that server.

Presentation**Notes****Preventing the SYS Volume from Running Out of Space**

- Emphasize the importance of maintaining adequate disk space for the SYS volume.

- Provide the syntax for setting the low volume warning threshold.

Running out of disk space on the SYS volume causes TTS to shut down. This can cause unpredictable problems with, and damage to, replicas that are stored on that server.

SET VOLUME LOW WARNING THRESHOLD=0 to 1000000.

Preparing a Server for Downtime

The NDS database is designed to withstand periods during which servers that store replicas are unavailable. The Directory on the unavailable server automatically synchronizes itself when it becomes available again.

If you must bring down a server for more than a few days, consider taking the actions listed in Table 10-1.

Event	Action
Bringing down a server that contains the only replica of a partition.	Use NDS Manager to move the replica to another server first.
Bringing down a server or WAN link permanently.	Back up NDS; then use NWCONFIG.NLM to remove NDS from the server.
Bringing down a server or WAN link temporarily to replace the hard disk that contains the SYS volume.	
Bringing down a server or WAN link temporarily if any of the following are required: <ul style="list-style-type: none"> ■ Partition operations ■ Large numbers of changes, additions, or deletions of replicas ■ Relocation of the server to another site 	Remove replicas from the server before bringing down the server or disconnecting WAN links. (Bindery services are lost when replicas are removed.)

Table 10-1: Managing NDS During Planned Shutdowns

Presentation**Notes****Preparing a Server for Downtime**

- Explain how to handle regularly scheduled downtime.

If the server is down for more than a few days, the network administrator should delete the server from the tree and reinstall NDS on that server when the server is restarted.

Servers that have changes to report to the unavailable server have a backoff algorithm that tells them not to send changes because the server is not connected.

The disconnected server also has a routine that periodically requests changes if no changes have been received for a specified period of time. The downed server relies on this algorithm to synchronize its database once it comes back online.

If a server holding a replica is down or unavailable, partition operations will not be completed until the server is brought up again.

Troubleshooting NDS Inconsistencies

The NDS database is inconsistent when replicas of a partition cannot be synchronized and the shared information becomes dissimilar or corrupted.

The NDS database is a loosely consistent database and it needs time to replicate and synchronize changes. However, persistent problems might indicate that replicas are out of synchronization.

To troubleshoot NDS database inconsistencies, do the following:

1. Identify the inconsistency.
2. Use documented help to create a strategy for resolving the inconsistency.
3. Perform corrective actions.

Identifying NDS Database Inconsistencies

NDS database inconsistencies show up in three forms:

- Client symptoms
- Unknown objects in NDS
- NDS error messages

Client Symptoms

The following client problems might indicate that replicas are out of synchronization:

- The client prompts for a password when none exists for the user account.
- Client login takes dramatically more time than usual.
- Modifications to the Directory seem to have disappeared.
- NDS rights assigned previously seem to have disappeared.
- Client performance is inconsistent; errors cannot always be duplicated.

If these symptoms occur, check for synchronization errors as described on the next pages.

Presentation**Notes****Troubleshooting NDS Inconsistencies**

- Describe NDS inconsistencies.

- Point out that servers and their replicas might be unsynchronized for a short period of time without experiencing any consequences.

- Review the basic troubleshooting steps listed on the student page.

Identifying NDS Database Inconsistencies

- Introduce how NDS database inconsistencies can be detected.

Client Symptoms

- Mention the client symptoms of replicas that are not synchronized.

At times, replicas will not be synchronized with the rest of the network. This usually happens as a result of a partition operation such as merging or creation.

The replicas will eventually resynchronize. Even if changes occurred during the out-of-sync condition, data is not lost or corrupted. The changes are applied to the proper replicas without problem.

The symptoms are listed on the student page. These types of problems are not serious. They usually correct themselves after a few minutes.

If the symptoms persist, the network administrator should check for synchronization errors.

Unknown Object Types

The presence of unknown objects in the NDS tree can indicate a problem with synchronization.

Sometimes objects become unknown during Merge Partition and Create Partition operations. This is normal because a partition root is changing. The objects will return to a known state when the operation is completed.

If these symptoms occur, check for synchronization errors as described earlier.

NDS Error Messages

The NetWare server produces NDS synchronization error messages whenever the server is unable to complete the synchronization process with another server. To view these messages, you can:

- Check for synchronization errors with SET
- Check partition synchronization in NDS Manager
- Check partition continuity in NDS Manager

Check for Synchronization Errors with SET. You can use a SET parameter to watch the synchronization of the Directory database.

Enter SET NDS TRACE TO SCREEN=ON at the server console. This command brings up another screen on which you can watch the replicas synchronize with each other.

The following message indicates an inability between two servers to synchronize replicas:

**SYNC: failed to communicate with server <CN=FS2> ERROR
-625**

SYNC: End sync of partition <name>. All processed = NO



For more information, see “Novell Directory Services Parameters” under “SET” in *Utilities Reference*.

Presentation**Notes****Unknown Object Types**

- Discuss unknown objects.

The unknown object will appear when the network administrator creates or merges a partition. This object indicates that the Directory is holding a place for the information contained in that object and that, during the operation, the object is not displayed properly.

Note: The appearance of the unknown object does not mean that the data has been lost or that the Directory has been corrupted in any way. For example, when the schema has been extended and a snap-in has not been applied to NetWare Administrator, the new objects appear as unknown objects. These objects are represented by a white square containing a question mark.

Yellow circles containing a question mark represent corrupted objects.

Volume objects also become unknown objects when the server object has been deleted. They should be deleted.

NDS Error Messages

- Discuss NDS error messages.



Briefly demonstrate SET NDS TRACE.

Enter SET NDS TRACE TO SCREEN = ON at the FS1 server console and discuss synchronization processes that occur.

Note: SET NDS TRACE is the documented version of SET DSTRACE, although SET DSTRACE is still functional.

Check Partition Synchronization in NDS Manager. To view partition synchronization information in NDS Manager, do the following:

1. Locate and highlight the partition root object in NDS Manager.
2. In the object menu, click **Check Synchronization**.

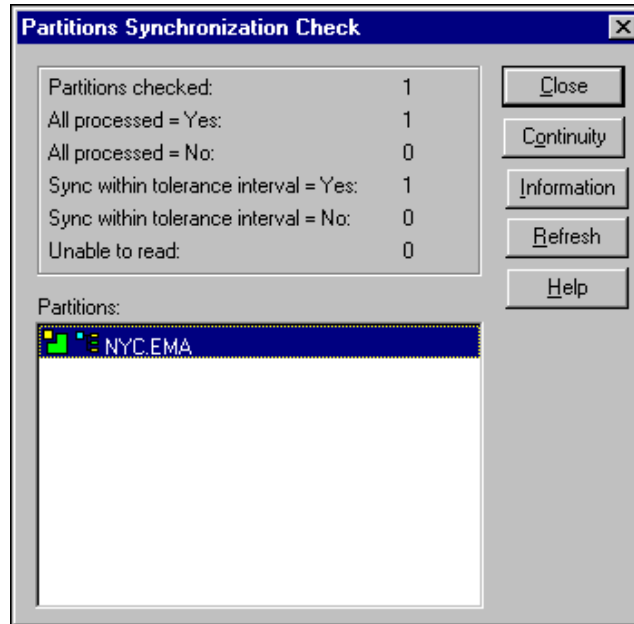


Figure 10-4: Partition Synchronization Window in NDS Manager

3. To read the partition status for the selected partition only, click **OK**.
4. To continue with the operation after preconditions have been met, click **Yes**.

A synchronization problem is indicated when the All processed = No line has a value greater than 0.



This action might provide incomplete information because it only checks for synchronization errors on the first server in the replica list that responds to the request. Synchronization errors might be occurring on other servers in the replica list.

To check for synchronization errors among all servers in a replica list, check the partition continuity.

Presentation**Notes****NDS Error Messages** *(continued)*

10-4 (Figure 10-4: Partition Synchronization Window in NDS Manager)



Demonstrate the Check Synchronization option in NDS Manager.



Point out the limitation of Check Synchronization.

Additionally, Check Synchronization does not work on versions of NDS earlier than version 489.

Check Synchronization is most useful as a quick check of the health of a large number of partitions, if not the entire tree. To do this, complete the following steps:

1. In the Tree view, navigate to a partition root container containing a large number of child partitions. (The [Root] partition contains all child partitions.)
2. Change to the **Partitions and Servers** view.
3. Select a partition in the Partitions window.
4. From the Object menu, Click **Check Synchronization**.
5. Click the **All Partitions contained in the partition list** button.
6. To initiate the Check Partition process, click **OK**.
7. To continue with the operation after preconditions have been met, click **OK**.

Check Partition Continuity in NDS Manager. To check for synchronization errors on all servers in a replica list, do the following:

1. Locate and select the *partition root object* in NDS Manager.
2. In the Object menu, click **Partition Continuity**.

A replica icon with an exclamation point indicates a server with synchronization errors.

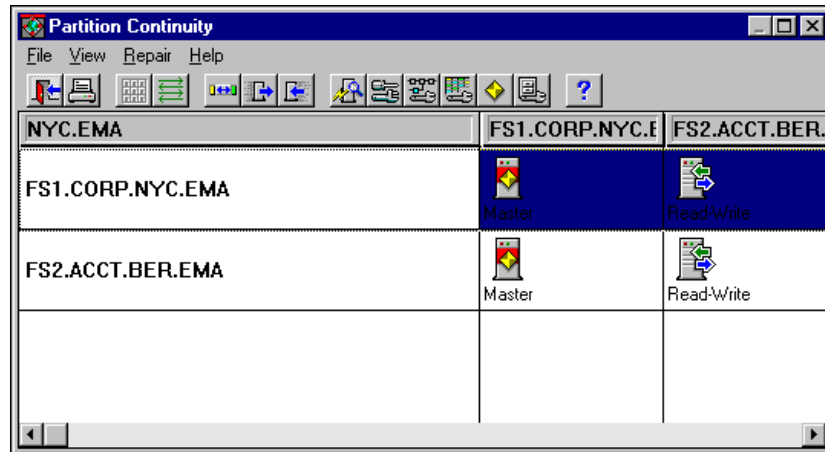


Figure 10-5: Partition Continuity Window in NDS Manager

Additionally, the Partition Continuity window identifies replica list inconsistencies. Each row in the Partition Continuity window is a server and its replica list. Each column should contain the same replica type icons, indicating that the replica lists of all servers (row heading) agree on the replica type (icon in cell) stored on a specific server (column heading).

A replica list problem is identified whenever the replica types in a column are not all the same, or whenever a row or column does not contain a replica type icon in each cell.

Presentation**Notes****NDS Error Messages** *(continued)*

10-5 (Figure 10-5: Partition Continuity Window in NDS Manager)



Demonstrate the Partition Continuity option in NDS Manager.

- Point out that using NDS Manager to correct synchronization problems is covered later in this section.

Point out the following facts:

- NDS Manager connects with each server in the replica list. NDS Manager then polls each server for its replica list, for information that server has on each of its replicas, and for error messages the server is recording.
- Most NDS repair procedures are executed from the Partition Continuity window. Send Update, Receive Updates, and Change Type are also available from the Object menu in the main NDS Manager window.
- If a server is reporting synchronization errors about a replica, the replica icon will have an exclamation point over it.
- If possible, demonstrate a replica icon with an error code.

(See the instructor notes of Exercise 10-1 for actions you can perform to generate NDS errors.)

Finding Help for Resolving Inconsistencies

After the error code has been identified, you can consult the NDS Manager Help system or NetWare 5 product documentation for a description of the error and the actions you can take to resolve the problem.

The error code documentation provides a brief description of the problem and presents a series of actions to help you resolve the specific problem.

To view error code information in NDS Manager, do the following:

1. Using Partition Continuity, identify a server generating an error.



Figure 10-6: Replica Icon Indicating a Synchronization Error

2. Double-click the **server error code icon**.
The error code is displayed in the “Current sync error” field.
3. To view help information on the error code, click the ? (Help) button to the right of the “Current sync error” field.

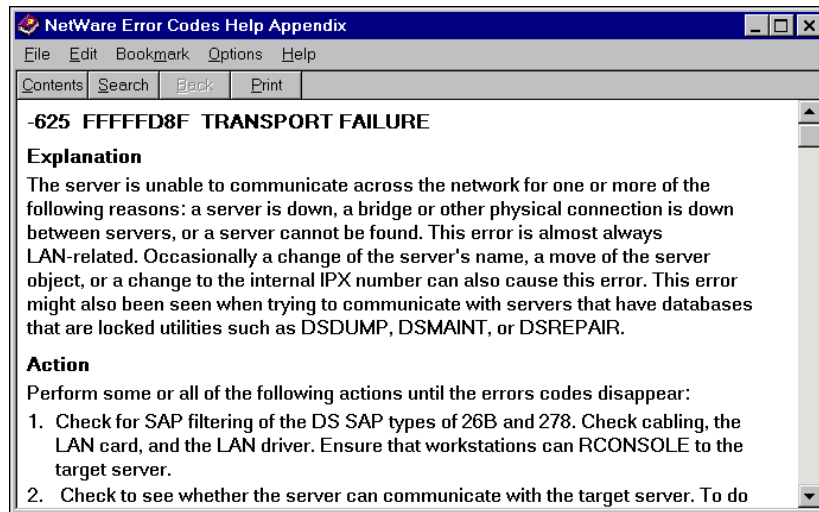


Figure 10-7: NetWare Error Codes Help Appendix

Presentation**Notes****Finding Help for Resolving Inconsistencies**

10-6 (Figure 10-7: NetWare Error Codes Help Appendix)

- Demonstrate how to access error code information in Partition Continuity.
- Emphasize that the online Help is the best source for identifying solutions.

NDS inconsistency errors can be caused by a wide range of problems. Many of the actions that attempt to repair the database can cause problems if executed improperly or at the wrong time.

For these reasons, we strongly suggest that students follow the recommended troubleshooting actions described in the online Help.

In NDS Manager, you can also find help information about an NDS error code by doing the following:

1. In the Help menu, click **Contents**.
2. Under Reference, click **NDS and Server Codes**.
3. Under NetWare Directory Services Error Codes, click **List of Codes**.
4. Click the specific **error code** you want information on.

Presentation

Notes

Finding Help for Resolving Inconsistencies *(continued)*

- Demonstrate how to access error code information through the Help menu.

Repairing NDS

The action you take to resolve NDS database inconsistencies will depend on the specific error being reported. When repairing NDS database inconsistencies, follow these guidelines:

- Let the system run for a few hours. It might synchronize and correct itself.
- Do not bring down the server; you will prevent self-correction.
- Perform repair actions only when they are called for in the error code help or documentation.
- Do not attempt partition operations on a partition that is already experiencing problems. You might cause more synchronization problems.

Correcting Database Inconsistencies

Most NDS inconsistencies can be corrected from the Partition Continuity window in NDS Manager.

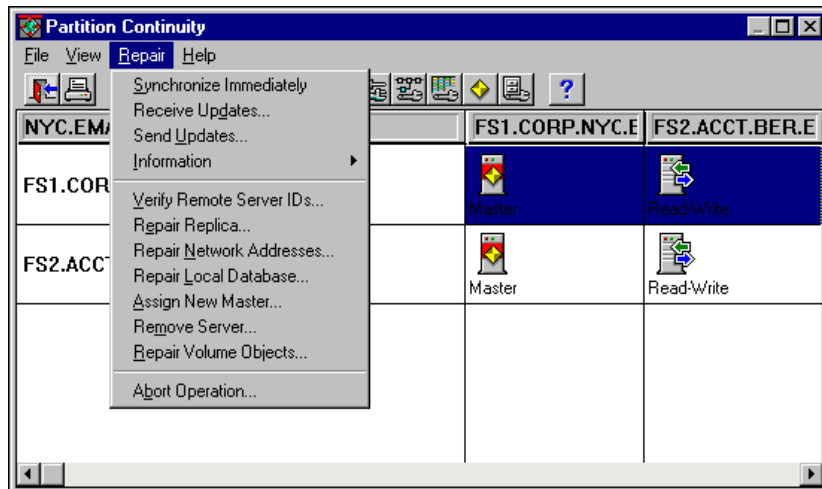


Figure 10-8: NDS Repair Menu in the Partition Continuity Window

Repairing NDS

- Explain the repair guidelines.

Correcting Database Inconsistencies



10-7 (Figure 10-8: NDS Repair Menu in the Partition Continuity Window)

- Point out that most NDS inconsistencies can be corrected in NDS Manager.

Table 10-2 describes common NDS repair tasks that you can perform from NDS Manager.

Action	Description
Synchronize Immediately	Forces all servers in the replica list to synchronize immediately.
Receive Update	Deletes a replica on a server, and replaces it with a copy from the master replica. Performed from the target server when its replica is known to be corrupted and the replica on the master server is not corrupted.
Send Update	Forces the selected server to synchronize immediately.
Verify Remote Server IDs	Confirms and corrects the replica lists and server IDs for all replicas held on a specific server. This ensures the server can communicate with all servers holding the same replicas.
Repair Replica	Confirms and corrects the replica list and server IDs for a specific replica on a server. This ensures the server can communicate with all servers holding that replica.
Repair Network Addresses	Corrects inconsistencies in network address information between servers on a replica list. Inconsistent network address information between servers results in communication failure (a -625 error) between the servers.
Repair Local Database	Corrects specific inconsistencies within all replicas on a server. This action is similar to the action taken by VREPAIR to repair local volumes.
Assign New Master (Change Type)	Changes a read/write or read-only replica into the master replica. Performed when the master replica has become corrupted or is unavailable.
Remove Server	Removes a selected server from a replica list. Used when a server is no longer available and has not been removed from the replica list.
Repair Volume Objects	Confirms that volume objects exist in NDS for all volumes mounted on a server. Creates volume objects that are missing. Can also confirm that objects exist in NDS for all trustee assignments on the volumes, and remove trustee assignments that do not have objects in NDS.
Delete Server	Deletes a server object from the NDS tree. You should only delete the server object for a server that has been permanently removed from the network, but still has an object in NDS.

Table 10-2: Repair Options for NDS Database Inconsistencies



Use extreme caution when deleting servers, assigning new master replicas, and receiving updates. If done incorrectly, you can create additional problems.

Presentation**Notes****Correcting Database Inconsistencies** *(continued)*

- Briefly describe each repair action.



Demonstrate where each action is performed in NDS Manager.

- Provide warnings on using the Receive Update, Remove Server, and Assign New Master options.

The network administrator should not receive updates unless he or she has exhausted all other possibilities.

Receiving updates can cause excessive traffic on a network because the entire replica is sent to the server receiving the updates.

- Point out that Remove Server and Delete Server are different actions.

Remove Server is performed in Partitions Continuity and removes a server from a replica list. Delete Server is performed from the Object menu in the main NDS Manager window.

Performing either action on an active server will cause problems. An active server whose server object is deleted must have NDS reinstalled and all replicas re-added.

- Remind students to delete the volume objects and repair replica lists after they delete the server object.

The volume objects will immediately show up as unknown objects when the network administrator deletes the server.

- Point out that all these actions can also be performed with DSREPAIR.

Here is a list of DSREPAIR actions you might want to be familiar with (they are not covered in this course):

- Global schema update
- Repair time stamp and declare a new epoch
- Delete unknown object

Removing a Server from the Network

In some cases, you might need to remove a server from the NDS tree. For example, you could remove a server if the server will be down for an extended period.

Removing a server requires special consideration because the server might contain replicas and other essential references to NDS. These references must be deleted so that synchronization can continue.



Do not make partition changes while a server that will return is down.

If you are going to bring down a server permanently or for an extended period (greater than a few days), you should remove NDS from the server.



Removing NDS is the recommended method of removing a server object from the NDS tree because this method also deletes volume objects related to the server, handles replica placement issues, informs other servers of the server's status, and removes other essential references.

To remove NDS from a server, do the following:

1. At the server console, load **NWCONFIG**.
2. Select **Directory options**.
3. Select **Remove Directory Services from this server**.
A window appears with a warning about removing NDS.
4. To close the window, press **Enter**.
5. To confirm the action, select **Yes**.
6. Log in to the server as a user with Supervisor object rights to all replicas on the server.
A window might appear warning that master replicas of a partition exist on this server.

Presentation**Notes****Removing a Server from the Network**

- Explain why a network administrator would remove a server from the network.
- Explain why an administrator would remove NDS from a server instead of deleting the server object.
- Explain how to remove NDS from a server.

NWCONFIG might not be able to remove NDS if certain preconditions are not met. To remove NDS from a server unconditionally, the network administrator must load NWCONFIG with the DSREMOVE option:

LOAD NWCONFIG -DSREMOVE

To some, the ability to remove NDS at any cost might appear to create a security breach. Novell cannot guarantee the security of a server whose console can be accessed physically or remotely.

7. After reading the message, press **Enter** to close the window.
If this server is the only server in the tree, a window will appear indicating that NDS has been removed.
8. If this server is one of many servers in a tree, identify a server to receive the master replicas currently stored on this server.
 - a. Select **Do it automatically** if you want the server to automatically choose a server that already contains a read/write replica of the partition.
The NWCONFIG program might choose a subordinate reference on another server if no other replica is available.
 - b. Select **Designate which servers yourself** if you want to choose which read/write replica you want to become the master.

Presentation

Notes

Removing a Server from the Network *(continued)*

- Continue explaining how to remove NDS from a server.

Recovering from a Crashed SYS Volume

Because the Directory is located on the SYS volume, a hard disk failure involving the SYS volume is equivalent to removing NetWare 5 from the NetWare server. You will need to reinstall NetWare 5 and NDS before you restore your data.

To restore replicas to the server that experienced the hard disk failure, you must complete the following tasks:

1. Document the replicas that are located on the server.

To do this, use NDS Manager to select the server object; then record the replicas listed.



Step 1 must be performed before the server has gone down; otherwise, you will need to check the replica lists of all partitions in the Directory to determine which replicas were stored on the server.

2. If any replica displayed in Step 1 is a master replica, you will have to designate a new master on a different server in the NDS tree.

To designate a new master replica in NDS Manager, do the following for each master replica stored on the failed server:

- a. Locate and select a **server** that contains a read/write or read-only replica of the partition.
 - b. Click the **replica** that you want to change into the master replica.
 - c. In the Object menu, click **Replica**.
 - d. In the Replica menu, click **Change Type**.
 - e. Click **Master**.
 - f. Click **OK**.
3. Using NDS Manager, delete the server object of the server on which the hard disk crashed.
 - a. In NDS Manager, locate and select the **server object**.
 - b. In the Object menu, click **Delete**.

The server object is also deleted on other servers that have replicas.

Recovering from a Crashed SYS Volume

- Explain how to handle unexpected downtime.

- Provide an overview of the major steps.



Using NDS Manager, demonstrate how to print the list of replicas stored on a server.



Demonstrate the initial steps used to change a read/write replica to a master replica.



Demonstrate how to delete a server object.

If a server fails because of a disk problem (such as volume failure), the network administrator must delete the server from the NDS tree using NDS Manager and then reinstall NDS.

If the server fails because of a communication or other problem and the SYS volume is still intact, the network administrator can bring that server back online; the server's replicas (even the master replicas) will then be synchronized with the network.

The network administrator can use the NDS Print option to print a replica list.

Important: Do not complete Step 2e; it will change the replica to a master replica.

Important: Do not complete Step 3b; it will delete the server object.

4. In NetWare Administrator, delete the **volume objects** associated with the server.
5. In NDS Manager, select the **partition** that contained the deleted server object.
6. Click **Partition Continuity**.
7. Resolve all errors before continuing.
8. If a -625 error occurs while NDS is trying to connect to the server deleted in NDS Manager, wait to see if the error clears up. If the error remains, perform the steps listed below.



Normally, you need to perform the following steps only on the master replica. NDS should synchronize the deletion. If following the steps below does not clear up the -625 errors, you will have to perform the same steps on all the servers containing replicas of the partition in question.

To remove the deleted server from the replica list, complete the following steps:

- a. Load **NDS Manager**.
- b. Locate and select the **partition**.
- c. Click **Partition Continuity**.
- d. Highlight the **deleted server name**.
- e. In the Repair menu, click **Remove Server**.
- f. To continue the operation, click **Yes**.
- g. If the deleted server held replicas of multiple partitions, repeat these steps for each partition.



Use these procedures only to remove a deleted server object from the replica list. Using this procedure to try to delete a functioning server from a replica list will corrupt the list.

9. Install the new hard disk.

Using procedures recommended by the manufacturer, verify that the hard disk is working properly. We recommend that the new hard disk have the same or greater storage capacity than the disk it replaces.

Presentation**Notes****Recovering from a Crashed
SYS Volume** *(continued)*

Demonstrate how to remove a server from the replica list.

- Emphasize the warning about removing a functioning server.

Important: Do not perform Step 8f; it will remove the server.

10. Reinstall NetWare using the same method you used previously to install it.

After you have defined the configuration and copied the NetWare 5 files, the NDS portion of the installation program appears on the screen. Install the server in the original context.

11. Use NDS Manager and the list you generated in Step 1 to place replicas on the server.

The completion time needed to restore replicas depends on the speed of your LAN or WAN environment.

12. Use the backup system to restore the server's file system data.

The backup system restores not only data but file ownership and user trustee information. If the backup system is unable to restore file ownership and trustees, you will have to recreate them manually.

13. Set the bindery context (if needed).

The restoration of the server and volume is complete.

Recovering from a Crashed SYS Volume *(continued)*



Demonstrate how to change the SET BINDERY CONTEXT = command.

- Remind students that the SET BINDERY CONTEXT = command is included in the AUTOEXEC.NCF file.

The network administrator must add the SET BINDERY CONTEXT = command to the AUTOEXEC.NCF file. To do so, he or she can edit the file directly with NWCONFIG.NLM or EDIT.NLM.

Hands-On Exercise 10-1: Identifying NDS Errors

In this exercise, you perform synchronization status procedures in NDS Manager to determine the health of your NDS tree. You also identify a simple problem created by your instructor and use the NDS Manager Help to determine a strategy for resolving the error.

Complete the following steps:

1. From PUBLICWIN32, load **NDS Manager** (NDSMGR32.EXE).
2. Check the synchronization status for all partitions in the classroom tree.
 - a. Select **View | Set Context**.
 - b. Browse to **[Root]**.
 - c. Select **View | Partitions and Servers**.

A dialog appears showing the workstation's search status and identifying partitions and servers.
 - d. In the Partitions list, click your *partition*.
 - e. Select **Object | Check Synchronization**.
 - f. Click **All Partitions contained in the partition list**.
 - g. To initiate the procedure, click **OK**.
 - h. To continue the operation after preconditions have been met, click **Yes**.

Did any partitions report All processed = no? (Hint: Is the number to the right greater than 0?)

If so, which partitions?
3. Close the **Check Synchronization** window.

Hands-On Exercise 10-1: Identifying NDS Errors

- Introduce the exercise.



- :15** Have students complete the exercise.

- Prepare for Steps 7 through 9.

- Point out other errors created when generating a -625 error.

- Review the exercise.

Perform one of the following actions:

- To generate a -621 error, type **DISABLE TTS** at the server console. To enable TTS, type **ENABLE TTS** at the server console.
- To generate a -625 error, unload DS.NLM, lock the NDS database, unload the LAN driver, or bring down the server.

This will generate error dialogs when the student selects the Partitions and Servers view. Tell the students to continue.

In the Partition Continuity window, the replica icons for the FS1 server will change to "Unable to read." Remind the students to find the replica icons with exclamation points.

- To generate a -701 error, type **SET DSTRACE=!D** at the server console. To disable this SET parameter, type **SET DSTRACE=!E** at the server console.

Note: You might need to wait several minutes before an error code is generated.

Answers:

2. Answers vary.

4. Check the partition continuity of your organizational unit partition.
 - a. In the Partitions list, click your **partition**.
 - b. Select **Object | Partition Continuity**.
5. Close the **Partition Continuity** window.
6. Check the partition continuity of the **[Root] partition**.
Synchronization errors should be evident.



If you are not seeing any error codes, check with your instructor.

7. Identify and record the error code that is being generated.
 - a. Double-click any **replica icon** marked with the exclamation point.
 - b. Read the **error code** in the Current sync error field.
What is the error code?
8. To display the Help information for this error code, click ? to the right of the Current sync error field.
9. In Table 10-3, briefly describe the error and list at least one action you might take to correct the problem.

Error Description
Possible Actions

Table 10-3: Error Description

10. Exit NDS Manager.

(End of Exercise)

Hands-On Exercise 10-1: Identifying NDS Errors (continued)

- Review the exercise.

Answers (continued):

7. Answer vary. Three errors commonly generated in class are -621, -625, and -701.

9. Here are answers for three error codes.

Error Description
-621 FFFFFFFD93 TRANSACTIONS DISABLED TTS has been disabled.
Possible Actions
At the server, type ENABLE TTS . Run VREPAIR on the SYS volume.

Error Description
-625 FFFFFFFD8F TRANSPORT FAILURE The server is unable to communicate across the network.
Possible Actions
Check for SAP filtering. Type DISPLAY SERVERS at the server console. Attach and log in to the target server. In NDS Manager, determine if every server reports an error on the target. Run DSREPAIR to repair network addresses on the source server.

Error Description
-701 FFFFFFFD43 SYNCHRONIZATION DISABLED Schema synchronization has been disabled.
Possible Actions
Type SET DSTRACE =!S1 to enable schema synchronization.

Summary

To maintain a healthy NDS database, you should use preventive maintenance techniques, such as

- Regulating partition management rights
- Planning replica placement carefully
- Backing up the Directory on each server
- Maintaining a standard version of NDS
- Maintaining sufficient disk space on the SYS volume
- Preparing servers properly for downtime

If the NDS database does become inconsistent, you can troubleshoot the problem by

- Identifying the error code generated by the problem
- Using online help or documentation to develop a strategy for resolving the error
- Performing actions to further troubleshoot and resolve the error

If the SYS volume fails, you will need to remove the server from the Directory and replica lists, restore NDS, and re-add replicas to the server.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Explain NDS replication.
2. Explain preventive maintenance procedures for the NDS database.
3. Troubleshoot NDS database inconsistencies.
4. Explain NDS database repair procedures that can be accomplished in NDS Manager, including creating a new master replica, repairing a local database, sending and receiving updates, repairing network addresses, and repairing server IDs.
5. Explain the procedure for recovering NDS from a failed server or volume.

Notes

10-30

SECTION 11 Setting Up Server Remote Access and Mobile Clients

Duration 02:30

Preparation

Complete the following:

- Provide the telephone numbers students will use when connecting to and testing their NIAS Remote Access servers and clients.
- Provide the modem make, model, and COM port used by the students' client PCs.
- Provide separate IP and IPX addresses for use in the section exercises.
- Furnish working telephone lines and modems to each workstation and server. (Have at least two phone lines and two modems to perform a demonstration of connecting by remote access.)
- Provide access to Windows 95 and Windows NT CAB files.
- Ensure that students have Supervisor rights to the Root of the tree to extend the schema.



This section has the instructor extend the NDS schema as part of a demonstration. If you choose not to perform this demonstration, you must extend the NDS schema before starting Exercise 11-3.

SECTION 11

Setting Up Server Remote Access and Mobile Clients

In this section, you set up and use the remote access services provided by NetWare 5.

Objectives

Upon completing this section, you should be able to

1. Explain the capabilities and requirements of NIAS Remote Access.
2. Evaluate the current network and user environment.
3. Select an appropriate data transmission technology.
4. Design a secure remote access solution.
5. Design optimal performance in a remote access solution.
6. Configure NIAS remote access software on the server.
7. Configure Windows 95 or Windows NT clients for remote access.
8. Connect remotely to a server using a modem-equipped Windows client.
9. Explain remote authentication.

Presentation

Notes

Setting Up Server Remote Access and Mobile Clients

- Introduce the section.

- If modems or phone lines are limited, explain what students will be able to accomplish in this section.

Objectives

- Present the section objectives.

Understanding the Capabilities and Requirements of NIAS Remote Access

NetWare 5 provides support for remote access via Novell Internet Access Service (NIAS) remote access.

NIAS runs at the server. It enables the server to

- Operate one or more modems connected to the server
- Provide virtually all network services to a remote user
- Enforce network security across a remote connection

To run NIAS Remote Access, your server needs 5 MB of RAM in addition to that already needed by the server. NetWare 5's server requirements are normally sufficient for normal remote access operation.

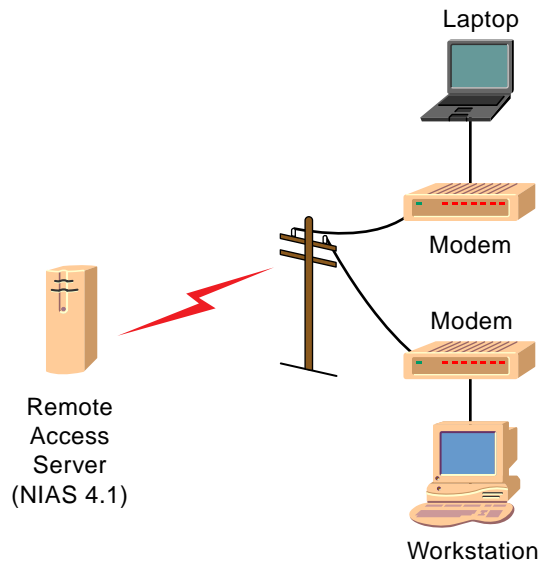


Figure 11-1: Remote Connection Overview

Understanding the Capabilities and Requirements of NIAS Remote Access



11-1 (Figure 11-1: Remote Connection Overview)

- Introduce the concept of remote access.
- Briefly describe how data travels from the remote client to the server.
- Explain what NIAS remote access enables the server to do.

The modem becomes the network card. Telecom voice lines become the data path to and from the server.

Network Services Available Anywhere

Once NIAS is configured, a remote user can do the following

- Log in and authenticate to NDS.
- Run applications such as email and database programs.
- Print documents remotely.
- Connect to the Internet or intranet.
- Obtain routing to distant network services.

Virtually all network services available to a LAN user are available to remote access users.

To access a remote server, a remote user must have a modem-equipped workstation. In addition, the workstation must be specially configured to support remote access connections.

A remote access workstation will dial the telephone number of the NIAS remote access server and connect across voice telephone lines.

Remote access is commonly used by mobile salespeople, telecommuters, and business people who need access to network services while at home or while traveling.

Presentation

Notes

Network Services Available Anywhere

- Discuss the services available to remote workstations.

- Explain the purpose of a modem and how it connects to a remote server.

- Briefly discuss the types of people who rely on remote access.

Differences Between NIAS Remote Access Connections and Direct LAN Connections

While NIAS remote access can provide virtually all network resources, NIAS remote access cannot duplicate the speed LAN users enjoy. Voice telephone lines were not designed to carry network data. Voice telephone lines are inherently

- Slower than direct connections
- Less secure than direct connections
- More expensive than direct connections



A well-designed and configured NIAS setup reduces these speed, security, and expense concerns

Connection Speed

A directly connected Ethernet LAN connection can support 10 or 100 megabits per second. In contrast, a voice telephone connection supports only 28.8K-56K bps per second.

NIAS remote access can help compensate for performance differences. It cannot eliminate them.

Connection Security

Remote access connections are less secure than direct LAN connections. This is true because voice telephone lines are anonymous and widely available.

The global voice telephone network provides the means for unauthorized users, located anywhere in the world, to attempt to access your network.

NIAS remote access supports several security options to help block unauthorized remote users.

Presentation

Notes

Differences Between NIAS Remote Access Connections and Direct LAN Connections

- Explain why remote access speed, security, and expense are disadvantaged compared to a LAN connection.

- Discuss the bandwidth difference.

- Emphasize that a well-designed remote access plan is essential.

28.8K-56K bps modem connection versus 10-100 megabits per second of an Ethernet connection

Connection Expense

Remote access users might have to pay long-distance or other measured rate charges to connect to the NIAS remote access server. Careful deployment and siting NIAS remote access servers might help avoid unnecessary telecom expenses.

Overview of Required Tasks to Enable Remote Access

To set up NIAS, you must complete several remote access design and configuration tasks.

1. Evaluate your current network and user environment in preparation for building a remote access solution.
2. Select an appropriate data transmission medium for use between the server and remote workstations.
3. Ensure that unauthorized remote users are prevented from accessing the network.
4. Tune remote client and server configurations for maximum performance.
5. Install and configure appropriate software to enable remote access on a network.

This section covers these tasks.

Presentation

Notes

Overview of Required Tasks to Enable Remote Access

- Point out the tasks listed in the student manual.

- Explain that completing these tasks will lead to a well-designed and implemented remote access system.

Evaluating the Current Network and User Environment

To create a remote access design or strategy, you must first:

- Select the best physical location for the NIAS remote access server.
- Determine the locations and needs of remote users.

Selecting the Best Physical Server Locations

To select the best host locations and servers for remote access, consider the following:

- Inventory existing network hardware at each potential remote access location. Is there a server with spare capacity to run NIAS available?
- Is this server physically located in an area which offers the cheapest connections for most remote users?
- Does this server have adequate routing and WAN links to handle additional network traffic generated by the remote clients?

Determining Users and Services

To determine the needs of remote users, determine the following:

- At which locations in your organization do you want to offer remote access dial-in capability?
- How many remote access users do you expect at each site?
- How many simultaneous remote access connections do you anticipate each day?
- What is the projected growth rate of remote access users?
- Which users and groups need remote access?

Presentation

Notes

Evaluating the Current Network and User Environment

- Explain the need to plan and design a remote access solution before configuring it.

Selecting the Best Physical Server Locations

- Discuss the selection criteria used to determine the best choices.

Determining Users and Services

- Discuss the criteria used to determine which users and which services should be offered.

Selecting an Appropriate Data Transmission Technology

The next step in designing an efficient remote access design is selecting the most appropriate data transmission technology for both the server and the remote workstation.



This section refers to a Local Exchange Carrier (LEC) or telephone company as a “telecom.”

Telecoms provide the data transmission, or connection, between your NIAS remote access server and the remote user.

Some data transmission choices might be better than others for your needs. Usually the speed of the connection, or bandwidth is a prime concern.

Data transmission choices commonly include

- Integrated Services Digital Network (ISDN)
- Plain Old Telephone Service (POTS)
- Digital Subscriber Line (xDSL)

Select the most appropriate transmission technology by answering the following questions:

- What telecom services are available at the NIAS remote access server's location?
- Which telecom services can the remote server support?
- Which transmission technology is economically feasible?
- What connection speed, or bandwidth, is required by each remote user?
- How much additional bandwidth could you require in the future?

Presentation

Notes

Selecting an Appropriate Data Transmission Technology

- ❑ Point out the need to carefully select the best telecom and transmission device.

- ❑ Point out how these telecom services are usually sold or made available to customers.

In some locations, both the telecom service (the data line) and the transmission device (such as a modem) are sold as one turnkey product. In other locations, the telecom offers only the “line” and not the equipment.

Evaluating Common Data Transmission Choices

Before you make a remote access transmission choice, you need to evaluate the transmission technologies that are available in your area. Three common remote access transmission technologies include

- ISDN
- POTS
- xDSL

ISDN

ISDN is a digital transmission service that was designed to replace analog telephone service. ISDN is offered in two formats: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI is the most common format.

Typically, the BRI is composed of two Bearer or "B" channels and data Data or "D" channel. Each B channel can support up to 64 KB. You can combine both B channels to achieve a single maximum rate of 128 KB. This is accomplished via server hardware, and software, such as NIAS Remote Access, that supports Multilink Point to Point Protocol (MPPP)

Use of ISDN requires the support of a Terminal Adaptor (TA) and a Network Termination 1 device (NT1) on the client and server. The NT1 connects your server to the telecom. It provides call setup capabilities.

ISDN is a good choice for remote access solutions that need to offer reasonably fast digital links to remote clients.

Presentation

Notes

Evaluating Common Data Transmission Choices

- Discuss the general criteria used to select the best telecom “line” or service.

ISDN

- Describe the general technical features of ISDN.
- Describe some circumstances that would make ISDN a good choice.

- Remote users who need fast, all-digital links to the server
- Areas served by affordable ISDN services

POTS

“Plain Old Telephone Service” or traditional voice phone lines, are often a good choice for remote access servers which

- Are not physically served by other telecom services
- Do not serve remote clients who demand the fastest service
- Require a low cost telecom connection

To use POTS lines, the client and the server must have a modem.

Although modems supporting speeds of 56 Kb are available, most achieve this speed only on the “download” connection from the server to the client. To achieve 56 Kb speeds at the server, the server might require a special 56 Kb modem interface device served by a digital connection such as an ISDN PRI or a T1 (E1) connection.

In contrast, 33.6 Kb modems, which need only a POTS line, and can transmit at 33.6 Kb in both “upload” and “download” directions.

Presentation

Notes

POTS

- Explain the circumstances in which POTS would be a good choice for a remote access server.

- Point out the transmission speeds possible using POTS lines.

- Point out the limitations that current 56 Kb modems have.

xDSL

xDSL is the name of a new family of high-speed digital transmission technology. xDSL is designed to work on top of existing analog telephone service over twisted-pair copper telephone lines.

Analog telephone service and xDSL service are designed to co-exist simultaneously using the same copper twisted-pair telephone wire.

Potentially, xDSL service can provide multiple high-speed remote connections over existing telephone lines.



Unlike POTS or ISDN, xDSL connections require no call setup or dialing. xDSL connections normally are dedicated point to point links, which are always up.

Several DSL variants currently exist including

- Asynchronous Digital Subscriber Line (ADSL). ADSL offers 8.192 Mbps download speeds with a slower upload connection.
- High Speed Digital Subscriber Line (HDSL). HDSL enables T1 speeds of 1.544 Mbps in both upload and download connections.
- “Splitterless” DSL. “Splitterless” DSL typically offers speeds of less than 1 Mbps, but requires no special line equipment or splitter to exist at the user’s location.

Various hardware manufacturers produce xDSL adaptors for use on servers and workstations. “Splitterless” DSL adaptors often resemble modems in their set up and operation. Some “splitterless” DSL adaptors can support either DSL or 56 Kb POTS modem connections.



Many xDSL services are not yet available in all areas but are expected to become widespread. Please check with your telecom or data transmission service provider for further information.

Presentation	Notes
xDSL	
<input type="checkbox"/> Describe the xDSL technology family.	<p>xDSL provides megabit speeds over existing analog copper lines without disturbing existing POTS service.</p>
<input type="checkbox"/> Briefly describe the features of one to two DSL variants.	<p>The x in xDSL stands for all potential DSL variants, such as ADSL or HDSL.</p>
<input type="checkbox"/> Point out that xDSL is not yet widely available and that it is distance sensitive.	<p>“Splitterless” DSL is a new consumer grade version of DSL that requires no special adaptor or splitter at the customer’s location. This reduces installation costs, but also reduces performance.</p> <p>xDSL services may be distance sensitive. The greater the distance the server or workstation is from the telecom’s central office, the slower the connection may be.</p>
<input type="checkbox"/> Point out that xDSL is not yet widely available and that it is distance sensitive.	<p>Various telecoms have announced 1998-1999 as potential xDSL rollout dates in certain areas. Alliances among telecom, hardware and software firms might help increase the availability of this service.</p>
<input type="checkbox"/> Point out that xDSL is not yet widely available and that it is distance sensitive.	<p>Several data transmission technology forums, such as ADSL Forum, are available. The ADSL web site is at WWW.ADSL.COM</p>

Written Exercise 11-1: Selecting the Best Data Transmission Technologies For Your Organization

In this exercise you begin the process of building a remote access design. By answering the questions found in this exercise, you develop an overall design.

Write or draw the answers to the following questions

1. Which telecom services seem attractive to your organization?

2. What is the best telecom service for most remote workstations in your organization?

3. What remote access communications equipment might you need for remote access servers and workstations?

(End of Exercise)

Written Exercise 11-1: Selecting the Best Data Transmission Technologies for Your Organization

- Introduce the exercise.



:10

- Have students complete the exercise.
- Have students think about their own organizations in answering the exercise questions.
- Review the exercise.

Designing a Secure Remote Access Solution

Security is critical to any remote access design. To create an effective remote security solution, carefully consider security early in the design process. A remote access security solution imposed later on an existing remote access setup might be more difficult to achieve.

By default, NIAS Remote Access services are installed to offer unrestricted access to any user, and unlimited access to any service via any port. We strongly recommend that you adjust this default level of security before permitting users to dial-in.

Security concerns can be divided into three levels

- Develop remote access security policies.
- Isolate remote access servers in a secure data zone, such as a demilitarized zone.
- Meet unique security requirements of the organization by developing effective network configurations and security policies.

Determining an Organizational Security Policy

To develop a remote access security policy for your organization, consider the following

- What are the overall quantifiable goals your security policy must achieve? For example, do you want to stop 100% of all unauthorized users? To delay authorized users by no more than a few seconds?
- Who in the organization will have primary responsibility to enforce the security policy? Who will have a secondary responsibility?
- How will you train users and network administrators to maintain security on a day-to-day level?
- Does your security policy seem flexible enough to permit adaptation to new or emerging security threats?
- What specific procedures should be followed when intruders are suspected? Who should be notified?
- How will you test the on going effectiveness of your security solution?

Presentation**Notes****Designing a Secure Remote Access Solution**

- Emphasize the importance of designing and building an effective security solution.

- Point out the need to adjust the unlimited access NIAS Remote Access sets up by default.

- Explain that a security design can be broken down into three levels such as
 - User policy
 - Data isolation
 - Unique organization requirements

(Optional) Relate a security related story or incident.

Classifying security into levels can help organize overall security design.

Determining an Organizational Security Policy

- Discuss the issues involved in setting up remote access organizational security.

Determining a Network Security Policy

Consider the following mid-level security questions. These questions generally involve specific network configurations, usually NIAS Remote Access Server and NetWare 5 setup.

- Will your security policies be based on individual users? Groups?
- By default, will user access be restricted to certain locations only? By default, will users have access to the entire network?
- How often will users be required to change passwords? What is the minimum length of user passwords?
- Will you require remote access passwords be encrypted when remote clients attempt to log in?
- By default, will users have remote login time restrictions? Location restrictions?
- Should certain types of data, files, or programs on servers that should never be accessed remotely?
- Could there be any old or inactive user accounts be used or enabled for unauthorized remote access?
- Do you want to allow remote users to use the same password when logging in remotely as when they log in to the LAN?

Determining a Data-Level Security Policy

Consider the following questions in developing a data-level security policy:

- Do you need to modify your routers to limit access to and from your remote access servers?
- Will you require users to utilize encrypted connections when remotely connecting to the network?
- Is access through NIAS Remote Access the only option remote users have of connecting to the network? For example, can users dial in to an Internet Service Provider (ISP) and connect to the network?
- Do you want the remote server to call back the remote user to ensure the location of the remote user?

Presentation

Notes

Determining a Network Security Policy

- Talk about the questions that help develop a security policy.
- Discuss the criteria involved in creating network security policies.

Determining a Data-Level Security Policy

- Explain that data-level security covers routing and other low-level security criteria.
- Discuss the issues related to data-level security policy.

Isolating a Remote Access Server

It is critical to protect your network from unauthorized users. This often means isolating the remote access server from the rest of the network.

If security were somehow compromised and an unauthorized user managed to connect to the remote access server, that server should not provide easy access to the rest of the network.

One way to set up this design is to create a demilitarized zone. A demilitarized zone prevents network intruders from connecting beyond the remote access server.

Demilitarized Zone Security Design

All remote access traffic destined for an organization connects first with a server in a *demilitarized zone*. All entering the demilitarized zone is considered inherently insecure. A *screening router* filters then accepts or rejects remote access traffic from traveling further into the organization's network.

The demilitarized zone becomes the entrance for all remote access traffic. A NetWare 5 server or dedicated screening router can screen and connect the remote access server to the private network as needed.

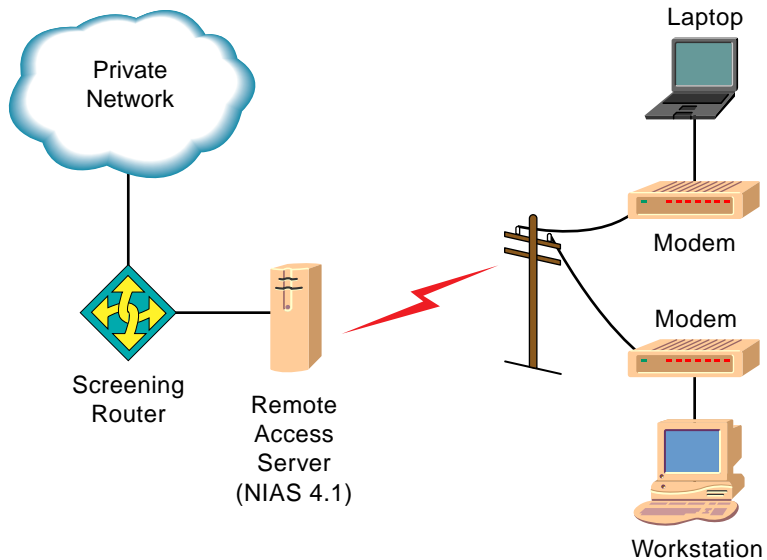


Figure 11-2: Demilitarized Zone Design

Presentation**Notes****Isolating a Remote Access Server**

- Explain that, by default, NIAS offers unrestricted access to any user, for any length of time, on any modem port.

Demilitarized Zone Security Design

11-2 (Figure 11-2:
Demilitarized Zone Design)

- Explain the theory and benefit of setting up a remote access server in a demilitarized zone with the use of a *screening router*.
- Point out that students may want to use routing or remote access design specialist for creating a demilitarized zone.

Further discussion on creating a demilitarized zone is beyond the scope of this section.

Special Security Concerns

Some data might be too sensitive to risk even the potential of a remote access security failure. Certain organizations must follow strict security policies. Before implementing any remote access service on your network, check with the appropriate security personnel in your organization.

Presentation

Notes

Special Security Concerns

- Point out security concerns that might limit or prevent use of remote access.

Special situations might include government security classification, protection of critical intellectual property, or strict legal requirements.

Designing Optimal Remote Access Performance

Maximizing performance and reducing administration make up an important task in designing an effective remote access solution. Remote access performance and its day-to-day administration may become the most visible aspects of your design once your remote access operation is in place.

Maximizing Client Performance

All current remote access links are substantially slower than typical LAN connections. Because of this, remote access users often complain of slow performance.

Slow performance can

- Increase telecom charges
- Decrease links available to other remote users

Remote Client Performance Issues

Remote user complaints often include

- Slow login, login script execution, and mapping performance
- Extremely slow execution of applications, such as databases, and spreadsheets, called from the remote server.
- Slow file transfers
- Long waits to display large lists of data, such as file directory contents, NDS tree information, or available servers

Presentation

Notes

Designing Optimal Remote Access Performance

- Express the importance of having a high-performance and low-management remote access environment.

Maximizing Client Performance

- Point out the negative aspects of slow performance.

Remote Client Performance Issues

- Explain the kinds of complaints remote users generate.

Tuning the Client for Maximum Performance

Each of these situations can be improved by careful planning. Consider the following performance-enhancing suggestions:

- Create minimal login scripts for each remote access user.
- Install frequently used applications locally on the remote workstation.
- Set and use compression settings on the remote workstation.
- Reduce the need to transfer files to remote workstations by re-arranging work patterns, or pro-actively copying files to the remote workstation when connected to the LAN (such as a notebook PC).
- Create Windows shortcuts for commonly used remote files or servers on the remote workstation desktop. This eliminates the long wait for large lists of files or servers to be displayed.
- Upgrade slower modems to faster models.
- Evaluate alternative telecom services.
- Optimize workstation resources available to Windows.
- Train users to expect slow performance and plan their remote network use accordingly.

Maximizing Server Performance

Steps can be taken on the server to ensure maximum remote access throughput. Ensure that each remote server has

- The recommended amount of memory for the number of users expected to use it
- Available CPU resources to log in remote users and route their data to other locations on the network
- Adequate LAN or WAN bandwidth to provide efficient connections to other locations on the network
- The most recent remote access device drivers installed

Presentation

Notes

Tuning the Client for Maximum Performance

- Discuss the suggestions for improving slow performance.

Training users to make efficient use of a remote access link, and telling them to expect slow service are often an important step to increasing satisfaction.

Maximizing Server Performance

- Explain the suggestions increasing server performance.

Optimizing Remote Access Administration

Administration tasks often fall into one of the following categories:

- Configuring users and groups and managing accounts
- Monitoring and enforcing security
- Troubleshooting remote access configurations and links (this topic is beyond the scope of this section)

NDS and Remote User Management

Because NIAS supports NDS, individual user and group remote access configurations can be combined with standard network and LAN based user and group management. Remote users and groups can be managed from both NetWare Administrator and the remote access server console.

NIAS Remote Access supports Remote Access Management Agent (RAMA) service. With RAMA, any SNMP-based management tool, such as ManageWise, can view and support a NIAS Remote Access server.

Remote Access Administration and Security

User and group management often involves security configuration. Individual user and group access can be restricted

- By hour or by day
- To specific dial-in ports
- To specific protocols or remote access services

Depending on your design and configuration, you can create a user environment which has one of the following:

- Many restrictions by default. The environment relies on the network administrator works on a case by case basis to grant exceptions as needed
- Few restrictions by default. The environment relies on continuous network administrator surveillance of remote access operations and rapid response to security breaches as needed.

Presentation**Notes****Optimizing Remote Access Administration**

- Point out the common categories of remote access administration.

NDS and Remote User Management

- Point out that NDS tools can manage remote users and groups.
- Point out that NIAS Remote Access supports SNMP management via its RAMA service.

Remote Access Administration and Security

- Point out the trade-off often made between administration and security.

Optimizing Remote Access IP Administration

All TCP/IP workstations require an IP address, DNS service, and access to a gateway router. In the past, these parameters were manually configured on each workstation.

NIAS Remote Access server eliminates the need for manual administration of remote IP clients. The NIAS Remote Access server can supply the following to the Windows remote client:

- An IP address valid for the length of the remote connection via Dynamic Host Configuration Protocol (DHCP)
- A DNS server address and domain
- A default gateway router

These abilities eliminate the need to manually configure IP information on each Windows remote client. However, you may still manually configure each parameter and have full NIAS Remote Access server support.

DHCP is a protocol designed to “lease” an IP address to a client that requests one. The IP addresses come from a range of IP addresses you specify while configuring NIAS Remote Access server.

DHCP address ranges normally must be addresses from a separate network other than the IP network used by the NIAS Remote Access server itself.

In later exercises, you can configure the NIAS Remote Access server and Windows to automatically handle all required IP parameters.

IPX addressing and routing occurs automatically and needs no special settings.

Presentation

Notes

Optimizing Remote Access IP Administration

- Point out that IP addresses can be assigned to remote clients statically or dynamically.

- Discuss the administration requirements for statically and dynamically assigned IP addresses.

- Explain the purpose and function of the NIAS DHCP protocol.

Written Exercise 11-2: Optimizing Performance and Administration for a Remote Access Solution

This exercise focuses on maximizing performance and minimizing administration tasks.

Referring to the previous exercise as needed, write or draw the answers to the following questions.

Maximizing Remote Access Performance

1. What overall configuration parameters will you specify in your design? For Windows clients?
2. What performance-enhancing suggestions could you offer users who might ask you to provide faster performance?
3. What can you specify in your design to enhance remote access server performance?

Presentation**Notes****Written Exercise 11-2:
Optimizing Performance and
Administration for a Remote
Access Solution**

- Introduce the exercise.



:10

- Have the students complete the exercise.

- Assist students as necessary.

Suggested answers

1. Windows clients with minimal login scripts and shortcuts to folders.
2. Use faster modems, install applications locally, ensure aggressive use of file compression.
3. Ensure that sufficient memory and CPU resources are available. Consider using a faster transmission technology.

Optimizing Security and Administration

1. What types of security and administration tasks can you plan or anticipate at this point?

2. Does your administration plan anticipate enforcement of remote access security? How?

3. How will you configure remote clients for IP service?

4. Who in your organization is primarily responsible for remote access security? Who has a secondary responsibility?

5. Will you offer after-hours remote access server monitoring? How will you support remote users?

6. Do you want to enable an SNMP network management tool to support the NIAS Remote Access server?

7. Can you develop procedures to use if anyone encounters or suspects remote security problems?

(End of Exercise)

Presentation

Notes

**Written Exercise 11-2:
Optimizing Performance and
Administration for a Remote
Access Solution** *(continued)*

- Review the exercise.

- Review the entire design process.

Configuring NIAS Remote Access on the Server

To enable the server to support remote access networking, you must complete several configuration tasks. These steps may involve decisions and selections you made previously in this section.

Overview of Remote Access Server Tasks

To enable remote access on the server, you must perform the following main tasks at the server:

- If necessary, install remote access hardware such as modems and cables.
- Configure NIAS Remote Access Server:
 - Load and define an Asynchronous Input and Output (AIO) port.
 - Specify the type of modem or other device connected to the server.
 - Select the remote services you want, such as PPPRNS and RAMA.
 - Configure IP and IPX addresses and related information.
- Configure NIAS Remote Access to meet your design requirements, such as those involving security, performance, and administration.

A later exercise will provide detailed steps to help you configure your server for remote access. Hardware such as modems may already be connected to your server.

Presentation**Notes****Configuring NIAS Remote Access on the Server**

- Explain that students are now ready to configure the server and client.

Overview of Remote Access Server Tasks

- Provide an overview of the tasks used to configure the server.



Demonstrate how to install NIAS on FS1.

This demonstration extends the schema. You must complete it before Exercise 11-3.

Hands-On Exercise 11-3: Configuring the NIAS Remote Access Server

Refer to the design work you performed in previous exercises to assist in the configuration process.

In this exercise, you configure the NIAS Remote Access Server.

Your instructor will provide you with the following parameters:

- IP address
- IPX address

Complete the following steps at the server console

1. Load **NIASCFG.NLM**.
2. To transfer driver commands press **Enter**.
3. Press **Enter**.
4. Exit and Restart the server.
5. Load **NIASCFG.NLM**.
6. Select **Configure NIAS**.
7. Select **Remote Access**.
8. Authenticate to the EMA_TREE.
9. Select **Yes** to Do You Want Instructions?
10. Read the instructions, which provide an overview of the configuration process, and press **Esc** when complete.
11. Press **Enter**.
12. Press **Enter** to begin the setup process.
13. Select **No** to "Do You Have Any Synchronous Adaptors?" You will configure an asynchronous modem for remote client access.
14. Press **Enter** to load and define an AIO port.
15. Scroll down to the Serial Port (COMx) entry and press **Enter**.

Presentation**Notes**

Hands-On Exercise 11-3: Configuring the NIAS Remote Access Server

- Introduce the exercise.



:20

- Have students complete the exercise.

- Provide students with unique, valid and unused IP and IPX address numbers

- Provide students with their COM port and modem type.

- Assist students as necessary.

Ensure that students have Supervisor rights to the Root of the tree so they can extend the schema.

Suggested IP addresses:

195.126.82.16
195.126.82.17
195.126.82.18
195.126.82.19

Suggested IPX addresses:

100
101
102
103

If students have difficulty displaying or selecting remote services, have them issue the following command at the server console prompt:

```
LOAD SVCDEF.NLM  
SYS:SYSTEM\CONNECT\SVCS.DEF
```

Have students restart the server and the exercise.

16. Press **Enter** when the console reports that the driver was loaded successfully.
17. Select **No** to Do you need to load more AIO drivers. (If you had additional modems on other ports you might say yes.)
18. Ensure your modem is connected to the server's COM port, and that the modem is turned on.
19. Press **Enter** when you are ready for NIAS to look for your modem
20. Ensure that NIAS found a modem on a licensed port. If not, select **Try Modem Discovery Again** to repeat this process.
21. Press **Enter** to continue the exercise.
22. If prompted, select **Yes** to Auto-Detect Modem Types. (Due to the vast number of modem models and types, auto-detection does not always succeed.) If NIAS did succeed, proceed to the next step. Otherwise, complete the following
 - Press **Enter** to continue if NIAS reports it cannot determine the modem type.
 - Press **Enter** again to display a list of modem types.
 - Scroll and select your modem.
23. Select **PPRNS**.
24. Select **IP**.
25. Enter a valid **IP address** as supplied by your instructor. For example, 195.126.82.16.

To enable IP routing beyond the server, this address may need to be on a different network or subnetwork than the server's own bound IP address.
26. Ensure the subnet mask is set to 255.255.255.0 or another value as supplied by your instructor.
27. Select **Yes** to enable Header Compression.
28. Select **Yes** to specify a client range if your design specified using dynamic IP address assignment.

Presentation

Notes

**Hands-On Exercise 11-3:
Configuring the NIAS Remote
Access Server** *(continued)*

- Continue the exercise.

29. Enter a range of valid IP addresses on the same network as specified in the Local IP Address field. For example, if you specified a local IP address of 195.126.85.16, and want a range of 8 addresses, a potential address range could start at 195.126.82.17 and end at 195.126.82.25.
30. Press **Esc** and select **Yes** to save changes. Do not enter a secondary client address range.
31. Select **IPX**.
32. Enter a unique **IPX address** as supplied by your instructor. For example 100.
33. Press **Enter** to activate the changes.
34. Press **Esc** and select **Yes** to save changes.
35. Press **Esc** and **Yes** to save current settings to a file.
36. Read the message stating that the current configuration will be activated. Any active connections will be lost.
37. Press **Enter** to continue. Wait for reinitialization to complete.
38. Select **Yes** to Do You Want to Start This Service Now? (This will start PPPRNS).
39. Select **RAMA** and select **Yes** if you want NIAS Remote Server to allow management via an SNMP-based tool.
40. Press **Esc** to complete the basic NIAS Remote Access configuration. Read the security note that states that all users can access all ports and services at all times.

You are now ready to configure basic NIAS Remote Access password security. Continue to the following steps to begin this process.

41. Press **Enter** to continue.
42. Select **Configure Security**.
43. Select **Set User Remote Client Password Restrictions**.

**Hands-On Exercise 11-3:
Configuring the NIAS Remote
Access Server** *(continued)*

- Continue the exercise.

Set parameters to ensure secure access to your organization.

44. Select **Enable Long Password**. This setting allows passwords of up to 16 bytes instead of 8 bytes. Legacy NetWare Connect servers do not support long passwords.
45. Set Maximum Invalid Login Attempts to no more than 3. A value of -1 allows unlimited attempts.
46. Press **Esc** and select **Yes** to save changes
47. Select **Set User Remote Client Password**.
48. Select a **user** or **group** from the tree.
49. Enter the desired **password** and press **Enter**. Confirm the password. If you do not set up a password, users must use their password set up in NDS.
50. Press **Esc** and select Yes to save these settings.
51. Inspect all other choices available. Set parameters to support any special security need of your organization.
52. Press **Esc** and select **Yes** to save changes.

Your server is now ready to accept modem calls from remote clients.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 11-3:
Configuring the NIAS Remote
Access Server** *(continued)*

- Continue the exercise.

- Review the exercise.

Configuring Windows 95 or Windows NT Clients for Remote Access

Both Windows 95 and Windows NT provide a native remote access client. You need to set up and configure the Windows native remote access client before you can connect to the remote access server.

Hardware such as modems and cables may already be attached to your Windows client.

The Novell Client and Remote Access

The Novell Client works with Windows to ensure a remote access user can properly connect to a NIAS remote access server and use all NetWare services.

Some versions of the Novell Client may feature a Dial-Up tab after clicking the Advanced button displayed on the log in window. The Dial-Up tab allows you to optionally set the Novell Client to always connect to the network using Windows Dial-Up Networking.

Overview of Tasks to Configure a Remote Access Windows Client

The following tasks need to be completed to configure a Windows workstation for remote access:

- Make sure the latest Novell Client is installed in Windows.
- Install remote access hardware such as a modem.
- Install and configure Windows Remote Access Service or Dial-Up Network service.
- Configure network parameters to enable a connection to a server.
- Modify login scripts and security access to ensure adequate security and performance.

Exercises with detailed instructions will help you perform these tasks. Slight variations exist between Windows 95 and Windows NT. Complete the correct portion of the exercise for your version of Windows.

Presentation**Notes**

Configuring Windows 95 or Windows NT Clients for Remote Access

- Explain that Windows itself provides a native remote access client.

The Novell Client and Remote Access

- Explain that students should ensure the latest version of the Novell Client is installed in Windows to assure access of all NetWare services.



If available, display and discuss the Dial-Up tab after clicking the Advanced button on the initial Novell Client login window.

This tab may only be available in the Novell Client for Windows NT.

This tab can set the client to use Windows Dial-Up Networking in order to connect to the network.

Overview of Tasks to Configure a Remote Access Windows Client

- Outline the major tasks students need to complete in order to configure a remote access Windows client.

Hands-On Exercise 11-4: Configuring Windows for Remote Access

In this exercise you set up Windows to remotely access, via modem, your NIAS remote access server.

Refer to previous exercises to help guide your configuration choices in this exercise.

Part I - Windows 95 Steps

Complete the following steps if you are using a Windows 95 workstation

1. Install Windows Dial-Up Networking
 - a. From the Windows 95 Control Panel, double click **Add/Remove Programs**.
 - b. Click the **Windows Setup** tab.
 - c. In the Components window, double-click **Communications**.
 - d. Check the box for **Dial-Up Networking**; then click **OK**.
 - e. Click **OK**.
 - f. Wait while Windows copies files.
2. Configure the Windows 95 Dial-Up Networking adapter.
 - a. Double click **My Computer**.
 - b. Double click **Dial-Up Networking**.
 - c. When the welcome screen appears, click **Next**.
 - d. To have the program autodetect your modem and communications port follow the screen prompts.
 - e. If Windows fails to detect your modem, select the correct modem manually.
 - f. When the program indicates it is finished setting up your modem, click **Next**.
 - g. Enter the telephone number of the server modem (this will be provided to you by the instructor) and click **Next**.
 - h. Read the message and click **Finish**.

Hands-On Exercise 11-4: Configuring Windows for Remote Access

- Introduce the exercise.



:15

- Have students complete the appropriate portion of the exercise.

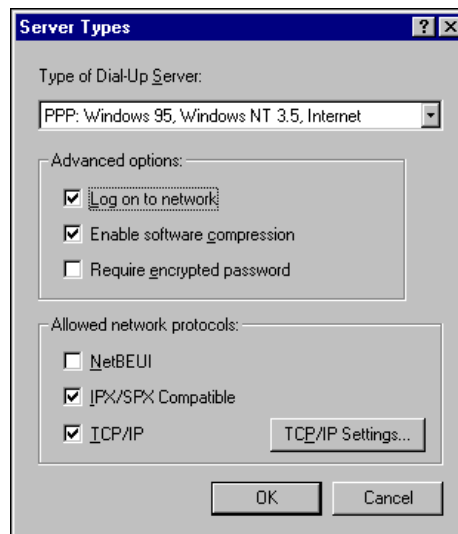
- Ensure that students have access to the Windows CAB files.

- Provide students with the client's modem COM port and modem type.

- Provide students with the server's telephone number.

- Assist students as necessary to complete each step.

- i. Type the **name** of the computer you will be dialing and click **Next**.
 - j. Enter the **number** to call to reach the remote access server.
 - k. Click **Next**.
 - l. Click **Finish**.
3. At the Windows 95 Desktop click once to select the Dial-up server icon you just created.
 4. Right-click and select **Properties**.
 5. Click **Server Type**.



6. Make sure that the Type of Dial-Up Server field has the following selection:
PPP: Windows 95, Windows NT 3.5, Internet
7. Check all the boxes in Advanced Options, if you want to use encrypted passwords and software compression.
8. In the Allow Network Protocol area check both
IPX/SPX Compatible
TCP/IP

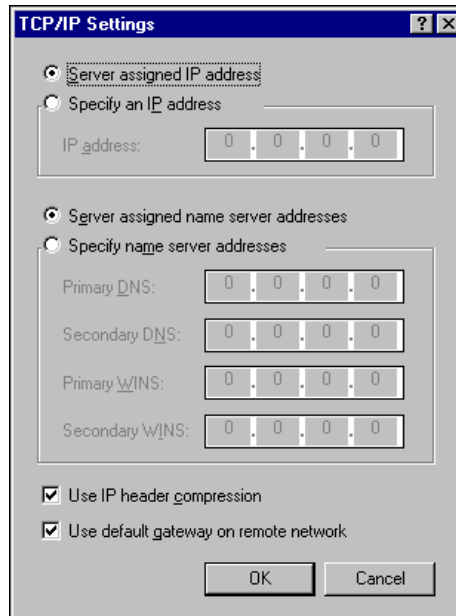
Presentation

Notes

**Hands-On Exercise 11-4:
Configuring Windows for
Remote Access** *(continued)*

- Continue the exercise.

9. Click TCP/IP Settings.



10. Enable both

Use IP Header compression

Use Default Gateway

if your design calls for compression and server assigned IP gateway router settings.

11. Click **OK** multiple times to return to the Control Panel.

Clicking **OK** sets up a connection between your workstation and the server. An icon with the name of the server is placed in your Dial-Up Networking directory.

Your Windows 95 workstation is now ready to connect to the remote access server.

Presentation

Notes

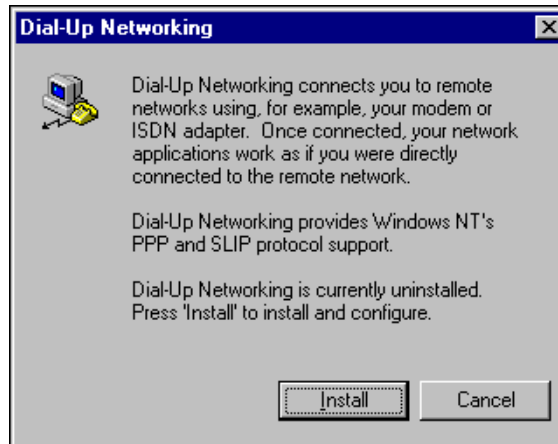
**Hands-On Exercise 11-4:
Configuring Windows for
Remote Access** *(continued)*

- Continue the exercise.

Part II - Windows NT

Complete the following steps if you are using a Windows NT workstation

1. Double-click the My Computer icon.
2. Double click the Dial Up Networking icon.
3. If dial up networking capability has not been installed you should see the following window. Click **Install**.



4. Click **Yes** when Remote Access Setup reports there are no RAS capable devices to add.
5. Click **Next** when NT reports it will now try to detect your modem.
6. Click **Next** after NT has detected your modem.



If this step failed to detect the correct modem or COM port notify your instructor

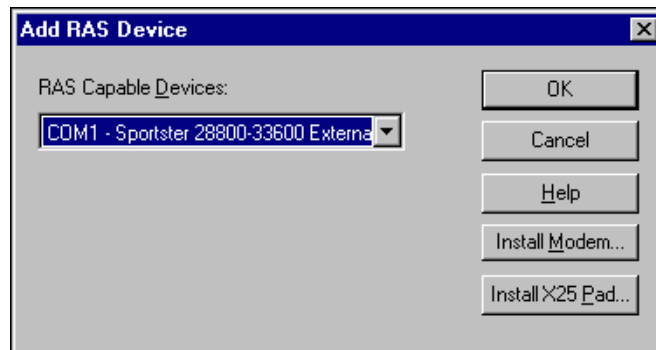
Presentation

Notes

**Hands-On Exercise 11-4:
Configuring Windows for
Remote Access** *(continued)*

- Continue the exercise.

7. Enter the area code, number for an outside line, and indicate tone dialing, then click **Next**.
8. Enter the phone number supplied by the instructor and click.
9. Click **Finish** when your modem has been configured.
10. At the Add RAS Device dialog box, ensure your modem is displayed; then click **OK**.



11. Click **Continue** to confirm the modem choice in the Remote Access Setup window.
12. Wait while NT automatically completes this portion of the install process.
13. Click **Restart** when the Dial Up Networking dialog box reports installation was successful.
14. Login as your Admin object.
15. Double-click **Dialup Networking** in the My Computer window.
16. Click **OK** to add a new entry in the NT phone book after NT reboots.
17. Click **Next** to confirm the name of the phone book.
18. Place a check in the I Am Calling the Internet box. This setting configures the dial up connection to support IP.

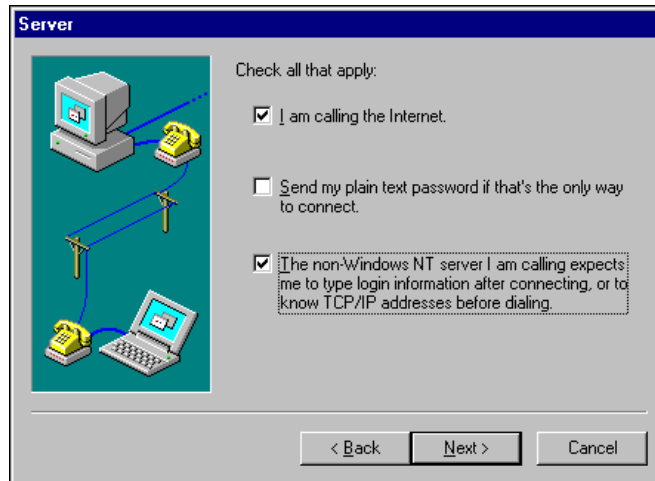
Presentation

Notes

**Hands-On Exercise 11-4:
Configuring Windows for
Remote Access** *(continued)*

- Continue the exercise.

19. Place a check in the “The non-Windows NT server I am calling expects me to type login information after connecting, or to know TCP/IP addresses before dialing” box.



20. Click **Next**.
21. Enter the phone number of your Remote Access Server as supplied by your instructor, then click **Next**.
22. Click **Point-to-Point (PPP)** at the Serial Line Protocol window; then click **Next**.
23. Ensure **None** is selected at the Login Script dialog box; then click **Next**.
24. Ensure that *0.0.0.0* is entered in the My IP address field; then click **Next**. NIAS remote access server can automatically lease the remote workstation an IP address. However, If you want to manually configure an address, then enter the workstation's permanent IP address instead of *0.0.0.0*.
25. Ensure that *0.0.0.0* appears in both the DNS and WINS fields. The NIAS remote access server can automatically provide the workstation with a DNS server address. If your want to manually configure DNS information, enter the that information instead of *0.0.0.0*.
26. Click Finish.
27. Click **Close**.

Your Windows NT workstation is now ready to connect to a NIAS remote access server.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 11-4:
Configuring Windows for
Remote Access** *(continued)*

- Continue the exercise.

- Review the exercise.

Connecting Remotely to a Server

After you have configured the server and client, you can connect remotely to the server. The client generally initiates all calls to the server.

The server and the client must have their own specified links, such as a telephone line, for a remote connection to take place.

Connecting a Remote Client

Connecting a remote client to a server is generally similar to the process of connecting and logging in to the network using a LAN connection. Creating a remote connection requires

- launching a remote access login utility
- entering a user ID and Password

In general, the only difference is that the remote access login utility might request the phone number of the remote server. Once this information has been provided, the client's modem becomes the remote equivalent of a LAN card.

Ensure that you follow the correct portion of the exercise for your version of Windows.

Presentation

Notes

Connecting Remotely to a Server

- Explain that remote access connections can be made when configuration on the server and client are complete.

Connecting a Remote Client

- Point out the similarities and differences of initiating a LAN and remote client connection.

The modem becomes the network board.

Hands-On Exercise 11-5: Connecting to the Remote Server with Windows

In this exercise you dial into the remote server using the Windows client you setup in the previous exercise.

Complete Part I if you are using Windows 95. Complete Part II of you are using Windows NT.

Part I: Windows 95

1. Double-click the My Computer icon.
2. Double-click on the Dial-up networking icon.
3. Double-click the icon matching your NIAS remote access server.



4. Enter the user name, including NDS context and password for your Admin object then click **Connect**.
5. Click **OK** if you see a message stating that LAN connections will be inaccessible.
6. Wait for the modem to dial and connect to your remote access server. You will see status messages stating that verification of the user name and log in are taking place

Presentation

Notes

Hands-On Exercise 11-5: Connecting to the Remote Server with Windows

- Introduce the exercise.



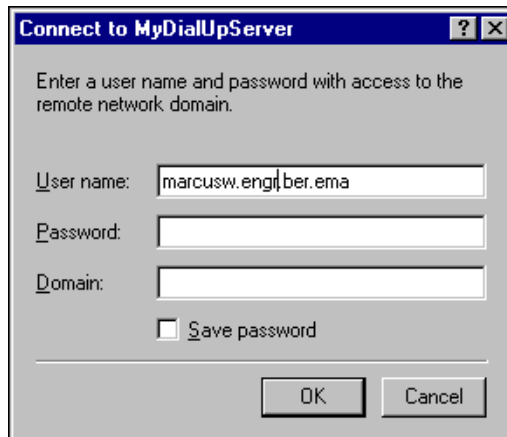
:15

- Have students complete the appropriate portion of the exercise.
- Assist the students as necessary.

7. Depending on your configuration you may see a Novell Client login window. If you enabled Log on to Network you may see the Novell Client login window once the workstation has connected to NIAS.
8. If a login screen appears, log in to the network.
9. Double-click on the Network Neighborhood icon.
10. Display available server and network services. Note the dial-up status icons in the task bar, normally next to the clock at the bottom right of your screen. This confirms that your workstation has a live remote access connection.
11. Click the Dial-Up status icon in the task bar.
12. Click **Disconnect** to end the connection.

Part II: Windows NT

1. Double-click on **My Computer**.
2. Double-click on **Dial-Up Networking**. At this point, you should see the Phonebook you configured earlier.
3. Click the Phonebook entry that corresponds to your NIAS remote access server.
4. Click **Dial**.



**Hands-On Exercise 11-5:
Connecting to the Remote
Server with Windows** *(continued)*

- Continue the exercise.

5. Enter the user name, including the NDS context and password for your Admin object, then click **OK**.
6. Wait for the modem to dial and connect to your NIAS remote server.
7. Press **OK** when you see the Connection Complete window.
8. Double-click the Network Neighborhood icon and display available servers and network resources. Note the dial-up status icons in the task bar, normally next to the clock at the bottom right of your screen. The icons confirm that your workstation has a live remote access connection.
9. To end the connection to the NIAS remote access server, double-click the Dial-Up Networking icon and select **Hang Up**.

(End of Exercise)

Presentation

Notes

**Hands-On Exercise 11-5:
Connecting to the Remote
Server with Windows** *(continued)*

- Assist the students as necessary.

- Review the exercise.

Understanding Remote Authentication Dial-In User Service (RADIUS)

The Remote Authentication Dial In User Service (RADIUS) protocol allows remote access users to securely dial in to NetWare networks. Novell BorderManager supports RADIUS.

A host server running the RADIUS protocol (the RADIUS server) retrieves all dial-in user and authentication information from a central database.

A host server running the RADIUS accounting protocol (the RADIUS accounting server) is responsible for logging information about dial-in user connections.

The accounting information is typically used for statistical analysis, troubleshooting, and billing.

The RADIUS protocol is supported by many network access server vendors and is an IETF Proposed Standard (RFC 2138). The RADIUS accounting protocol is also an IETF Proposed Standard (RFC 2139).

The RADIUS protocol provides

- Centralized administration
- Client/server model
- Network security
- Support for multiple authentication mechanisms
- User configuration and access control

RADIUS Proxy

RADIUS proxy permits remote access users to connect to an Internet Service Provider (ISP) and remotely authenticate to their organization's NDS tree.

With RADIUS, you do not have to maintain and manage internal modem banks or remote access servers to service remote users.

Presentation

Notes

Understanding Remote Authentication Dial-In User Service (RADIUS)

- Introduce the concept of Remote Authentication Dial In User Service (RADIUS).

- Point out the key features of the RADIUS protocol.

RADIUS Proxy

- Explain how a RADIUS Proxy allows a remote user to dial in to a corporate network via an Internet Service Provider.

RADIUS and Internet Service Providers (ISPs)

You can use RADIUS proxy to outsource the management of dial-in hardware to an Internet Service Provider (ISP) while you manage the users in your NDS™ tree. This gives you the flexibility to manage dial-in users without having to purchase dial-in hardware.

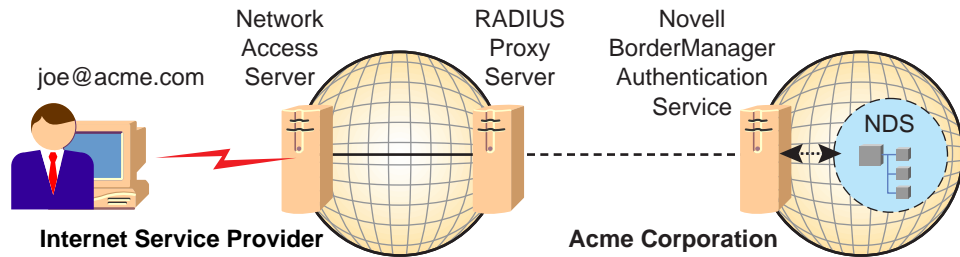


Figure 11-3: RADIUS Proxy Connections Using an ISP

Using RADIUS proxy, a remote user (such as jane@acme.com) dials in to an ISP network. The user access request (user ID and password) is forwarded to a RADIUS proxy server on the ISP network.

The ISP proxy RADIUS server forwards the access request to your company RADIUS server.

The RADIUS server then checks the information in the access request and either accepts or rejects the request.

If the RADIUS server accepts the request, it returns configuration information specifying the type of connection service (such as PPP or Telnet) to be delivered to the user.

Presentation**Notes****RADIUS and Internet Service Providers (ISPs)**

11-3 (Figure 11-3: RADIUS Proxy Connections Using an ISP)

- Describe how a remote user could dial in to an ISP and authenticate to his or her organization's NDS tree.

- Explain the advantages this could bring to an organization seeking to avoid the expense of maintaining in-house remote access equipment.

Summary

Novell Internet Access Server (NIAS) allows you to configure your network for access by remote users. This remote access is not as fast as a LAN connection, but can be used to access network resources when away from the LAN.

Remote Authentication Dial In User Service (RADIUS) is another method which can be used to provide remote access to your network. Using RADIUS, you can connect to your network through an Internet Service Provider.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Explain the capabilities and requirements of NIAS Remote Access.
2. Evaluate the current network and user environment.
3. Select an appropriate data transmission technology.
4. Design a secure remote access solution.
5. Design optimal performance in a remote access solution.
6. Configure NIAS remote access software on the server.
7. Configure Windows 95 or Windows NT clients for remote access.
8. Connect remotely to a server using a modem-equipped Windows client.
9. Explain remote authentication.

Notes

SECTION 12 **Integrating Other Novell Services**

Duration 02:00

Preparation

None

SECTION 12 Integrating Other Novell Services

In this section you learn about four key networking solutions offered by Novell: BorderManager™, NDS for NT, GroupWise®, and ManageWise®.

Objectives

Upon completing this section, you should be able to

1. Identify networking solutions offered by Novell.
2. Explain the benefits of securing your network with BorderManager.
3. List the components of a firewall.
4. Identify the firewall components of BorderManager.
5. Explain the benefits of placing Windows NT domains into NDS.
6. Explain the purpose of the components of NDS for NT.
7. Describe how GroupWise integrates with NetWare.
8. List the basic components of a GroupWise system and describe the function of each component.
9. Explain how GroupWise components work together to provide GroupWise messaging services.
10. Describe the major features of ManageWise.
11. Identify the components of ManageWise.

Presentation

Notes

Integrating Other Novell Services

- Introduce the section.

Objectives

- Present the section objectives.

Networking Services from Novell

After your network has been configured, it must provide services to network users. NetWare 5 includes a variety of networking services, but it might not include every network service your users require.

Some of the main networking services needed on networks are listed below:

- Secure Internet access
- Integration with other operating systems
- Email
- Management

As a network administrator, you will be asked to provide solutions that solve a variety of business needs. It is important for you to know what additional Novell products are available, what purpose they serve, and what problems they solve. You need to be able to sell those solutions to the businesses that need them.

This section briefly describes the following Novell products:

- BorderManager™
- NDS for NT
- GroupWise®
- ManageWise®

Presentation**Notes****Networking Services from Novell**

- ❑ Briefly introduce BorderManager, NDS for NT, GroupWise, and ManageWise.

- ❑ Point out that Novell offers elective CNE courses on each of these products.

Note: The following courses are electives for a CNE:

- Course 770, Securing Intranets with BorderManager
- Course 555, intraNetWare®: Integrating Windows NT
- Course 350, GroupWise 5 Administration
- Course 730, Network Management Using ManageWise

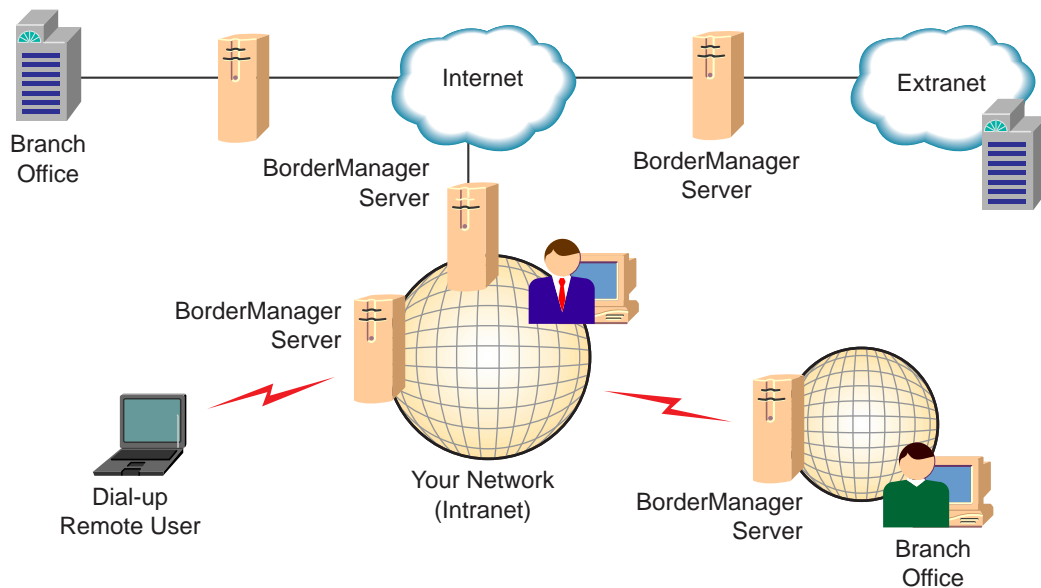


Figure 12-1: Using BorderManager between Private and Public Networks

BorderManager Services

When an organization connects its network to the Internet, it must manage access to Internet resources. This complicates network management and increases the probability of unauthorized access to information.

BorderManager provides the solution. BorderManager derives its name from the border area between a private corporate network and the public Internet.

Placing BorderManager services at the border enables organizations to

- Monitor and control inbound and outbound access to the Internet
- Implement performance accelerators at the border
- Implement user, service, and content access control

BorderManager Services



12-1 (Figure 12-1: Using BorderManager between Private and Public Networks)

- Discuss the need for managing access to the Internet.

- Explain what BorderManager enables organizations to do.

Firewalls and Firewall Components

Historically, brick walls were built between buildings and wood houses. If a fire broke out, the wall would prevent the fire from spreading to the next building. These brick walls were called *firewalls*.

In a computer environment, a firewall is a control mechanism for inbound and outbound access between networks.



The term *outbound* refers to traffic leaving the private network for the public network; *inbound* means the opposite.

A firewall prevents unauthorized access between

- A private network (an *intranet*) and a public network (the Internet)
- An intranet linked to an external intranet (an *extranet*)
- One division's access to another division's intranet within an organization (for example, Manufacturing's access to Research)

Presentation**Notes****Firewalls and Firewall Components**

- Define *firewall*.
- Define *intranet*.
- Define *extranet*.
- Make sure students understand *inbound* and *outbound*.

Outbound access control limits access to the Internet. For example, you can limit user access to Web sites considered necessary for work-related objectives.

Inbound access control protects intranet servers against being accessed by unauthorized users on the Internet.

Figure 12-2 illustrates a firewall controlling inbound and outbound access.

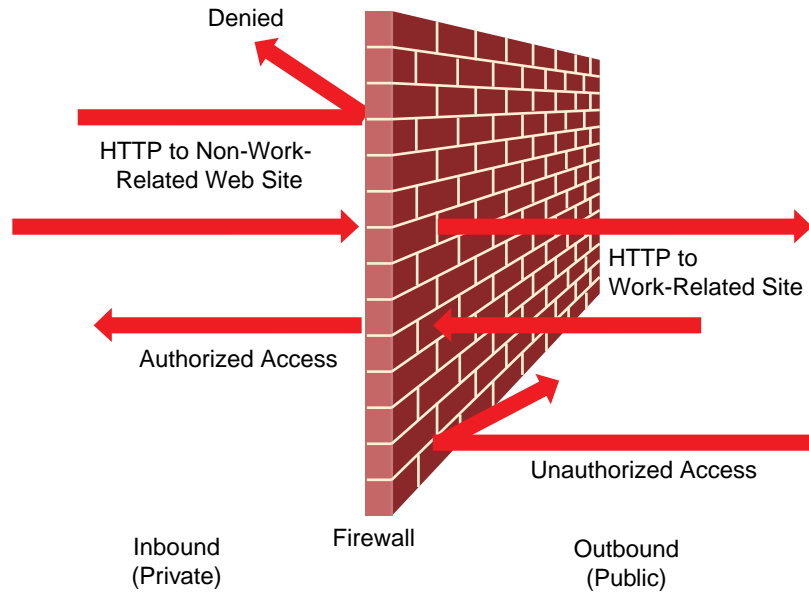


Figure 12-2: Inbound and Outbound Access Control with Firewalls

A firewall commonly contains packet-filtering routers, circuit gateways, and application gateways.

A firewall can be a packet-filtering router, a packet-filtering router combined with a circuit gateway, or the *combination* of a packet-filtering router, circuit gateway, and application gateway.

Most often, an effective firewall is made up of a combination of components.

Firewalls and Firewall Components *(continued)*



12-2 (Figure 12-2: Inbound and Outbound Access Control with Firewalls)

- Discuss how access can be controlled with firewalls.
- State the common components of a firewall.
- Explain that a firewall is most often a combination of components.

Firewall Components and the OSI Model

Used together, firewall components provide access control at various layers of the OSI model. Following are firewall components and how they correspond to the OSI model:

- **Packet-filtering routers**, also called *screening routers*, can restrict incoming traffic to the intranet by filtering out unauthorized source IP addresses and port numbers.

Packet-filtering routers are implemented at the Data Link, Network, and Transport layers of the OSI model.



A router's packet filters can operate using port addresses, network addresses, node addresses, or a combination. Therefore, they can operate at one, two, or three OSI layers.

- **Circuit gateways**, also called *circuit-level proxies*, implement access control at the Session layer of the OSI model.

When an intranet user requests Internet access, the user's request is sent to a known port on the gateway. Software at the gateway validates a TCP or UDP session before opening a connection or circuit. (TCP and UDP are Transport layer protocols.)

The gateway services the request and can substitute its own IP address for that of the requester.

Circuit gateways implement routing policies based on higher-level protocols such as HTTP.

- **Application gateways**, also called *application-level proxies*, are generally considered the most secure type of firewall. Access control occurs at the Application layer of the OSI model.

Application gateways are implemented at the Presentation and Application layers.

Presentation

Notes

Firewall Components and the OSI Model

- Describe how firewall components correspond to OSI layers.

Firewall Components in BorderManager

You can use the following major components of BorderManager to create a firewall:

- Novell Internet Access Server (NIAS) 4.1 software
- Remote Access
- IP gateway software
- Proxy cache software
- Virtual private network (VPN) encryption software

NIAS 4.1 Software

NIAS 4.1 provides the following routing and connectivity features, which are fundamental to BorderManager's operation:

- Multiprotocol routing
- WAN support
- Packet filtering
- Network address translator (NAT), used to translate private IP addresses to registered addresses
- IPX mapping gateway, used to translate private IPX addresses to registered addresses
- Inbound and outbound remote access



NIAS 4.1 replaces NetWare Connect™ 2.0 and NetWare MPR™ 3.1, and offers enhanced capabilities over NIAS 4.0.

Remote Access

BorderManager uses NIAS Remote Access software which allows you to access your intranet using telephone lines. This server-based program allows modem-equipped, dial-in clients to access the network.



For more information regarding remote access, see Section 11, "Setting Up Server Remote Access and Mobile Clients."

Presentation

Notes

Firewall Components in BorderManager

- List the major BorderManager components.

NIAS 4.1 Software

- Briefly explain NIAS 4.1.

Remote Access

- Explain that Remote Access software is part of NIAS 4.1.

IP Gateway Software

An IP gateway lets organizations use an unregistered TCP/IP address scheme within the enterprise while maintaining compatible addressing with the Internet.

The IP gateway sends user requests to an Internet site that uses its own public IP address on behalf of the client. When the gateway receives a response, it forwards the response back to the client using the client's private IP or IPX address.

The IP gateway operates in one of two possible modes:

- IPX-to-IP translation (IPX/IP gateway) is used primarily in *IPX-only networks* where TCP/IP is not used. It allows IPX clients to access IP hosts through the gateway.
- IP-to-IP translation (IP/IP gateway) is used in NetWare 5 environments that are using the Compatibility Mode driver. The IP-to-IP gateway translates *unregistered* IP addresses to the gateway's registered IP address.

Proxy Cache Software

The proxy cache services provided in BorderManager accelerate Web access performance, reduce WAN traffic, and off-load Web server requests.



In NetWare Administrator, the *proxy cache* is called *Web proxy cache*.

Acceleration is needed because browsers usually communicate directly with an *origin* Web server (the source server accessed over the Internet) that has a *high-latency* (delayed) connection.

When a BorderManager proxy server is deployed, browsing performance increases because browsers receive data from a local source where Web content has been cached.

Presentation

Notes

IP Gateway Software

- Explain IP gateway software and how it is used.

Proxy Cache Software

- Describe proxy cache services.

Proxy cache can improve performance when used as one of the following:

- Standard proxy cache
- HTTP accelerator
- Hierarchical proxy cache

Standard Proxy Cache

When configured as a standard proxy cache (also called a *client accelerator*), BorderManager uses its cache to store frequently accessed Web pages locally, reducing response times from the Internet.

Users spend less time waiting for information to be delivered and the traffic on WAN links is significantly reduced.

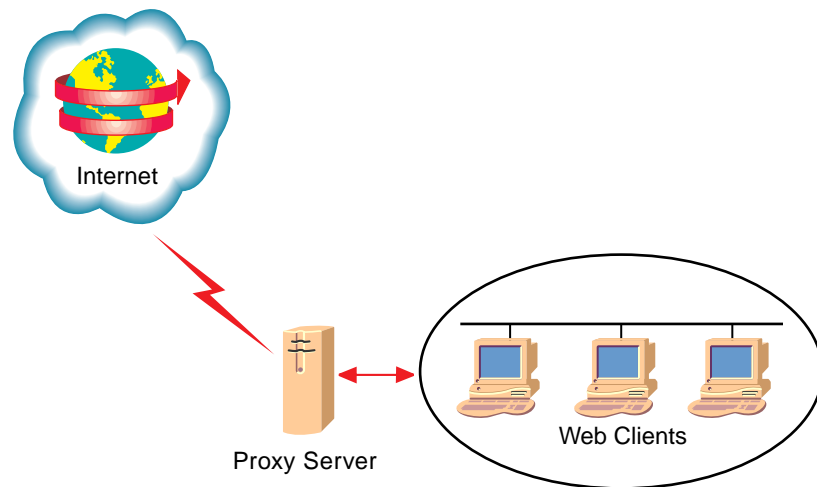


Figure 12-3: Proxy Cache Placement for Internet Access

Presentation**Notes****Proxy Cache Software** *(continued)*

- Explain the benefits of proxy caching, including improved performance and reduced WAN traffic.

Standard Proxy Cache

- Describe a standard proxy cache and its benefits.



12-3 (Figure 12-3: Proxy Cache Placement for Internet Access)

HTTP Accelerator

The caching capability of BorderManager can be used as a public front-end to Web servers on your private intranet.

Web servers can be a bottleneck in your corporate intranet because they can quickly run out of connections, resulting in slow response times.

With an HTTP accelerator (also called a *Web server accelerator* or *reverse proxy*), BorderManager uses a dedicated cache in place of the Web server.

The bottleneck is eliminated because a dedicated cache handles requests for all the Web servers' cacheable content directly from its own cache.

Typical Web sites are constructed with 95 to 100% cacheable content. After material is retrieved from the Web server and cached in the HTTP accelerator, the accelerator can handle all requests for that content.

However, a small number of dynamic requests are passed through the HTTP accelerator for the Web server to process.

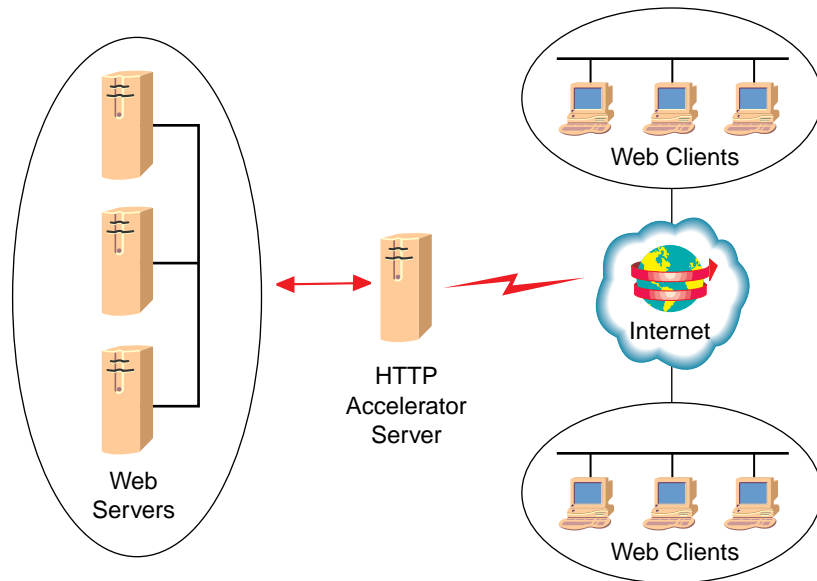


Figure 12-4: HTTP Accelerator Proxy Cache Placement

Presentation

Notes

HTTP Accelerator

- Explain the purpose and benefits of an HTTP accelerator.



12-4 (Figure 12-4: HTTP Accelerator Proxy Cache Placement)

Hierarchical Proxy Cache

A hierarchical proxy cache allows you to place multiple caches within your organization, storing popular content on the same side of WAN links as those who use it.

Configured this way, BorderManager retrieves first-time accesses and cache-misses from other caches in your organization, rather than returning to the source Web server.

If a user can access information on a proxy server instead of retrieving it from the source server, access time can be reduced tenfold or more.

Virtual Private Network (VPN) Encryption Software

A Virtual Private Network (VPN) uses NIAS 4.1 tunneling and multiple encryption layers to create a secure private network over the Internet or between intranets. This eliminates the need for expensive, dedicated private lines.

Because the tunnel appears to the IP and IPX stacks as a single point-to-point link, connection is simplified. Tunneling can be used at full speed over T1 and T3 lines and symmetric multiprocessing (SMP) servers.

Tunneling is cost effective because it allows VPN sites to share information with each other over the Internet without exposing the information to the public.

Presentation**Notes****Hierarchical Proxy Cache**

- Explain that a hierarchical proxy cache places multiple caches within an organization.

- Explain the benefits of a hierarchical proxy cache.

- Explain that one example of a hierarchical cache could be a corporation's home page, placed in a hierarchical proxy cache for remote users.

**Virtual Private Network (VPN)
Encryption Software**

- Introduce the function of a VPN.

To establish the initial network-to-network link, BorderManager uses Diffie-Hellman public-key, private-key encrypted authentication.

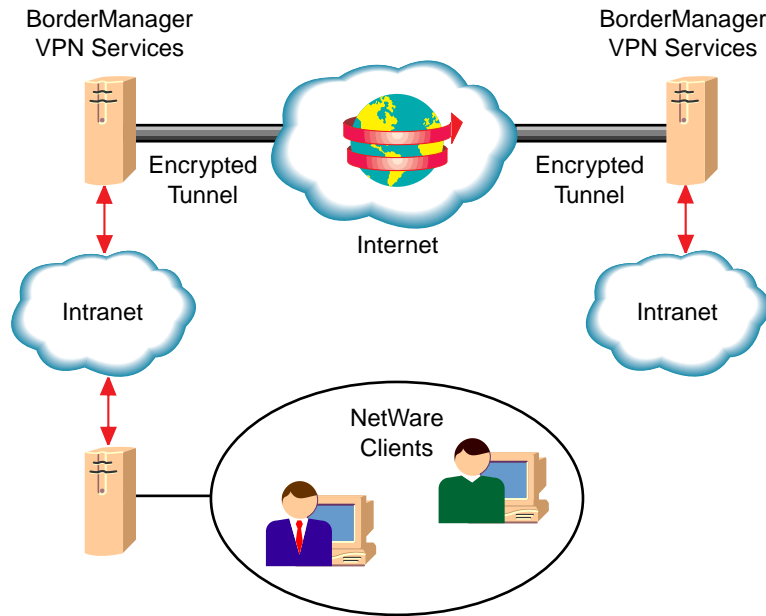


Figure 12-5: VPN Tunneling over the Internet

Presentation**Notes****Virtual Private Network (VPN)
Encryption Software** *(continued)*

12-5 (Figure 12-5: VPN Tunneling over the Internet)

- Explain that a VPN uses tunneling and multiple layers of encryption technology in addition to Diffie-Hellman public and private keys.

BorderManager Components, the OSI Model, and Firewalls

BorderManager components can be classified by their relationship to the OSI model, as shown in Table 12-1.

OSI Layer	Gateway Type	BorderManager Component				
		NIAS 4.1	IP Gateway	Web Proxy Cache	VPN	
Application	Application Gateway			IP Gateway (access control)	Web Proxy Cache	VPN
Presentation						
Session	Circuit Gateway			IP Gateway		
Transport	Packet Filtering Gateway		Packet Filtering			
Network		NAT		IP Gateway (address translation)		
Data Link						
Physical						

Table 12-1: BorderManager Components, Gateway Types, and the OSI Model

You can use BorderManager components to make a complete firewall:

- The packet filtering and NAT capability of NIAS 4.1 can be used as a packet-filtering firewall.
- The IP gateway can function as a circuit-level gateway.
- The proxy cache can function as an application-level gateway.
- The VPN can function at all layers of the OSI model (except the physical layer). This is achieved as a result of end-to-end data encryption.



For complete training on BorderManager, contact your nearest NAEC about taking Novell Education Course 770, Securing Intranets with BorderManager.

To locate your nearest NAEC, go to

http://db.netpub.com/nov_edu/x/naecloc

Presentation**Notes****BorderManager Components, the OSI Model, and Firewalls**

- Discuss how BorderManager components map to the layers of the OSI model.

- Explain that VPN encryption mechanisms implement security across all layers of the OSI model, except the Physical layer.

- Recommend Course 770 to students who want more information regarding BorderManager.

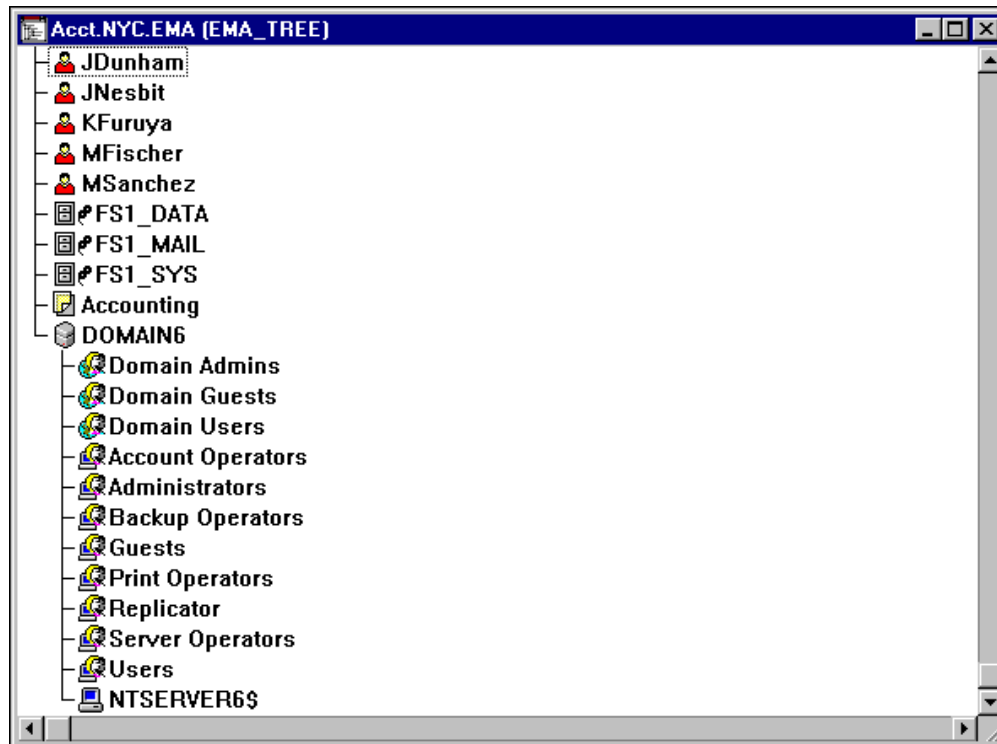


Figure 12-6: Managing Windows NT Domains in NDS

NDS for NT

NDS for NT extends the schema of NDS. This extension allows you to place Windows NT domains in the NDS tree, thereby creating a single, unified directory from which to manage all components of your network.

With an extended schema, NDS can fulfill Windows NT domain requests made from Windows NT Servers and Windows NT Workstations.

Presentation**Notes****NDS for NT**

12-6 (Figure 12-6: Managing Windows NT Domains in NDS)

- Introduce NDS for NT.

- Explain that the NDS schema is extended so that Windows NT domains can be managed from within NDS.

NDS for NT provides the following benefits:

- Single database from which to administer all components of a network
- NDS support for applications that require domains
- Single login to the network
- Additional management capabilities that are not available in Windows NT networking

Administering All Components of a Network from a Single Database

NDS for NT allows you to put NT domain user accounts into NDS. This provides a single point of administration, which

- Simplifies user administration
- Reduces administration costs

Simplified User Administration

Extending NDS so that it contains all the attributes and objects of the Windows NT domain provides you with a single database from which to administer all components of the network.

This approach eliminates the need to administer two separate databases or to synchronize databases. It also eliminates the problems posed when duplicated databases become unsynchronized.

Reduced Administration Costs

By providing a single point of administration for users and groups in a mixed environment, NDS for NT greatly simplifies the entire network administration process and substantially reduces the cost of owning and managing your heterogeneous network.

Combining NDS and domain user accounts reduces the cost of administering a mixed NetWare and Windows NT environment by eliminating duplicate work on accounts. It also eliminates the administration costs of configuring complex domain trust relationships.

Managing user accounts in NDS also allows you to use cost-saving features such as templates. This simplifies processes such as creating new user accounts.

Presentation**Notes****NDS for NT** *(continued)*

- Discuss the benefits of NDS for NT.

Administering All Components of a Network from a Single Database

- Discuss the benefits of having a single database from which all network resources are administered.

NDS Support for Applications That Require Domains

Some Windows NT applications require access to the Windows NT domain. Because NDS for NT puts the Windows NT domain into NDS, any application requesting domain services can be serviced by NDS without needing modification.

A domain request from an application is redirected to NDS just as a print job is redirected from the local operating system to the network. The application's domain request is fulfilled as if the domain database existed on a domain controller.

Single Login to the Network

Without NDS for NT, a user must log in as an NDS user to access the NetWare network and then log in as a Windows NT user to access the Windows NT network.

After integration, a user can authenticate to both platforms using a single user account. NDS keeps track of the password formats required by each platform. To access all authorized network services, including Windows NT domains, the user needs to log in using only the NDS user account.

Having one NDS user account for all access is a simpler solution than using Novell Administrator for Windows NT, which synchronizes two separate user accounts between two databases.

It is also a much simpler solution than creating and maintaining trust relationships between Windows NT domains or creating a user account in each domain that a user needs to access.

Presentation

Notes

NDS Support for Applications That Require Domains

- Point out that NDS supports applications that require the Windows NT domain.

Single Login to the Network

- Discuss how NDS for NT provides a single login solution.

Additional Management Capabilities of NDS

The addition of NDS to a Windows NT Server provides you with several management capabilities not obtainable in a Windows NT domain network. These include

- Easy configuration of user access to multiple domains
- Security determination from a single user account
- Easy movement of user accounts
- Per-object administration

Easy Configuration of User Access to Multiple Domains

Traditionally, giving Windows NT users access to global resources meant having to set up complicated trust relationships between domains.

NDS for NT reduces the complexity of managing multiple domains, saving you time and giving users easy access to all network resources. It can eliminate the need for trust relationships.

By managing integrated network users with NetWare Administrator and NDS, you can configure access to multiple domains as easily as making an NDS user a member of an NDS group.

Presentation

Notes

Additional Management Capabilities of NDS

- Discuss additional management capabilities NDS brings to the Windows NT platform.

Easy Configuration of User Access to Multiple Domains

- Explain how NDS simplifies configuration of access to multiple domains.

Security Determination from a Single User Account

In the NDS database, each user account exists only once. Because all network resources are in the same database, you do not need to create a user account on each server or domain a user needs to access. As a result, you can determine from a single location what access rights a user has to any network resource.

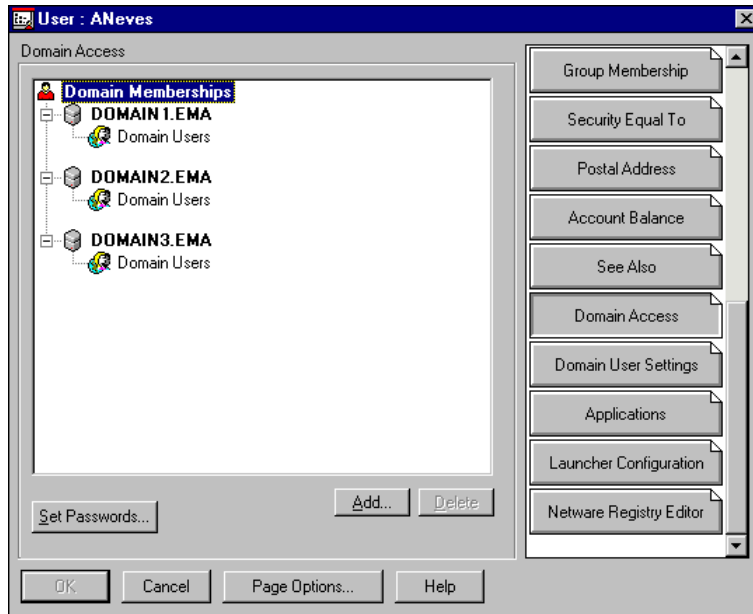


Figure 12-7: Determining All NT Domain Access from a Single NDS User Account

NDS also allows you to remove access to all network resources by deleting a single user account. You can be assured that there are no other accounts (security holes) residing on other servers or domains for that user.



Having a single user object in NDS does not create a single point of failure for network access. Because the NDS database that the user resides in can be partitioned and replicated to as many servers as needed on the network, the user object should always be available.

Presentation

Notes

Security Determination from a Single User Account



12-7 (Figure 12-7:
Determining All NT Domain
Access from a Single NDS
User Account)

- Discuss administering user access from a single location.

Easy Movement of User Accounts

Moving a user account from one domain to another is a cumbersome task under the Windows NT domain system. It involves recording user information on a piece of paper, deleting the user account, and then recreating that account in another domain.

In NDS, because user accounts reside in an administrative container called an organizational unit, moving a user from one organizational unit to another is a simple procedure.

For example, if Bill moves from marketing to engineering, you can move Bill's user account from the marketing organizational unit to the engineering organizational unit. Because the user account was not deleted, all the properties associated with Bill's user account are maintained.

In NDS, users do not need to be moved from one NT domain to another. Windows NT domains are treated as groups to which NDS users can belong. A user can be a member of as many domains as needed.

Per-Object Administration

In Windows NT domains, administrative rights are granted on a per-domain, per-object-type basis. For example, you cannot grant a user administrative rights to just one printer in a domain. You must grant the user administrative rights to all printers in the domain.

In NDS, administrative rights are granted on a per-object basis. Each object has a trustees list that determines other objects' access to that object.

Presentation

Notes

Easy Movement of User Accounts

- Discuss how easily users can be moved with NetWare Administrator.

Per-Object Administration

- Discuss the level to which administration rights can be granted in NDS.

NDS for NT Components and Their Functions

To allow Windows NT domains to be managed from a single NDS database, NDS for NT provides the following components:

- SAMSrv.DLL
- Domain Object Wizard
- Novell NDS for NT Client
- NetWare Administrator
- Mailbox Manager for Exchange

Presentation

Notes

NDS for NT Components and Their Functions

- Introduce the NDS for NT components.

SAMSRV.DLL

An application, such as NetLogon or User Manager for Domains, that needs access to information from the Windows NT domain makes a request to SAMLIB.DLL. This includes applications that run on either a Windows NT Server or a Windows NT Workstation.

Using Remote Procedure Calls (RPC), the SAMLIB.DLL communicates to SAMSRV.DLL. SAMSRV.DLL then accesses the Windows NT Security Accounts Manager (SAM) where the domain database is stored and performs the requested operation.

If an application is running on the Windows NT Server, this process is completed internally. If an application is running on a Windows NT Workstation, RPC requests are sent to the Windows NT Server over the network.

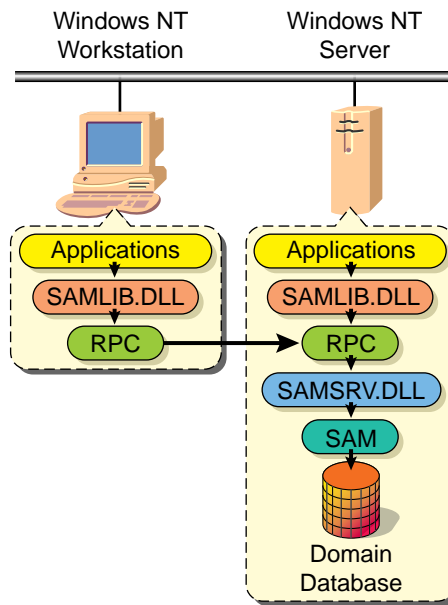


Figure 12-8: Windows NT Server Domain Architecture

Presentation**Notes****SAMSRV.DLL**

12-8 (Figure 12-8: Windows NT Server Domain Architecture)

- Review how the domain database is accessed from Windows NT Workstations and Windows NT Servers before NDS for NT is installed.

NDS for NT renames the original SAMSRV.DLL file to MSSAMSRV.DLL and replaces it with a new DLL. The new DLL uses the original name, SAMSRV.DLL.

The new SAMSRV.DLL from Novell redirects domain access calls to NDS. Thus, NDS can fulfill domain requests for Windows NT Servers, Windows NT Workstations, and applications.

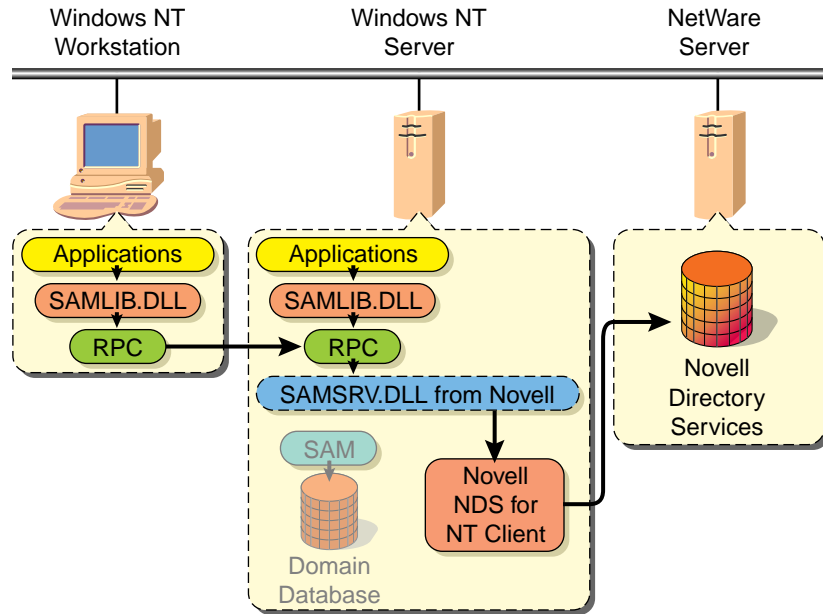


Figure 12-9: NDS for NT Architecture

You must install the new SAMSRV.DLL on every domain controller in the Windows NT domain that you are placing in NDS. You must install NDS for NT on the Primary Domain Controller (PDC) first, and then on every Backup Domain Controller (BDC) to accomplish this.

You do not need to install NDS for NT on member servers of a domain; the member servers are placed in NDS when the domain from the PDC is placed in NDS.

Each time a shutdown is initiated on a Windows NT Server, NDS for NT checks to see if the SAMSRV.DLL from Novell is there; if not, NDS for NT copies it back so it will be available when the Windows NT Server comes up again.

Presentation**Notes****SAMSRV.DLL** *(continued)*

12-9 (Figure 12-9: NDS for NT Architecture)

- Explain how the new SAMSRV.DLL file redirects requests from the domain to NDS.

- Compare domain request redirection to file and print redirection, if needed, to clarify this concept.

Note: The Domain Object Wizard is the component that renames the original SAMSRV.DLL to MSSAMSRV.DLL.

Domain Object Wizard

NDS for NT includes a Domain Object Wizard. The Domain Object Wizard is a graphical user interface that extends the schema of the NDS tree and migrates existing domain objects from the SAM database into NDS. You do not need to recreate the domain objects in NDS.

The Domain Object Wizard needs to be run only once. It executes automatically the first time your Windows NT Server reboots after NDS for NT has been installed.

You can manually launch the Domain Object Wizard from the Start menu at any time. The Domain Object Wizard attempts to associate domain users with NDS users and allows you to specify where to place the Windows NT domain in the NDS tree.

Running the Domain Object Wizard a second time allows you to uninstall NDS for NT.

Novell NDS for NT Client

Novell NDS for NT Client is required for every Windows NT Server needing to run NDS for NT. The client is installed during the NDS for NT installation process. The client can access NDS running on any platform to which NDS has been ported.

NetWare Administrator

NetWare Administrator is a graphical network administration tool that allows you to manage all the network resources in NDS from a single point of administration.

NDS for NT also provides snap-ins that are used by NetWare Administrator to administer domain objects that have been migrated to the NDS tree.

Presentation

Notes

Domain Object Wizard

- Discuss the purpose of the Domain Object Wizard.

Novell NDS for NT Client

- Explain that NDS for NT requires Novell NDS for NT Client.

NetWare Administrator

- Discuss the purpose of NetWare Administrator.

Mailbox Manager for Exchange

Mailbox Manager for Exchange is a snap-in for NetWare Administrator that allows you to create, edit, and delete Exchange mailboxes from within NetWare Administrator.

When changes are made in NetWare Administrator, the changes are automatically synchronized to the Exchange server.

Currently, the Mailbox Manager for Exchange does not automatically synchronize changes made in Microsoft's Exchange Manager to NDS. It does, however, provide the capability to manually synchronize information in the Exchange database with NDS.

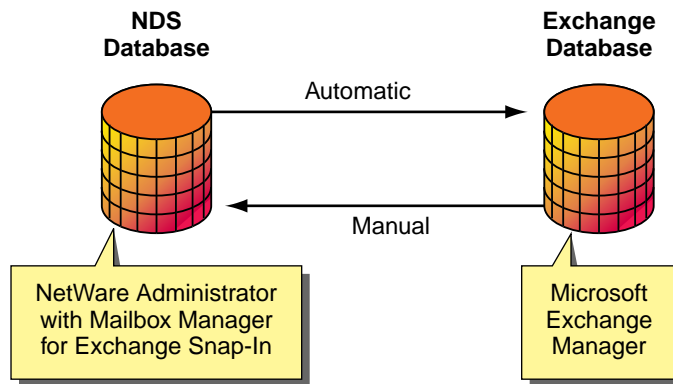


Figure 12-10: Synchronization of NDS and Exchange Databases



For complete training on NDS for NT, contact your nearest NAEC about taking Novell Education Course 555, intraNetWare: Integrating Windows NT.

To locate your nearest NAEC, go to

http://db.netpub.com/nov_edu/x/naecloc

Presentation**Notes****Mailbox Manager for Exchange**

12-10 (Figure 12-10:
Synchronization of NDS and
Exchange Databases)

- Discuss the functionality provided by the Mailbox Manager for Exchange.

- Refer students to Course 555 for more information regarding NDS for NT.

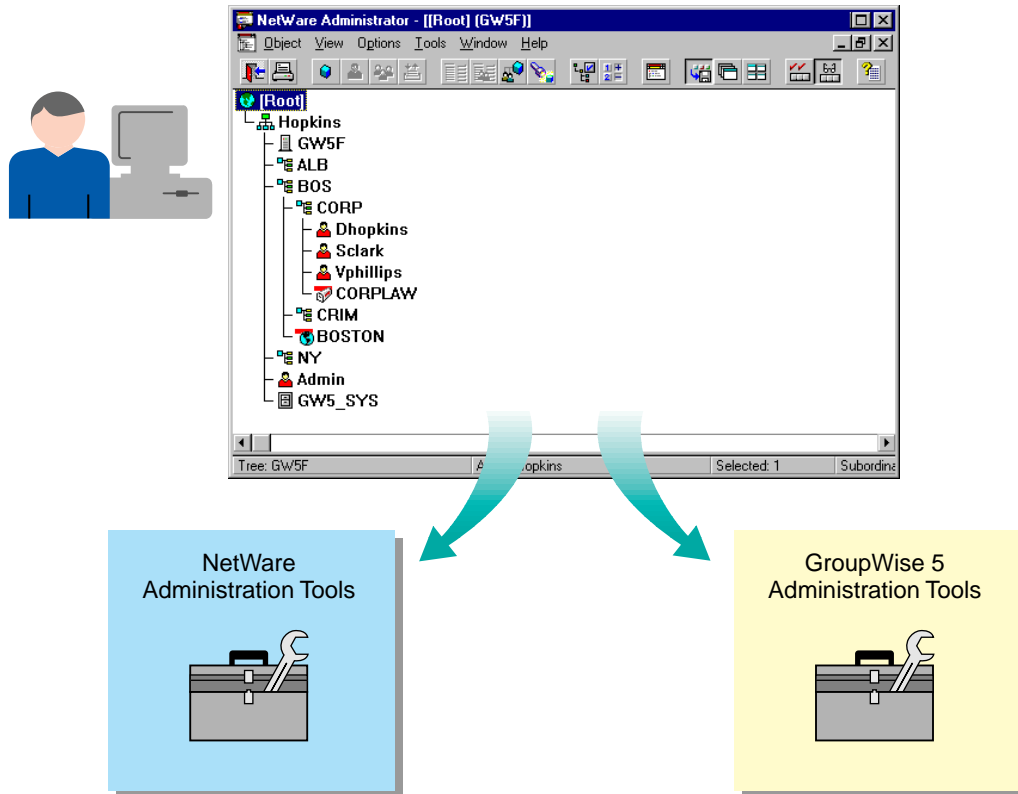


Figure 12-11: Centralized Network and GroupWise Administration

GroupWise 5 and NetWare

GroupWise 5™ is a messaging system that has been integrated with NetWare so that it uses NDS and can be centrally administered through NetWare Administrator.

It also integrates calendaring, scheduling, task management, shared folders, threaded conferencing, workflow, and remote and Internet access.

Using NetWare Administrator, you can administer both NetWare and GroupWise from one application.

GroupWise 5 and NetWare



12-11 (Figure 12-11:
Centralized Network and
GroupWise Administration)

- Introduce GroupWise and its features.

- Emphasize the advantage of administering GroupWise and NetWare from one application.

- Point out that the code added to NetWare Administrator is sometimes called the *GroupWise administration module* or the *snap-in module*.

You can perform the following GroupWise-related tasks using NetWare Administrator:

- Configure and modify the GroupWise system.
- Add, modify, and remove GroupWise properties for network users.
- Modify user properties and user preferences.
- Manage and maintain the message store.
- Run system diagnostics.
- Manage client software.

Two events must occur before you can administer GroupWise from NetWare Administrator:

1. The NDS schema (or database template) must be extended so it can accommodate GroupWise information.

Before GroupWise domains and other information about GroupWise can be added to the NDS database, the schema must be extended to accommodate this information.

GroupWise 5 extends the schema during administration software installation.



Because extending the schema affects the entire NDS tree and cannot be removed, you should back up the NDS tree prior to extending the schema.

2. The GroupWise administration module must be added to NetWare Administrator.

Presentation**Notes****GroupWise 5 and NetWare***(continued)*

- Discuss the GroupWise administration tasks that can be completed through NetWare Administrator.

- Review the steps needed to run GroupWise with NetWare.

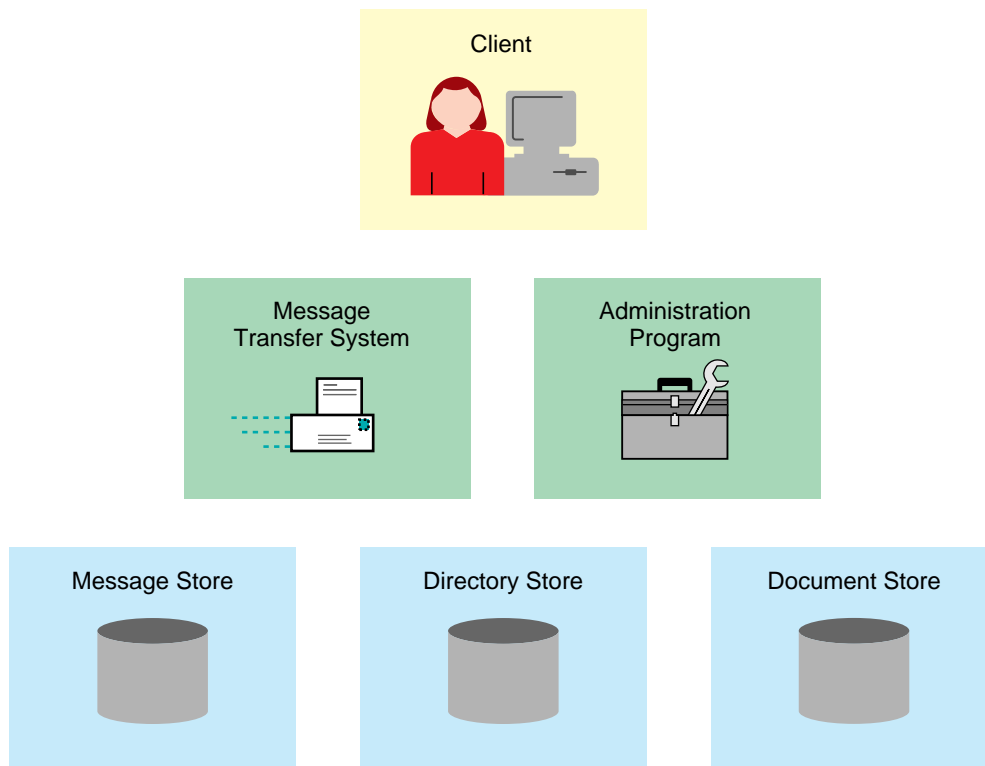


Figure 12-12: GroupWise 5 System Components

GroupWise 5 System Components

Figure 12-12 shows the fundamental components of a GroupWise 5 messaging system. Four of these components—the client, the message transfer system, the message store, and the directory store—are related to message delivery and storage.

The document store is unique to GroupWise. The document store allows documents and files to be stored in GroupWise libraries so they can be shared by members of a workgroup and others on the GroupWise system.

GroupWise 5 System Components



12-12 (Figure 12-12:
GroupWise 5 System
Components)

- Introduce the basic GroupWise 5 components.

The Client

The GroupWise client is the part of the email system that the user sees. Users access the client to

- Create messages
- Send and receive messages
- Manage incoming and outgoing messages
- Manage their personal calendars
- Access documents in a GroupWise library
- Schedule meetings with other GroupWise users

The client is shown in Figure 12-13.

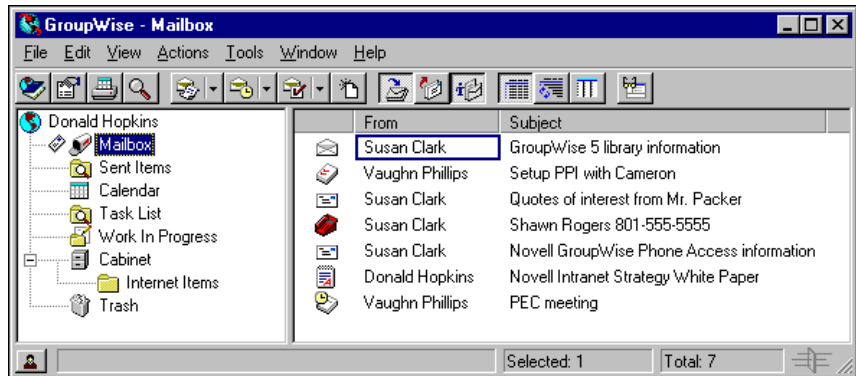


Figure 12-13: GroupWise 5 Client Interface



The GroupWise Client is available for Windows 95, Windows NT Workstation (32-bit), Windows 3.1 (16-bit), Macintosh, and UNIX.

Presentation

Notes

The Client

- Review the functions of the GroupWise client program.



12-13 (Figure 12-13:
GroupWise 5 Client Interface)

The Message Transfer System

The GroupWise 5 message transfer system moves messages from the sender to the recipient and comprises two main components, the message transfer agent (MTA) and the post office agent (POA).

Figure 12-14 illustrates the GroupWise 5 message transfer system.

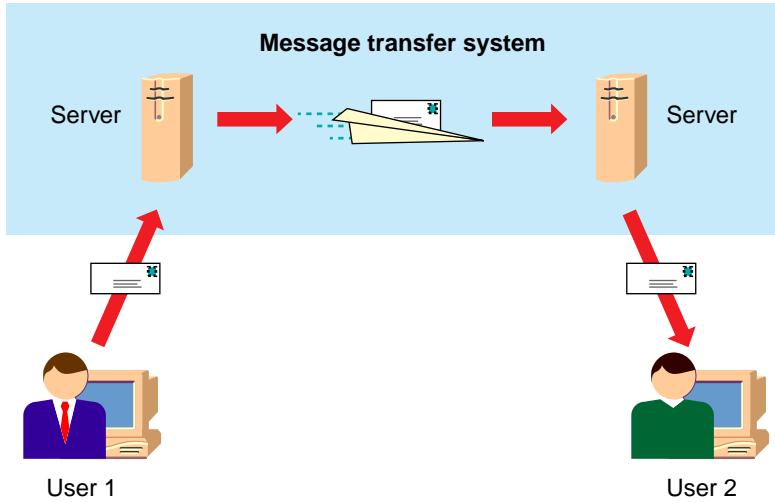


Figure 12-14: GroupWise 5 Message Transfer System

In Figure 12-14, User 1 is sending a message to User 2; however, the users are in different geographical locations and don't share the same server.

When User 1 sends the message, the message transfer system moves the message to a location on a server accessible to User 2.



Gateways are another important part of message delivery. GroupWise gateways are explained in Novell Education Course 354, GroupWise Net Access and Connectivity.

Presentation**Notes****The Message Transfer System**

- Describe how GroupWise transfers messages.



12-14 (Figure 12-14:
GroupWise 5 Message
Transfer System)

- Point out that, depending on the GroupWise system configuration, one or more processes can be involved in message delivery.

GroupWise 5 Administration Program

As a GroupWise system administrator, you use a GroupWise administration component installed in NetWare Administrator to set up and maintain the GroupWise system.

The administration component provides the interface for maintaining the GroupWise system. The GroupWise administration component is part of NetWare Administrator and cannot be used separately.

The Message Store

Email systems store messages for later access by users.

The GroupWise message store holds messages for a GroupWise system. The message store is located on a network server that users can access with the GroupWise Client.

When a GroupWise user sends a message to another GroupWise user, a copy of that message is kept in a message store that can be accessed by the sender.

Email systems that use this method of message storage and transfer are referred to as *store-and-forward* messaging systems.

Presentation**Notes****GroupWise 5 Administration Program**

- Explain that the GroupWise administration component is integrated into NetWare Administrator.

The Message Store

- Explain how the message store is a key component of the messaging system.

A major benefit of email is that messages are sent and processed at the user's convenience. This implies that messages are also stored for access at the user's convenience.

Because GroupWise 5 provides a way for a sender to access messages he or she has sent, often more than one copy of the message must be stored.

Figure 12-15 illustrates how a GroupWise message store functions.

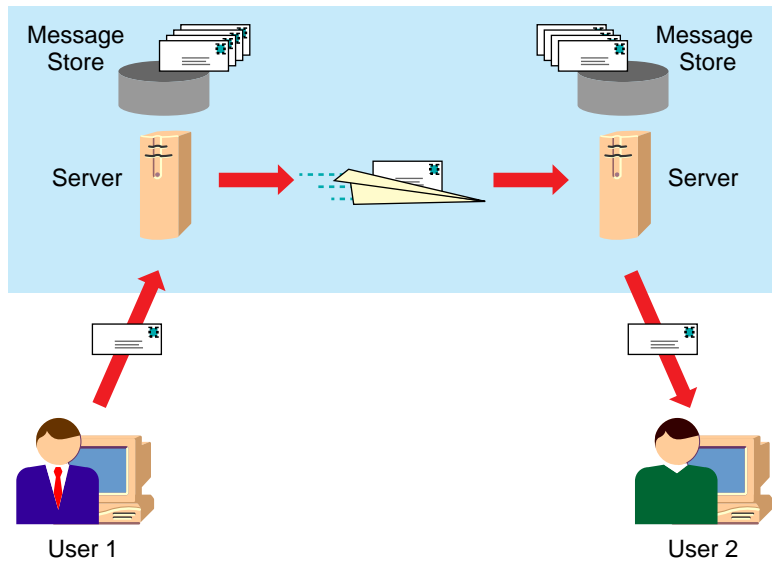


Figure 12-15: Message Stores

GroupWise uses both file-based and database message storage. As a general rule, GroupWise messages are stored in databases; attached files are stored as files in the message store.

Presentation**Notes****The Message Store** *(continued)*

12-15 (Figure 12-15:
Message Stores)

- (Optional) Contrast the GroupWise message storage system with other systems.

Some email systems are file based. In a file-based email system, each message is stored as a file.

GroupWise 5 primarily operates as a database-based messaging system, although it also uses a file-based system for files that are too large to be efficiently stored in a database.

The Directory Store

Novell Directory Services (NDS) functions as the master directory for both NetWare and GroupWise 5. However, GroupWise 5 maintains a separate directory store so the GroupWise components can efficiently access directory information.

The GroupWise directory store is like a telephone directory: It contains the names of all GroupWise users and information about their location in the GroupWise system. It also contains other information such as the user's department and telephone number.

Physically, the directory store is a distributed database. Because the database must be accessed by all email users, it is stored in several locations.

The database is constantly updated with new directory information. Therefore, a mechanism must be available to constantly update all copies of the database.

This process is known as *directory synchronization*.

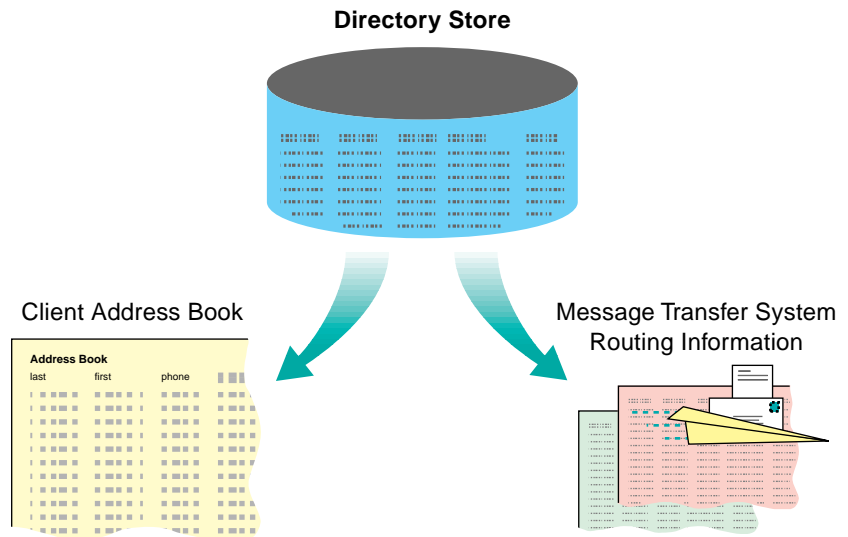


Figure 12-16: The Directory Store

Presentation**Notes****The Directory Store**

- Point out that the GroupWise directory receives information from NDS.



12-16 (Figure 12-16: The Directory Store)

- Emphasize that in this context, the term *directory* refers to a listing of users and other objects.

Students often confuse the term *directory* used in this context with a file storage directory. Make sure students understand that, in this use, *directory* refers to a list of users and their properties.

As shown in Figure 12-16, the directory store serves two purposes:

1. It provides message routing information for the message transfer system.
2. It provides information for the GroupWise Address Book.

When a GroupWise component needs directory information, the component reads the GroupWise directory, not NDS.

Figure 12-17 shows the relationship between NDS and the GroupWise directory.

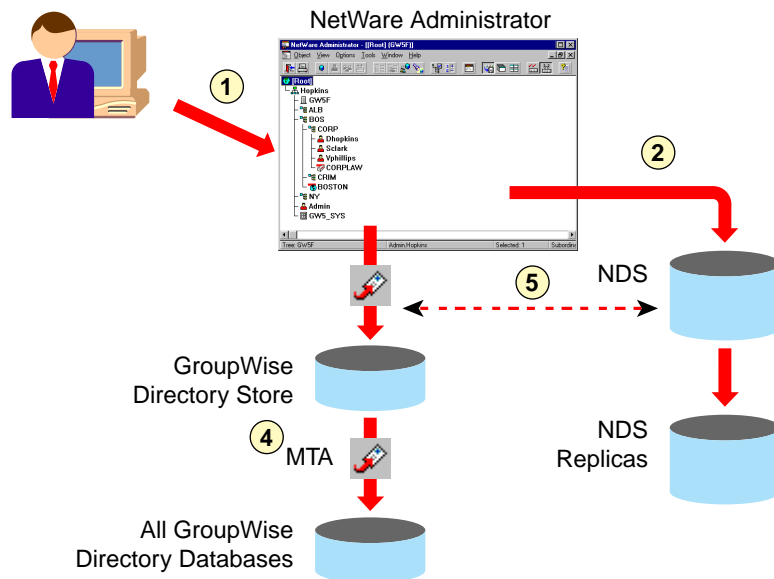


Figure 12-17: NDS and GroupWise Directory

These events occur when GroupWise information is added:

1. The Administrator uses GroupWise Administrator in NetWare Administrator to add, modify, or delete a GroupWise object in a single-domain, single-post office GroupWise system.
An object could be a GroupWise user, resource, distribution list, post office, secondary domain, and so on.
2. The information is stored in NDS and replicated to other NDS replicas.

Presentation**Notes****The Directory Store** *(continued)*

- Explain the purpose of the GroupWise directory store.



12-17 (Figure 12-17: NDS and GroupWise Directory)

- Explain the steps in the graphic.

3. NetWare Administrator writes an administrative message to the current domain's administration input queue.
4. The MTA updates the GroupWise directory store.
5. Changes made to NDS that also affect the GroupWise directory, such as changing a user's telephone number, are automatically synchronized between GroupWise and NDS.

Message Delivery Information

The GroupWise 5 message transfer system uses information in the directory store to determine how to deliver messages to their intended recipients.

For example, suppose a GroupWise user sends a message to user KWilliams. The message transfer system uses the information contained in the directory store to determine where KWilliams is located and then moves the message to KWilliams' message store.

Address Book

The GroupWise 5 directory store provides information for the GroupWise Address Book so users can easily find other user addresses in the GroupWise system and send messages to them.

The Document Store

GroupWise 5 provides document management capabilities through GroupWise libraries. A GroupWise library is a shared location for documents and files used by a workgroup.

The GroupWise document store holds the documents contained in GroupWise libraries.

Presentation**Notes****The Directory Store** *(continued)*

- Explain that the message transfer system reads the directory store to determine how to deliver a message.

- Explain that the Address Book obtains its directory information from the directory store database.

The Document Store

- Explain that the document store houses documents stored in GroupWise libraries.

How the GroupWise System Components Work Together

Figure 12-18 shows how basic GroupWise 5 components work together.

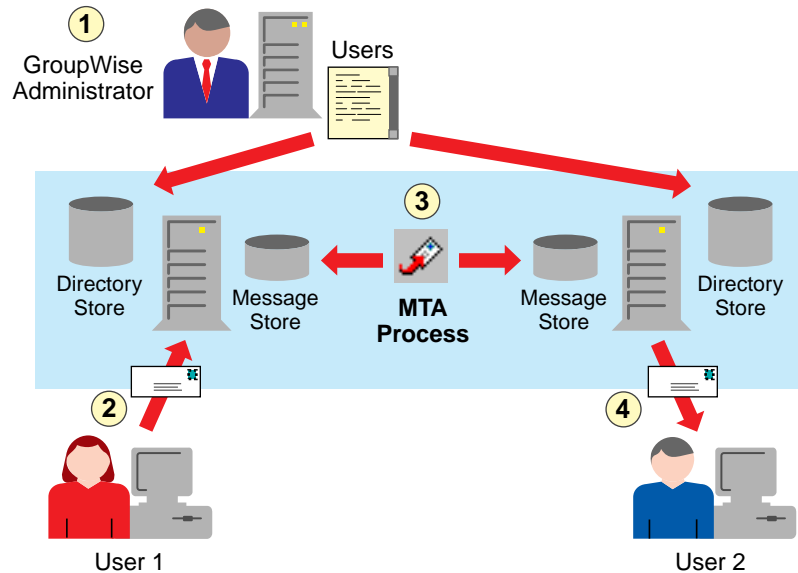


Figure 12-18: Role of GroupWise Components

1. The GroupWise administrator uses NetWare Administrator to add the information for User 1 and User 2 to the system. This information is added to the directory store databases.
2. User 1 uses the GroupWise 5 client and Address Book (directory store) to create and send a message.
3. The message transfer system moves the message to a message store that User 2 can access. The message transfer system uses the information in the directory store to transfer the message to User 2.
4. User 2 uses the client program to read the message in the message store.



For complete training on GroupWise, contact your nearest NAEC about taking Novell Education Course 350, GroupWise 5 Administration.

To locate your nearest NAEC, go to

http://db.netpub.com/nov_edu/x/naecloc

How the GroupWise System Components Work Together



12-18 (Figure 12-18: Role of GroupWise Components)

- Explain how GroupWise components work together to provide messaging services.

- Refer students to Course 350 for more information regarding GroupWise 5.

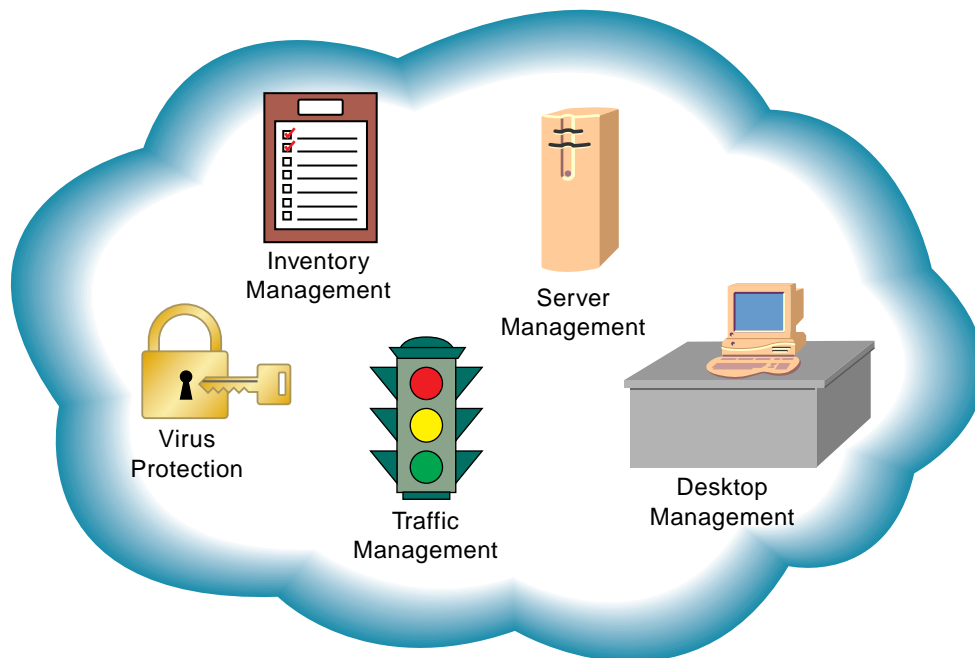


Figure 12-19: Primary Network Management Features of ManageWise

Network Management Using ManageWise

ManageWise allows you to manage and control a NetWare environment comprising different operating systems, desktops, and applications, and to maintain network reliability and optimum performance.

ManageWise can support you in the following tasks:

- Asset inventory and management
- Server monitoring and management
- Desktop management
- Network traffic analysis and management
- Network-wide virus protection

Network Management Using ManageWise



12-19 (Figure 12-19: Primary Network Management Features of ManageWise)

- Introduce ManageWise.

Refer to the graphic as you discuss the bulleted ManageWise tasks.

ManageWise helps network administrators perform the following tasks:

- Gather information:
 - Inventory the existing network system.
 - Monitor network devices.
 - Gather information for evaluating system performance.
- Analyze data:
 - Perform network analysis, including analysis on early warning systems.
 - Identify existing and potential network problem areas.
 - Identify performance bottlenecks, bad equipment or configurations, and solutions to network problems.
- Complete repairs:
 - Gather information about real-time problem notification, diagnosis, and solutions.
 - Re-engineer or expand existing systems and replace inadequate systems.
- Perform preventative maintenance:
 - Install an integrated, network-wide virus protection system.
 - Remotely access, manage, and troubleshoot network devices.

Asset Inventory and Management

You need network inventory information for troubleshooting problems, for creating inventory reports, and for planning upgrades.

ManageWise automatically tracks specific hardware and software components on all the segments of the network, reducing time-consuming inventory processes. It automates the information-gathering process and notifies you of changes.

ManageWise provides the following asset management features:

- **Automatic discovery**

ManageWise automatically discovers network devices—such as routers, servers, and workstations—regardless of protocols.

- **Integrated graphical maps**

The graphical maps display the devices on the network. The maps also provide links to tools used to monitor and manage devices.

- *Internetwork maps* (Figure 12-20) provide overviews of the network topology.
- *Segment maps* (Figure 12-21) display all the stations on a specific segment of the network.
- *Custom maps* (Figure 12-22) can be set up to show the geographical location of sites and devices.

- **Hardware and software inventory**

ManageWise automatically scans each node for component information, such as processor type, memory size, and installed software applications. You can also define and search for supplemental information during an asset scan.

- **IPX and IP address management**

ManageWise facilitates the management of IPX and IP network addresses by displaying a tabular report of network numbers in use and other information.

ManageWise identifies assigned addresses, helping you avoid duplications when you are adding new nodes to the network. ManageWise also identifies duplicate addresses to quickly isolate offending nodes.

Presentation

Notes

Asset Inventory and Management

- Describe the main features of ManageWise.

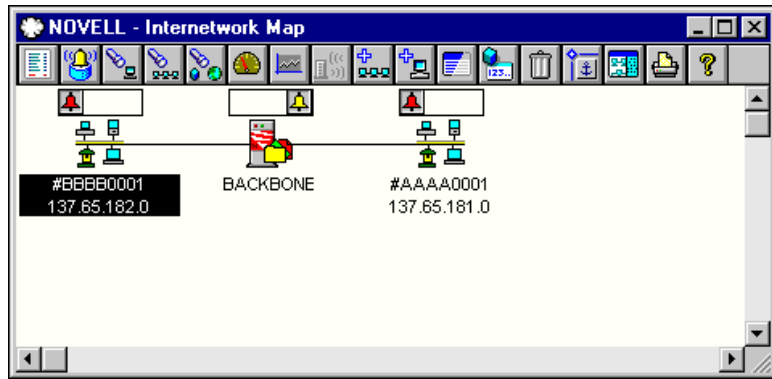


Figure 12-20: Internetwork Map

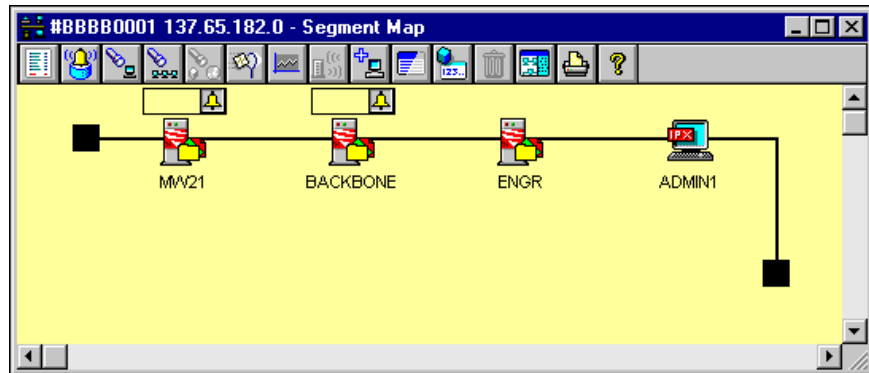


Figure 12-21: Segment Map

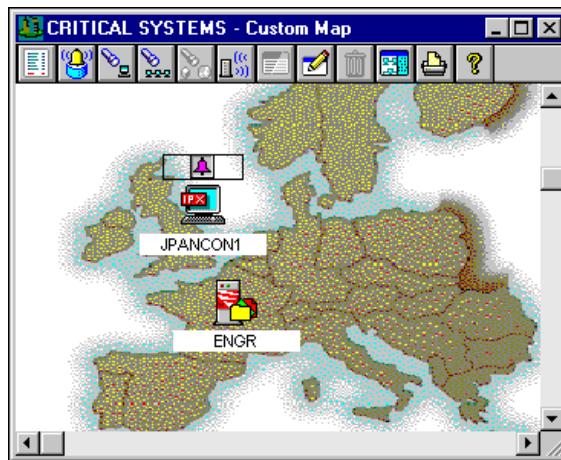


Figure 12-22: Custom Map

Presentation**Notes****Asset Inventory and Management***(continued)*

12-20 (Figure 12-20:
Internetwork Map)



12-21 (Figure 12-21:
Segment Map)



12-22 (Figure 12-22: Custom
Map)



Discuss the maps.

Server Monitoring and Management

If one or more servers are down, users cannot get their jobs done. Also, because servers often provide centralized data storage, information loss or corruption due to system failure can be costly.

ManageWise monitors more than 2,000 server conditions on NetWare servers. ManageWise continuously monitors the servers and pinpoints problems.

You can use ManageWise to chart trends, gather performance statistics, set thresholds to trigger alarms, and receive alarms.

ManageWise can help you perform the following NetWare server management tasks:

- **Multiple server management**

When you install ManageWise on every server, you can monitor, maintain, and manage your servers from a central site. You can compare multiple servers to optimize server configuration and performance.

- **Unattended monitoring**

ManageWise monitors NetWare servers 24 hours a day, 7 days a week. ManageWise will alert you before problems reach a critical state. You can customize alarm thresholds for such things as file activity, memory usage, and logged-in users.

- **Server optimization**

ManageWise allows you to monitor trends in server performance. It monitors such things as file activity, volume data, disk drive configuration, total packets, CPU utilization, memory, and print services. You can also analyze data collected from servers and take the necessary action.

- **Print queue monitoring**

ManageWise monitors and manages print queues on the network. It displays network print queue activity in tabular format and graphical format.

Figures 12-23 and 12-24 show two of the many reports you can create to help you manage and monitor your servers.

Presentation

Notes

Server Monitoring and Management

- Describe the NetWare server management features of ManageWise.

#BBBB0001 137.65.182.0 - Alarm Report

Se	Ac	Not	Receive Time	Affected No	Type	Summary
			2/20/97 6:10:33 PM	ADMIN1	Response Resumed	Target ADMIN1 at address BBBB0001:00C04FC9D4A9
			2/20/97 6:10:32 PM	ADMIN1	Response Resumed	Target ADMIN1 at address BBBB0001:00C04FC9D4A9
			2/19/97 10:53:38 AM	MW21	System: NLM loaded	NetWare 4.1 Remote Console NLM loaded on server
			2/19/97 7:01:01 PM	BACKBONE	Threshold - wait time of	Wait time of next ready job in queue 276 CN=Default
			2/19/97 11:54:14 AM	#BBBB0001	Rising Alarm	Multicasts exceeded 5 in 60 seconds on segment: #
			2/19/97 11:41:53 AM	#BBBB0001	Rising Alarm	Multicasts exceeded 5 in 60 seconds on segment: #
			2/19/97 11:15:11 AM	#BBBB0001	Rising Alarm	Multicasts exceeded 5 in 60 seconds on segment: #
			2/19/97 11:10:14 AM	#BBBB0001	Rising Alarm	Multicasts exceeded 5 in 60 seconds on segment: #
			2/19/97 10:56:53 AM	#BBBB0001	Rising Alarm	Multicasts exceeded 5 in 60 seconds on segment: #
			2/19/97 10:30:36 AM	MW21	System: NLM loaded	NetExplorer Console Utility NLM loaded on server MW
			2/19/97 10:29:18 AM	MW21	System: NLM unloaded	NetExplorer Console Utility NLM unloaded on server MW

2/20/97 6:10:33 PM Informational ADMIN1
 Response Resumed
 Target ADMIN1 at address BBBB0001:00C04FC9D4A9 started responding.
 Node Type: Workstation: IPX
 Agent Address: AAAA0001:00C04FC2F80C
 Unacknowledged

Figure 12-23: Alarm Report

BACKBONE - NLMs

Name	Version	Released	Memory (B)	Description	Copyright
SERVER.NLM	4.11	8/22/96	3,142,384	NetWare Server Operating System	
DS.NLM	5.73	7/29/96	728,872	NetWare 4.11 Directory Services	Copyright
NTREND.NLM	1.00	6/27/96	682,563	NetWare 4.x Trending MIB	Copyright
BTRIEVE.NLM	6.10f	5/3/96	643,168	Btrieve NLM	
PSERVER.NLM	4.15	5/10/96	490,004	NetWare 4.15 Print Server	Copyright
IPXRTR.NLM	5.07c	6/25/96	404,983	IPX NLSR Router	(c) Copyri
TCPIP.NLM	3.05d	5/28/96	360,370	Novell TCP/IP Module	Copyright
LANZMEM.NLM	1.10c	9/5/96	353,569	NetWare LANalyzer Agent (v1.10c), Memory Manager	Copyright
SERVER.NLM	0.00		347,040	Protected Alloc Memory	
THREADS.NLM	4.11	8/29/96	298,144	NetWare NLM Threads Package	Copyright

Total: 66 Code and Data memory: 11,135 KB

Figure 12-24: NLM Report

Presentation

Notes

Server Monitoring and Management

(continued)



12-23 (Figure 12-23: Alarm Report)



12-24 (Figure 12-24: NLM Report)

- Discuss the reports.

Desktop Management

In addition to monitoring your servers, ManageWise monitors your client workstations as well.

ManageWise includes a copy of Z.E.N.works™ for desktop management. Z.E.N.works stands for Zero Effort Networks.



For more training regarding Z.E.N.works, contact your nearest NAEC about taking Novell Education Course 560, NetWare 5 Administration, or Course 780, Managing Workstations Using Z.E.N.works.

Network Traffic Analysis and Management

Using ManageWise, you can analyze network traffic when you are concerned about the speed of the network. You can also analyze traffic when the network performs unreliably.

ManageWise allows you to analyze network traffic through the NetWare LANalyzer Agent™ software. You can then detect and troubleshoot many network problems before they cause expensive downtime.

ManageWise can perform the following network management tasks:

- **Traffic analysis**

ManageWise identifies nodes that are generating the greatest demand on network resources and shows you exactly what the devices are doing to create that demand.

You can identify overloaded network devices or segments, or users generating significant traffic, and rebalance the network load.

Presentation

Notes

Desktop Management

- Explain that desktop management in ManageWise is accomplished through Z.E.N.works.

Network Traffic Analysis and Management

- Describe the main features listed on the student page.

- **Detailed troubleshooting**

ManageWise monitors the traffic and alerts you to potential problems such as network errors, duplicate IP addresses, or network overload.

You can capture packets and analyze them to determine if certain error conditions exist on the network.

- **Common network and protocol support**

ManageWise supports multiple networks, including Ethernet, token ring, and variants of these standards, such as 100 Base-T and 100 VG-AnyLAN.

Along with supporting common hardware standards, ManageWise supports common network protocols such as IPX, NetWare/IP™, TCP/IP, AppleTalk®, and Systems Network Architecture (SNA).

Figures 12-25, 12-26, and 12-27 show three different network traffic analysis utilities: the Segment Trends graph, the Network Dashboard, and the Top Stations report.

Presentation

Notes

Network Traffic Analysis and Management *(continued)*

- Continue describing the main features listed on the student page.

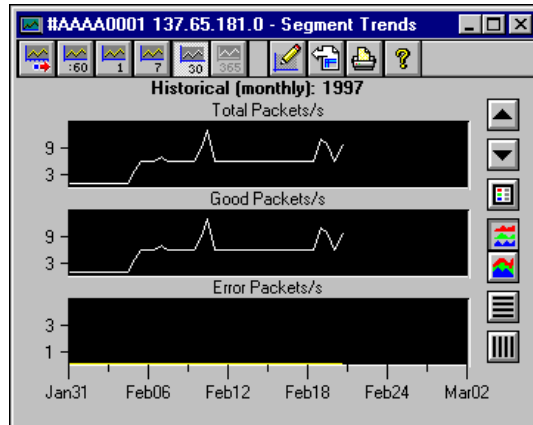


Figure 12-25: Segment Trends Graph

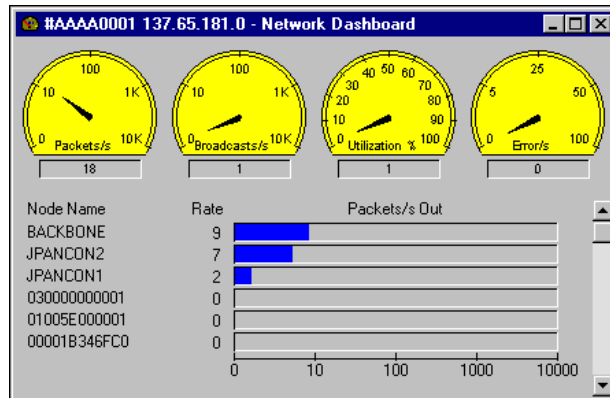


Figure 12-26: Network Dashboard

Node	Util. %	Pkts/s Out	Bytes/s Out	Errors/s	Pkts/s In	Bytes/s In
BACKBONE	1	4	452	0	4	427
JPANCON2	1	3	507	0	2	374
JPANCON1	1	2	107	0	2	107
030000000001	0	0	0	0	0	0
01005E000001	0	0	0	0	0	0
00001B346FC0	0	0	0	0	0	0
Broadcast	0	0	0	0	1	21

Figure 12-27: Top Stations Report

Presentation**Notes****Network Traffic Analysis and Management** *(continued)*

12-25 (Figure 12-25:
Segment Trends Graph)



12-26 (Figure 12-26: Network
Dashboard)



12-27 (Figure 12-27: Top
Stations Report)

- Discuss the graphics.

Network-Wide Virus Protection

Because viruses can destroy data and cause expensive downtime, virus protection is critical to your business.

ManageWise provides virus protection for the NetWare server and workstations. It provides the following features:

- **Comprehensive scanning**

ManageWise maintains network integrity by monitoring for viruses on all the workstations and servers on the network. It uses sophisticated pattern-based scanning to identify known viruses.

It uses intelligent rules-based detection capabilities to identify virus-like behavior of viruses designed to hide from scanners.

- **Continuous real-time protection**

ManageWise checks for infected files during:

- File transfers to and from the server
- Prescheduled and on-demand scanning of servers
- Continuous scanning of the workstation or at login

- **Workstation and mobile computer protection**

Whenever you log in to the network, ManageWise automatically checks for virus activity. It updates the server log and the virus pattern files on your workstation or mobile computer.

- **Automatic maintenance**

ManageWise can be configured to automatically quarantine, rename, clean, or delete infected files.

Presentation

Notes

Network-Wide Virus Protection

- Describe the main features listed on the student page.

ManageWise Software Components

Now that you have seen the various tasks that ManageWise can perform, refer to the following table to learn the software components that provide the functionality.

ManageWise Software Component	Network Management Task	Function of Software Component	Location
NetExplorer™	Asset Inventory and Management	Creates and manages the inventory database	Runs on at least one server on the internetwork
NetWare Management Agent™	Server Monitoring and Management	Allows servers to be remotely managed	Runs on each server
Z.E.N.works	Desktop Monitoring and Management	Allows workstations to be remotely controlled and managed	Contains elements that run on workstations and servers
NetWare LANalyzer Agent	Network Traffic Analysis and Management	Gathers segment statistics and captures packets for troubleshooting purposes	Runs on one server for each segment
Virus Protect	Network-Wide Virus Protection	Provides virus protection for the network	Contains elements that run on workstations and servers

Table 12-2: ManageWise Software Components

Presentation**Notes**

ManageWise Software Components

- List the ManageWise components and explain the purpose of each:
 - NetExplorer
 - NetWare Management Agent
 - Z.E.N.works
 - NetWare LANalyzer Agent
 - Virus Protect

Another important software component, ManageWise Console, provides the graphical user interface (GUI) that allows you to manage your network.

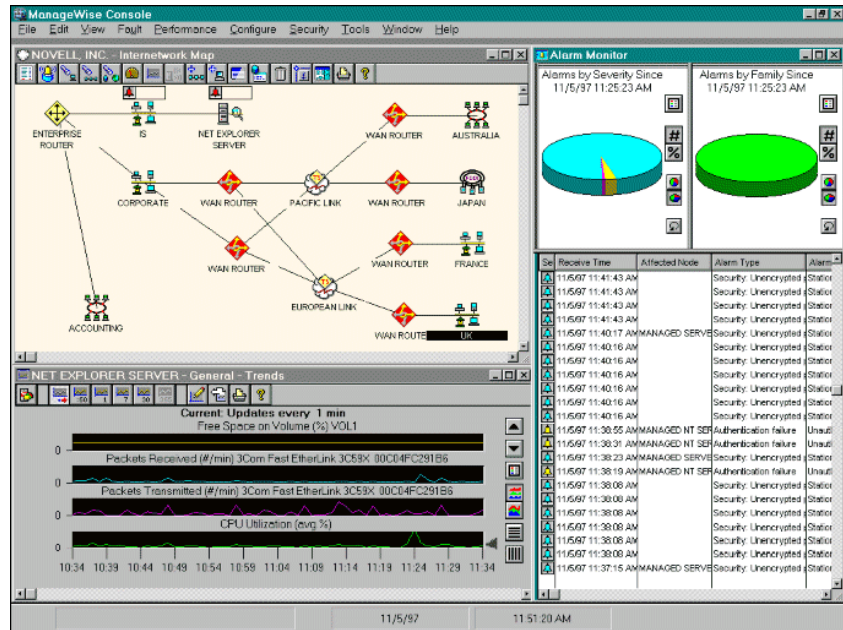


Figure 12-28: The ManageWise Console



For complete training on ManageWise, contact your nearest NAEC about taking Novell Education Course 730, Network Management Using ManageWise.

To locate your nearest NAEC, go to

http://db.netpub.com/nov_edu/x/naecloc

Presentation**Notes****ManageWise Software Components** *(continued)*

- Explain that ManageWise Console provides the graphical user interface for ManageWise.



12-28 (Figure 12-28: The ManageWise Console)

- Refer students to Course 730 for more information regarding ManageWise.

Summary

This section previewed the following key networking solutions offered by Novell:

- BorderManager securely ties your organization's network to the Internet using firewalls and performance accelerators.
- By integrating the NT domain into NDS, NDS for NT creates a single directory from which to manage all components of your network.
- GroupWise 5 is a messaging system that has been integrated with NDS. It provides email, calendaring, scheduling, task management, shared folders, threaded conferencing, workflow, and remote and internet access.
- ManageWise allows you to manage and control your NetWare environment and to maintain network reliability and optimum performance.

Presentation**Notes****Summary**

- Summarize the section.

Review the objectives and answer questions.

Objectives:

1. Identify networking solutions offered by Novell.
2. Explain the benefits of securing your network with BorderManager.
3. List the components of a firewall.
4. Identify the firewall components of BorderManager.
5. Explain the benefits of placing Windows NT domains into NDS.
6. Explain the purpose of the components of NDS for NT.
7. Describe how GroupWise integrates with NetWare.
8. List the basic components of a GroupWise system and describe the function of each component.
9. Explain how GroupWise components work together to provide GroupWise messaging services.
10. Describe the major features of ManageWise.
11. Identify the components of ManageWise.

Notes

APPENDIX A Answers to Exercises

This appendix contains the answers to student exercises used in this course.

Section 1

Exercise 1-2

6. This user is no longer the supervisor of the NetWare 5 server. The Admin object now controls the NDS tree.

Section 2

Exercise 2-1

3. **Console Commands**

CLS: Clears the console screen

VERSION: Displays the file server version and copyright information

SPEED: Displays the processor speed of the server

MEMORY: Displays the amount of server RAM that the kernel recognizes as being available for use

VOLUME: Displays a list of currently mounted volumes along with the name space supported on each volume

TIME: Displays the current date and time set on the server

MODULES: Displays a list of NLMs that are currently loaded in server memory

- 4d. Minimum Service Processes should be set to 60 by default

Exercise 2-2

- 6c. SOUND BELL FOR ALERTS should have been set to OFF.

Exercise 2-5

- 3a. Press **Alt+F1** to bring up the Available Options menu.
- 3c. Press **Alt+F2** to bring up the RCONSOLE Exit menu.
- 3e. Press **Alt+F3** to toggle through the running NLM screens in reverse order of what they would appear when toggling through them while actually at the console using Alt + Esc.
- 3f. Press **Alt+F4** to toggle through the running NLM screens in the same order as they would appear when toggling through them while actually at the console using Alt+Esc.
- 3g. Press **Alt+F5** to display the workstation address of the machine from which you are running RCONSOLE.

Section 3

Exercise 3-2

10. Status indicates that the job is being held.
12. Answers vary.
13. A default date ensures the file will print. NetWare Administrator sets the target date and time to the date and time the print job entered the print queue. PCONSOLE sets the print date and time to the next day at midnight.
14. Answers vary.
17. The last job is now first.

Section 5

Exercise 5-4

Observations might include the following:

- The utilization value changes, based on the activities performed in Step 4.
- Running NetWare Administrator causes a load on the processor and should result in an increase in the processor utilization value.
- The Long-Term Cache Hits value might not change drastically based on this one activity; the Long-Term Cache Hits value is affected only by excessive activity.
- Step 8 demonstrates the context-sensitive Help feature.

Exercise 5-5

Answers for MONITOR Information:

1. Utilization is 100%.
2. Determine if the network board is performing adequately or if an ill-behaved NLM exists.

Action is only required if utilization remains at 100% for an extended period and workstation performance is noticeably degraded.

Answers for Cache Utilization:

1. The Long-Term Cache Hits percentage is below 90%.
2. Add more RAM (most effective), unload noncritical NLMs (less effective), or remove DOS (least effective) to free memory.

Answers for network board statistics:

1. The "Receive discarded, no available buffers" count is high, in relationship to the "Total packets received" count.
2. Increase the packet receive buffer settings. The server might also need to be upgraded with a faster CPU or additional RAM.

Exercise 5-6

Answers:

1. Increased throughput; therefore, increased performance.
2. Yes. Increased throughput might be significant because of the reduction of the large number of reads and writes occurring with small files.
3. Yes, if the files are larger than 512 bytes.

Section 6

Exercise 6-1

Answers:

1. Windows 95 and Windows NT workstation file systems
NetWare file systems
NetWare DOS partitions
NDS
GroupWise databases
2. A full backup combined with incremental backups will back up only modified data from day to day. A full backup combined with differential backups will back up all data changed since the last full backup.
3. The full backup combined with incremental backups
4. Browse object and Read property rights to the container being backed up. Read and File Scan rights to the directories and files being backed up.

Section 9

Exercise 9-2

Part I

- 1d. Supervisor and Inheritable object rights.
- 1e. The users who are occupants of the organizational role object will have Supervisor object rights to all objects in the container and sub-containers (if any).
- 1f. Supervisor object right.
The Supervisor object right assigned to the organizational role at the organizational unit object flows down to the server object because the server object is in the organizational unit and the user has been granted the Inheritable object right which allows the user to inherit rights to objects in the container.
- 1g. Yes. The Supervisor object right to the server object gives the administrator Supervisor rights to the file system on all volumes attached to that server object.
- 8j. All rights including Supervisor.

Part II

3. An explicit rights assignment of Compare and Read property rights [CR] to the Object Trustees (ACL) property removes the Supervisor file system right from the volumes connected to the server.
The explicit rights assignment also takes away the ability of the user object to create trustees for the server object or to assign Supervisor rights to himself or herself.
4. The LMcCarter user has the Browse object right and JLeckie has all object rights [SBCRD].
LMcCarter's rights come from the Manager object, which was made a trustee in Step 2. JLeckie's rights come from the explicit assignment made in Part I, Step 6.

Part III

5. Neither user has the Supervisor object right. The LMcCarter user has Browse object rights and JLeckie has all object rights except Supervisor [BCDR].

Yes. This will affect both users' file system rights. LMcCarter and JLeckie will no longer have Supervisor rights in the file system.

Part IV

2. All rights including Supervisor.

Both users will have all rights to the files and directories in the volumes on the server.

Section 10

Exercise 10-1

2. Answers vary.
7. Answer vary. Three errors commonly generated in class are -621, -625, and -701.

8. Here are answers for three error codes:

Error Description
-621 FFFFFFFD93 TRANSACTIONS DISABLED TTS has been disabled.
Possible Actions
At the server, type ENABLE TTS. Run VREPAIR on the SYS: volume.

Error Description
-625 FFFFFFFD8F TRANSPORT FAILURE The server is unable to communicate across the network.
Possible Actions
Check for SAP filtering. Type DISPLAY SERVERS at the server console. Attach and log in to the target server. In NDS Manager, determine if every server reports an error on the target. Run DSREPAIR to repair network addresses on the source server.

Error Description
-701 FFFFFFFD43 SYNCHRONIZATION DISABLED Schema synchronization has been disabled.
Possible Actions
Type SET DSTRACE =!S1 to enable schema synchronization.

Section 11

Exercise11-2

1. Windows clients with minimal login scripts and shortcuts to folders.
2. Use faster modems, install applications locally, ensure aggressive use of file compression.
3. Ensure that sufficient memory and CPU resources are available. Consider using a faster transmission technology. Answers will vary.

APPENDIX B NDS Security Review Exercise

NDS Security Concepts List

1. Security Equal to Container Objects
2. Object Trustee
3. Similarities and Differences Between NDS and File System Security
4. Object Rights
5. Object and Property Rights Inheritance
6. Blocking Inheritance with New Trustee Assignment
7. Property Rights
8. All Properties versus Selected Properties
9. Supervisor Object Right to the Server Object
10. Object Trustees (ACL) Property
11. Blocking Inheritance—Inherited Rights Filter (IRF)
12. Effective Rights

Security Equal to Container Objects

In NDS, a user object is security equivalent to the containers the user object resides in. As a result, when the container is made a trustee of an object, the user object receives the rights granted to the container.

You can use security equivalence to create *natural groups* based on containers.

A user object is security equivalent to all parent containers in which the user object resides, up to and including [Root].

You should consider using containers as groups to assign rights to network resources when you design your Directory tree.

Give examples and elaborate on the concept.

Object Trustee

An Object trustee is an NDS object that is placed in the Object Trustees (ACL) property of another object.

Each object in the Directory has an Object Trustees (ACL) property that records the trustees who can manipulate that object and who can access or change information stored in the object properties.

Give examples and elaborate on the concept.

Similarities and Differences Between NDS and File System Security

Similarities with file system security:

- Trustees
- Rights
- Inheritance
- Inherited Rights Filter (IRF)
- Effective rights

As in file system security, a user must be made a trustee to an object and then granted rights in order to access the object or its properties.

NDS security differs from file system security in the following ways:

- It has two distinct sets of rights: object and property.
- Rights do not flow from NDS into the file system except in one instance—when Supervisor object rights are assigned to the server object.
- Both the Supervisor object right and the Supervisor property right can be blocked in NDS security by an Inherited Rights Filter (IRF).

Give examples and elaborate on the concept.

Object Rights

Object rights control what a trustee can do with the object, such as viewing, renaming, or deleting the object. These rights control the object as a single piece in the NDS tree. Object rights control access to the object but not to the object's property values.

You must be a trustee of an object to be granted rights to the object.

Object rights include the following:

- Supervisor. Grants all access privileges. A trustee with the Supervisor right has access to all properties.
- Browse. Grants the right to see the object in the NDS tree.
- Create. Grants the right to create a new object below this object in the NDS tree. This right is only available on container objects.
- Delete. Grants the right to delete the object from the NDS tree.
- Rename. Grants the right to change the name of the object, in effect changing the name property.
- Inheritable. Grants the right to inherit all other assigned object rights to objects and subcontainers in a container. This right is only available on container objects.

Give examples and elaborate on the concept.

Object and Property Rights Inheritance

NDS, like the file system, uses rights inheritance. Inheritance minimizes the individual rights assignments needed to administer the network.

Since NDS is a hierarchical structure, rights flow downward from a container to subcontainers unless the Inheritable right is revoked.

Property rights can be inherited. However, in the case of property rights, only rights assigned through the All Properties option are automatically inherited.

Rights assigned through the Selected Properties option are not automatically inherited because each object has different properties. However, rights to selected properties of container objects can be inherited to subcontainers when the Inheritable property right is manually granted to a specific property. The Inheritable property right is only available in container objects.

Give examples and elaborate on the concept.

Blocking Inheritance with New Trustee Assignments

If object rights are granted at a higher level in the Directory tree, a new trustee assignment at a lower level in the tree will change the user's rights from that level down.

Making a new trustee assignment is especially useful for overwriting property rights granted with the All Properties option.

Rights granted to a particular property through the Selected Properties option overwrite property rights granted through the All Properties option to that particular property.

Give examples and elaborate on the concept.

Property Rights

Property rights control access to the information stored within the object properties. They allow users to see, search for, or change values stored in the object properties. You must be a trustee of an object to be granted property rights.

Property rights include the following:

Supervisor. Grants all rights to the property.

Compare. Grants the right to compare any value to a value of the property. An operation can return True or False, but you cannot see the value of the property.

Read. Grants the right to read the values of the property. The Read right includes the Compare right.

Write. Grants the right to add, change, or remove any values of the property. The Write right includes Add Self.

Add Self. Grants a trustee the right to add or remove itself as a value of the property. This right is only meaningful for properties that contain object names as values, such as group membership lists and mailing lists.

Inheritable. Grants the right to inherit all other assigned property rights to objects and subcontainers in a container. This right is only available on container objects.

Give examples and elaborate on the concept.

All Properties versus Selected Properties

Property rights for all properties of an object can be set at the same time using the All Properties option.

Property rights can be granted independently for each property with the Selected Properties option.

Rights granted through Selected Properties overwrite property rights granted through All Properties for the selected property.

Give examples and elaborate on the concept.

Supervisor Object Rights to the Server Object

The Supervisor object right to the server object gives Supervisor file system rights to all volumes linked to that server.

The Supervisor object right assignment should only be made after considering the implications of a network administrator having access to all files on all volumes linked to a particular server.

The Supervisor object right to the server object can also be obtained by assigning Supervisor object rights to the container in which the server object resides.

Give examples and elaborate on the concept.

Object Trustees (ACL) Property

The Write property right to the Object Trustees (ACL) property effectively gives the trustee the ability to grant anyone, including himself or herself, all rights, including the Supervisor right.

This is another reason to use extreme care when making rights assignments with All Properties.

Give examples and elaborate on the concept.

Blocking Inheritance—Inherited Rights Filter (IRF)

NetWare 4 uses IRFs in both the file system and NDS. In NDS, IRFs filter rights inheritance in the Directory tree. An IRF can be placed to block inheritance of object rights or property rights assigned through the All Properties option.

The Supervisor object right can be blocked by an IRF in the Directory tree; it cannot be blocked by an IRF in the file system.

Give examples and elaborate on the concept.

Effective Rights

A user's effective rights are determined by the combination of rights received through the following rights assignments minus any IRFs:

- Explicit trustee assignments to a user object
- Membership in a group object
- Occupancy of an organizational role object
- Security equivalences to other user objects
- Trustee assignment to the container or parent container in which the user object resides
- Rights given to the [Public] trustee

Give examples and elaborate on the concept.

Notes

Novell.

To order a Novell Press book, please contact your nearest Novell Authorized Education Center (NAEC) or Novell Education Academic Partner (NEAP). To find a center or partner near you, call 1-800-233-EDUC or 1-801-222-7800, or go online to education.novell.com. For more information about Novell Press Books, go online to www.novell.com/programs/press.

Title	Author(s)	Novell P/N SKU	ISBN	Available
Novell's CNE Update to NetWare 5 Study Guide	David James Clarke, IV	00785555545595	0-7645-4559-0	4th Qtr 1998
Novell's CNA Study Guide for NetWare 5	David James Clarke, IV	00785555545427	0-7645-4542-6	4th Qtr 1998
Novell's CNE Study Guide for NetWare 5	David James Clarke, IV	00785555545434	0-7645-4543-4	1st Qtr 1999
Novell's Certified Internet Business Strategist Study Guide	Jim Bowman	00785555545496	0-7645-4549-3	
Novell's Certified Web Designer Study Guide	Jim Bowman	00785555545489	0-7645-4548-5	
Novell's CNE Study Guide Set IntranetWare/ NetWare 4.11	David James Clarke, IV	00785555545335	0-7645-4533-7	
Novell's CNE Study Guide IntranetWare/NetWare 4.11	David James Clarke, IV	00785555545120	0-7645-4512-4	
Novell's CNE Study for Core Technologies	David James Clarke, IV	00785555545014	0-7645-4501-9	
Novell's CNA Study Guide IntranetWare/NetWare 4.11	David James Clarke, IV	00785555545137	0-7645-4513-2	
Novell's Guide to NetWare 5 Networks	Jeffrey F. Hughes & Blair W. Thomas	00785555545441	0-7645-4544-2	4th Qtr 1998
Novell's NetWare 5 Administrator's Handbook	Kelley J. P. Lindberg	00785555545212	0-7645-4546-9	4th Qtr 1998
Novell's Guide to Troubleshooting NetWare 5	Rick San't Angelo	00785555545588	0-7645-4558-2	1st Qtr 1999
Novell's Guide to NetWare for Small Business 4.11	Eric Harper & David L. Gardner	00785555545045	0-7645-4504-3	
NDS for NT	Jeffrey F. Hughes & Blair W. Thomas	00785555545519	0-7645-4551-5	
Novell's NDS Developer's Guide	Chris Andrew, Bill Bodine, Kent Boogert, Brian Brown, Karl Bunnel, David Fox, Michael Hiatt, David Shelley, Ed Shropshire, Jim Thatcher, & David Ward	00785555545571	0-7645-4557-4	4th Qtr 1998
Novell's Guide to IntranetWare Networks	Jeffrey F. Hughes & Blair W. Thomas	00785555545168	0-7645-4516-7	
Novell's IntranetWare Administrator's Handbook	Kelley J. P. Lindberg	00785555545175	0-7645-4517-5	
Novell's Introduction to intraNetWare	Kelley J. P. Lindberg	00785555545304	0-7645-4530-2	
Novell's Guide to Integrating intraNetWare and NT	JD Marymee & Sandy Stevens	00785555545236	0-7645-4523-X	
Novell's Guide to TCP/IP and IntranetWare	Drew Heywood	00785555545328	0-7645-4532-9	
Novell's Guide to NetWare 4.1 Networks	Jeffrey F. Hughes & Blair W. Thomas	00785555847361	1-56884-736-X	
Novell's NetWare 4.1 Administrator's Handbook	Kelley J. P. Lindberg	00785555847378	1-56884-737-8	
Novell's Guide to Integrating NetWare and TCP/IP	Drew Heywood	00785555848184	1-56884-818-8	
Novell's Four Principles of NDS Design	Jeffrey F. Hughes & Blair W. Thomas	00785555545229	0-7645-4522-1	
Novell's Guide to NetWare Printing	JD Marymee & Sandy Stevens	00785555545144	0-7645-4514-0	
Novell's GroupWise 5.5 Administrator's Guide	Shawn B. Rogers & Richard H. McTague	00785555545564	0-7645-4556-6	4th Qtr 1998
Novell's GroupWise 5.5 User's Handbook	Shawn B. Rogers & Richard H. McTague	00785555545526	0-7645-4552-3	3rd Qtr 1998
Novell's GroupWise 5 Administrator's Guide	Shawn B. Rogers & Richard H. McTague	00785555545212	0-7645-4521-3	
Novell's GroupWise 5 User's Handbook	Shawn B. Rogers & Richard H. McTague	00785555545090	0-7645-4509-4	
Novell's GroupWise 4 User's Handbook	Shawn B. Rogers & Richard H. McTague	00785555545021	0-7645-4502-7	
Novell's ManageWise Administrator's Handbook	Randi E. Constable	00785555848177	1-56884-817-X	
Novell's Guide to BorderManager	JD Marymee & Sandy Stevens	00785555545403	0-7645-4540-X	
Novell's Internet Plumbing Handbook	Peter Rybaczyk	00785555545373	0-7645-4537-X	
Novell's Guide to Web Site Management	Jim Bowman	00785555545298	0-7645-4529-9	
Novell's Guide to Internet Access Solutions	Roger L. Spicer, Laura A. Chappell, & Colin E. Dixon	00785555545151	0-7645-4515-9	
Novell's Guide to Creating IntranetWare Intranets	Karanjit Siyan, Ph. D.	00785555545311	0-7645-4531-0	
Novell's The Web at Work: Publishing Within and Beyond the Corporation	Peter Jerram	00785555545199	0-7645-4519-1	
Novell's Guide to LAN/WAN Analysis: IPX/SPX	Laura A. Chappell	00785555545083	0-7645-4508-6	
Novell's Guide to Resolving Critical Server Issues	Brad Dayley & Rich Jensen	00785555545502	0-7645-4500-7	
Novell's Encyclopedia of Networking	Kevin Shafer	00785555545113	0-7645-4511-6	
Novell's Dictionary of Networking	Kevin Shafer	00785555545281	0-7645-4528-0	
Novell's Guide to Networking Hardware	Kevin Shafer	00785555545533	0-7645-4553-1	3rd Qtr 1998
Novell's Introduction to Networking	Cheryl C. Currid & Co.	00785555545250	0-7645-4525-6	