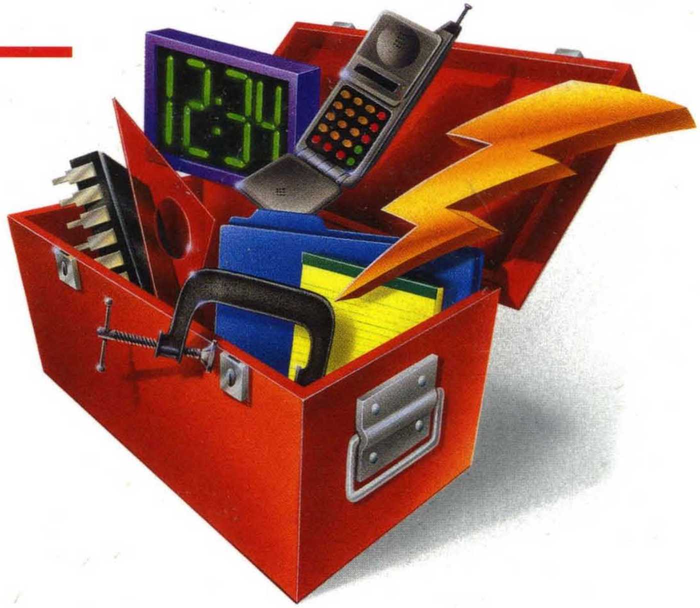
CD INCLUDED

Microsoft® Windows NT™ Resource Kit

Exclusively for Owners of the Windows NT Resource Kit Version 3.5



Version 3.51 Update

For Windows NT Workstation and Windows NT Server

Microsoft® Press

Version 3.51 Update

Microsoft® Windows NT™ Resource Kit

For Windows NT Workstation and Windows NT Server Version 3.51

Microsoft Press®

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Cataloging-in-Publication Data
Microsoft Windows NT resource guide : for Windows NT Workstation and
Windows NT Server version 3.5 / by Microsoft Corporation.
p. cm.
Includes index.
v. 5. version 3.51 update
ISBN 1-55615-929-3 (v. 5.).
1. Operating systems (Computers) 2. Microsoft Windows NT.
I. Microsoft Corporation.
QA76.76O63M5244 1995
005.4'469--dc20 94-45564
CIP

Printed and bound in the United States of America.

2 3 4 5 6 7 8 9 QMQM 0 9 8 7 6

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office. Or contact Microsoft Press International directly at fax (206) 936-7329.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation.

This book is dedicated to the miracle-working Windows NT Resource Kit documentation team, whose great teamwork shows again in this latest book! It is also dedicated to those wonderful developers who spend their "free" time creating and updating the utilities and online documents included on the CD!

Contributors to this book include the following:

Technical Writers:
Janice Breyer, Kat Cordell, Peter Costantini, Peggy Etchevers, Jeff Howard, Chris Kagen, Sharon Kay, Cary Reinstein, Laura Sheppard, Pamela Stanton-Wyman

Technical Consultants:
Dieter Achtelstetter, Gert Gustedt, Eric Hough, Katy Hunter, Louis Kahn, Jim Kelly, Sachin Kukreja, Ryan Marshall, Ken Moss, Lenny Turetsky, Bob Watson, and numerous Windows NT Developers, Program Managers, and Product Support Specialists

Technical Editor:
Sharon Tighe

Managing Editor:
Sonia Marie Moore

Software Program Managers:
Louis Kahn, Lenny Turetsky

Documentation Project Manager:
Peggy Etchevers

Indexer:
Jane Dow

Production Team:
Cheryl Capriola, Karye Cattrell, Cathy Pfarr, and Keri Segna

Graphic Designers:
Kathy Hall, Sue Wyble

Contents

Introduction

Welcome to the *Microsoft® Windows NT™ Resource Kit Volume 5: Windows NT Update 1* book.

The Microsoft *Windows NT Resource Kit for Windows NT Workstation and Windows NT Server version 3.51* consists of the four volumes that were shipped with the version 3.5 release, this new fifth volume, and a single compact disc (CD) containing new utilities and updated versions of the existing ones. Floppy disks are no longer available.

The *Windows NT Update 1* book presents detailed information on topics that are either new for version 3.51 or reflect issues that our Product Support people consider timely and important! The appendices also include information on changes that have been made to the four-volume set of books for version 3.5.

The information provided in this volume is a technical supplement to the documentation included as part of the Windows NT Workstation and Windows NT Server version 3.51 product and does not replace that information as the source for learning how to use the product features and utilities.

This introduction includes four kinds of information you can use to get started:

- The first section outlines the contents of this book, so that you can quickly find pertinent technical details.
- The second section introduces the *Windows NT Resource Kit* CD.
- The third section describes the support policy for the *Windows NT Resource Kit.*
- The fourth section describes the conventions used to present information in this book.

About the Update 1 Book

This book includes the following chapters.

Chapter 1, "Setup," discusses issues concerning the setting up of Windows NT Workstation and Windows NT Server, and introduces utilities included in this resource kit that are designed to make it easier to set up. In particular, it discusses fine points of and enhancements to the Computer Profile Setup (CPS) utility.

Chapter 2, "Licensing," provides information on how to choose the appropriate licensing mode, a list of many common situations that use up licenses from the pool of available licenses, some of the license purchasing requirements for specific Microsoft BackOffice server products, and additional technical information, such as a Visual Basic for Applications (VBA) code example for using OLE to export user data to a spreadsheet and what files to copy to install License Manager on a computer running Windows NT Workstation.

Chapter 3, "Security," addresses security issues that face administrators of computers and computer networks. It discusses the Windows NT security features that you can implement to establish various levels of security, and criteria for choosing whether or not to use specific security options. It also introduces the C2CONFIG utility, which helps you set up a computer system that satisfies the federal requirements for C2-level security certification.

Chapter 4, "Internet Services and Security," introduces the utilities included in this resource kit, and the functionality in Windows NT Server, that make Windows NT Server an excellent platform for Internet content providers. It also provides tips on using Windows NT Workstation to connect to the Internet. And it addresses some of the security issues you should be aware of when you connect your computer to the Internet in any capacity.

Chapter 5, "SNMP," describes the Simple Network Management Protocol (SNMP), a member of the TCP/IP protocol family. It includes overview information about SNMP, instructions for installing and configuring SNMP, information on how a network administrator can use SNMP, and high-level information of interest to programmers. The chapter concludes with a list of reference material.

Chapter 6, "Troubleshooting," provides information for troubleshooting problems in addition to that included in Chapter 18, "Troubleshooting," in the *Windows NT Resource Guide*.

Appendix A, "Major Revisions to the Windows NT Networking Guide," includes revised versions of sections from Chapter 9 and Chapter 22 in the *Windows NT Networking Guide* and a totally revised Appendix B, "MIB Object Types for Windows NT." These major changes were not incorporated into the revised edition of Volume 2 that accompanies this version of the *Windows NT Resource Kit.*

Appendix B, "Major Revision to Windows NT Messages," includes a totally rewritten version of "The Windows NT Debugger" section of Chapter 2, "Windows NT Executive Messages," in the *Windows NT Messages* book. It now reflects the new debugging tools that were included with the Windows NT Server and Windows NT Workstation version 3.51 release. It provides information on how to use the new utilities that can automatically read and interpret dump files. It also provides instructions for configuring the Kernel debuggers (KDs) for local debugging. This major change was not incorporated into the revised edition of Volume 3 that accompanies this version of the *Windows NT Resource Kit.*

Appendix C, "Minor Revisions to Existing Resource Kit Books," includes a list (organized by book, chapter, and page number) of all the changes that have been incorporated into the revised editions of the four-volume set of resource kit books for Version 3.5.

Appendix D, "Security in a Software Development Environment," provides detailed information on protecting and auditing objects that are not normally accessed by anything other than the Windows NT operating system itself. This chapter is of use in a software development environment, or in situations where custom software shares the system with sensitive data. This appendix also describes special cases of auditing that might be of interest to administrators of high-level security installations.

Appendix E, "Domain Planning for Your Enterprise," provides in-depth information on the implementation of Microsoft Windows NT Server 3.51, with a focus on domains and domain strategies, for those networking groups who may need assistance in planning the design and implementation of domains for their network. The goal of this appendix is to provide an understanding of the various domain models, the business and technical reasons for selecting one model as opposed to the others, as well as the advantages and trade-offs associated with each of the domain models.

Index to this *Windows NT Update 1* book.

Resource Kit Compact Disc

The compact disc (CD) that accompanies the *Windows NT Resource Kit* contains utilities that apply to information in the *Windows NT Resource Guide,* the *Windows NT Networking Guide*, and now also the *Windows NT Update 1* book. This CD includes a collection of information resources, tools, and utilities that can make networking and working with Windows NT even easier. The Windows NT Messages database and the utilities that apply to information in the *Optimizing Windows NT* book are also included on the *Windows NT Resource Kit* CD.

A complete list of all the tools in the *Windows NT Resource Kit,* and instructions on how to install them, is available on the CD in the README.WRI file. Instructions on how to use them are provided in the RKTOOLS.HLP file.

The *Windows NT Resource Kit* CD includes tools that fall under the following major categories. Many of the tools that were included in version 3.5 are described in the "Introduction" section of the *Windows NT Resource Guide.* A few of the new or significantly updated tools for version 3.51 are also described here.

Batch Tools

- Perl 5 is a scripting language ported from UNIX® to Windows NT Workstation and Windows NT Server. Perl 5 combines some of the features of C, sed, awk, and shell. This version of Perl 5 also enables you to work with the Registry and event logs, and can act as an OLE automation controller.
- Regina REXX is a full-batch scripting language with Registry access, event log functions, and OLE automation support.

Computer Administration/Configuration Tools

- The Windows NT C2 Configuration Manager, C2CONFIG.EXE, can be used to compare the current security configuration on your Windows NT Workstation with the C2-level security requirements of the federal government's National Computer Security Center, and then to configure the workstation to conform up to that C2 level.

Computer and Network Setup Tools

- CPS: Computer Profile Setup enables you to install easily either Windows NT Workstation or Windows NT Server on multiple identical x86-based computers. This release includes support for licensing and several bug fixes.

Computer Diagnostic Tools

- Crystal Reports Event Log Viewer is a full-feature report writer that allows you to view, sort/filter/group, save, and print Windows NT event logs from one or more computers in a variety of formats.

Desktop Tools

- The VDESK.EXE tool is a simple desktop switcher that enables a user to maintain multiple desktops on a computer running Windows NT Workstation version 3.51. It also provides a task manager as a replacement for the default Task Manager program that is provided by Program Manager. Users can also log on as another user, such as Administrator.

File Tools

- File Compress, COMPRESS.EXE, is a command-line utility that can be used to compress one or more files and also to make custom Setup floppy disks.
- The File Expansion Utility, EXPNDW32.EXE, can be used to expand one or more compressed files from the Windows NT floppy disks or CD. EXPNDW32.EXE is a 32-bit utility that provides a fully graphical interface for easy use. This release includes several bug fixes.

Internet and TCP/IP Services/Tools

- Mail Server is a Simple Mail Transport Protocol (SMTP) and Post Office Protocol (POP) server for Windows NT. The intermediate files and mailboxes are all spooled securely (when using the NTFS file system) on the computer running Windows NT Server and are accessed through any POP-compliant public domain (PD) or commercial clients.
- The Domain Name Server (DNS) Service is the Windows NT implementation of a protocol and system used throughout the Internet. This version has been substantially updated and is now a beta-quality product. A .TXT file containing Release Notes of potential problem areas has also been included.

Network Diagnostic Tools

- The performance monitor MIB Builder Tool, Perf2MIB, enables developers to create new ASN.1 syntax MIBs for their applications, services, or devices that use Performance Monitor counters. Administrators can then track performance of these components using any system-management program that supports SNMP. The tool also creates a .MIB file that can be used by an SNMP-based management console to perform SNMP requests for the performance data in question.
- Net Watcher, NETWATCH.EXE, shows what users are connected to shared directories. It has been enhanced for this release and can now simultaneously monitor multiple computers.

Registry Tools

- The Windows NT Registry Entries online Help file, REGENTRY.HLP, has been updated for this version. The corresponding chapter in the *Windows NT Resource Guide* has not been updated.

Server/Network Administration Tools

- DHCP Relay Agent enables your computer to receive and forward Dynamic Host Control Protocol (DHCP), messages from and to internet protocol (IP) interfaces across non-BootP routers, which allows companies to save money by not having to upgrade their routers that don't support BootP.

Tools for Developers

- Twenty-one POSIX utilities have been recompiled to operate on Windows NT Workstation and Windows NT Server version 3.51.

User Account Administration Tools

- Profile Control Panel, PROFILE.CPL, gives you an easy way to control a floating user profile, which allows you to log on to multiple Windows NT computers and use your own settings.

Resource Kit Support Policy

The SOFTWARE supplied in the *Windows NT Resource Kit* is not officially supported. We provide a way for customers who purchase the *Windows NT Resource Kit* to report bugs and receive possible fixes for their issues via the e-mail address RKINPUT@MICROSOFT.COM. This e-mail address is only for *Windows NT Resource Kit* issues. Microsoft Product Support Services (PSS) does not support the utilities. However, they may be able to provide additional information if available. There is no guarantee as to when or if bugs in the *Windows NT Resource Kit* SOFTWARE will be fixed or new features added.

The SOFTWARE (including instructions for its use and all printed and online documentation) is provided "AS IS" without warranty of any kind. Microsoft further disclaims all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The entire risk arising out of the use or performance of the SOFTWARE and documentation remains with you.

In no event shall Microsoft, its authors, or anyone else involved in the creation, production, or delivery of the SOFTWARE be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the SOFTWARE or documentation, even if Microsoft has been advised of the possibility of such damages.

Conventions in This Manual

This document assumes that you have read the Windows NT Workstation and/or Windows NT Server version 3.51 documentation sets and that you are familiar with using menus, dialog boxes, and other features of the Windows operating system family of products. It also assumes that you have installed Windows NT Workstation or Windows NT Server version 3.51 on your system and that you are using a mouse. For keyboard equivalents to menu and mouse actions, see Microsoft Windows NT online Help.

This document uses several conventions to help you identify information. The following table describes the typographical conventions used in the *Windows NT Update 1* book.

Convention	Used for
bold	MS-DOS–style command and utility names such as **copy** or **ping** and switches such as **/?** or **-h**. Also used for Registry value names, such as **IniFileMapping,** and OS/2 application programming interfaces (APIs).
italic	Parameters for which you can supply specific values. For example, the Windows NT root directory appears in a path name as *systemroot*\SYSTEM32, where *systemroot* can be C:\WINNT35 or some other value.
ALL CAPITALS	Directory names, filenames, and acronyms. For example, DLC stands for Data Link Control; C:\PAGEFILE.SYS is a file in the boot sector.
`Monospace`	Sample text from batch and .INI files, Registry paths, and screen text in non-Windows–based applications.

Other conventions in this document include the following:

- "MS-DOS" refers to Microsoft MS-DOS version 3.3 or later.
- "Windows-based application" is used as a shorthand term to refer to an application that is designed to run with 16-bit Windows and does not run without Windows. All 16-bit and 32-bit Windows applications follow similar conventions for the arrangement of menus, dialog box styles, and keyboard and mouse use.
- "MS-DOS–based application" is used as a shorthand term to refer to an application that is designed to run with MS-DOS but not specifically with Windows or Windows NT and is not able to take full advantage of their graphical or memory management features.
- "Command prompt" refers to the command line where you type MS-DOS–style commands. Typically, you see characters such as C:\> to show the location of the command prompt on your screen. In Windows NT, you can double-click the MS-DOS Prompt icon in Program Manager to use the command prompt.
- An instruction to "type" any information means to press a key or a sequence of keys, and then press the ENTER key.
- Mouse instructions in this document, such as "Click the OK button" or "Drag an icon in File Manager,'' use the same meanings as the descriptions of mouse actions in the *Windows NT System Guide* and the Windows online tutorial.

CHAPTER 1

Setup

This chapter discusses changes to Windows NT setup utilities, and clarifies some points about the Computer Profile Setup utility (CPS).

Hardware Requirements

The hardware requirements for a Windows NT Server or Windows NT Workstation depend on the demands you will put on the particular computer. The *Installation Guide* for each platform specifies the minimum requirements. This section offers a few recommendations for special cases.

For a production server that will handle more than 100 users at a time, you'll probably want at least 32 MB of physical random access memory (RAM), plus 1GB of disk space to hold the operating system, pagefiles, disk logs, user database, and so on. (Each backup domain controller (BDC) can support up to 2000 users. Up to 40,000 network objects, including user accounts, machine accounts, and group accounts, can be supported in a single domain.)

The following hardware specifications are recommended for a computer that is to be used as a primary domain controller (PDC) or BDC:

Number of users	**Minimum CPU needed**	**Required RAM**
up to 3000	486/33	32 MB
7500	486/66	32 MB
10,000	Pentium®, MIPS®, Alpha™	48 MB
15,000	Pentium, MIPS, Alpha	64 MB
> 15,000	Pentium, MIPS, Alpha	(memory should equal at least 2.5 * the size of the SAM)

For more information on setting up Windows NT domains, see Appendix E, "Domain Planning for Your Enterprise."

Computer Profile Setup Versus the WINNT Command

Two different applications, Computer Profile Setup (CPS) and Setup Manager/**winnt**, are available to make it easier to install Windows NT Workstation or Windows NT Server on large numbers of computers. Which one you use depends on whether you want identical or individualized installations.

CPS is used to pre-install *identical* copies of Windows NT on multiple Intel-based computers. CPS is used by hardware manufacturers and others who need to supply computers with Windows NT Workstation or Windows NT Server pre-installed.

CPS is documented in Chapter 3, "Customizing Windows NT Setup," in the *Windows NT Resource Guide*, and in the online Help. The online Help also has information on new features.

The **winnt** (or **winnt32**) command is used to install Windows NT over a network. It simplifies the task of installing Windows NT throughout an organization that has multiple Windows NT licenses. With this command, some or all of the questions the user is normally prompted for can be answered by an "answer file," which is created using the Setup Manager application. The user is prompted for any questions that are not answered in the answer file. You can create as many answer files as necessary—for example, you can tailor one to each user, or you can create one for each Group of users. In the latter case, the user's name would be left out of the answer file, and the user would be prompted for this information during setup.

The **winnt** (or **winnt32**) command and Setup Manager are documented in Chapter 3, "Customizing Windows NT Setup," in the *Windows NT Resource Guide*, and in the online Help.

Frequently Asked Questions About CPS

Is CPS a one-step process?

In many cases it's very close. However, since each customer's installation is unique, you might need to modify the CPS process. The additional steps can include such things as auto logon scripts, MS-Test scripts, batch or command files, custom programs, and so on.

It's best to think of CPS as a "starting point" to your installation process, rather than an "ending point."

Can I profile files with long filenames?

Long filenames are not supported by MS-DOS®. Since the files are copied from the distribution directory to the target computer using an MS-DOS program (WINNTP.EXE), only MS-DOS-based filenames (that is, those using the "8.3" format) are allowed.

As a workaround, you can use files that have 8.3 filenames in the WINNT system directories, and copy only the system directories using CPS. Then, after Windows NT has been installed on the target computer, use the **xcopy** command to copy the remaining files and directories.

I'm using TCP/IP. How can I assign an IP address during setup?

In the %systemroot%\SYSTEM32 directory there is a file named IPINFO.INF. See that file for information on manually configuring your IP addresses. Each target computer will require a unique IP address in the IPINFO.INF file. CPS will use the information from this file during setup.

If CPS won't transfer my application, service, or program, what should I do?

Some applications do not profile completely. If your installation requires an application that does not transfer correctly from the source to the target computers, the following steps can be taken:

1. Profile the system without the application(s) installed.
2. Install the application, while recording the steps using MS-Test. (MS-Test is a separate Microsoft product.)
3. Install the profiled system on the target computer.
4. Run the MS-Test script to install the application(s).

Why can't I just copy the contents on the hard disk from one computer to another?

Each computer is assigned a unique Security ID (SID) during setup so that it can be identified on the network. Most of the network services have this Security information encoded in their entries in the Registry during setup or subsequent installation. Copying the contents of one hard disk to another would give each computer the same SID, which would compromise security.

CPS works within this system by noting the network services that are installed on the source computer and then removing those entries from the profiled version of the Registry. During setup on the target computer, the target computer's unique SID is created, and then assigned to the network services that were found on the source computer as they are re-installed.

How do I get CPS to profile my network adapter?

If your network adapter card is not listed in the Registry under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft key, then you'll need to modify the CPS.INI file so as to point to the correct key. This is documented in online Help.

How can I use CPS to copy multiple network adapters, or Remote Access Service and a network adapter?

CPS is capable of profiling only a single-network adapter. RAS is configured to look like a network adapter and as such makes the system appear to have two network adapters, only one of which will be profiled and subsequently installed on the target computer.

As a workaround, complete the following steps:

1. Profile the system without the Remote Access Service (RAS) installed.
2. Install RAS, while recording the steps using MS-Test. (MS-Test is a separate Microsoft product.)
3. Install the profiled system on the target computer.
4. Run the MS-Test script to install RAS.

For multiple network adapters, follow the same steps, substituting the additional adapter(s) for RAS.

Why won't CPS copy the user accounts?

CPS only transfers domain accounts found on the source computer. (These are account names that are prefixed with a domain name, in the format DOMAIN\UserName). Local computer accounts are presumed by CPS to be unique to each computer. Also passwords are not copied from one computer to the next, for security reasons.

How can I transfer environment variables via CPS?

CPS does not copy environment variables to the target computer. As a workaround, complete the following steps:

1. Profile the system as usual.
2. Create a script file of the environment variables you want to copy. In the following sample file, lines without equal signs (=) designate a key path or subkey, and subkeys are indented. Lines that include an equal sign indicate a value. Use the value modifiers that appear in the Add Value dialog box in the Registry Editor.

```
\Registry\USER
    .DEFAULT
        Environment
            NewOne = REG_SZ new string
    S-1-5-21-2127521184-1604012920-1887927527-9600
        Environment
            NewOne = REG_SZ new string
```

3. Install the profiled system on the target computer.
4. Use the **regini** command to change the Registry on the target computer, using the script created in step 2.

For more information on the Registry Editor, see Part IV, "Windows NT Registry," of the *Windows NT Resource Guide*. For information on **regini**, see the RKTOOLS Help file.

Can I use CPS to transfer disk shares?

CPS does not transfer disk shares. You'll need to create the shares after using CPS to copy the profile.

Where can I find information about the .INI & .INF files?

The INI file contents are documented in RKTOOLS Help. The INF file contents are described in the *Programmer's Guide* of the Windows NT Device-Driver Development Kit (DDK) documentation.

How can I get CPS to transfer my personal Program Groups?

CPS profiles only the "common" program groups. If you have personal program groups, load them by using the REGTOGRP and GRPTOREG utilities provided with this resource kit.

Using Setup Manager and WINNT

Setup Manager and the **winnt** command are documented in the *Windows NT Resource Guide* and in the documentation for Windows NT Server and Windows NT Workstation 3.51. The following sections clarify a few points about these applications.

Disk Space Requirements for WINNT

When you run **winnt** with the **/b** option, two temporary directories are created: the $WINNT_$.~LS directory, which holds a copy of the installation tree, and the $WINNT_$.~BT directory, which holds all the boot files that are normally on the Windows NT setup boot floppy disks. This second temporary directory must be on your boot drive (C:) and requires approximately 4 to 5 MB of uncompressed space to hold the files needed by Windows NT to boot and load Setup. If you do not have this much uncompressed space on your boot drive, run **winnt** without the **/b** option. This creates three boot floppy disks instead of using space on drive C: for the boot files.

Whether or not you use the **/b** option, you will need about 1 MB of uncompressed space on drive C: for the files: NTLDR, NTDETEC.COM, BOOT.INI, and BOOTSECT.DOS.

Using the /O Option with WINNT

If you use **winnt** or **winnt32** with the **/o** option, boot floppy disks are created that require the presence of a local source directory with the installation files. You can create boot floppy disks that do not require this local directory (using retail installation media instead) by using the **/ox** option. This is preferred if you are installing from a compact disc rather than over the network.

In no case does the **winnt** or **winnt32** command create boot floppy disks that can install Windows NT Workstation or Windows NT Server in its entirety.

Specifying License Mode in Setup Manager

A new field in the Windows NT Setup Manager main dialog box allows you to specify the license mode (Per Seat or Per Server) when creating an unattended answer file for a Windows NT Server or domain controller. See the "Licensing" chapter in this *Windows NT Update 1* book for information about the licencing modes.

Other Installation Tools

In addition to CPS and Setup Manager, this resource kit includes several tools to make installation easier. The RKTOOLS Help file provides further information on these tools:

- The Windows NT Domain Planner is a Wizard that helps you plan the most effective domain model for your networked organization.
- The PUTINGRP.EXE tool is used to create program items and program groups, and to put program items into specified program groups.
- The REGTOGRP.EXE tool creates a Windows NT .GRP file in the current directory for each of your Program Manager groups. You can then use GRPTOREG.EXE to convert the .GRP file into the registry entries.

PCMCIA Support

Windows NT 3.51 supports a number of Personal Computer Memory International Association (PCMCIA) cards, which are listed in the *Hardware Compatibility List.* Supported PCMCIA cards are detected if they are in place when the computer is started. Supported cards installed while Windows NT is running are detected the next time Windows NT is restarted.

Conflicts between supported PCMCIA devices (serial ports, mouse port, and atdisk devices) and any other devices are not detected or resolved; you must resolve these conflicts yourself. In most cases, this step involves changing the IRQ of the device that is not a supported PCMCIA device. The exception is PCMCIA network adapters. The resources used by PCMCIA network adapters can be changed during installation, or by choosing Network from the Control Panel. The IRQs generally used by PCMCIA devices are as shown in the following table.

PCMCIA device type	IRQ level(s) used
Atdisk devices	14 or 15
Atdisk devices (Cirrus Logic PCMCIA controller)	7
Modems	3 or 4, or 5 if a mouse is using 3 or 4
SCSI® drive	15 and or lower
Network adapter card	10 or higher

It is especially important to make sure that there are no conflicts between a supported PCMCIA device and the boot SCSI device, since this could prevent the system from starting or from performing a bug check.

The SCSI PCMCIA device driver must be set up after installing Windows NT Workstation or Windows NT Server, as described in *Windows NT Server Update Information for Version 3.51*. It cannot be installed during text mode setup.

PCMCIA Installation Application

The Windows NT Control Panel application for PCMCIA peripherals is PCMCIA.CPL. It shows what PCMCIA cards are installed in which sockets, how they are configured, and what resources the PCMCIA controller is using. For network cards and SCSI PCMCIA devices, PCMCIA Control Panel suggests the correct device driver and allows you to install it.

To use PCMCIA Control Panel, double-click the PCMCIA icon in Control Panel.

Windows NT 3.51 Service Pack 1 and Windows NT Workstation Shell Technology Preview Update

The Windows NT Workstation Shell Technology Preview Update gives you the Windows 95 interface with the Windows NT Workstation 3.51 operating system. Be aware that the Windows NT 3.51 Service Pack 1 can only be installed before the Shell. If the Shell is already installed, it must be uninstalled (as directed in the Shell documentation) before the Service Pack is installed. The Shell can then be installed over the Service Pack.

Auto-Joining a Domain

If you specify a domain while installing Windows NT Workstation or Windows NT Server, the operating system will try to join that domain the first time you log on. It will be successful only if the computername you assigned during installation has not been previously used in logging on to the domain. If the auto-join feature seems not to work, use User Manager on a domain controller to delete the computername from the domain, and try again.

Replaceable Logon

Winlogon is the component of Windows NT that provides interactive logon support. Some aspects of Winlogon are replaceable. In particular, the identification and authentication aspects of Winlogon are implemented in a replaceable dynamic-link library (DLL). This replaceable DLL is referred to as the Graphical Identification and Authentication DLL, or *GINA*. GINA allows developers to implement smart-card, retinal-scan, or other authentication mechanisms in place of the standard Windows NT user name and password authentication.

A sample GINA.DLL and online documentation are available in the Windows NT Software Development Kit (SDK).

CHAPTER 2

Licensing

Windows NT Server 3.51 provides a new tool, License Manager, in the Network Administration program group to assist administrators in managing licensing for computers running Windows NT Server on which they have administrative rights. There is also a new Licensing option under Control Panel for users to manage certain aspects of licensing on their own computers.

Both of these tools are extensively documented in Chapter 5, "Licensing and License Manager," of the *Windows NT Server Update Information for Version 3.51* book. For more information on the licensing changes to the Setup process in Windows NT Server 3.51 and for detailed definitions with graphic descriptions of the Per Server and Per Seat licensing modes, along with more examples of when to use each mode, see Chapter 1, "New Programs and Features," in that same book.

This chapter assumes that you have already read all the information on licensing included in the product documentation. The purpose of this chapter is to provide even more information to help you in choosing the appropriate licensing mode, a list of many common situations that use up licenses from the pool of available licenses, some of the license purchasing requirements for specific Microsoft BackOffice server products, and additional technical information.

Choosing Between the Two Licensing Modes

Licensing

Licensing for the Microsoft BackOffice family of server products requires a Server License for each server and a Client Access License for each client computer to access the server. These licenses are acquired separately prior to using the product. For Windows NT Server, SQL Server, and SNA Server, the Client Access License can be used in one of two licensing modes (Per Server and Per Seat) offering customers the flexibility to choose the option that best meets their needs.

Which licensing mode to choose really depends on which applications you will be using. For example, if you use Windows NT Server mainly for file and print sharing and on multiple servers, you may be better off choosing the Per Seat option. However, if you use it as a dedicated Remote Access server, you may want to choose the Per Server concurrent connections option.

There are two rules of thumb for choosing between the two licensing modes:

- If you have only one server, you should choose the Per Server option since you can change once later to the Per Seat mode.
- If you have multiple servers and the total number of Client Access Licenses across all servers to support the Per Server mode is equal to or greater than the number of computers or workstations, you should choose or convert to the Per Seat option.

For example, if you have three servers to which 50 users can connect concurrently and you have 200 computers or workstations, you should choose the Per Server option. If, however, you add an additional 50-user server without adding any more computers or workstations, you should convert to the Per Seat option. Additional examples of situations under which you would use each licensing mode are provided in the *Windows NT Server Update Information for Version 3.51* book.

Notice that, within a single organization, you can also mix the Per Server and Per Seat modes, since your choice depends on how much the different server products are used in each department. You can also mix the Per Server and Per Seat modes on a single server if you are running multiple server products. However, a given server product, such as SQL Server, *cannot* be simultaneously run in two modes on the same server.

Finally, to determine which licensing mode to choose and how many licenses are needed, you need to know how many users and how many servers are, or will be, on your network. You do *not* need to determine which users are accessing which servers. You only need to determine how many users access each server.

Per Server Licensing

The Per Server licensing mode is a new option that has been added for Microsoft Windows NT Server 3.51 or later, Microsoft SNA Server 2.11 or later and, when released, Microsoft Exchange Server 1.0. This option enables users to take advantage of the concurrent connections (Per Server) option that has been available for Microsoft SQL Server 4.21a or later. It is not available for Microsoft Systems Management Server or the Microsoft BackOffice Client Access License.

If you are ever unsure, though, about which licensing mode to choose, select the Per Server option. If your network traffic later increases and more users need to connect at the same time, you are legally permitted to convert from Per Server mode to Per Seat mode at no additional cost. (Use the Licensing option in Control Panel for a server on which you are working and License Manager in the Network Administration program group for local or remote servers.) This is a one-time, one-way conversion option.

It is not necessary for you to notify Microsoft if you elect to make this change. However, you will need to reenter the licensing data in License Manager using the New Client Access License dialog box. You are *not* legally permitted to change the licensing mode from Per Seat to Per Server.

Note If you purchased Client Access Licenses for Windows NT Server 3.5 (which were in Per Seat mode because that was the only licensing mode available with Windows NT Server 3.5) and now want to use them with Windows NT Server 3.51 in the Per Server mode, you can designate them as Per Server mode when you upgrade (but not later). Normally, converting from the Per Seat mode to the Per Server mode is *not* allowed. However, since the Per Server mode is new, Microsoft is allowing customers that upgrade to Windows NT Server 3.51 to choose the most appropriate licensing mode for their requirements.

Concurrent Connections

With Per Server licensing, each Client Access License is assigned to a particular service (product) on a particular server and allows one connection to that service, such as basic network services, which include the following:

- File services—sharing and managing files and/or disk storage
- Printing services—sharing and managing printers
- Macintosh® connectivity—file sharing and printing services
- File and Print Services for NetWare® connectivity—file sharing and printing services for NetWare clients
- Remote access services—accessing the server from a remote location through a communications link

Notice that a connection, in this case, is to a server and not just to an individual share point or printer on that server. If you connect to \\PRODUCT\NEW and \\PRODUCT\OLD, that is considered as only one connection for licensing purposes. However, if you connect, in Per Server mode, to a server from two different computers using the same username, that is considered two connections.

You must have at least as many Client Access Licenses dedicated to a service on that server as the maximum number of client computers that will connect to that server at any point in time. If you select the Per Server option, you must specify during Setup, or upon purchasing new Client Access Licenses, the number of Client Access Licenses (which corresponds to the number of concurrent connections) that you have purchased for that server.

With Per Server licensing, once the specified limit for concurrent connections is reached, the server returns an error to the client's computer and does not allow more computer connections to that server. Connections made by administrators are also considered as part of the total number of concurrent connections. When the limit is reached, though, administrators are still allowed to connect to manage the lockout situation. New users, however, will not be allowed to connect again until enough users (including administrators) have disconnected to get below the specified limit.

Note You can also check the Application log in Event Viewer on the master server to view any license violation alerts, which appear every 6 hours as Error 71 and Event ID 201. Reports can be created using an OLE script (see "Using OLE To Export User Data to a Spreadsheet," later in this chapter) or the Crystal Reports for Windows NT utility included on the CD for the *Microsoft Windows NT Resource Kit for Windows NT Workstation and Windows NT Server Version 3.51.*

The Per Server option is often the most economical one for networks in which clients tend to connect to only one server or occasional-use or special-purpose servers, and they do not all need to connect at the same time. If a network environment has multiple servers, then each server licensed in Per Server mode must have at least as many Client Access Licenses dedicated to it as the maximum number of clients that will connect to it at any one point in time.

Per Seat Licensing

The Per Seat licensing mode requires a Client Access License for each computer that will access, on any Windows NT Server, a particular service, such as basic network services (file, print, and communications). Once a computer is licensed, it may be used to access any Windows NT Server computer at no additional charge. Multiple users may also log on to that single computer.

However, having a valid Per Seat mode Client Access License does *not* guarantee you access to a server that is licensed in the Per Server mode and has reached its specified limit. Such a connection would also consume one of the licenses assigned to the pool of available Per Server licenses, and so you would only be able to connect if there were Per Server licenses available.

For example, if a server in Per Server mode has 50 Client Access Licenses dedicated to that server and has less than 50 simultaneously connected clients, then additional clients can connect. If, however, that server has reached its specified limit, then additional clients *cannot* connect, even if they have a valid Per Seat mode license for that service.

If you select the Per Seat licensing mode, any number of licensed computers can be used to connect at any time to any Windows NT Server. However, remember that you must purchase a separate Client Access License for each computer even if you use client operating-system software from Microsoft (including Microsoft Windows for Workgroups, Microsoft Windows 95, or Microsoft Windows NT Workstation) or from a third-party vendor, or use any of the other client software supported by Windows NT Server. The Per Seat option is often the most economical one for networks in which clients tend to connect to more than one server.

Note A Client Access License is *not* included when you acquire Windows for Workgroups, Windows NT Workstation, and Windows 95. The license must be purchased separately in addition to the operating-system software.

Situations That Use Up Licenses

The following is a list of many common situations that use up one or more licenses from the pool of available licenses in either Per Seat or Per Server mode or both modes. These are situations under which License Manager assigns licenses. They do not always coincide with when you legally use a license, such as what happens with license groups.

- Disconnecting from a connection to basic network services on a Windows NT Server using the IPX protocol results in a license being held upon disconnection for up to the time value of the ConnectionlessAutoDisc function, which is a minimum of 15 minutes. In other words, this is the amount of time that it will take to free up that license for use by others, and you cannot shorten it. However, if you reconnect within that 15-minute period, you will use the same license and not consume another one. (Per Server only)
- If you connect to a server from two different computers using the same username, that is considered two connections. (Per Server only)

- If you are using SQL Server 6.0, to avoid incorrect license counts, you must use DBLIB 6.0 instead of DBLIB 4.2x, which requires updated DBLIB DLLs on the client computer. (Per Server only)
- In Windows NT Workstation and Windows NT Server, using the **net use** command with the **/u** option could result in another license being assigned. This depends on the name you specify with the **/u** option, and only happens when a name other than the user's domain name is used. For an example, see the "Counting Connections Twice for Licensing" section later in this chapter. (Per Seat only)
- The following list provides several examples of services whose connections use up from one to many licenses:
    - NTBackup, when used to back up to a remote server. Local backups do not use up a license. (Both modes)
    - SNA Server, when a client connects to an SNA Server (Both modes)
    - Exchange Server, when an Exchange client connects to an Exchange Server (Both modes)
    - SQL Server, when a client connects to an SQL Server (Both modes)
    - A Remote Access Server (RAS) connection to a Windows NT Server using PPP or SLIP (Both modes)
    - Macintosh connections using Services for Macintosh (Both modes)
    - NetWare client connections using File and Print Services for NetWare (FPNW) (Both modes)
    - File and print sharing connections to Windows NT Server using SMB (Server Message Block) (Both modes)
    - UNIX connections using the Windows NT Server UNIX-LPD service for print sharing (Both modes)
    - Microsoft logon scripts that exist on a Windows NT Server for execution on a workstation (Windows NT Workstation, Windows for Workgroups, or Windows 95) (Both modes)
    - Configuring Windows 95 to authenticate to a Windows NT Server domain, due to the policy profile feature (Both modes)
    - Systems Management Server (SMS), when workstations are inventoried (Per Seat only)

The following list provides several answers (but not all!) to the commonly asked question, "What situation does *not* use up a license?"

- Connecting to a remote server's Registry
- Remote administration of another computer using Performance Monitor, Server Manager, or User Manager for Domains
- Local logons to a server
- Using the FTP (File Transfer Protocol), Telnet, and Winsock Internet utilities, unless they are connecting to a computer (or an application) that does use up a license
- Using Windows Internet Name Service (WINS) and Dynamic Host Configuration Protocol (DHCP)
- Using Simple Network Management Protocol (SNMP)
- Using Network Dynamic Data Exchange (NetDDE)
- Using Remote Procedure Call (RPC), unless it connects to an application that does use up a license, such as SMB Server
- Using Named pipes, unless they connect to a service that does use up a license
- Connections to non-Microsoft server products, such as ORACLE®, unless they connect to an application that does use up a license

License Purchasing Requirements

Licensing

Before purchasing a product, it also helps to know whether or not you need to purchase licenses, how many, and what kind. The following examples provide detailed information on several Microsoft server products.

Microsoft SQL Server

With SQL Server, you can have a server running a SQL gateway application (that is, an application that maintains a single connection to the SQL Server database). Multiple clients can access the gateway, which manages the database queries on behalf of the clients. However, the clients do not connect directly to the SQL Server database and so License Manager cannot track the usage accurately.

License Manager, in this case, will only detect one licensed connection.

Our product license specifically addresses this type of multiplexing or pooling application. Our license states that using software or hardware that reduces the number of users directly accessing or using SQL Server, which is sometimes called multiplexing or pooling software or hardware, does *not* reduce the number of Client Access Licenses required. The required number of Client Access Licenses equals the number of distinct connections to the multiplexing or pooling software or hardware "front end."

Microsoft Mail 3.5

Microsoft Mail 3.5 does not necessarily require you to purchase Windows NT Server Client Access Licenses. It only requires them if the Mail Post Office is located on Windows NT Server.

To better understand how that affects your purchasing and deployment decisions, consider the following information. Microsoft Mail is network operating system (NOS)-independent. The Mail Post Office of shared file system mail, by definition, uses the underlying file-sharing services of the network upon which it runs. Microsoft Mail 3.5 has added a Windows NT-based multitasking message transfer agent (MMTA). The Mail Post Office and the MMTA can run on different servers with different NOSs.

If Windows NT Server is already providing licensed basic network file and print sharing services, then there is no additional Client Access License burden with running the Mail Post Office on that server. If Windows NT Server is *not* already providing those services, the Mail Post Office should be run on the network server (such as a NetWare server) that is providing the basic file and print services. The MMTA, though, would still run on Windows NT Server.

Microsoft Mail Server 3.5, like other server products, does require customers to have a Mail Server License to install the Post Office. If the Mail Post Office is running on Windows NT Server and that server does not already provide licensed basic network file and print sharing services, you also need to purchase a Windows NT Server Client Access License for each user accessing Microsoft Mail.

In addition to the Client Access Licenses for file and print sharing, you must also purchase client licenses for Microsoft Mail Server 3.5. These client licenses, though, are packaged differently from those of other server products, as follows:

- Ten client licenses are included in the Microsoft Mail Server package. Additional client licenses need to be acquired separately.
- One client license is included in each of the following products:
  - Windows for Workgroups
  - Windows NT Workstation
  - Microsoft Office and Office Professional
  - Client Paks (available in units of 5 or 20)

Microsoft Systems Management Server

In a Systems Management Server hierarchy, at least one Server License for a SQL Server is required and must be purchased separately. A Server License for Windows NT Server is also required for each server using server code (such as primary, secondary, and helper) for a Systems Management Server. Therefore, if you need to purchase Server Licenses to run three server products (Systems Management Server, SQL Server, and Windows NT Server) on the same computer, it is cheaper to purchase the BackOffice Server License.

Microsoft SNA Server

Microsoft SNA Server requires a Server License for the server and Client Access Licenses for all computers that access the SNA Server. You can access SNA Server in many different ways. The most common form of access is through an application, such as Attachmate® Extra or an application developed with Visual Basic, that is accessing SNA services. Although you are not directly connected to SNA Server, the application that you are using is connected and so an SNA Server Client Access License is required.

Microsoft BackOffice 1.5

Microsoft BackOffice 1.5 is an integrated family of server products, consisting of Windows NT Server 3.51, Microsoft SQL Server 6.0, Microsoft SNA Server 2.11, Microsoft Systems Management Server 1.1, and Microsoft Mail 3.5. Like the other server products, Microsoft BackOffice is available in both a Server License and a Client Access License.

Customers may acquire Microsoft BackOffice Client Access Licenses to access standalone servers. In other words, a BackOffice Client Access License gives that client the right to access the services of all the server products mentioned above, regardless of whether the Server Licenses for those products were acquired through a BackOffice Server License or through individual product Server Licenses. A BackOffice Client Access License can only be used in the Per Seat licensing mode.

Microsoft FPNW and Microsoft DSMN

If you want to use the File and Print Services for NetWare program with Windows NT Server 3.51, you must purchase Windows NT Server Client Access Licenses, which can be used in either the Per Seat or Per Server mode.

If you want to use the Directory Service Manager for NetWare program, you only need to purchase Windows NT Server Client Access Licenses if you are also using Windows NT Server basic network services.

Microsoft Services for Macintosh

If you want to use the Services for Macintosh program with Windows NT Server 3.51, you must purchase Windows NT Server Client Access Licenses, which can be used in either the Per Seat or Per Server mode.

FTP, Gopher, WWW, or RAS Server

To set up an FTP, Gopher, or WWW (World Wide Web) site, you only need to purchase a Server License. You do not need to make sure that every user has a Client Access License from Microsoft. Microsoft includes an FTP server with the Windows NT Server product, and you can use any public-domain or commercially available Gopher or Web server or the ones shipped with this *Windows NT Resource Kit.*

If you also want to use the Microsoft Remote Access Service for PPP or SLIP dial-in support, then you also need one Client Access License per connection. In other words, if the site supports 10 concurrent connections, you need to purchase a Server License and 10 Client Access Licenses for basic network services in the Per Server mode. If the site supports workstations in the Per Seat mode, you need to purchase a Server License and Client Access Licenses for basic network services for each workstation. If you increase the number of concurrent connections allowed, you must then purchase additional Client Access Licenses in the Per Server mode up to the maximum number of concurrent users of the Remote Access Service.

Technical Notes on Licensing

The following sections provide detailed technical information that was beyond the scope of the preceding discussions on licensing modes and purchasing requirements. However, some of these sections were referenced in those preceding sections.

Using OLE To Export User Data to a Spreadsheet

This section provides an example of how to connect to the license controller in your domain and download the Per Seat licensing information for all the registered server products into a Microsoft Excel 4.0 spreadsheet. The following detailed comments describe the code example, written in Visual Basic for Applications (VBA), that is shown at the end of this section. A Microsoft Word for Windows 2.0x file (LLSOBJT.DOC) containing descriptions of the properties of all the objects listed in this example is included on the *Windows NT Resource Kit* CD.

You must first create an instance of the Llsmgr Application object via CreateObject or GetObject. The Llsmgr Application object is listed in the Registry under "Llsmgr.Application.1," but this registration takes place during the startup of the License Manager application. This means that for this, or any other, macro involving the Llsmgr Application object to work properly, the Registry must first be updated either by running License Manager at least once or by manually adding the Llsmgr Application object Registry entries via the Registry Editor configuration utility.

Once the Llsmgr Application object has been properly registered and an instance of the object has been created, you must next locate (and connect to) the domain's enterprise server (either the primary domain controller or some specific server in the domain that has been configured as the repository of license information). The SelectDomain method of the Llsmgr Application object does just that. Given a domain name, the Llsmgr Application object searches for the enterprise server for that domain and then connects. If no domain name is given, the Llsmgr Application object attempts to find the local domain's enterprise server.

Once you are connected to the enterprise server, you can query the Llsmgr Application object for an instance of the Controller object respresenting the enterprise server. The ActiveController property of the Llsmgr Application object does exactly that. With the enterprise server's Controller object, you can query for the licensing information in which you are interested.

In this example, you want to view the Per Seat status of all the products registered in the domain. The enterprise server's Controller object has a property called Products, which is a collection object that contains a Product object for each of the registered server products in the domain. The number of Product objects in the collection (and, therefore, the number of registered server products in the domain) is described in the collection object's property Count, and an individual Product object can be accessed via the collection object's method Item(). By enumerating over the entire Products collection, statistics for each of the server products in the domain can be easily obtained.

Each Product object has a property called InUse and another called PerSeatLimit. The former describes the number of Per Seat licenses currently being consumed for the server product, and the latter describes the total number of Per Seat licenses registered for the server product. Simply by querying the properties of these objects, you can quickly determine license compliance status as well as server product usage to make more informed decisions about license and product purchases.

The preceding has described the following VBA code example:

```
Sub GetProducts()
    Dim Llsmgr As Object
    Set Llsmgr = CreateObject("Llsmgr.Application.1")

    Llsmgr.SelectDomain

    Dim EnterpriseServer As Object
    Set EnterpriseServer = Llsmgr.ActiveController

    Dim Products As Object
    Set Products = EnterpriseServer.Products

    Dim nProducts As Long
    nProducts = Products.Count

    Range("A1").Value = "Product Name"
    Range("B1").Value = "Licenses Purchased"
    Range("C1").Value = "Licenses In Use"

    Dim index As Long
    Dim Product As Object
    While nProducts
        nProducts = nProducts - 1
        Set Product = Products.Item(nProducts)
        ActiveCell.Offset(1, 0).Range("A1").Select
        ActiveCell.Offset(0, 0).Range("A1").Value = Product.Name
        ActiveCell.Offset(0, 1).Range("A1").Value = Product.PerSeatLimit
        ActiveCell.Offset(0, 2).Range("A1").Value = Product.InUse
    Wend
End Sub
```

Installing License Manager on Windows NT Workstation

To install and run License Manager (LLSMGR.EXE) on a Windows NT Workstation computer, you only need to copy the following files from a Windows NT Server computer into the \SYSTEM32 (or any other) directory on the Windows NT Workstation computer.

- LLSMGR.HLP
- LLSMGR.EXE
- LLSRPC.DLL

Counting Connections Twice for Licensing

Consider the following scenario in which two licenses are assigned to the same user. (This can only happen on Windows NT Workstation or Windows NT Server and not on Windows for Workgroups or Windows 95.) A primary domain controller (PDC) has its Guest account disabled. It has a share by the name of LLS and a user with the name DomUser, whose password is also DomUser.

From DomainA, the user connects, in Per Seat mode, to the PDC using the following command:

```
net use * \\pdc\lls /u:DomUser DomUser
```

This gets counted as DomainA\DomUser, and one license is assigned.

From DomainB, the user connects via RAS to the PDC using the same command as before. This gets counted as DomainB\DomUser, and another license is assigned.

What has happened is that you didn't specify the domain and so the local account on the PDC is giving you access, but your connection is still from the remote domain. To avoid this situation, the user must specify their domain name along with their username. For example, if you specify the same name from both domains, that is /u:DomainA\DomUser, the PDC will count it as a single connection and assign a single license.

Another solution, if you are using a notebook or laptop computer that is disconnected from the network, is to log on as the domain user account rather than as the local user. Then, if you connect via RAS to the network, you are only assigned one license and not two.

Reestablishing Lost Connections

A lost connection with a domain server will result in the error message "The RPC server is unavailable." To reestablish a lost connection with a server, reselect the domain.

CHAPTER 3

Security

Computer security refers to the protection of all components — hardware, software, and stored data — of a computer or a group of computers from damage, theft, or unauthorized use. A computer security plan that is well thought out, implemented, and monitored makes authorized computer use easy and unauthorized use or accidental damage difficult or impossible.

This chapter is written primarily for Windows NT system administrators. However, there are some issues that end users need to be aware of as well.

Establishing Computer Security

This section deals with the following topics on Windows NT security:

- Levels of security
- Off-the-shelf versus custom software
- Windows NT security features
- Performance monitoring

Levels of Security

Windows NT allows you to establish a full range of levels of security, from no security at all to the C2 level of security required by many government agencies. In this chapter we describe three levels of security — "Minimal," "Standard," and "High-Level" — and the options used to provide each level. These levels are arbitrary, and you will probably want to create your own "level" by blending characteristics of the levels presented here.

Why not have maximum security at all times? One reason is that the limits you set on access to computer resources make it a little harder for people to work with the protected resources. Another is that it is extra work to set up and maintain the protections you want. For example, if only users who are members of the HR user group are allowed to access employee records, and a new person is hired to do that job, then someone needs to set up an account for the new hire and add that account to the HR group. If the new account is created but not added to HR, the new hire cannot access the employee records and therefore cannot perform his or her job.

If the security is too tight, users will try to circumvent security in order to get work done. For example, if you set the password policy so that passwords are hard to remember, users will write them down to avoid being locked out. If some users are blocked from files they need to use, their colleagues might share their own passwords in order to promote the flow of work.

The first step in establishing security is to make an accurate assessment of your needs. Then choose the elements of security that you want, and implement them. Make sure your users know what they need to do to maintain security, and why it is important. Finally, monitor your system and make adjustments as needed.

Off-the-Shelf vs. Custom Software

If you are using software made especially for your installation, or if you are using shareware that you aren't sure you can trust, and you want to maintain fairly high security, you might want to look at Appendix D, "Security In a Software Development Environment." This provides information on settings and calls that can support — or circumvent — security settings.

Windows NT Security Features

Windows NT has features designed to make it easy to give permissions to some groups of users while denying those permissions to others. These features are discussed in detail in the documentation for Windows NT Workstation or Windows NT Server, and elsewhere in the *Windows NT Resource Kit.* You'll need to become familiar with this information in order to plan and implement the security configuration of your choice.

The following table lists documents that are referred to in this discussion of computer security.

For information on	See
audit policy	"User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide.*
auditing	"User Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide;* "Event Viewer" chapter of the Windows NT Workstation or Windows NT Server *System Guide*; "Auditing Security Events" in Chapter 2, "Windows NT Security Model," of the *Windows NT Resource Guide.*
automatic logon	Chapter 12, "Configuration Management and the Registry," of the *Windows NT Resource Guide.*
Backup utility	"Backup" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*
file and directory protections	"File Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*
file protection inheritance	Chapter 2, "Windows NT Security Model," in the *Windows NT Resource Guide.*
Guest account	"User Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*
Internet security issues	Chapter 20, "Using Windows NT on the Internet," in the *Windows NT Networking Guide* (part of the Windows NT Resource Kit for Windows NT version 3.5).
password enforcement options	"User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide.*
Performance Monitor	"Performance Monitor" chapter in the Windows NT Server *System Guide;* *Optimizing Windows NT*, in the Windows NT Resource Kit.
printer access settings	"Print Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*
programming calls that affect security settings	Appendix D, "Security In a Software Development Environment," of this *Windows NT Update 1* book .
Registry and the Registry Editor; protecting keys in the Registry	Part IV, "Windows NT Registry," of the *Windows NT Resource Guide.*
screen savers and how to set (including lock) them	"Control Panel" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

For information on	See
security log	"Event Viewer" chapter of the Windows NT Workstation or Windows NT Server *System Guide;.* Chapter 2, "Windows NT Security Model," of the *Windows NT Resource Guide;* Appendix D, "Security In a Software Development Environment," of this *Windows NT Update 1* book.
user accounts	"User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide.*
User Manager features	"User Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

User Accounts

The key to Windows NT security is the user accounts. You can create as many accounts as are needed, and you can include any user account in as many groups of accounts as are appropriate. You can then permit or limit access to any computer resource to individual accounts or to groups. User accounts are discussed in detail in the "User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide*.

Passwords

In the "User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide* you'll also find a description of the password enforcement options, such as minimum password length, minimum and maximum password age, password "uniqueness" (how often a password can be reused), and controls over whether a user can — or must — change his or her password.

File and Directory Protection

A range of file protections can be set on a per-file or per-directory basis. The protections can be on a per-user or per-group basis. This feature is described in the "Securing Directories and Files" section of the "File Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide* and in Chapter 2, "Windows NT Security Model," in the *Windows NT Resource Guide*. Note particularly the section on "Access Control Inheritance" in Chapter 2 of the *Windows NT Resource Guide*. Specific files to protect are discussed later in this manual, in the section "Protecting Files and Directories" under "High-Level Security."

Registry Protection

Since the Registry is the repository of all system configuration information, it is important to protect it from unauthorized changes. At the same time, individuals and programs that need to access or alter information in the Registry must be allowed to do so. Part IV, "Windows NT Registry," of the *Windows NT Resource Guide* discusses the Registry and the Registry Editor, including information on protecting keys in the Registry. Specific keys to protect are discussed later in this manual, in the "Protecting the Registry" sections under "Standard Security" and "High-Level Security."

Printer Protection

You can prevent specific users from printing to a system printer for all or part of the day. This feature is described in the "Print Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

Auditing

Auditing is built into Windows NT. This allows you to track which user account was used to attempt what kind of access to files or other objects. Auditing also can be used to track logon attempts, system shutdowns or restarts, and similar events. Auditing is described in the "Event Viewer" chapter of the Windows NT Workstation or Windows NT Server *System Guide* and in Chapter 2, "Windows NT Security Model," in the *Windows NT Resource Guide.*

Monitoring Performance

The Windows NT Performance Monitor not only helps administrators fine-tune performance, it can also give warning of approaching problems before they are noticeable by the computer user. Performance Monitor can also help you spot the activity of a virus (by spotting performance degradation) or an attempted break–in (by tracking logon attempts). Performance Monitor can be set to send an alert to one or more administrators when certain events occur. The "Performance Monitor" chapter in the Windows NT Server *System Guide* documents the use of this utility.

For a thorough discussion of performance monitoring in Windows NT, see *Optimizing Windows NT*, in the *Windows NT Resource Kit.*

Minimal Security

You might not be concerned with security at all if the computer is not used to store or access sensitive data or if it is in a very secure location. For example, if the computer is in the home office of a sole proprietor of a business, or if it is used as a test machine in the locked lab of a software development company, then security precautions might be unnecessarily cumbersome. Windows NT allows you to make the system fully accessible, with no protections at all, if that is what your setup requires.

Physical Security Considerations

Take the precautions you would with any piece of valuable equipment to protect against casual theft. This step can include locking the room the computer is in when no one is there to keep an eye on it, or attaching the unit to a wall with a locked cable. You might also want to establish procedures for moving or repairing the computer, so that the computer or its components cannot be taken under false pretenses.

Use a surge protector or power conditioner to protect the computer and its peripherals from power spikes. Also, perform regular disk scans and defragmentation to isolate bad sectors and to maintain the highest possible disk performance.

Software Security Considerations

For minimal security, none of the Windows NT security features are used. In fact, you can allow automatic logon to the Administrator account (or any other user account) by following the directions in Chapter 12, "Configuration Management and the Registry," of the *Windows NT Resource Guide*. This allows anyone with physical access to the computer to turn it on and immediately have full access to the computer's resources.

By default, access is limited to certain files. For minimal security, give the Everyone group full access to all files.

You should still take precautions against viruses, since they can disable programs you want to use or use the minimally secure computer as a vector to infect other computer systems.

Standard Security

Most often, computers are used to store sensitive and/or valuable data. This data could be anything from financial data to personnel files to personal correspondence. Also, you might need to protect against accidental or deliberate changes to the way the computer is set up. But the computer's users need to be able to do their work, with minimal barriers to the resources they need.

Physical Security Considerations

As with minimal security, the computer should be protected as any valuable equipment would be. Generally, this involves keeping the computer in a building that is locked to unauthorized users, as most homes and offices are. In some instances you might want to use a cable and lock to secure the computer to its location. If the computer has a physical lock, you can lock it and keep the key in a safe place for additional security. However, if the key is lost or inaccessible, an authorized user might be unable to work on the computer.

Software Security Considerations

A secure system requires effort from both the system administrators, who maintain certain software settings, and the everyday users, who must cultivate habits such as logging off at the end of the day and memorizing (rather than writing down) their passwords.

Displaying a Legal Notice Before Logon

Windows NT can display a message box with the caption and text of your choice before a user logs on. Many organizations use this message box to display a warning message that notifies potential users that they can be held legally liable if they attempt to use the computer without having been properly authorized to do so. The absence of such a notice could be construed as an invitation, without restriction, to enter and browse the system.

The logon notice can also be used in settings (such as an information kiosk) where users might require instruction on how to supply a username and password for the appropriate account.

To display a legal notice, use the Registry Editor to create or assign the following Registry key values on the workstation to be protected:

Hive:	HKEY_LOCAL_MACHINE
Key:	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeCaption
Type:	REG_SZ
Value:	Whatever you want for the title of the message box

Hive:	HKEY_LOCAL_MACHINE
Key:	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeText
Type:	REG_SZ
Value:	Whatever you want for the text of the message box

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Examples

Welcome to the XYZ Information Kiosk

Log on using account name Guest and password XYZCorp.

Authorized Users Only

Only individuals currently assigned an account on this computer by XYZCorp may access data on this computer. All information stored on this computer is the property of XYZCorp and is subject to all the protections accorded intellectual property.

User Accounts and Groups

With standard security, a user account (username) and password should be required in order to use the computer. You can establish, delete, or disable user accounts with User Manager, which is in the Administrative Tools program group. User Manager also allows you to set password policies and organize user accounts into Groups. The "User Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide* provides detailed information on the features available through User Manager, and how to implement them.

Note Changes to the Windows NT computer user rights policy take effect when the user next logs on.

Administrative Accounts versus User Accounts

Use separate accounts for administrative activity and general user activity. Individuals who do administrative work on the computer should each have two user accounts on the system: one for administrative tasks, and one for general activity. To avoid accidental changes to protected resources, the account with the least privilege that can do the task at hand should be used. For example, viruses can do much more damage if activated from an account with Administrator privileges.

It is a good idea to rename the built-in Administrator account to something less obvious. This powerful account is the one account that can never be locked out due to repeated failed logon attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. By renaming the account, you force hackers to guess the account name as well as the password.

The Guest Account

Limited access can be permitted for casual users through the built-in Guest account. If the computer is for public use, the Guest account can be used for public logons. Prohibit Guest from Writing or Deleting any files, directories, or Registry keys (with the possible exception of a directory where information can be left). In a standard security configuration, a computer that allows Guest access can also be used by other users for files that they don't want accessible to the general public. These users can log on with their own user names and access files in directories on which they have set the appropriate permissions. They will want to be especially careful to log off or lock the workstation before they leave it. The Guest account is discussed in the "User Manager" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

Logging On

All users should *always* press CTRL+ALT+DEL before logging on. Programs designed to collect account passwords can appear as a logon screen that is there waiting for you. By pressing CTRL+ALT+DEL you can foil these programs and get the secure logon screen provided by Windows NT.

Logging Off or Locking the Workstation

Users should either log off or lock the workstation if they will be away from the computer for any length of time. Logging off allows other users to log on (if they know the password to an account); locking the workstation does not. The workstation can be set to lock automatically if it is not used for a set period of time by using any 32-bit screen saver with the Password Protected option. Screen savers and how to set them are discussed in the "Control Panel" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

Passwords

Anyone who knows a username and the associated password can log in as that user. Users should take care to keep their passwords secret. Here are a few tips:

- Change passwords frequently, and avoid reusing passwords.
- Avoid using easily guessed words and words that appear in the dictionary. A phrase or a combination of letters and numbers works well.
- Don't write a password down — choose one that is easy for you to remember.

Protecting Files and Directories

The NTFS file system provides more security features than the FAT system, and should be used whenever security is a concern. The only reason to use FAT is for the boot partition of an ARC-compliant RISC system. A system partition using FAT can be secured in its entirety using the Secure System Partition command on the Partition menu of the Disk Administrator utility.

With NTFS, you can assign a variety of protections to files and directories, specifying which groups or individual accounts can access these resources in which ways. By using the inherited permissions feature and by assigning permissions to groups rather than to individual accounts, you can simplify the chore of maintaining appropriate protections. See the "File Manager" chapter of your Windows NT Workstation or Windows NT Server *System Guide* for information on assigning file and directory protections. For a discussion of inherited permissions, including how and when they are applied, see Chapter 2, "Windows NT Security Model," in the *Windows NT Resource Guide.*

In particular, make sure that users know that if they move rather than copy a file to a different directory on the same volume, it continues to have the protections it had before it was moved. If they copy the file, it inherits the protections (either more or less restrictive) from the directory it is copied to.

For example, a user might copy a sensitive document to a directory that is accessible to people who should not be allowed to read the document, thinking that the protections assigned to the document in its old location would still apply. In this case the protections should be set on the document as soon as it is copied, or else it should be first moved to the new directory, then copied back to the original directory.

On the other hand, if a file that was created in a protected directory is being placed in a shared directory so that other users can read it, it should be copied to the new directory, or if it is moved to the new directory the protections on the file should be promptly changed so that other users can read the file.

When permissions are changed on a file or directory, the new permissions apply any time the file or directory is subsequently opened. Users who already have the file or directory open when you change the permissions are still allowed access according to the permissions that were in effect when they opened the file or directory.

Backups

Regular backups protect your data from hardware failures and honest mistakes, as well as from viruses and other malicious mischief. The Windows NT Backup utility is described in the "Backup" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

Obviously, files must be read to be backed up, and they must be written to be restored. Backup privileges should be limited to Administrators and Backup operators — people to whom you are comfortable giving read and write access on all files.

Protecting the Registry

All the initialization and configuration information used by Windows NT is stored in the Registry. Normally, the keys in the Registry are changed indirectly, through the administrative tools such as the Control Panel. This method is recommended. The Registry can also be altered directly, with the Registry Editor; some keys can be altered in no other way.

The Registry Editor should be used only by individuals who thoroughly understand the tool, the Registry itself, and the effects of changes to various keys in the Registry. Mistakes made in the Registry Editor could render part or all of the system unusable.

The Backup utility included with Windows NT allows you to back up the Registry as well as files and directories.

Auditing

Auditing can inform you of actions that could pose a security risk and also identify the user accounts from which audited actions were taken. Auditing is discussed in the "User Manager" and "Event Viewer" chapters of the Windows NT Workstation or Windows NT Server *System Guide* and in Chapter 2, "Windows NT Security Model," of the *Windows NT Resource Guide.*

Note that auditing only tells you what user accounts were used for the audited events. If passwords are adequately protected, this in turn indicates which user attempted the audited events. However, if a password has been stolen or if actions were taken while a user was logged on but away from the computer, the action could have been initiated by someone other than the person to whom the user account is assigned.

When you establish an audit policy you'll need to weigh the cost (in disk space and CPU cycles) of the various auditing options against the advantages of these options. You'll want to at least audit failed logon attempts, attempts to access sensitive data, and changes to security settings. Here are some common security threats and the type of auditing that can help track them:

Threat	Action
Hacker-type break-in using random passwords	Enable failure auditing for logon and logoff events.
Break-in using stolen password	Enable success auditing for logon and logoff events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as logons at odd hours or on days when you would not expect any activity.
Misuse of administrative privileges by authorized users	Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events. (Note: Because of the high volume of events that would be recorded, Windows NT does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights. Appendix D, "Security In a Software Development Environment," explains how to enable auditing of the use of these rights.)
Virus outbreak	Enable success and failure write access auditing for program files such as files with .EXE and .DLL extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.
Improper access to sensitive files	Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.
Improper access to printers	Enable success and failure auditing for file- and object-access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

For step-by-step procedures for using User Manager to set up your system's audit policy, see the "User Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide.*

Managing the Security Log

You can specify the maximum size for the security log, and what happens when that size is reached, by following the directions in the "Event Viewer" chapter of the Windows NT Workstation or Windows NT Server *System Guide.*

One of the regular tasks of network administration is examining the security log to track significant events and monitor system usage, and clearing the log as necessary. It is recommended that you routinely archive the log before clearing it.

In additon to the "Event Viewer" chapter in the Windows NT Workstation or Windows NT Server *System Guide*, Chapter 2, "Windows NT Security Model," of the *Windows NT Resource Guide* provides information on viewing and managing the security log. If you need more detailed information, see the Appendix D, "Security In a Software Development Environment."

High-Level Security

The standard security precautions are sufficient for most installations. However, additional precautions are available for computers that contain very sensitive data, or that are at high risk for data theft or the accidental or malicious disruption of the system.

Physical Security Considerations

The physical security considerations discussed for mimimal and standard security configurations also apply here. In addition, you might want to examine the physical link provided by your computer network, and in some cases use controls built in to certain hardware platforms to restrict who can turn on the computer.

Networks and Security

When you put a computer on a network, you add an access route to the computer, and you'll want that route to be secure. User validation and protections on files and other objects are sufficient for standard-level security, but for high-level security you'll need to make sure the network itself is secure, or in some cases isolate the computer completely.

The two risks from network connections are other users on the network and unauthorized taps on the network. If everyone on the network has the security clearance needed to access your secure computer, you will probably prefer to include the computer in the network, to make it easier for these people to access data on the computer.

If the network is entirely contained in a secure building, the risk of unauthorized taps is minimized or eliminated. If the cabling must pass through unsecured areas, use optical fiber links rather than twisted pair to foil attempts to tap the wire and collect transmitted data.

If your installation needs access to the Internet, you should be aware of the security issues involved in providing access to—and from—the Internet community. Chapter 20, "Using Windows NT on the Internet," in the *Windows NT Networking Guide* contains information on using network topology to provide security.

Controlling Access to the Power Switch

You might choose to keep unauthorized users away from the power or reset switches on the computer, particularly if your computer's rights policy denies them the right to shut down the computer. The most secure computers (other than those in locked and guarded rooms) expose only the computer's keyboard, monitor, mouse, and (when appropriate) printer to users. The CPU and removable media drives can be locked away where only specifically authorized personnel can access them.

On many hardware platforms, the system can be protected using a *power-on password.* A power-on password prevents unauthorized personnel from starting an operating system other than Windows NT, which would compromise system security. Power-on passwords are a function of the computer hardware, not the operating system software. Therefore the procedure for setting up the power-on password depends on the type of computer, and is available in the vendor's documentation supplied with the system.

Software Security Considerations

Some high-security options can be implemented only by using the Registry Editor. The Registry Editor should be used only by administrators who are familiar with the material in Part IV, "Windows NT Registry," of the *Windows NT Resource Guide.*

User Rights

There are several user rights that administrators of high-security installations should be aware of and possibly audit. Of these, you might want to change the default permissions on two rights, as follows:

User Right	**Groups assigned this right by default**	**Recommended change**
Log on locally Allows a user to log on at the computer, from the computer's keyboard.	Administrators, Backup Operators, Everyone, Guests, Power Users, and Users	Deny Everyone and Guests this right.
Shut down the system (SeShutdownPrivilege) Allows a user to shut down Windows NT.	Administrators, Backup Operators, Everyone, Power Users, and Users	Deny Everyone and Users this right.

The rights in the following table generally require no changes to the default settings, even in the most highly secure installations.

User Right	**Allows**	**Initially assigned to**
Access this computer from the network	A user to connect over the network to the computer.	Administrators, Everyone, Power Users
Act as part of the operating system (SeTcbPrivilege)	A process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(None)
Add workstations to the domain (SeMachineAccountPrivilege)	Nothing. This right has no effect on computers running Windows NT.	(None)
Back up files and directories (SeBackupPrivilege)	A user to back up files and directories. This right supersedes file and directory permissions.	Administrators, Backup Operators
Bypass traverse checking (SeChangeNotifyPrivilege)	A user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Everyone
Change the system time (SeSystemTimePrivilege)	A user to set the time for the internal clock of the computer.	Administrators, Power Users

User Right	Allows	Initially assigned to
Create a pagefile (SeCreatePagefilePrivilege)	Nothing. This right has no effect in current versions of Windows NT.	Administrators
Create permanent shared objects (SeCreatePermanentPrivilege)	A user to create special permanent objects, such as \\Device, that are used within Windows NT.	(None)
Force shutdown from a remote system (SeRemoteShutdownPrivilege)	Nothing. This right has no effect in current versions of Windows NT.	Administrators, Power Users
Increase quotas (SeIncreaseQuotaPrivilege)	Nothing. This right has no effect in current versions of Windows NT.	(None)
Increase scheduling priority (SeIncreaseBasePriorityPrivilege)	A user to boost the execution priority of a process.	Administrators, Power Users
Load and unload device drivers (SeLoadDriverPrivilege)	A user to install and remove device drivers.	Administrators
Lock pages in memory (SeLockMemoryPrivilege)	A user to lock pages in memory so they cannot be paged out to a backing store such as PAGEFILE.SYS.	(None)
Log on as a batch job	Nothing. This right has no effect in current versions of Windows NT.	(None)
Log on as a service	A process to register with the system as a service.	(None)
Manage auditing and security log (SeSecurityPrivilege)	A user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Also, members of the Administrators group always have the ability to view and clear the security log.	Administrators

User Right	Allows	Initially assigned to
Modify firmware environment variables (SeSystemEnvironmentPrivilege)	A user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Administrators
Profile single process (SeProfSingleProcess)	Nothing. This right has no effect on computers running Windows NT.	Administrators, Power Users
Profile system performance (SeSystemProfilePrivilege)	A user to perform profiling (performance sampling) on the system.	Administrators
Replace a process-level token (SeAssignPrimaryTokenPrivilege)	A user to modify a process's security access token. This is a powerful right used only by the system.	(None)
Restore files and directories (SeRestorePrivilege)	A user to restore backed-up files and directories. This right supersedes file and directory permissions.	Administrators, Backup Operators
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	A user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators

Protecting Files and Directories

Among the files and directories to be protected are those that comprise the operating system software itself. The standard set of permissions on system files and directories provide a reasonable degree of security without interfering with the computer's usability. For very high level security installations, however, you might want to set directory permissions to all subdirectories and existing files, as shown in the following list, immediately after Windows NT is installed. Be sure to apply permissions to parent directories before applying permissions to subdirectories.

Directory	Permissions
\WINNT35	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\REPAIR	Administrators: Full Control

Directory	Permissions
\WINNT35\SYSTEM	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control
\WINNT35\SYSTEM32\DHCP	(Delete this directory)
\WINNT35\SYSTEM32\DRIVERS	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\RAS	(Delete this directory)
\WINNT35\SYSTEM32\OS2	(Delete this directory)
\WINNT35\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control
\WINNT35\SYSTEM32\WINS	(Delete this directory)

Several critical operating system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. In high-security installations you might want to assign the following permissions to these files:

File	C2-Level Permissions
\BOOT.INI, \NTDETECT.COM, \NTLDR	Administrators: Full Control SYSTEM: Full Control
\AUTOEXEC.BAT, \CONFIG.SYS	Everybody: Read Administrators: Full Control SYSTEM: Full Control

To view these files in File Manager, choose the By File Type command from the View menu, then select the Show Hidden/System Files check box in the By File Type dialog box.

Protecting the Registry

In addition to the considerations for standard security, the administrator of a high-security installation might want to set protections on certain keys in the Registry.

By default, protections are set on the various components of the Registry that allow work to be done while providing standard level security. For high-level security, you might want to assign access rights to specific Registry keys. This should be done with caution, since programs that the users require to do their jobs often need to access certain keys on the users' behalf. For more information, see Chapter 11, "Registry Editor and Registry Administration," in the *Windows NT Resource Guide.*

In particular, you might want to change the protections of the following keys so that the group Everyone is only allowed QueryValue, Enumerate Subkeys, Notify, and Read Control accesses.

In the HKEY_LOCAL_MACHINE on Local Machine dialog:

\Software\Microsoft\RPC (and its subkeys)

\Software\Microsoft\Windows NT\CurrentVersion

And under the \Software\Microsoft\Windows NT\CurrentVersion\ subtree:

Profile List

AeDebug

Compatibility

Drivers

Embedding

Fonts

FontSubstitutes

GRE_Initialize

MCI

FontSubstitutes

GRE_Initialize

MCI

MCI Extensions

Port (and all subkeys)

WOW (and all subkeys)

Windows3.1MigrationStatus (and all subkeys)

In the HKEY_CLASSES_ROOT on Local Machine dialog:

\HKEY_CLASSES_ROOT (and all subkeys)

The Schedule Service (AT Command)

The Schedule service (also known as the AT command) is used to schedule tasks to run automatically at a preset time. Because the scheduled task is run in the context run by the Schedule service (typically the operating system's context), this service should not be used in a highly secure environment.

By default, only Administrators can submit AT commands. To allow System Operators to also submit AT commands, use the Registry Editor to create or assign the following Registry key value:

Hive	HKEY_LOCAL_MACHINE\System
Key	\CurrentControlSet\Control\Lsa
Name	Submit Control
Type	REG_DWORD
Value	1

There is no way to allow anyone else to submit AT commands. The changes will take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Hiding the Last Username

By default, Windows NT places the username of the last user to log on the computer in the Username text box of the logon dialog. This makes it more convenient for the most frequent user to log on. To help keep usernames secret, you can prevent Windows NT from displaying the username from the last logon. This is especially important if a computer that is generally accessible is being used for the (renamed) built-in Administrator account.

To prevent display of a username in the Logon dialog box, use the Registry Editor to create or assign the following Registry key value:

Hive	HKEY_LOCAL_MACHINE
Key	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Name	DontDisplayLastUserName
Type	REG_SZ
Value	1

Restricting the Boot Process

Most personal computers today support the ability to start a number of different operating systems. For example, even if you normally start Windows NT from the C: drive, someone could select another version of Windows on another drive, including a floppy drive or CD-ROM drive. If this happens, any security precautions you have taken within your normal version of Windows NT might be circumvented.

In general, you should install only those operating systems that you want to be used on the computer you are setting up. For a highly secure system, this will probably mean installing one version of Windows NT. However, you still need to protect the CPU physically to ensure that no other operating system is loaded. Depending on your circumstances, you might choose to remove the floppy drive or drives. In some computers you can disable booting from the floppy drive by setting switches or jumpers inside the CPU. If you use hardware settings to disable booting from the floppy drive, you might want to lock the computer case (if that is an option with the computer you have) or lock the machine in a cabinet with a hole in the front to provide access to the floppy drive. If the CPU is in a locked area away from the keyboard and monitor, drives cannot be added or hardware settings changed for the purpose of starting from another operating system.

Allowing Only Logged-On Users to Shut Down the Computer

Normally, you can shut down a computer running Windows NT Workstation without logging on by choosing Shutdown in the Logon dialog box. This is appropriate where the computer's operational switches can be accessed by users; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down Windows NT Workstation. However, you can remove this feature if the CPU is locked away so users cannot reset it or turn off its power. This step is not required for Windows NT Server, because it is configured this way by default.

To require users to log on before shutting down the computer, use the Registry Editor to create or assign the following Registry key value:

Hive	HKEY_LOCAL_MACHINE
Key	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Name	ShutdownWithoutLogon
Type	REG_SZ
Value	0

The changes will take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Controlling Access to Removable Media

By default, Windows NT allows any program to access files on floppy disks and CD-ROMs. In a highly secure, multi-user environment, you might want to allow only the person interactively logged on to access those devices. This allows the interactive user to write sensitive information to these drives, confident that no other user or program can see or modify that data.

When operating in this mode, the floppy disks and/or CD-ROMs on your system are allocated to a user as part of the interactive logon process. These devices are automatically freed for general use or for reallocation when that user logs out. Because of this, it is important to remove sensitive data from the floppy or CD-ROM drives before logging off.

Note Windows NT allows all users access to the tape drive, and therefore any user can read and write the contents of any tape in the drive. In general this is not a concern, because only one user is interactively logged on at a time. However, in some rare instances, a program started by a user can continue running after the user logs off. When another user logs on and puts a tape in the tape drive, this program can secretly transfer sensitive data from the tape. If this is a concern, restart the computer before using the tape drive.

Allocating Floppy Drives During Logon

To allocate floppy drives during logon, use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE
Key:	Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateFloppies
Type:	REG_DWORD
Value:	1

If the value does not exist, or is set to any other value, then floppy devices will be available for shared use by all processes on the system.

This value will take effect at the next logon. If a user is already logged on when this value is set, it will have no effect for that logon session. The user must log off and log on again to cause the device(s) to be allocated.

▸ **To allocate CD-ROMs during logon**

Use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE
Key:	Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateCDRoms
Type:	REG_DWORD
Value:	1

If the value does not exist, or is set to any other value, then CD-ROM devices will be available for shared use by all processes on the system.

This value will take effect at the next logon. If a user is already logged on when this value is set, it will have no effect for that logon session. The user must log off and log on again to cause the device(s) to be allocated.

C2 Security

The National Computer Security Center (NCSC) is the United States government agency responsible for performing software product security evaluations. These evaluations are carried out against a set of requirements outlined in the NCSC publication "*Department of Defense Trusted Computer System Evaluation Criteria,*" which is commonly referred to as the "Orange Book." Windows NT 3.5 has been successfully evaluated by the NCSC at the C2 security level as defined in the Orange Book.

Evaluation versus Certification

The National Computer Security Center (NCSC) evaluation process does a good job of ensuring that Windows NT can properly enforce your security policy, but it does not dictate what your security policy must be. There are many features of Windows NT that need to be considered when determining how to use the computer within your specific environment. What level of auditing will you require? How should your files be protected to ensure that only the right people can access them? What applications should you allow people to run? Should you use a network? If so, what level of physical isolation of the actual network cable is needed?

To address the environmental aspects of a computing environment, the NCSC has produced a document called *Introduction to Certification and Accreditation.* In this document "certification" is described as a plan to use computer systems in a specific environment, and "accreditation" is the evaluation of that plan by administrative authorities. It is this certification plan, and the subsequent accreditation procedure, that balances the sensitivity of the data being protected against the environmental risks present in the way the computing systems are used. For example, a certification plan for a university computing lab might require that computers be configured to prevent starting from a floppy disk, to minimize the risk of infection by virus or Trojan Horse programs. In a top-secret Defense Department development lab, it might be necessary to have a fiber-optic LAN to prevent generation of electronic emissions. A good certification plan covers all aspects of security, from backup/recovery mechanisms to the Marine guards standing at the front door of your building.

Additional C2 Evaluation Information

If you need to set up a C2-certifiable system, contact the Microsoft Federal Office for a copy of "Microsoft Report on C2 Evaluation of Windows NT." This document lists the hardware configurations in which Windows NT has been evaluated; the list is updated as more configurations are tested. The document also specifies the set of features that were implemented for C2 evaluation, so that you can duplicate them if necessary for your own C2-certifiable system. These features are essentially those recommended for high-level security in this document.

For your C2 certification, you will need to choose the combination of security features described in this document, in the Windows NT documentation, and in the *Windows NT Resource Kit* that fits your particular combination of resources, personnel, work flow, and perceived risks. You might also want to study Appendix D, "Security In a Software Development Environment," especially if you are using custom or in-house software. This appendix also provides information on managing and interpreting the security log, and technical details on special-case auditing (for example, auditing base objects).

Setting Up a C2-compliant System

To make it easier to set up a C2-compliant system, the C2Config application has been created and included in this *Windows NT Resource Kit.* C2CONFIG.EXE lets you choose from the settings used in evaluating Windows NT for C2 security, and implement the settings you want to use in your installation. For details, see the online Help included with the application.

CHAPTER 4

Internet Services and Security

The easiest way to become an information content provider on the Internet is with a Windows NT Server and the software included in the *Windows NT 3.51 Resource Kit*. This platform is transparent to your Internet clients—connections are made in the same way as with any other information provider. But as the administrator of the Internet server, you'll appreciate the ease of administration that you get with Windows NT. Also, with Windows NT you are not tied to any particular manufacturer for the computer you use as an Internet server. And, of course, a computer running Windows NT can be used for a wide variety of tasks.

Any computer with the hardware requirements to run Windows NT Server can be used as an Internet information provider. The only additional items you need are a modem, an account with an Internet provider supporting PPP or SLIP, and ideally an ISDN line, frame relay, or dedicated leased line to support the traffic an information provider might encounter. Depending on the usage your server handles, you might choose to exceed the minimums for memory and disk space recommended for a Windows NT Server.

To set up your Internet server, install the following software from the *Windows NT 3.51 Resource Kit* CD.

- File Transfer Protocol (FTP) Server service
- Gopher Server service
- World Wide Web (WWW) Server service
- Wide Area Information Server (WAIS) service
- WAIS Toolkit
- Telnet Server service
- Mail Server service

All of these components are documented in online Help and in the *Windows NT Networking Guide*, except for the Telnet and Mail Server utilities, which are not included in the *Networking Guide*. They are documented in the following sections.

Telnet Server Service

The Telnet Server service has two components: the service itself (TELNETD.EXE) and an underlying component, the *Remote Session Manager*. The Telnet Server service operates by connecting to the Remote Session Manager component, which in turn is responsible for initiating, terminating, and managing telnet sessions. Remote Session Manager includes a number of command-line utilities designed to make it easier to work in a remote character session environment.

Mail Server Service

The Mail Server service is an implementation of the SendMail daemon and POP 2 and POP 3 protocols, for Windows NT Workstation and Windows NT Server. The Mail Server installation program adds Mail Server and the supporting services to the Service Controller and starts Mail Server. Mail Server supports Internet-based mail clients, and is completely separate from the MS-Mail program.

Caution Mail Server only supports the cleartext password authentication of POP 3. It does not support the APOP command. Since the user's password travels over the network in the clear, administrators should use caution when installing a mail system such as this.

Because Mail Server is integrated with the local account database, an account must be created (via User Manager) for each user who is to receive mail at the computer where Mail Server is running. Mail Server automatically creates a mail folder for a user when mail is received for that user or when the user connects via POP.

The intermediate files required by Mail Server, and the mailboxes, are all spooled on the Windows NT server. They can then be accessed through PD or through commercial clients such as Eudora™ from Qualcomm.

Mail Server includes the following services:

- MtpSrv, which handles receiving SMTP mail
- Pop3Srv, which handles POP clients
- LocalMail, which handles delivery of local mail
- PasswdSrv, which handles Eudora password change requests. By default, PasswdSrv is not enabled, since it allows password changes based on unencrypted requests.

Registry Entries for Mail Server

The Registry entries look something like the following:

```
MACHINE\System\CurrentControlSet\Services\MailSrv
    Parameters
        MailDirectory
        LoggingLevel
        SMTP Retry
        Local Retry
        SmtpGateway
        Inbound Transforms
        Outbound Transforms
        Alias
        Alias...
```

where:

MailDirectory
Is the top of the mail directory hierarchy.

LoggingLevel
Specifies flags indicating how much to dump into the event log.

SMTP Retry
Specifies the retry interval in seconds for outbound SMTP messages.

Local Retry
Specifies the retry interval in seconds for local messages.

SmtpGateway
Specifies the gateway to use for all SMTP mail. (No DNS resolving is done.)

Inbound Transforms
Are rules applied to addresses coming in. See the following section for details.

Outbound Transforms
Are rules applied to addresses going out. See the following section for details.

Alias
Specifies one alias per line. They are completely dynamic. Two examples are placed there during installation, one for Postmaster, which is required and must not be deleted, and one for MAILER_DAEMON.

Transforms

The transforms are rules applied to addresses coming in and going out. Primarily they are there so that if you own a domain, you can mask out the computernames within the domain, and vice versa.

Inbound Transforms and Outbound Transforms are each of type REG_MULTI_SZ. Each line in the MULTI_SZ is a transform, and they are searched in the order they appear. If a rule matches, it is applied, and the search is completed. If no rules are matched, then the address is unchanged.

Each transform is in the following format:

```
pattern > the transformed pattern
```

For example:

```
$1@$2.bitnet > $1%$2.bitnet@cunyvm.cuny.edu
```

The following special tokens are recognized:

- **$(Me)**, which corresponds to **hostname.domain**
- **$(Hostname)**, which corresponds to **hostname**
- **$(Domain)**, which corresponds to **domain**

For example, the address richardw@microsoft.com would be tokenized as follows:

```
$1@$2            richardw = 1, microsoft.com = 2
$1@microsoft.com     richardw = 1
```

The address rbw@williams.bitnet would be:

```
$1@$2.bitnet > $1%$2.bitnet@cunyvm.cuny.edu
rbw = 1
williams = 2
final = rbw%williams.bitnet@cunyvm.cuny.edu
```

Using Windows NT Workstation as an Internet Client

From the client side, Windows NT Workstation is an easy way to access the Internet. All you need is Windows NT Workstation installed on a computer with at least the minimum hardware requirements, a modem, and an account with an Internet provider that supports PPP or SLIP. You can then use Remote Access Service (RAS) to access the Internet.

When you add the phone number for your Internet provider to your RAS phone book, you'll need to either enter the IP address assigned to you by your provider or specify that the IP address is received from the host. Unless you are sure your provider is using Windows NT Server to receive your connection, you'll also need to make sure that the Domain Name field is blank for your provider's phone number.

Security and the Internet

While a computer is open to the Internet, it is open to a wide range of computer users. Some of these users might want to access data you do not intend to share, or might try to use your computer as an entry point to sensitive data elsewhere on the Internet. Therefore, you might want to maintain a higher level of security on a computer that connects to the Internet than you would if the computer were used on your local network only. Chapter 3, "Security," in this *Windows NT Update 1* book provides a discussion of various levels of security and how to implement them.

CHAPTER 5

SNMP

Simple Network Management Procotol (SNMP) is a network management protocol widely used in TCP/IP networks, and, more recently, with Internet Package Exchange (IPX) networks. This chapter assumes that you are familiar with network management and TCP/IP. For more information about these subjects, see the *Windows NT Networking Guide* and the books in the "Reference Materials" section at the end of this chapter.

SNMP communicates between a management program run by an administrator and the network management agent running on a host. SNMP defines the form and meaning of the messages exchanged, the representation of names and values in the messages, and administrative relationships among hosts being managed.

In this chapter the following terminology is used.

- *Host* is any computer running SNMP
- *Management system* is any computer running SNMP management software.
- *Agent* is any computer running SNMP agent software, typically a server or router.

This chapter combines information from several earlier sources into a single location, and includes new material to tie the subject into a cohesive unit. It supersedes SNMP materials in the following sources:

- Chapters 10, 11, 12, and 14 of the *Windows NT Networking Guide*
- Chapter 4 in the *Windows NT Server Update Information for Version 3.51* books
- The Windows NT Software Development Kit (SDK) CD-ROM file \MSTOOLS\BIN\WINNT\SNMP.TXT, titled *NOTES ON SNMP DEVELOPMENT FOR WINDOWS/NT*

This chapter also contains information from the following Windows NT Knowledge Base (KB) articles:

- SNMP Agent Responds to Any Community Name (Q99880)
- TCP, IP, ICMP, UDP Counters with PERFMON.EXE (Q102629)
- REG: SNMP Service Entries (Q102970)
- SNMP Agent Breaks Up Variable Bindings List (Q127870)
- How To Add an SNMP Extension Agent to the NT Registry (Q128729)
- PRB: SnmpMgrStrToOid Assumes Oid Is in Mgmt Subtree (Q129063)

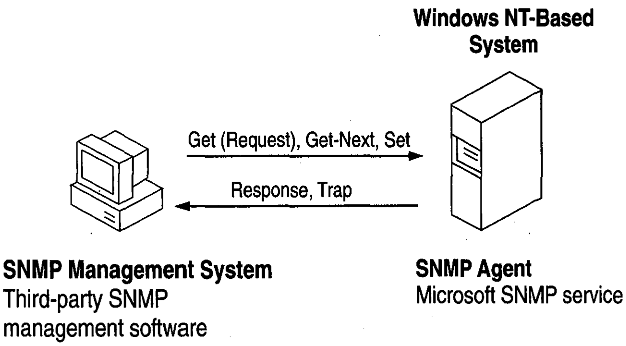
This chapter begins with a general discussion of SNMP and its implementation on Windows NT servers and workstations. The chapter continues with information on installing and configuring SNMP, using SNMP, and programming considerations for SNMP. The chapter concludes with a list of reference materials.

What is SNMP?

SNMP is a part of the TCP/IP protocol suite. It was originally developed in the Internet community to monitor and troubleshoot routers and bridges. SNMP transports management information and commands between a management system and an SNMP agent, with management tools such as Hewlett-Packard® OpenView, IBM® NetView®, and Sun® Net Manager. The SNMP agent sends status information to one or more hosts when the host requests it or when a significant event occurs.

These are some of the entities that administrators can use SNMP to monitor and control:

- Computers running Windows NT
- LAN Manager servers
- Routers or gateways
- Bridges and concentrators
- Minicomputers or mainframe computers
- Terminal servers



The primary function of a management system is to request information from an agent. A management system can initiate the **get**, **get-next**, and **set** operations.

- The **get** operation is a request for a specific value, such as the amount of hard disk space available.
- The **get-next** operation is a request for the "next" value. This operation traverses a conceptual table of objects.
- The **set** operation changes the value of a variable. Only variables with read-write access can be set.

The primary function of an agent is to perform the **get**, **get-next**, and **set** operations requested by a management system. The only operation initiated by an agent is a **trap**, which alerts management systems to an extraordinary event, such as a password violation.

Windows NT Implementation Information

Windows NT implements version 1 of the SNMP protocol.

The SNMP service works with any computer running Windows NT and the TCP/IP and/or IPX protocol. It can handle requests from one or more hosts and can report traps to one or more hosts. The SNMP service uses the unique host names, IP addresses, or IPX addresses of devices to recognize the host(s) to which it reports information and from which it receives requests.

SNMP is installed as part of Custom Setup when you install TCP/IP on Windows NT.

Note Currently, you must install SNMP by using TCP/IP installation, even if you want to use IPX as the network protocol.

The Windows NT SNMP service allows a Windows NT computer to be monitored remotely but does not include an application to monitor other SNMP systems on the network. SNMPUTIL.EXE, a utility program to get SNMP information from a host, is included on the *Windows NT Resource Kit* CD.

SNMP can monitor Dynamic Host Configuration Protocol (DHCP) servers and monitor and configure Windows Internet Name Service (WINS) servers. WINS servers and DHCP servers are Windows NT server features only.

Understanding MIBs

SNMP defines a set of variables that the host must keep, and specifies that all SNMP operations on the host are side effects of getting, putting, or setting the data variables. Because different network-management services are used for different types of devices or for different network-management protocols, each service has its own set of objects. The entire set of objects that any service or protocol uses is referred to as its Management Information Base (MIB).

Each MIB consists of a list of object identifiers describing a managed entity. The MIB handler retrieves object values from the managed entity and sends them to the SNMP console. When a network manager wants information about a device on the network, SNMP management software can determine object values that represent network status. For example, the management station might request an object called **SvStatOpens**, which would be the total number of files open on the Windows NT computer.

The Windows NT SNMP service includes MIB II (based on RFC 1213) and LAN Manager MIB II, plus Microsoft proprietary MIBs for DHCP and WINS servers. The section "MIB Object Types for Windows NT" in Appendix A contains information about each of the MIBs, including a description of each variable.

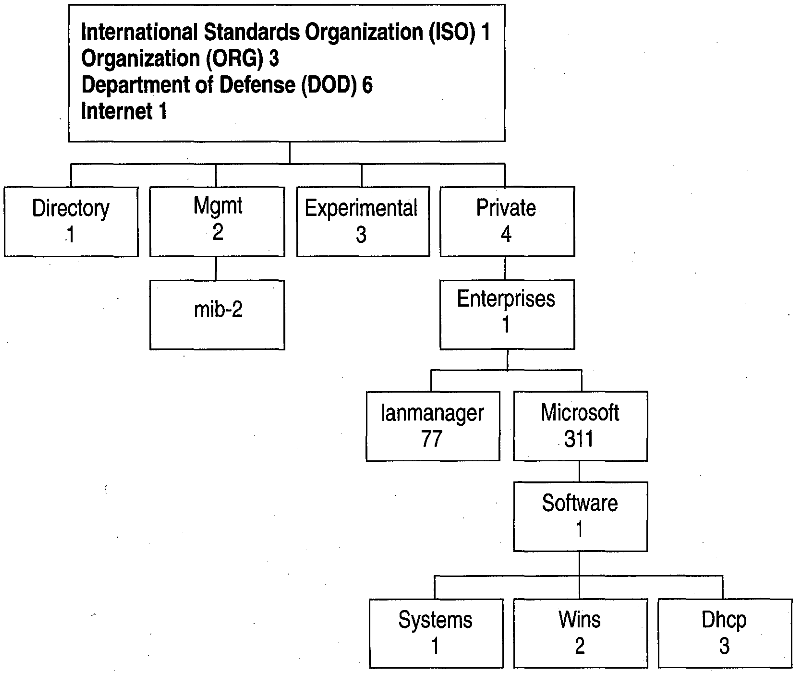
The SNMP service for Windows NT supports multiple MIBs through an agent Application Programming Interface (API) extension interface. At SNMP service startup time, the SNMP service loads all of the SNMP extension-agent dynamic-link libraries (DLLs) that are defined in the Windows NT Registry. There is a separate extension-agent DLL to access each of the MIBs that come with Windows NT. With this SNMP architecture, third parties can develop their own MIBs and DLLs and include them in Windows NT by updating the Registry.

MIB Name Tree

The name space for MIB objects is hierarchical. This structure allows assignment of a globally unique name to each manageable object.

Authority for parts of the name space is assigned to individual organizations. This allows organizations to assign names without consulting an Internet authority for each assignment. For example, the name space assigned to Microsoft is 1.3.6.1.4.1.311. Microsoft has the authority to assign names to objects anywhere below that name space.

The following figure shows the name tree for the MIBs included with Windows NT.



The object identifier in the hierarchy is written as a sequence of labels beginning at the root and ending at the object. Labels are separated with a period. The following table shows the object identifier for each of the MIBs used in Windows NT.

MIB	Object name	Object number	Contents
MIB_II.MIB	iso.org.dod.internet. mgmt.mib-2	1.3.6.1.2.1	Defines objects essential for either configuration or fault analysis. Internet MIB II is defined in RFC 1213.
LMMIB2.MIB	iso.org.dod.internet. private.enterprise. lanmanager	1.3.6.1.4.1.77	Defines objects that include such items as statistical, share, session, user, and logon information.
—	iso.org.dod.internet. private.enterprise. microsoft.software. systems	1.3.6.1.4.1.311.1.1	Currently, there are no objects or DLL for this object name.
WINS.MIB	iso.org.dod.internet. private.enterprise. microsoft.software. wins	1.3.6.1.4.1.311.1.2	Contains information for the WINS server, including statistics, database information, and push and pull data.
DHCP.MIB	iso.org.dod.internet. private.enterprise. microsoft.software. dhcp	1.3.6.1.4.1.311.1.3	Contains statistics for the DHCP server and DHCP scope information.

Note The Windows NT SDK CD contains the source code for each of the Windows NT MIBs. See "SNMP Files on the SDK" in the "Programming Considerations" section later in this chapter for the filenames of the MIB files.

Relevant RFCs

Requests for Comments (RFCs) define TCP/IP standards. RFCs are published by the Internet Engineering Task Force (IETF) and other working groups. The RFCs that are relevant to the discussion of SNMP in this chapter are:

RFC #	Title	Why relevant
1155	Structure and Identification of Management Information for TCP/IP-based Internets	defines SMI.MIB
1157	Simple Network Management Protocol (SNMP)	defines SNMP
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	defines MIB_II.MIB

The following sections contain implementation details concerning RFCs 1157 and 1213.

RFC 1157

Windows NT provides support for SNMP on TCP/IP and IPX networks. The security options for SNMP include a list of community names. If you remove all the community names, including the default name, Public, SNMP will respond to any community names presented.

This is expected behavior, as described in RFC 1157:

> An SNMP message originated by an SNMP application entity that in fact belongs to the SNMP community named by the community component of said message is called an authentic SNMP message. The set of rules by which an SNMP message is identified as an authentic SNMP message for a particular SNMP community is called an authentication scheme. An implementation of a function that identifies authentic SNMP messages according to one or more authentication schemes is called an authentication service.
>
> Clearly, effective management of administrative relationships among SNMP application entities requires authentication services that (by the use of encryption or other techniques) are able to identify authentic SNMP messages with a high degree of certainty. Some SNMP implementations may wish to support only a trivial authentication service that identifies all SNMP messages as authentic SNMP messages.

When there are no community names identified, Windows NT follows the behavior described in the preceding sentence.

RFC 1213

RFC 1213 defines the Internet MIB-II. The section "MIB Object Types for Windows NT" in Appendix A contains a description of this MIB, and the Windows NT SDK CD contains the source file.

Windows NT does not implement any of the variables in the SNMP and EGP groups of MIB-II. Because Windows NT does not implement EGP, it does not implement the variables in this group.

The SNMP group was not implemented in Windows NT 3.1 because the extension mechanism only allowed a MIB DLL to register for the entire branch of the namespace. The SNMP group is part of the Internet MIB but the statistics required for the SNMP group must be maintained by the SNMP agent.

This limitation was removed in Windows NT 3.5 but the code has not been changed.

Installing and Configuring SNMP

Although the Windows NT Server SNMP service supports managing consoles over both the IPX protocol and User Datagram Protocol (UDP), SNMP must be installed and configured in conjunction with the other TCP/IP services to use the IPX protocol. Once you have installed and configured SNMP, it automatically runs with either protocol.

To use SNMP on Windows NT computers, you need to install it:

- on each Windows NT server and Windows NT workstation that will be either an SNMP management system and/or an agent
- on a DHCP server if you want to monitor DHCP performance using SNMP
- on a WINS server if you want to monitor and control the WINS server using SNMP.

You must be logged on as a member of the Administrators group on the local computer to install and configure SNMP.

Prior to Installing the SNMP Service

You need to obtain the following information from a network administrator before you install the SNMP service on your computer:

- Community names in your network
- Trap destination for each community
- IP addresses, IPX addresses, or computer names for SNMP management hosts

The following sections discuss each of these items.

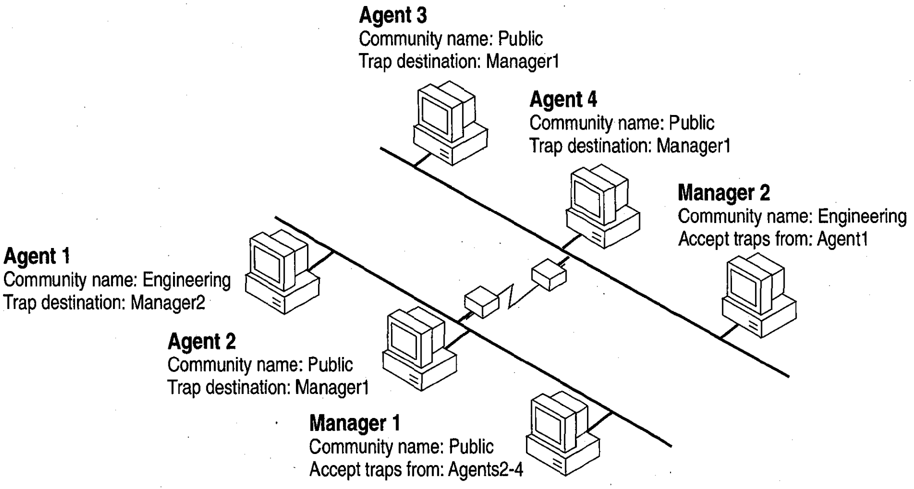
Community Names

A community is a group of hosts to which a Windows NT computer running the SNMP service belongs. Communities are identified by a community name. The use of a community name provides primitive security and context checking for SNMP agents and management systems.

You can specify one or more communities to which the Windows NT computer using SNMP will send traps. The community name is placed in the SNMP packet when the trap is sent.

An SNMP agent won't accept a request from a management system outside the community. When the SNMP agent receives a request for information that does not contain the correct community name or does not match an accepted host name for the service, the SNMP agent can send a trap to the trap destination(s), indicating that the request failed authentication. Whether the SNMP agent sends a trap for failed authentication depends upon what you configured for SNMP security.

In the following example, there are two communities—Public and Engineering.


Agent 3
Community name: Public
Trap destination: Manager1
Agent 4
Community name: Public
Trap destination: Manager1
Manager 2
Community name: Engineering
Accept traps from: Agent1
Agent 1
Community name: Engineering
Trap destination: Manager2
Agent 2
Community name: Public
Trap destination: Manager1
Manager 1
Community name: Public
Accept traps from: Agents2-4

Only the agents and managers that are members of the same community can communicate with each other.

- Agent1 can send messages to Manager2 because they are both members of the Engineering community.
- Agent2 through Agent4 can send messages to Manager1 because they are all members of the Public default community.

Trap Destinations

Trap destinations are the names, IP addresses, or IPX addresses of hosts to which you want the SNMP service to send traps with the selected community name. The traps SNMP sends depend on its configuration information, and can include events such as system startup, system shutdown, or password violation.

Host Names, IP Addresses, and/or IPX Addresses

Before you install the SNMP service, make sure you have the host names, IP addresses, or IPX addresses of hosts to which your system will send SNMP traps or from which your system will receive SNMP requests.

Installing SNMP

You must be logged on as a member of the Administrators group for the local computer to install and configure SNMP. To use IPX protocol with SNMP, you must also install TCP/IP.

For more information about installing TCP/IP, see, "Installing and Configuring Microsoft TCP/IP and SNMP," in Chapter 11 of the *Windows NT Networking Guide*.

▸ **To install Microsoft TCP/IP and SNMP on a Windows NT computer**

1. Double-click the Network icon in Control Panel to display the Network Settings dialog box.
2. Choose the Add Software button to display the Add Network Software dialog box.
3. Select TCP/IP Protocol And Related Components from the Network Software box, and then choose the Continue button.
4. In the Windows NT TCP/IP Installation Options dialog box, select the options for the TCP/IP components you want to install, including SNMP Service. If any TCP/IP elements have been installed previously, they are dimmed and not available. When you have selected the options you want, choose the Continue button.

   Windows NT Setup displays a message prompting for the full path to the Windows NT distribution files.
5. In the Windows NT Setup dialog box, enter the full path to the Windows NT distribution files, and then choose the Continue button.

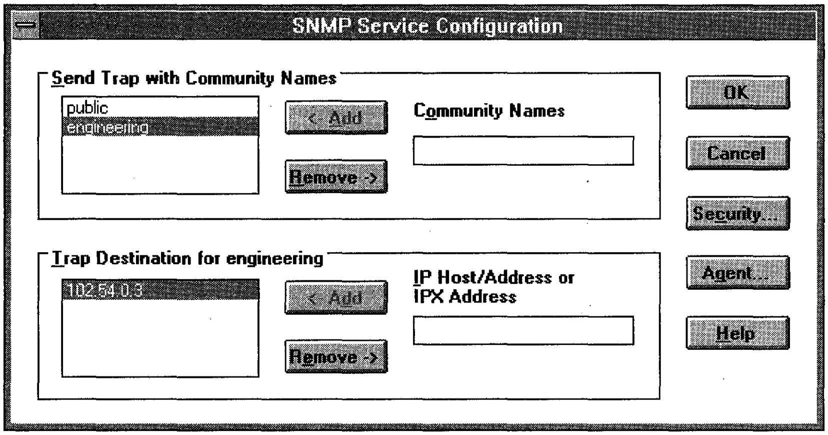
   All necessary files are copied to your hard disk.
6. The SNMP Service Configuration dialog box automatically opens when the SNMP installation completes. See the next section, "Configuring SNMP," for information about this dialog box.

Configuring SNMP

After the SNMP service software is installed on your computer, you must configure it with valid information for SNMP to operate.

▸ To configure the SNMP Service

1. Double-click the Network icon in Control Panel to display the Network Settings dialog box.
2. In the Installed Network Software list box, select SNMP Service, and click the Configure button. The SNMP Service Configuration dialog box appears.



public
engineering

102.54.0.3

3. To identify each community to which you want this computer to send traps, type the name in the Community Names box. After typing each name, choose the Add button to move the name to the Send Traps With Community Names list on the left.

   You might want to use SNMP for statistics, but may not care about identifying communities or traps. In this case, you can specify the "public" community name when you configure the SNMP service.

   To delete an entry in the list, select it and choose the Remove button.

Note Community names are case sensitive.

4. To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, type the hosts in the IP Host/Address Or IPX Address box. Then choose the Add button to move the host name, IP address, or IPX address to the Trap Destination for the selected community list on the left.

   You can enter a host name, its IP address, or its IPX address.

   Enter each IP address as four octets, AAA.BBB.CCC.DDD. You do not need to enter leading zeroes.

   Enter each IPX address in 8.12 format, XXXXXXXX.YYYYYYYYYYYY, where X represents the network number and Y represents the network address of the computer.

   To delete an entry in the list, select it and choose the Remove button.

5. To enable additional security for the SNMP service, choose the Security button. Continue with the configuration procedure, as described in the next section, "Configuring SNMP Security."
6. To specify Agent information (comments about the user, location, and services), choose the Agent button. Continue with the configuration procedure, as described in "Configuring SNMP Agent Information" later in this chapter.
7. When you have completed all procedures, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

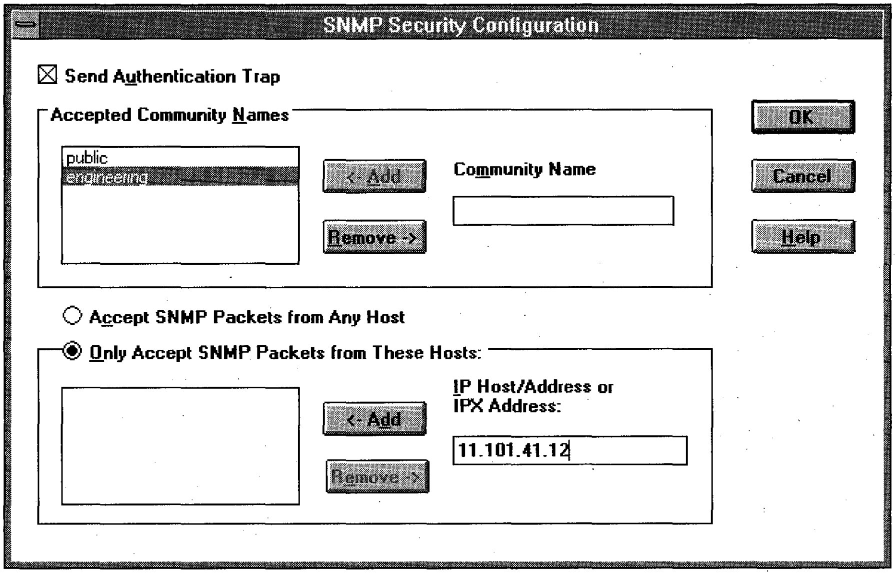
The Microsoft SNMP service has been configured and is ready to start. It is not necessary to restart the computer.

Configuring SNMP Security

SNMP security allows you to specify the communities and hosts a computer will accept requests from, and to specify whether to send an authentication trap when an unauthorized community or host requests information.

▸ To configure SNMP security

1. Double-click the Network icon in Control Panel to display the Network Settings dialog box.
2. In the Installed Network Software list box, select SNMP Service, and click the Configure button. The SNMP Service Configuration dialog box appears.
3. In the SNMP Service Configuration dialog box, choose the Security button.



SNMP Security Configuration

☒ Send Authentication Trap

Accepted Community Names

public
engineering

Community Name

○ Accept SNMP Packets from Any Host

● Only Accept SNMP Packets from These Hosts:

IP Host/Address or IPX Address: 11.101.41.12

4. If you want to send a trap for failed authentications, select the Send Authentication Trap check box in the SNMP Security Configuration dialog box.
5. In the Community Name box, type the community names from which you will accept requests. Choose the Add button after typing each name to move the name to the Accepted Community Names list on the left.

   A host must belong to a community that appears on this list for the SNMP agent to accept requests from that host. Typically, all hosts belong to public, which is the standard name for the common community of all hosts.

   To delete an entry in the list, select it and choose the Remove button.

6. Select an option to specify whether to accept SNMP packets from any host or from only specified hosts.
   - If the Accept SNMP Packets From Any Host option is selected, no SNMP packets are rejected on the basis of source host ID. The list of hosts under Only Accept SNMP Packets From These Hosts has no effect.
   - If the Only Accept SNMP Packets From These Hosts option is selected, SNMP packets will be accepted only from the hosts listed. In the IP Host/Address Or IPX Address box, type the host names, IP addresses, or IPX addresses of the hosts from which you will accept requests. Then choose the Add button to move the host name, IP address, or IPX address to the list box on the left. To delete an entry in the list, select it and choose the Remove button.

Note The earlier section "Configuring SNMP" describes the format for IP and IPX addresses.

7. Choose the OK button. The SNMP Service Configuration dialog box reappears.

   To specify Agent information (comments about the user, location, and services), choose the Agent button. Continue with the configuration procedure, as described in the next section.
8. After you complete all procedures, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

The Microsoft SNMP service and SNMP security have been configured and are ready to start. You do not need to restart the computer.

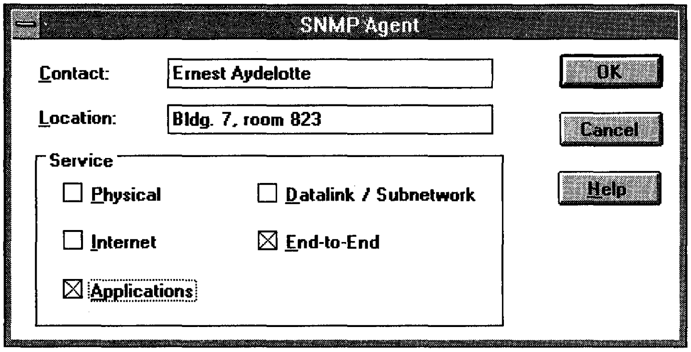
Configuring SNMP Agent Information

SNMP agent information allows you to specify comments about the user and the physical location of the computer, and to indicate the types of service to report. The types of service that can be reported are based on the computer's configuration.

▸ **To configure SNMP agent information**

1. Double-click the Network icon in Control Panel to display the Network Settings dialog box.
2. In the Installed Network Software list box, select SNMP Service, and click the Configure button. The SNMP Service Configuration dialog box appears.

3. In the SNMP Service Configuration dialog box, choose the Agent button to display the SNMP Agent dialog box.



Contact: Ernest Aydelotte

Location: Bldg. 7, room 823

Service

☐ Physical ☐ Datalink / Subnetwork

☐ Internet ☒ End-to-End

☒ Applications

4. Type the computer user's name in the Contact box and the computer's physical location in the Location box. These entries cannot include embedded control characters.
5. Select the services to report in the Service box. Check all boxes that indicate network capabilities provided by your Windows NT computer. SNMP must have this information to manage the enabled services.

Service Option	Select this option if this Windows NT computer:
Physical	Manages any physical TCP/IP device, such as a repeater.
Datalink/Subnetwork	Manages a TCP/IP subnetwork or datalink, such as a bridge.
Internet	Acts as an IP gateway.
End-to-End	Acts as an IP host. This option should be selected for all Windows NT installations.
Applications	Includes any applications that use TCP/IP, such as electronic mail. This option should be selected for all Windows NT installations.

Note If you have installed additional TCP/IP services, such as a bridge or router, you should consult RFC 1213 for additional information.

6. Choose the OK button.
7. When the SNMP Service Configuration dialog box reappears, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

SNMP is now ready to operate without restarting the computer.

Removing SNMP

If errors occur during SNMP installation and SNMP is not successfully installed, you will need to remove SNMP and reinstall it.

When you remove network software, Windows NT warns you that the action permanently removes that component. You cannot reinstall a component that has been removed until after you restart the computer.

▸ **To remove SNMP**

1. Double-click the Network option in Control Panel to display the Network Settings dialog box.
2. In the Installed Network Software list, select SNMP Service.
3. Choose the Remove button to permanently remove SNMP.

Windows NT Files Installed for SNMP

This table describes the files that are installed when you install SNMP.

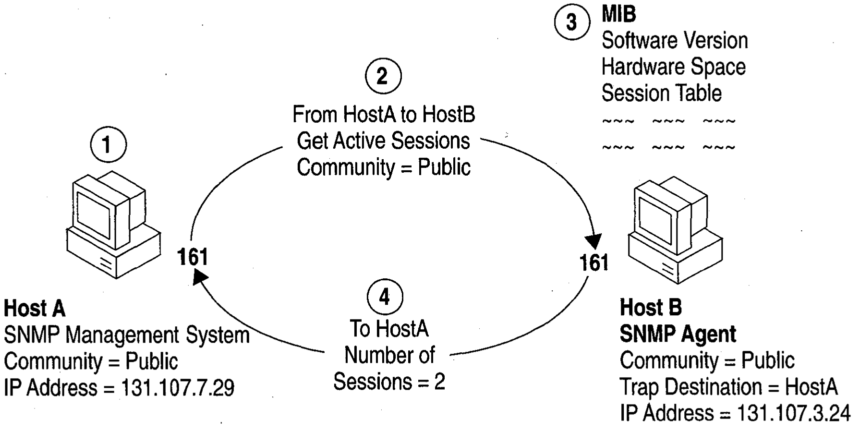
Filename	Description
DHCPMIB.DLL	DHCP extension-agent DLL. Only installed on DHCP servers. This DLL is available for Windows NT 3.5 and later.
INETMIB1.DLL	Internet MIB II extension-agent DLL
LMMIB2.DLL	LAN Manager MIB 2 extension-agent DLL
MGMTAPI.DLL	SNMP Management API library
MIB.BIN	Binary file containing all of the MIBs
SNMP.EXE	SNMP Agent Service; proxy agent that listens for requests and hands them off to the appropriate SNMP DLL
SNMPTRAP.EXE	Receives SNMP traps and forwards them to MGMTAPI.DLL
WINSMIB.DLL	WINS extension-agent DLL. Only installed on WINS servers. This DLL is available for Windows NT 3.5 and later.

Using SNMP

This section contains information primarily of interest to network administrators.

Processing of an SNMP Request

This section describes, at a high level, the processing that occurs when a management system sends a request to a Windows NT SNMP agent.



The numbers here correspond to the numbers in the preceding figure.

1. The network management system initiates a request to SNMP agent Host A. The SNMP packet contains the following information:
    - A **get**, **get-next**, or **set** request for one or more objects. In this case, the request is Get Active Session.
    - A community name and other validating information.
2. The request is passed by the application to socket 161, where the host name is resolved to an IP or IPX address. The packet is routed to socket 161 on the agent.

3. The SNMP agent receives and processes the request.

   The community name is verified. If the community name is invalid or the packet is ill-formed, the SNMP agent discards the request.

   If the community name is valid, the agent verifies the source host name, IP address, or IPX address. The agent must be authorized to accept packets from the management system, or it discards the packet.

   The SNMP agent passes the request to the appropriate DLL, which retrieves the information from the associated MIB. The table in the preceding section, "Windows NT Files Installed for SNMP," identifies the DLLs.

   The DLL returns the information to the SNMP agent.

4. The SNMP agent builds the "response" packet with the requested information and sends it to the SNMP manager.

Note Port 161 is used for SNMP messages and port 162 is used for SNMP traps.

SNMP and the Network Administrator

When SNMP has been installed on a server, a network administrator can use it to:

- View and change parameters in the LAN Manager and MIB II MIBs
- View and change parameters for any WINS servers on the internetwork
- Monitor DHCP servers

Installing SNMP also allows the network administrator to use the Performance Monitor to look at TCP/IP, FTP, and WINS counters.

A network manager can use SNMP management tools to obtain information from any of the MIBs that are installed on the Windows NT computer.

Once SNMP has been installed on a Windows NT computer, it automatically starts when the computer is started.

Using SNMP With Other Windows NT Tools

When you install DHCP and WINS servers, the DHCP Manager and WINS Manager are added to the Network Administrator group in Program Manager. You can use these tools to view and to change information for DHCP and WINS servers. Similarily, you can use the FTP Server service to configure FTP servers.

You can also use Performance Monitor to monitor WINS servers, FTP Server service traffic, and each of the different elements that make up the TCP/IP protocol suite.

Why would you want to use SNMP to view and change any of this information? Because some of the data cannot be changed except by using SNMP or by editing the Registry. All of the WINS configuration parameters can be set using SNMP.

Caution You can impair or disable Windows NT if you make incorrect changes in the Registry while using Registry Editor. Whenever possible, use WINS Manager or SNMP to make configuration changes, rather than using Registry Editor. If you make errors while changing values with Registry Editor, you will not be warned, because Registry Editor does not recognize semantic errors.

For more information about DHCP, see Chapter 13, "Installing and Configuring DHCP Servers," in the *Windows NT Networking Guide.*

For more information about WINS, see Chapter 14, "Installing and Configuring WINS Servers," in the *Windows NT Networking Guide.*

For more information about Performance Monitor, see Chapter 17, "Using Performance Monitor with TCP/IP Services," in the *Windows NT Networking Guide* and the index in *Optimizing Windows NT.*

For information about which WINS parameters can be set using SNMP, see the section "MIB Object Types for Windows NT" in Appendix A.

Turning SNMP On and Off

You can start and stop SNMP from the MS-DOS console window or by using the Services icon in Control Panel. Since SNMP starts when you install it, you will usually not need to start SNMP. If you stop SNMP, it does not start when you restart your computer. If SNMP is already running on the computer, you need to stop it before you can restart it.

One reason to stop and start SNMP is to configure error logging of the SNMP agent. This is settable only from the MS-DOS console window, not from the Control Panel.

The syntax of this command is:

net start snmp *[/LOGLEVEL:level] [/LOGTYPE:type]*

where

/LOGLEVEL:level

determines which events to log. The higher the level number, the more events will be logged. The default for level is 1; the range is 1-20.

/LOGTYPE:type

determines where the log will be created. The possible values are 2 for file and 4 for eventlog. The default is 4. To log events in both a file and the eventlog, use the value 6. The file option creates the file \<WINDIR>\SYSTEM\SNMPDBG.LOG.

You can type

net help start snmp

in the MS-DOS console window to see how to configure error logging of the SNMP agent.

A second reason to stop and restart SNMP is to load new extension-agent DLLs. You can do this either from the MS-DOS console window using "NET STOP SNMP" and "NET START SNMP" or from the Control Panel Services option. Changes made from the MS-DOS console window are not reflected in the Control Panel Services option.

Stopping a service cancels any network connections the service is using.

You must be logged on as a member of the Administrators group to start or stop the SNMP service.

SNMP Utilities

This table describes the SNMP utilities and files that are available on the *Windows NT Resource Kit* CD.

Filename	**Description**	**For more information, see**
LMMIB2.MIB	LAN Manager MIB	Section "MIB Object Types for Windows NT" in Appendix A
MIB_II.MIB	MIB II	Section "MIB Object Types for Windows NT" in Appendix A
MIBCC.EXE	SNMP MIB Compiler	Section "SNMP Files on the SDK"

Filename	Description	For more information, see
PERF2MIB.EXE	MIB builder tool	Section "MIB Builder Tool (PERF2MIB.EXE)"
SMI.MIB	SMI	RFC 1155
SNMPUTIL.EXE	Simple SNMP manager application that implements Get, Get Next, Walk, and Trap	Section "SNMP Files on the SDK"

Troubleshooting SNMP

This section discusses problems that you might encounter using SNMP and what to do to resolve them.

Timeout on WINS Server Queries

When querying a WINS server, it might be necessary to increase the SNMP timeout on the SNMP management system. If some WINS queries work, and others time out, increase the timeout.

Identifying SNMP Service Errors

Event Viewer is the first place you should look to identify a problem with the SNMP service. SNMP service errors and activity are recorded in the system log, depending upon the specified LOGLEVEL. If there is no SNMP information in the event log, you may need to change the LOGLEVEL. See the earlier section "Turning SNMP On and Off" for information about this parameter.

For more information about Event Viewer, see online Help or the Event Viewer chapter in the *Windows NT System Guide* manual of the Windows NT 3.5 documentation set.

► **To use Event Viewer**

1. In Program Manager, open the Administrative Tools group.
2. Double-click the Event Viewer icon.
3. Click the message about which you want more information. In the View menu, select Detail and Event Viewer displays more information about the message.

Application is Unable to Get Requested Variables

The SNMP Manager API SnmpMgrStrToOid assumes that the Oid is under the Internet MIB in the mgmt subtree (1.3.6.1.2.1.x).

To get variables that are not under the mgmt subtree, the Oid must be preceded by a period (.). For example, if the application is trying to get the system group and passes an Oid of 1.3.6.1.2.1.1, the application will try to get

iso.org.dod.internet.mgmt.1.1.3.6.1.2.1.1

which does not exist. The correct way to get the system group is to pass .1.3.6.1.2.1.1 as the Oid parameter.

To walk the enterprises tree, specify .1.3.6.1.4.1 rather than 1.3.6.1.4.1.

SNMP Agent Breaks Up Variable Bindings List

When the SNMP agent receives a request for multiple variables in a single packet, the agent queries the required subagent (in this case the DLL acting as the agent) for each variable in the bindings list, packs the results in a response variable bindings list, and returns a single packet.

This table gives an example of variables requested and their respective MIBs.

Variable	MIB
ip.iplnReceives	Internet MIB II
tcp.tcpMaxConn	Internet MIB II
iso.org.dod.internet.private.enterprises.lanmanager. lanmgr-2.common.comVersionMaj	LAN Manager MIB II
icmp.icmpOutErrors	Internet MIB II

The agent queries INETMIB1.DLL twice, LMMIB2.DLL once, and INETMIB1.DLL once. It packs the result in a response packet and sends it to the requesting manager. There is no "snapshot" of the MIB.

No Counters Appear in Performance Monitor

You must install the SNMP service to see any of the TCP/IP, FTP, Internet Control Message Protocol (ICMP), or UDP performance counters in Performance Monitor. Installing SNMP installs the MIBs into which the performance information is accumulated, and starts SNMP.

SNMP is not installed by default when you install TCP/IP. See the earlier section "Installing and Configuring SNMP" for more information.

For more information about Performance Monitor and the counters, see Chapter 17, "Using Performance Monitor with TCP/IP Services," in the *Windows NT Networking Guide*.

Messages Specific to SNMP

There are two messages specific to SNMP.

The sentence in bold text is the message, followed by an explanation of the message.

***text* is an invalid Trap Destination.**

Trap destinations are the names, IP addresses, or IPX addresses of hosts to which you want the SNMP service to send traps with the selected community name.

In the IP Host/Address Or IPX Address box text box, enter the name, IP address, or IPX address of a computer in the community you have selected. Then choose Add.

SNMP service encountered a fatal error.

The SNMP component was not installed correctly.

Remove the SNMP service and then reinstall it.

Programming Considerations

This section contains high-level information about SNMP from a programming point of view.

SNMP Files on the SDK

The Windows Systems Developers Kit (SDK) is a set of libraries, header files, tools, books, online Help, and sample source programs to help you create Windows applications. The Windows NT SDK contains SNMP files, tools, and information in the following directories:

Directory	File	Description
\DOC\MISC	PROGREF.RTF	Microsoft Windows/NT SNMP Programmer's Reference
\MSTOOLS\BIN\WINNT	DHCP.MIB	Microsoft proprietary MIB for DHCP, described in the section “MIB Object Types for Windows NT” in Appendix A
	LMMIB2.MIB	LAN Manager MIB II, described in the section “MIB Object Types for Windows NT” in Appendix A
	MIB_II.MIB	This MIB is described in RFC 1213 and the section “MIB Object Types for Windows NT” in Appendix A
	SMI.MIB	This MIB is described in RFC 1155

Directory	File	Description
	SNMP.TXT	Notes on SNMP development for Windows NT — incorporated into this chapter
	TOASTER.MIB	MIB for the sample extension-agent TESTDLL.DLL
	WINS.MIB	Microsoft proprietary MIB for WINS, described in the section "MIB Object Types for Windows NT" in Appendix A
\MSTOOLS\BIN\WINNT\ ALPHA, I386, and MIPS	MIB.BIN	Output from the MIB compiler
\MSTOOLS\BIN\WINNT\ ALPHA, I386, and MIPS	MIBCC.EXE	MIB compiler, described in PROGREF.RTF
\MSTOOLS\SAMPLES\ WIN32\WINNT\SNMP\ SNMPUTIL	SNMPUTIL.C	Example of how to code management applications using the SNMP Management APIs for Windows NT
\MSTOOLS\SAMPLES\ WIN32\WINNT\SNMP\ TESTDLL	*.*	Example of how to structure an extension-agent DLL that works in conjunction with the Windows NT SNMP agent.

SNMP Source Code

There are two sets of sample code on the SDK.

SNMPUTIL

The files in the SNMPUTIL directory contain the source code for the SNMPUTIL.EXE utility. This utility will allow you to retrieve data from any SNMP agent.

To use the utility, type **snmputil** with the appropriate switches:

snmputil [get|getnext|walk] *agent community oid* [*oid*]

or

snmputil trap

Where:

get
Gets the current value of the specified *oid*(s).

getnext
Gets the current value of the item in the MIB that follows the item whose *oid* is specified.

walk
Steps through the MIB and retrieves the values of all items in the branch of the MIB specified by *oid.*

agent
Specifies the computer to query. This can be an IP address, an IPX address, or a hostname.

community
Specifies a community name, which is used to group computers together into management groups.

oid
The ASN.1 name of the variable being queried, of the form .N.N.N.N (that is, a string of numbers separated by periods or, alternately, a string of names separated by periods). See the section "Application is Unable to Get Requested Variables" under "Troubleshooting SNMP" earlier in this chapter for more information about this parameter.

trap
Tells SNMPUTIL to listen for traps.

For example:

```
snmputil get jb486 public
    .iso.org.dod.internet.mgmt.mib2.system.sysDescr.0
```

Would return a text description of the type of computer hardware and software being used on the computer named jb486.

TESTDLL

The files in the TESTDLL directory are the sources for the TESTDLL.DLL. This DLL implements the toaster MIB. See the next section, "SNMP Information in the Registry," for information about installing this DLL.

MIBs and the MIB Compiler

You can use the MIB compiler, MIBCC.EXE, to compile your own private MIBs. The file MIB.BIN must be placed in the path for the SNMP Manager APIs to be able to function properly. MIBCC.EXE by default places the file MIB.BIN in the <WINDIR>\SYSTEM32 directory.

The Microsoft Windows NT SNMP Programmer's Reference document describes the usage of the MIB compiler, which creates the file MIB.BIN that the SNMPUTIL.EXE program uses.

MIB Builder Tool (PERF2MIB.EXE)

You can use the Performance Monitor MIB builder tool, PERF2MIB.EXE, to create new ASN.1 syntax MIBs to track performance using any system management program. This utility is available on the *Windows NT 3.51 Resource Kit* CD.

PERF2MIB.EXE creates a MIB file that can be used by an SNMP management console to perform SNMP requests for the performance data in question. This lets all performance data available through the HKEY_EPRFORMANCE_DATA Registry key be exposed through SNMP, allowing remote performance monitoring.

The syntax for PERF2MIB.EXE is as follows:

perf2mib *MIBfilename INIfilename [ObjectName MIBIndex MIBPrefix [...]]*

where

MIBfilename
Is the name of the MIB file to create.

INIfilename
Is the name of the generated configuration file. This file is used by the Windows NT SNMP extension agent to map performance counters to MIB variables.

ObjectName
Is the name of the performance object whose counters you want to expose (such as Processor or Memory).

MIBIndex
Is the numeric ID of the MIB branch where the particular object's data should be placed.

MIBPrefix
Is the abbreviation that should be placed before counter names belonging to this object (such as "mem" for Memory counters or "proc" for Processor counters).

Note The last three parameters can be repeated to map multiple object types with one call. If multiple object types are specified, the resulting MIB and MIB agent configuration information is concatenated into one MIB file.

Example:

```
perf2mib test.mib test.ini Memory 1 mem Processor 2 proc System 3 sys
```

▸ To create and compile a MIB for a new component

1. Run PERF2MIB, specifying the object for which you want to create a MIB. A configuration file (INI) file will also be generated.
2. Copy the MIB file to the console device.
3. Run the MIB compiler to compile the management station with the MIB file.

   For example, if you are using HP OpenView, to populate the map with a new object, run the HP OpenView MIB compiler with the MIB file and then associate the resulting icon with an object and place it on the map.

   This step enables the management station to read the component's MIB via SNMP.

SNMP Information in the Registry

SNMP parameters are contained in the Registry, and so is the information about which extension-agent DLLs SNMP loads. To examine or change information in the Registry, use the REGEDT32.EXE program that comes with Windows NT.

SNMP Parameters

This section lists Windows NT SNMP network parameters. These parameters are contained in the Registry in the following key:

```
HKEY_LOCAL_MACHINE\
    SYSTEM\
        CurrentControlSet\
            Services\
                SNMP\
                    Parameters
```

Registry parameter	Description
EnableAuthenticationTraps Units: Boolean Range: 0 (off) or 1 (on) Default: on	A value of On (1) indicates that the SNMP service sends a trap whenever it receives a request that does not match any community name or host filter in its lists. Off (0) indicates that the SNMP service does not send a trap when this occurs.
ExtensionAgents	Contains information about each of the extension-agent DLLs to load. See the next section "SNMP Extension Agent Information."
ValidCommunities Units: names Range: — Default: public	Specifies one or more community names defining groups of hosts from which the SNMP service will accept requests.
TrapConfiguration Units: name Range: — Default: —	Specifies one or more host names, IP addresses, or IPX addresses defining hosts to which the SNMP service sends traps. Under the TrapConfiguration key, there is a key for each community. Under the community key, there are trap destination values for that community.

SNMP Extension Agent Information

If you are developing an extension-agent DLL, you must configure the Registry so that the SNMP agent will load the extension-agent DLL. You can use the REGEDT32.EXE program that comes with Windows NT to add this information, or you can have your SNMP extension-agent installation program configure the Registry using the Win32 Registry APIs.

These are the steps to configure an SNMP extension-agent in the Registry.

1. Locate the following key:

   ```
   HKEY_LOCAL_MACHINE\
       SYSTEM\
         CurrentControlSet\
           Services\
             SNMP\
               Parameters\
                 ExtensionAgents
   ```

2. For the new extension-agent, create a value under this key with a Value Name of the next available integer and a type of REG_SZ. For the SNMP Toaster sample in the SDK, the entry is:

   3:REG_SZ:SOFTWARE\CompanyName\toaster\CurrentVersion

   This entry provides a pointer to another Registry entry (see next step), which contains the physical path where the extension-agent DLL can be found. The "CompanyName" and "toaster" strings are used in the next step.

3. Locate the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE

   and create a CompanyName\toaster\CurrentVersion key that corresponds to the new entry in step 2. The keys Microsoft\RFC1156Agent\CurrentVersion and Microsoft\LANManagerMIB2Agent\CurrentVersion show the format of the information.

4. Assign the path of the extension-agent DLL as the value for the CurrentVersion key. Remember that the names and values in the Windows NT Registry are case sensitive.

   For instance, if you have copied the SNMP toaster sample agent DLL to drive D, the entry is:

   Pathname:REG_SZ:D:\mstools\samples\snmp\testdll\testdll.dll.

5. Stop and restart the SNMP service from the Control Panel Services icon. You need to do this for the SNMP agent to load the new extension agent that you have just added to the system.

   You can use Event Viewer in the Administrative Tools program group to view errors encountered during the startup process of the SNMP service and extension agents.

Note The key name and values are case sensitive. Make sure that they match. If you have problems, look in the system log. You can also type "Net Help Start SNMP" to see how to configure error logging of the SNMP agent.

You must stop and restart the SNMP service for it to load the new extension-agent DLLs.

Reference Materials

The following books contain more information about SNMP:

SNMP, SNMPv2, and CMIP: The Practical Guide to Network-Management Standards
by William Stallings
Addison-Wesley Publishing Company, Inc 1993
ISBN 0-201-63331-0

The Simple Book: An Introduction to Management of TCP/IP-based Internets
by Marshall T. Rose
Prentice-Hall, Inc., 1994
ISBN 0-13-177254-6

Internetworking with TCP/IP
Volume 1: Principles, Protocols, and Architecture (third edition)
by Douglas E. Comer
Prentice-Hall, Inc.
ISBN 0-13-468505-9

CHAPTER 6

Troubleshooting

This chapter contains additional information beyond that provided in Chapter 18, "Troubleshooting," in the *Windows NT Resource Guide*. Information in Chapter 18 is not repeated here.

You can find additional troubleshooting information in the following sources:

- The index in each of the books in the *Windows NT Resource Kit* lists the troubleshooting topics in the respective books.
- The *Comprehensive Index* manual for the *Windows NT Server* documentation set lists all of the troubleshooting topics in the documentation set. Each manual in the documentation set also has its own index with troubleshooting topics.
- Appendix A in the *Windows NT Resource Guide* describes how to get answers to technical questions and has a list of resources to support learning and using Windows NT.
- The SNMP chapter in this book contains a section titled "Troubleshooting SNMP."
- Windows NT utilities such as Event Viewer and Performance Monitor provide information that can be useful for troubleshooting.
- The online version of the Windows NT documentation is located on the Windows NT CD. Double-click the README.WRI icon in your Main program group to get more information about Books Online.

Technical Notes

This section is based on information in Knowledge Base articles and e-mail describing problems and solutions.

Event Viewer Log File Information

Event Viewer stores event information in three binary log files in the %SYSTEMROOT%\SYSTEM32\CONFIG directory:

- APPEVENT.EVT—application log
- SECEVENT.EVT—security log
- SYSEVENT.EVT—system log

You can access the logs using the Win32 event logging API set. These APIs are documented on the Microsoft Development Library (MSDN) CD. The following functions are available:

- BackupEventLog
- ClearEventLog
- CloseEventLog
- DeregisterEventSource
- GetNumberOfEventLogRecords
- GetOldestEventLogRecord
- NotifyChangeEventLog
- OpenBackupEventLog
- OpenEventLog
- ReadEventLog
- RegisterEventSource
- ReportEvent

Importing LMHOST File Never Completes

If there is a non-numeric character as the first character of the address, the import of the LMHOST file will never finish.

Memory Problems

If your PC crashes randomly and inconsistently, you may have memory problems. Memory problems are not uncommon and are documented in the Knowledge Base.

This section presents general information on preventing memory problems, followed by a more detailed discussion of memory errors.

In general, you should first carefully clean the system of dust. This includes the areas allowing ventilation so that heat does not build up abnormally. The contacts of all boards and SIMMs should be cleaned. Be certain that all boards are firmly seated in their slots or sockets. It may be necessary to replace old cabling, which will degrade over time and under high temperatures. Power supplies can also cause many problems, so have the output voltages checked, if possible. Even monitors can cause strange behaviors on your system. Computers should be placed on some type of surge suppression power strip since after a power outage occurs, the return of power is usually a fairly high surge and can permanently damage sensitive electrical components of your system.

When 9-bit memory detects a parity difference, it signals the CPU through a Non-Maskable Interrupt (NMI). Depending on where and when this happens, Windows NT determines if this is an I/O board parity error, memory bus error, etc. Windows NT can also report I/O channel parity errors from cards in slots.

Since memory errors are very serious, the system shuts down.

Eight-bit memory doesn't do parity checking. When the system is having single-bit memory errors, which only seems to happen on 8-bit memory, then we are using corrupted memory.

Microsoft has been using a high quality SIMM tester to study what may be causing some of the NMI Memory Parity Errors on Windows NT. Although the results are not conclusive and the research continues, the information is important enough to include here.

Both IBM's OS/2 2.x and Windows NT experience problems that appear to be associated with system memory in some circumstances. It is frustrating to have a system that is able to run MS-DOS, Windows 3.1, or OS/2 1.x and suddenly find it can't run Windows NT due to memory problems. The first issue to clear up is that not all NMI errors are due to memory. Other boards in the system can cause this problem, and even components directly on the system motherboard can be at fault.

In addition, the timing of the memory is quite critical to Windows NT. Speed drifting in the range of 15ns can cause extreme memory problems and not be reported as an NMI Parity Error.

When memory is at fault, it can be for any of the following reasons:

- The memory is not functioning at the specified access rate as required by the system board. If the system specifications call for 80ns access rate, Windows NT will most likely fail if memory is really accessing at a slower rate such as 90ns. Even though the chips may be marked as 80ns, some fail to meet this access rate. Quite often chips will run at a slower speed when they reach operating temperature. This produces an effect called "speed drift." The symptoms are a system that runs Windows NT when first turned on, but after 15 minutes or so will start having memory errors. A high quality SIMM tester can cycle the chips through various voltage and heat cycles, so this is fairly easy to see.
- The memory meets the system specifications but the speeds are different between individual SIMM modules. The average access rate may be 70ns on one SIMM module while the next module is running at 60ns. SIMMs stamped at the factory as 70ns average access rate can actually be running as fast as 50ns. Although the SIMMs are obviously well under the system-required access specifications, the difference of 10ns or more between them can often cause problems on some systems. If you can move these to a different system board that is using a different BIOS and Chipset, it may not have any memory problems. This is because each BIOS and Chipset regulate the "refresh wait states" used for timing, and this difference often allows for variance in speed to be acceptable. If your system's BIOS allows you to adjust the "wait states" for memory refresh, this often will allow the system to run with SIMMs or DRAM memory chips that are running at different access rates. The downside to increasing the number of wait states is a slower system.
- The individual chips on the SIMM module are running at different access rates. Determining this requires a sensitive memory testing device. It must be able to gauge the access rate of each individual bit (chip) on the module. A difference of 10ns or more between bits has been known to cause problems. This also can be regulated somewhat by the BIOS and Chipset of the system board if it allows you to lengthen the refresh wait states for memory access.

- One of the memory chips is being affected by “cell leakage.” This ends up being a true parity error and is also known as a “soft error.” This occurs when the change in the state of an individual cell (a zero or one) electrically leaks into a neighboring cell, changing its state. When the memory is read back, it no longer matches the parity bit’s checksum value, and an NMI is issued to the processor signaling a parity error has occurred. This memory SIMM must be replaced. If problems persist with replacement chips, it is quite possible a voltage or heat anomaly is occurring with the socket or circuitry, which is damaging the chips.
- Cache memory is another thing to suspect. There are cases where the cache memory access rates were too slow, which caused enormous problems. On most 486 computers, 15ns to 25ns is normal. You will most likely have problems if it is slower than 25ns. The system manufacturer can provide the specifications and locations of these chips.

DHCP Server

This section discusses DHCP server failures, redundancy, and lease time-outs.

There is no address sharing or DHCP server-to-server protocol.

A DHCP server failure is not nearly as critical as a WINS server failure. This is because a DHCP server must be down for half of the lease time until existing clients lose their leases. The only immediate problem when there is no DHCP server on the net is that new clients cannot get addresses.

Do not, under any circumstances, put the same address(es) on two or more DHCP servers. Any overlap in address pools on two DHCP servers will surely result in multiple machines on the network with the same IP address.

A mirrored backup machine would be a nightmare to keep correct, and it defeats the entire management simplicity DHCP is designed to provide.

To provide redundancy, simply break up each subnet’s address pools over two DHCP servers. A 50/50 split is fine. The idea is to have unused addresses on both machines so that if one goes down, there will always be new addresses available on every subnet.

When a DHCP lease times out, the server will delete the lease and return the address to the address pool. (DHCP actually waits one day to return it to the pool as security against time zone problems.)

There is no special case to handle a client moving from one subnet to another on the same server. The old lease will be deleted only when it times out.

A reservation—a specific address given to a specific client—is handled differently. The lease times out but the server continues to hold the address for the client to use. It is not returned to the address pool.

Altering Startup Boot Menu

To alter the startup boot menu when the multiboot comes up in Windows NT:

On an x86, modify c:\boot.ini. You have to unhide the file first by doing a

```
c:\attrib -r -h -s boot.ini
```

On Mips/AXP, choose Setup from the ROM menu.

Special Characters in Domain Names

The following special characters are illegal in domain names (in addition to * and space):

```
#define ILLEGAL_NAME_CHARS_STR TEXT ("\"/\\[]:|<>+=;,?")
CTRL_CHARS_STR
```

Even though some special characters such as period (.) are valid, underscore (_) and dash (-) would be better choices as special characters in domain names.

Reconstructing a Volume Set

If you have a Windows NT Emergency Repair Disk, you can reconstruct a volume set without having saved the configuration information by using Disk Administrator (in the Administrative Tools program group).

Expand the set of hives from the latest Emergency Repair Risk onto a floppy and use Disk Administrator to read the disk.

Error Messages in Console Window

To obtain additional information about message numbers that you see in the console window, type

```
NET HELPMSG #
```

where # is the message number for which you want help. The help message explains why an error occurred and tells you what action will solve the problem.

Problems in WINDIFF.EXE

The following problems existed with the WINDIFF.EXE utility shipped on the *Windows NT 3.5 Resource Kit* CD.

There is a problem in the working set in the WINDIFF.EXE utility when doing a large compare. The working set grows to large values. The memory is finally freed up when WINDIFF terminates. If you monitor the working set using Performance Monitor while doing a large compare, you will see a steady climb in the size. When the compare finishes, the size will suddenly drop down to a base value of around 3 to 4 MB.

Command line switches for this utility do not have any effect on the files listed or their order.

Named Pipes

This section describes limitations and problems involving the use of named pipes in Windows NT 3.5.

To upgrade from Windows for Workgroups to Windows NT 3.5, installing IPX/SPX protocol in addition to NetBEUI protocol, you need to install a new VREDIR.386, which is available on the Windows NT Server CD in \clients\wfw\update\vredir.386.

Make sure the default frame type is correct. It has been changed from ethernet_802.3 to ethernet_802.2. If you are using 802.3, you need to change the following entry in the protocol.ini under the [nwlink] section:

```
FRAME=ETHERNET_802.3
```

Windows NT Server 3.5 can support a maximum of 512 named pipes. Each SNA Server client uses two named pipes, so you can run out of SMB server resources at around 250 clients if you are using named pipes as the transport. The 20xx events in the Event Log typically result from SMB running out of these MaxWorkItem resources.

The maximum is raised to 4096 in Windows NT Server 3.51, and the SNA Server 2.11 automatically sets this entry to 4096. The default is still set to 512 if you are running SNA Server 2.1 on Windows NT 3.51, so you'll have to manually change this parameter. There are some other improvements in SNA Server 2.11, including not having to log on twice, so you should upgrade to it.

It would be a good idea to switch to sockets from named pipes for several reasons:

- TCP/IP or IPX connections don't have the resource limitation described here
- You can get up to a 30 percent improvement in performance
- Negotiating a session with sockets takes one third less traffic on the network compared to using named pipes
- Named pipes consume quite a bit more memory on the server

Getting Tape Backups to Run Faster in Windows NT 3.5

You should be able to speed up backups from UNC shares in Windows NT 3.5. The problem is the case of a value in the Registry.

In Registry Editor, open the following HKEY_LOCAL_MACHINE key:

System\CurrentControlSet\Services\LanmanWorkstation\netprovider

This key has several values. Double-click the "Devicename" value and change the case of the first letter in the data to uppercase. You'll be changing

"\device\LanmanRedirector" to "\Device\LanmanRedirector"

Why does this make a difference? Whenever there is a file that could be a POSIX file, Windows NT needs to open the file in a POSIX-compatible way. This means that the path and filename must match exactly with respect to case-sensitivity.

However, the case of "device" is wrong, so the operating system refuses to open the file when POSIX semantics are requested—it returns ERROR_FILE_NOT_FOUND. The application must open the file a second time, this time specifying not to use POSIX semantics. Thus, the performance penalty occurs.

The case of the Devicename value has been changed to uppercase in Windows NT 3.51.

Optimizing Windows NT

The book *Optimizing Windows NT* should be your first source for information on tuning and optimizing Windows NT.

The SizeReqBuf parameter is the only one that you might want to change to improve network performance. See Appendix B, "Registry Value Entries," in *Optimizing Windows NT* for information about this parameter.

Windows NT includes PMTU detection that automatically determines the optimal segment size on a per connection basis. Therefore, you don't need to edit the Registry to set the MTU size for the network interface(s).

Viruses

This section describes two problems that are caused by viruses.

Several boot sector viruses can cause the processor to stop after the Blue Screen appears showing the Windows NT version. The error is:

Stop 0x0000007B

Inaccessible_boot_device

Scan with a good virus scanner if this occurs.

The second problem occurred when trying to upgrade from Windows NT 3.5 to 3.51. Upon rebooting, there was an additional entry in BOOT.INI that displays "Windows NT 3.51 installation/upgrade" and will start in 5 seconds. NTLDR entered in an endless loop of displaying BOOT.INI and restarting.

The solution was to run the latest version of f-prot, which, at the time, was 2.16 dated 2/2/95.

Gateway 2000 CD-ROM Drives

This problem occured in Windows NT 3.5 and was fixed in Service Pack 2. There is no problem with these CD-ROM drives in Windows NT 3.51.

Windows NT 3.5 had problems with Gateway 2000 CD-ROM drives manufactured by Mitsumi. The CD-ROM drives manufactured after early 1995 were not fully compatible with Windows NT, which occasionally reports read errors when copying data from a CD-ROM. The problem occurred on Gateway 2000 Pentium PCI bus PCs using the ATAPI 1.2 IDE driver with the Windows NT 3.5 Server.

Installing Windows NT on an ESDI Disk Drive With More Than 1024 Cylinders

In some cases on disk drives with more than 1024 cylinders, Windows NT installation proceeds normally until the first boot from the hard drive where Windows NT is installed. The Windows NT Boot Loader will load various files and then produce a Fatal System Error: 0x0000006b with the message that Phase 1 Process Initialization failed. Following this message will be some type of hexadecimal dump and the system will lock up. If you experience this problem, the information in this section can help you.

Microsoft has tested ESDI controllers using a hard drive with a capacity exceeding 516 MB (1MB = 1,048,576 bytes), formatted. The MS-DOS limit of 1024 cylinders creates a situation where special BIOS mapping on the controller is used to change the geometry of the drive.

ESDI drives are capable of being prepped with various values of sector per track (SPT), such as 53 or 63 SPT geometry, during a low-level format. Here are two examples:

1024 cylinders x 15 heads x 53 SPT x 512 bytes per sector = 398 MB

1024 cylinders x 15 heads x 63 SPT x 512 bytes per sector = 472 MB

Thus, using 63 SPT yields 74 MB more space. Windows NT is compatible with either geometry, and, depending on the drive or controller, can access cylinders beyond 1024. This space can be partitioned and formatted but not accessed by MS-DOS. However, some controllers can remap the remaining cylinders beyond 1024 so that either MS-DOS or Windows NT can use the entire capacity. For example,

1632 cylinders x 15 heads x 53 SPT x 512 bytes per sector = 634 MB

Microsoft has tested the ESDI controllers described in the following table.

Controller	Achieving Maximum Capacity
Data Technology Corp. (DTC) Model 6282-24	The maximum Windows NT-compatible geometry is 63 sectors per track (SPT) and a limit of 1024 cylinders under MS-DOS. Windows NT will be able to access the cylinders beyond 1024. Do not perform a low-level format on the drive using Head Mapping mode.
Data Technology Corp. (DTC) Model 6290-24	The maximum Windows NT-compatible geometry is 63 SPT and a limit of 1024 cylinders under MS-DOS. Since this card does not have an on-board BIOS, Windows NT cannot access the cylinders beyond 1024.
Data Technology Corp. (DTC) Model 6290 SEZ (Dual SCSI/ESDI Controller)	The maximum Windows NT-compatible geometry is 63 SPT and a limit of 1024 cylinders under MS-DOS. Windows NT will be able to access the cylinders beyond 1024.
Data Technology Corp. (DTC) Model 6295-24	The maximum Windows NT-compatible geometry is 63 SPT and a limit of 1024 cylinders under MS-DOS. This card does have an on-board BIOS, so Windows NT will be able to access the cylinders beyond 1024. Do not perform a low-level format on the drive using Head Mapping mode.

Controller	Achieving Maximum Capacity
Adaptec Model 2322D	Option 1. Disable drive translation and the on-board controller BIOS. Use a user-defined drive type with the actual drive parameters, such as Drive Type in CMOS=48, Cylinders=1632, Heads=15, SPT=53. This will give 634 MB capacity. MS-DOS is limited to the first 1024 cylinders, which makes 398 MB available. Windows NT can access beyond cylinder 1024, yielding another 236 MB. Option 2. Both MS-DOS and Windows NT can access the entire drive. Set jumpers on the controller for Drive Splitting. Disable drive translation and the on-board controller BIOS. Set up the first physical drive in CMOS as Cylinders=1024, Heads=15, SPT=53. This gives a drive capacity of 398 MB. Set up the second drive (it appears as a physical drive) in the CMOS as Cylinders=606, Heads=15, SPT=53. This yields another 236 MB. Windows NT sees the drive as two physical drives.
UltraStor with PROM versions < nnnn-009	Maximum Windows NT-compatible geometry is to use 63 SPT and a limit of 1024 cylinders under MS-DOS. Windows NT can access the cylinders beyond 1024.
UltraStor with PROM versions > nnnn-009	Maximum Windows NT-compatible geometry is to use Track Mapping during low-level formatting. Both MS-DOS and Windows NT have access to the entire drive capacity.

APPENDIX A

Major Revisions to the Windows NT Networking Guide

Three of the chapters from the *Windows NT Networking Guide* have been heavily revised and the affected sections of those chapters are included here in their entirety. They include the following:

- Chapter 9, “Using Remote Access Service,” in which the former section, “Using Terminal and Script Setting for Remote Logons,” is replaced with the new version, “Logging on to Remote Computers Using RAS Terminal and Scripts.”
- Chapter 22, “Remote Access Service and the Internet,” in which the section, “Installing a Simple Internet Router That Uses PPP,” has been updated.
- Appendix B, “MIB Object Types for Windows NT,” has been updated and greatly enhanced.

Chapter 9 Using Remote Access Service

This section replaces “Using Terminal and Script Setting for Remote Logons,” and includes new information on scripting.

Logging on to Remote Computers Using RAS Terminal and Scripts

The exact logon process for remote computers varies as widely as the remote computers themselves. Remote computers you might log on to include a Windows Remote Access Service (RAS) server giving you access to your corporate network or the Internet, a UNIX computer in a commercial network that gives you an Internet connection, or a proprietary security computer that protects your corporate network from intruders.

Most remote logons require you to provide a username (frequently called login) and a password. This chapter covers how you provide the username, password, and any other information required by remote computers before you log on.

This chapter also describes how to connect to Microsoft, Point-to-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP) servers, when and how to use RAS Terminal, how to create and activate scripts that automate remote logons, and how to debug your scripts.

Most of the information regarding Terminal screens, scripts, and DEVICE.LOG also applies to RAS for Windows for Workgroups version 3.11. However, the PPP, SLIP, and <username> and <password> macro information does not apply.

Connecting to Remote Servers

The three most common remote connections are to:

- Microsoft RAS servers. These include LAN Manager 2.1, Windows for Workgroups 3.11 with server extension, Windows NT 3.1 or later, and Windows 95.
- Non-Microsoft PPP servers
- SLIP servers

Connecting to a Microsoft RAS server is a simple process that uses the credentials you specified when you logged on to Windows NT. If you use Windows NT RAS to connect to computers that are not running Windows NT RAS, the remote computer may require a specific sequence of commands and responses through a terminal window to successfully log you on to the remote system.

Microsoft RAS Servers

If the client is a Windows NT computer and the remote server is any Microsoft RAS server, logon is completely automated using Windows NT security. By default, you are authenticated using the credentials (username, password, and domain) you specified when you logged on to Windows NT.

If you wish to authenticate using different credentials, clear the Authenticate Using Current User Name and Password check box in the Edit Phone Book Entry dialog box. You will then be prompted for credentials when you dial.

PPP Servers

Point-to-Point Protocol (PPP) is a newer protocol used to negotiate connections between remote computers. Remote server and client software that support PPP authentication protocols automatically negotiate network and authentication settings. The following steps are necessary to connect to a PPP server.

1. The currently logged-on user's credentials will not work with any non-Microsoft server, so clear the Authenticate Using Current User Name and Password check box in the Edit Phone Book Entry dialog box. You will then be prompted for credentials when you dial.
2. In the Edit Phone Book Entry dialog box, choose the Network button. In the Network Protocol Settings dialog box, select the PPP option. This is the default selection.
3. In the Security Settings dialog box, if the server you are calling requires a text-based logon exchange, select the Use Clear Text Terminal Login Only option. Now, during the connect sequence, a terminal dialog pops up that allows you to perform the text-based logon exchange, and the Authentication dialog box does not appear.

   The PPP standard provides for fully automated authentication, using encrypted or clear-text authentication protocols. Most PPP providers today do not implement the PPP authentication protocols and instead require a text-based exchange prior to starting PPP.

It is possible to automate the text-based exchange by using a SWITCH.INF script instead of the clear-text logon dialog. For more information, see the next section, "Automating Remote Logons Using SWITCH.INF Scripts," and "Activating SWITCH.INF Scripts," and "Troubleshooting Scripts Using DEVICE.LOG" later in this chapter.

SLIP Servers

Serial Line Internet Protocol (SLIP) is an older protocol that does not support authentication as part of the protocol. SLIP connections typically rely on text-based logon sessions. Encryption and automatic network parameter negotiations are not supported. The following steps are important when you are connecting to a SLIP server.

1. SLIP always prompts you for credentials when you dial, so the Authenticate Using Current User Name and Password check box in the Edit Phone Book Entry dialog box is ignored.

2. Windows NT RAS is not a SLIP server, but Windows NT RAS clients can connect to SLIP servers. In the Edit Phone Book Entry dialog box, select the Network button, and then select the SLIP option in the Network Protocol Settings dialog box for the entry.
3. SLIP is programmed to always use Terminal. Thus, to connect to a SLIP server, you do not need to select Terminal in the After Dialing box or to configure any Security settings. You will need to change only the After Dialing box when you are selecting a script to use for automating remote logons.

For more information, see "Automating Remote Logons Using SWITCH.INF Scripts," "Activating SWITCH.INF Scripts," and "Troubleshooting Scripts Using DEVICE.LOG" later in this chapter.

Using RAS Terminal for Remote Logons

For a PPP server, if the remote computer you dial in to requires you to log on with a terminal screen, you must configure the Security settings for that RAS entry to use a RAS Terminal logon. SLIP servers automatically use a RAS Terminal logon and do not require you to configure any Security settings.

After RAS connects to the remote system, a character-based window appears and displays the logon sequence from the remote computer. You use this window to interact with the remote computer for logging on. Alternatively, you can automate this manual logon as described in the section, "Automating Remote Logons Using SWITCH.INF Scripts."

On some commercial networks, you will be presented with a large menu of available services before you log on. On old, established SLIP servers, you may go through an extensive sequence of commands that updates files, collects data about you, or configures your SLIP connection during your logon process. On a new PPP server, you may be prompted for only your username and password before you are given a connection.

Note If the remote computer is a Microsoft RAS server, you do not need to use a terminal logon. Instead, logon is completely automated for you.

▸ **To configure a Windows NT RAS entry to use RAS Terminal after dialing**

1. In Remote Access, select the entry to which you want to connect.
2. Choose the Edit button.
3. If the Security button is not visible, choose the Advanced button.
4. Choose the Security button.
5. Select the Use Clear Text Terminal Login Only option. You do not need to select Terminal in the After Dialing box. The Terminal option is used with intermediary devices and not for remote logons.

   Note This is for PPP servers. SLIP servers automatically use Terminal and do not require you to configure the Security settings.

6. Choose the OK button until you return to the main Remote Access screen.

After you dial and connect to this entry, the After Dial Terminal window appears and you will see prompts from the remote computer. You then log on to the remote computer using the After Dial Terminal window. After you have completed all interactions with the remote computer, choose the Done button. If you are connecting to a SLIP server, you must also enter an IP address in the bottom right corner of the SLIP Terminal window and choose the Done button.

If the logon sequence does not vary, you can write a script that automatically passes information to the remote computer during the logon sequence, enabling completely automatic connections. If you are connecting to a SLIP server and the logon sequence is consistent, you can automate everything except passing the IP address and choosing the Done button.

After you activate a script, for non-SLIP connections, you will no longer see the Terminal window.

For more information, see "Automating Remote Logons Using SWITCH.INF Scripts," "Activating SWITCH.INF Scripts," and "Troubleshooting Scripts Using DEVICE.LOG" later in this chapter.

Automating Remote Logons Using SWITCH.INF Scripts

You can use the SWITCH.INF file (or PAD.INF on X.25 networks) to automate the logon process instead of using the manual RAS Terminal window described in the preceding section,"Using RAS Terminal for Remote Logons."

Automated scripts are especially useful when a constant connection to a remote computer is needed. If a remote connection fails, RAS automatically redials the number and reestablishes the connection if the RAS entry is configured to use a script. However, this is only true for non-SLIP connections. Scripts are also timesavers if you frequently log on to a remote system, and do not want to manually log on each time.

The script language described in this chapter was also designed to communicate with other devices, including modems. If you are not familiar with modem scripts, scripting can be difficult to understand. The following section explains how to create scripts, although you will probably find it easiest to copy, then modify, one of the generic sample scripts.

The SWITCH.INF file provides a generic script that will probably work with little or no modification when connecting to many PPP servers. It is recommended that you first try to connect using the generic script. Then, if that does not work, you can copy, then modify the generic script to match the logon sequence of the remote computer you want to connect to.

The first step in automating a remote logon is creating a script in the SWITCH.INF file. Then you must enable the script by selecting it in the Before Dialing or After Dialing boxes in the Security Settings dialog box. The After Dialing box applies in most cases. For directions about activating the generic script provided in RAS, see "Activating SWITCH.INF Scripts" later in this chapter.

Creating Scripts for RAS

The SWITCH.INF file is like a set of small batch files (scripts) contained in one file. The SWITCH.INF file can contain a different script for each intermediary device or online service that the RAS user will call.

A SWITCH.INF script has six elements: a section header, comments, commands, responses, response keywords, and macros.

Section Headers

Section headers divide the SWITCH.INF file into individual scripts. A section header marks the beginning of a script for a certain remote computer and must not exceed 31 characters. The text of a section header will appear in RAS when you activate the script. The section header is enclosed in square brackets. For example:

```
[Route 66 Logon]
```

Comment Lines

Comment lines must have a semicolon (;) in column one and can appear anywhere in the file. Comment lines contain information for those who maintain the SWITCH.INF file. For example:

```
; This script was created by MariaG on September 29, 1996
```

Commands

Each line in a script is a command from your local computer to the remote computer or a response from the remote computer to your local computer. Each command or response is a stream of data or text. For example, this command sends a username (MariaG) and a carriage return (the macro **<cr>**) to the remote computer.

COMMAND=MariaG<cr>

The commands and responses must be in the exact order in which the remote device expects them. Branching statements, such as GOTO or IF, are not supported.

The required sequence of commands and responses for a specific remote device should be in the documentation for the device, or, if you are connecting to a commercial service, from the support staff of that service. If the exact sequence is not available, activate the generic script provided with RAS and modify it to match the logon sequence of the remote computer as described in the section "Troubleshooting Scripts Using DEVICE.LOG," later in this chapter.

The COMMAND= statement can be used in two additional ways:

```
COMMAND=
NoResponse
```

This is the default behavior and causes an approximate two-second delay. This can be useful when the intermediate device requires a delay.

```
COMMAND= string
```

Note *string* is not followed by a carriage return (<**cr**>). This is useful when a device requires slow input. Instead of receiving the whole command string, the device requires characters to be sent one-by-one.

The following is an example where the intermediary device is so slow that it is only able to receive and process one character of the command PPP at a time.

```
COMMAND=P
NoResponse

COMMAND=P
NoResponse

COMMAND=P
NoResponse
```

Responses

A response is sent from the remote device or computer. To write an automatic script, you must know the responses you will receive from the remote device. If there is a gap of two or more seconds between characters, the received text is sent as a response. This gap is the only cue that a response is over. For more information, see the following section, "Getting Through Large Blocks of Text and Two-Second Gaps" later in this chapter.

Response Keywords

The keyword in a response line specifies what to do with the responses you receive from the remote computer:

OK=*remote computer response<macro>*
The script continues to the next line if the response or macro is encountered.

LOOP=*remote computer response<macro>*
The script returns to the previous line if the response or macro is encountered.

CONNECT=*remote computer response <macro>*
Used at the end of a successful modem script. Not generally useful for the SWITCH.INF file.

ERROR= *remote computer response <macro>*
Causes RAS to display a generic error message if the response is encountered. Useful for notifying the RAS user when the remote computer reports a specific error.

ERROR_DIAGNOSTICS= *remote computer response* **<diagnostics>**
Causes RAS to display the specific cause for an error returned by the device. Not all devices report specific errors. Use **ERROR=** if your device does not return specific errors that can be identified with Microsoft RAS diagnostics.

NoResponse
Used when no response will come from the remote device.

RAS on the local computer always expects a response from the remote device and will wait until a response is received unless a **NoResponse** statement follows the **COMMAND=** line. If there is no statement for a response following a **COMMAND=** line, the **COMMAND=** line will execute and stop the script at that point.

Macros

Macros are enclosed in angle brackets (< >). Macros perform the following special functions.

<cr>
Inserts a carriage return.

<lf>
Inserts a line feed.

<match> "*string*"
Reports a match if the string enclosed in quotation marks is found in the device response. Each character in the string is matched according to uppercase and lowercase. For example, **<match>** "Smith" matches Jane Smith and John Smith III, but not SMITH.

<?>
Inserts a wildcard character, for example, **CO<?><?>2** matches COOL2 or COAT2, but not COOL3.

<hXX> (XX are hexadecimal digits)
Allows any hexadecimal character to appear in a string including the zero byte, **<h00>**.

<ignore>
Ignores the rest of a response from the macro on.

<diagnostics>
Passes specific error information from a device to RAS. This enables RAS to display the specific error to RAS users. Otherwise, a nonspecific error message appears.

New Macros in Windows NT 3.51

The following two macros enable your username and password logon credentials to be automatically passed to the remote computer.

<username>
The username entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

<password>
The password entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

- **If both of the following situations are true, a Retry Authentication dialog box appears with a message that your logon credentials have failed**

1. You are calling into a system with an intermediary security device. This situation would generally not apply if you are using RAS to call an Internet provider.
2. After the security device has logged you on successfully, you are attempting to log on to a Windows NT RAS server.

   The reason this message appears is that the RAS Authentication dialog box username and password boxes are used by the two new username and password macros as well as by Windows NT RAS servers.

   For example, if the logon information for an intermediary security device that is plugged in between the Windows NT RAS server and its modem is username: "BB318" and password: "34554377", but on the Windows NT RAS server it is username: "BB318" and password: "treehouse", then your logon to the intermediary device will succeed, but your logon to the Windows NT RAS server will fail.

   Logon will fail because the security device password of "34554377" is different from the Windows NT domain password. Windows NT will prompt you with the Retry Authentication dialog box to obtain your proper Windows NT logon credentials, in this case the password.

- **To eliminate the Retry Authentication dialog box, you have the following options**

1. Ask your administrator to make your username and password identical on both systems, although this is not advisable because it would defeat the purpose of the security device.
2. Do not use the shared dialog box for the intermediary device logon credentials by entering the username and password in clear text into the SWITCH.INF file according to the [Generic login for YourLoginHere] script provided in SWITCH.INF. In order to keep your clear-text password confidential you need to use Windows NT file system (NTFS) file permissions to prevent other users from accessing this file.

Stepping Through an Example Script

This section describes each part of the generic script provided in the SWITCH.INF file included with RAS.

Every script must start with a command to the remote computer followed by one or more response lines. This initial command often may be simply to wait for the remote computer to initialize and send its logon banner. The default initial command is to wait two seconds for the logon banner. It would look like this in the SWITCH.INF file:

COMMAND=

If the response, (the logon banner from the remote computer) is the following:

```
Welcome to Gibraltar Net. Please enter your login:
```

then the corresponding response line in the SWITCH.INF file should be:

OK=<match>"Please enter your login:"

This line indicates that everything is correct if the remote computer sends the string "Please enter your login:". You respond by sending a command with the characters in your username and the carriage return.

COMMAND=MariaG<cr>

If the response from the remote computer is the following:

```
Please enter your password:
```

then the corresponding response line in the SWITCH.INF file should be:

OK=<match>"Please enter your password:"

To send your password, you would send the command:

COMMAND=mUs3naB<cr>

On many PPP computers, this script would automatically log you on.

Automating Log On to SLIP Computers

On SLIP systems you are also required to enter an IP address, so even though you can automate much of the logon sequence, you must manually enter your IP address in the SLIP terminal window. A permanent IP address may be provided to you in advance, or the SLIP Login Terminal window may provide a different IP Address each time you log on. This is an example of why PPP connections are usually easier to use.

However, it is possible to fully automate connections to a SLIP provider using the command-line utility RASDIAL.EXE, but only if all of the following conditions are true:

- The SLIP provider assigns you the same IP address every time you call.
- You have called at least once using the Remote Access program and filled in the IP address field at the lower right corner of the SLIP Terminal window so that the permanent IP address can be stored by RAS for the next connection with the RASDIAL.EXE utility.
- The SLIP logon sequence is automated by an After Dialing SWITCH.INF script. Note that the script you create would not have to include any commands or responses using the IP address because the IP address is permanently stored by RAS (until you delete your particular phonebook entry).

If any of the above conditions are not true, you cannot use the RASDIAL.EXE utility to connect to your SLIP provider because your IP address will not get set correctly.

Note RASDIAL.EXE is in your *systemroot*\SYSTEM32 directory. The automatic redial upon link failure feature, which is present in the Remote Access program (RASPHONE.EXE), is not part of RASDIAL.EXE. For help on RASDIAL.EXE, type RASDIAL /? at a Windows NT command prompt.

Getting Through Large Blocks of Text and Two-Second Gaps

If the remote computer has a two-second gap in the data stream reponse to your computer, RAS assumes that the gap is the end of the response. These gaps may occur anywhere, including between words, and can only be detected using DEVICE.LOG. For more information, see the "Troubleshooting Scripts Using DEVICE.LOG" section later in this chapter.

If you write a script that seems to fail for no reason, consult DEVICE.LOG to see if a response ends in the middle of a word. If so, your script must account for the two-second gap. A simple way to do this is to include the command:

```
COMMAND=<cr>
```

You can skip to the end of large blocks of text that contain multiple gaps by using the **LOOP=** keyword and by matching text at the end of a block. For example,

```
COMMAND=<cr>
OK=<match>"Enter the service to start:"
LOOP=<ignore>
```

In this example, RAS sends a null command (waits two seconds), RAS then waits for the message “Enter the service to start:”. If this is a long block of text, RAS does not find the string so RAS then moves to the **LOOP** command. The **LOOP** command causes RAS to return to the line above, and RAS waits for the words “Enter the service to start:” in the second response. In this manner, you can loop though long blocks of text until you reach the text of the desired prompt.

Commands and Carriage Returns

Usually, you must include **<cr>,** which indicates a carriage return, at the end of a command. The carriage return causes the remote computer to process the command immediately. If you do not include **<cr>**, the remote computer may not recognize the command.

In other situations, **<cr>** cannot be used because the remote computer accepts the command without a carriage return and requires time to process the command. This situation mainly applies when you are sending a series of commands without expecting a response.

Activating SWITCH.INF Scripts

After you have created a script in SWITCH.INF, you can configure a RAS entry to execute the script before dialing, after dialing, or both.

► **To activate a script in Windows NT**

1. In Remote Access, select the entry to which you want to connect.
2. Choose the Edit button.
3. If the Security button is not visible, choose the Advanced button.
4. Choose the Security button.
5. In the Security Settings dialog box, in the After Dialing or Before Dialing box, select the name of the script.

   By default, None is selected. The section header in SWITCH.INF appears as the name of the script.

6. Select the Accept Any Authentication Including Clear Text option.

   You only need to configure this for PPP connections.

   Selecting this option turns off the terminal and the Authentication dialog box appears. To prevent this dialog box from appearing, in the Edit Phone Book Entry dialog box, select the Authenticate Using Current User Name and Password check box.
7. Choose the OK button until you return to the main Remote Access screen.

When you dial this entry, the selected script will execute and complete all communication with the remote device before or after RAS dials the remote host.

Troubleshooting Scripts Using DEVICE.LOG

Windows NT allows you to log all information passed between RAS, the modem, and the remote device, including errors reported by the remote device. This allows you to find errors that prevent your scripts from working.

The DEVICE.LOG file is created by enabling logging in the Registry. The DEVICE.LOG file is in the *systemroot*\SYSTEM32\RAS directory.

▸ **To create the DEVICE.LOG file**

1. Hang up any connections, and then exit from Remote Access.
2. Start the Registry Editor by running the REGEDT32.EXE program.
3. Locate HKEY_LOCAL_MACHINE, and then access the following key: \SYSTEM\CurrentControlSet\Services\RasMan\Parameters
4. Change the value of the Logging parameter to 1. When changed, the parameter should look like this:

   Logging:REG_DWORD:0x1
5. Close the Registry Editor.

Logging begins when you restart Remote Access or start the Remote Access Server service (if your computer is receiving calls). You do not need to shut down and restart Windows NT.

After you dial a number and connect, a script will start. If an error is encountered during script execution, execution halts. You should exit RAS, and then determine the problem by using any text editor to view DEVICE.LOG. The following topic is an example of an incomplete script that failed and the DEVICE.LOG file created when a connection was attempted.

Note The traces from all calls will be appended to DEVICE.LOG as long as RAS or the Remote Access Server service are not stopped and restarted. So, if you need to save a DEVICE.LOG file with useful information for later review or troubleshooting, make a copy of the file, giving the file another name before you restart RAS or the Remote Access Server service.

Example of an Incomplete SWITCH.INF Script

The following script is incomplete for the service to which the user tried to connect. This script was used with DEVICE.LOG to discover that the remote computer expected additional commands from the script. See the sample DEVICE.LOG for the complete output that was generated.

```
[Gibraltar Net Login for MariaG]
; FIRST COMMAND TO INITIALIZE REMOTE COMPUTER
COMMAND=

; Skip to login prompt. That is, loop through blocks of text
; separated by 2-second gaps until the login prompt is encountered.
OK=<match>"Login:"
LOOP=<ignore>

; Provide username to remote computer
COMMAND=MariaG<cr>

; Since no 2-second gap is present, immediately match "Password:"
OK=<match>"Password:"

; Provide password to remote computer
COMMAND=mUs3naB
```

Sample DEVICE.LOG

This is the DEVICE.LOG file created by using the sample generic script. Note that DEVICE.LOG comment lines in all uppercase letters are writer comments added after the file was created to help you understand the contents of the file.

```
Remote Access Service Device Log 08/23/1996 13:52:21
-------------------------------------------------------------
; THIS SECTION IS THE COMMUNICATION BETWEEN RAS AND THE MODEM
Port:COM1 Command to Device:AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55
Port:COM1 Echo from Device :AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55
Port:COM1 Response from Device:
OK
Port:COM1 Command to Device:AT\Q3\N7%C0M1
Port:COM1 Echo from Device :AT\Q3\N7%C0M1
Port:COM1 Response from Device:
OK

; COMMAND TO DIAL REMOTE COMPUTER AND SUCCESSFUL CONNECTION
Port:COM1 Command to Device:ATDT1 206 555 5500
Port:COM1 Echo from Device :ATDT1 206 555 5500
Port:COM1 Response from Device:
CONNECT 14400/REL
Port:COM1 Connect BPS:19200
Port:COM1 Carrier BPS:14400

; INITIAL NULL COMMAND SENT TO DEVICE
Port:COM1 Command to Device:
Port:COM1 Response from Device:
_[2J_[H
Welcome to Gibraltar Net, a service of: Trey Computing,  Inc.

Problems logging in?  Call us at 555-5500 between 8:00am and 8:00pm Mon-
Sat.

NOTE: Your software must support VT100 (or higher) terminal emulation!

Port:COM1 Response from Device:P

; THE LINE ABOVE INDICATES A TWO-SECOND GAP IN THE MIDDLE
; OF THE WORD “PLEASE” IF YOUR SCRIPT FAILED AND DEVICE.LOG ENDED
; AFTER THE RESPONSE ABOVE, YOU WOULD ACCOUNT FOR THIS
; TWO-SECOND GAP IN YOUR SCRIPT BY USING A NULL COMMAND= LINE OR THE
; OK=response AND LOOP=<match> COMBINATION.
Port:COM1 Response from Device:lease turn OFF your Caps Lock if it is on
now.

Please enter your login name and password at the prompts below.
  - Log in as "guest" to take a look around the system.
  - Log in as "new" to create an account for yourself.
```

```
Login:

; SEND YOUR USERNAME AS A COMMAND
Port:COM1 Command to Device:MariaG
Port:COM1 Echo from Device :MariaG
Port:COM1 Response from Device:
Password:

; SEND YOUR PASSWORD AS A COMMAND
Port:COM1 Command to Device: mUs3naB
Port:COM1 Echo from Device : mUs3naB

; THE LOGIN SEQUENCE CONTINUES ON THE REMOTE COMPUTER
; BUT THE SCRIPT DOES NOT CONTINUE FROM HERE.
; THE AUTOMATED LOG IN WOULD FAIL AT THIS POINT.
Port:COM1 Response from Device:
```

This script would be complete for many remote computers, but the remote computer sent more responses and expected a command to start a service. To complete the script you must know the remainder of the responses from the remote computer. If you logged on manually using RAS Terminal and found the remainder of the logon sequence looked like this:

```
Gibraltar Net offers you several network services:

Service
-----------------------------------------------------------------------
SHell
UPload
DOwnload
PAssword
PPP
SLIP

Please enter a service:
```

you would complete the script with these lines:

COMMAND=<cr>
OK=<match>"Please enter a service:"
LOOP=<ignore>

If you added the lines above to your script, restarted RAS and redialed, you would successfully connect.

If the generic script in RAS does not work, these guidelines should help you modify the generic script to work for your connections. It is suggested you first copy the generic script to the end of SWITCH.INF, then modify the copy to work with your connections.

Using Scripts with Other Microsoft RAS Clients

Microsoft RAS version 1.0 (which runs on LAN Manager) does not have the capability to invoke RAS Terminal or use scripts in .INF files.

Microsoft RAS version 1.1a (which runs on LAN Manager) supports PAD.INF only. Note that the syntax used in the PAD.INF file differs slightly from subsequent versions of Microsoft RAS.

Microsoft RAS for Windows for Workgroups version 3.11 and Windows NT version 3.1 or later support RAS Terminal and scripts in SWITCH.INF and PAD.INF.

Chapter 22 Remote Access Service and the Internet

The following section has been updated in this chapter.

Installing a Simple Internet Router that Uses PPP

Windows NT RAS version 3.5 or later was not designed to route packets from a large local area network over a dial-up link. However, by correctly configuring both the RAS computer acting as a router and the other computers on your small LAN with a static network configuration, you can use the computer running Windows NT RAS as a simple router to the Internet or to an enterprise TCP/IP network.

The following requirements are necessary for using Windows NT RAS as a dial-up router between your LAN and the Internet.

- A Windows NT computer with a high-speed modem and a network adapter card
- A Point-to-Point Protocol (PPP) connection to the Internet
- A valid network, or a subnet different from the subnet of the Internet service provider
- The proper Registry and Default Gateway configurations on the computer acting as a router and on the LAN clients. The configurations are described later in this section.
- A small LAN that does not require the automatic routing configuration provided by RIP. (You probably do not need RIP functionality if you have a small LAN that is not expected to grow or change.)

To be identified using names rather than IP addresses, you also need a domain name. Your Internet service provider might help you obtain a domain name.

Once you have a PPP connection, IP addresses for your subnet (and correct subnet mask), and (optionally) a domain name, you can then configure the RAS and LAN computers for Internet gateway as described in the following procedure.

▸ **To configure a small LAN for routing to the Internet over a dedicated PPP account**

1. On the RAS computer that will route packets from the LAN to the Internet, add the value **DisableOtherSrcPackets** to the Registry path shown below, and then set the value to 0.

   By default, the header of each packet sent by the RAS computer over the PPP link uses the IP address of the RAS computer as the source. Since the packets that come from LAN clients are not originating from the RAS computer, you must set **DisableOtherSrcPackets** to 0 so that the packets will be forwarded over the PPP link.

   ```
   \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
       \RasArp\Parameters
   ```

   DisableOtherSrcPackets **REG_DWORD**
   Range: 0-1
   Default: 1 (not in Registry)

2. If the subnet you have is in the same network class as your service provider, (which is very likely in this scenario), you must also add the value **PriorityBasedOnSubNetwork** to the Registry of the RAS computer that routes packets from the LAN to the Internet, and then set this parameter to 1.

   A computer can connect to the LAN using a network card and a RAS connection. If the RAS connection and the LAN network adapter card are assigned addresses with the same network number, and the Use Default Gateway On Remote Network check box is selected, then all packets are sent over the RAS connection, even though the two addresses are in different subnetworks within the same network.

   For example, if the network adapter card has IP address 17.1.1.1 (subnet mask 255.255.0.0) and the RAS connection is assigned the address 17.2.1.1, RAS sends all 17.x.x.x packets using the RAS connection. If the parameter is set, RAS sends 17.2.x.x packets using the RAS connection and 17.1.x.x packets using the network adapter card.

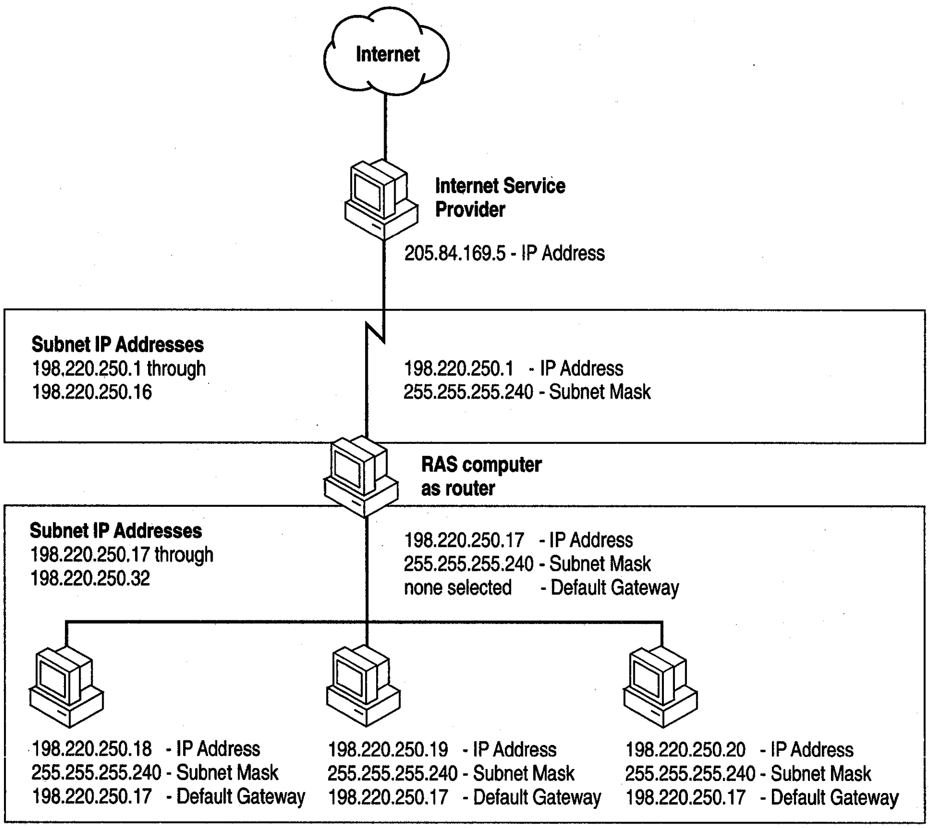
   ```
   \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
       \RasMan\PPP\IPCP
   ```

   PriorityBasedOnSubNetwork **REG_DWORD**
   Range: 0-1
   Default: 0 (not in Registry)

3. Configure the default gateway of all the computers on the LAN using the Network option in Control Panel.

   The default gateway is set when you configure the TCP/IP protocol.

   Use the IP address of the network card adapter in the RAS computer acting as a router to the Internet as the default gateway for all computers on the LAN except this computer. The default gateway for the computer acting as the router to the Internet should be left blank. Refer to the following figure to determine the correct assignment pattern of IP addresses, subnet masks, and default gateways.


Internet
Internet Service Provider
205.84.169.5 - IP Address
Subnet IP Addresses
198.220.250.1 through
198.220.250.16
198.220.250.1 - IP Address
255.255.255.240 - Subnet Mask
RAS computer as router
Subnet IP Addresses
198.220.250.17 through
198.220.250.32
198.220.250.17 - IP Address
255.255.255.240 - Subnet Mask
none selected - Default Gateway
198.220.250.18 - IP Address
255.255.255.240 - Subnet Mask
198.220.250.17 - Default Gateway
198.220.250.19 - IP Address
255.255.255.240 - Subnet Mask
198.220.250.17 - Default Gateway
198.220.250.20 - IP Address
255.255.255.240 - Subnet Mask
198.220.250.17 - Default Gateway

Sample Configuration using RAS as a Simple Internet Router

Appendix B MIB Object Types for Windows NT

This appendix contains information about each of the MIBs supported by Windows NT. It replaces Appendix B in the *Windows NT Networking Guide.*

These are the MIBs supported in Windows NT 3.5 and 3.51:

MIB	Contents
LMMIB2.MIB	LAN Manager MIB II for Windows NT objects, including Common group, Server group, Workstation group, and Domain group
DHCP.MIB	Microsoft DHCP objects
WINS.MIB	Microsoft WINS objects
MIB_II.MIB	Internet MIB II (based on RFC 1213)

This appendix assumes that you are familiar with network management, TCP/IP, and SNMP. It also assumes that you are familiar with the concept of a *management information base* (MIB). If you are not familiar with TCP/IP or the Internet MIB 2, see *Internetworking with TCP/IP* by Douglas E. Comer (Prentice Hall, 1991) and *The Simple Book* by Marshall T. Rose (Prentice Hall, 1994).

LAN Manager MIB II for Windows NT Objects

The LAN Manager MIB II for Windows NT contains a set of objects specifically designed to support computers running Windows NT. Notice that there are fewer objects in the LAN Manager MIB II for Windows NT than the LAN Manager MIB II for OS/2 because of differences in the operating systems.

All LAN Manager MIB II objects apply to computers running Windows NT Workstation and Windows NT Server.

Common Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.lanmanager.lanmgr-2.common .3.6.1.4.1.77.1.1)

comVersionMaj {common 1}
The major release version number of the Windows NT software.
SYNTAX OCTET STRING
ACCESS read-only

comVersionMin {common 2}
The minor release version number of the Windows NT software.
SYNTAX OCTET STRING
ACCESS read-only

comType {common 3}
The type of Windows NT software this system is running.
SYNTAX OCTET STRING
ACCESS read-only

comStatStart {common 4}
The time at which time the Windows NT statistics on this node were last cleared. The time is the number of seconds since January 1, 1970.
SYNTAX INTEGER
ACCESS read-only

The **comStatStart** object applies to the following statistical objects:

comStatNumNetIOs
comStatFiNetIOs
comStatFcNetIOs
svStatOpens
svStatDevOpens
svStatQueuedJobs
svStatSOpens
svStatErrorOuts
svStatPwErrors
svStatPermErrors
svStatSysErrors
svStatSentBytes
svStatRcvdBytes
svStatAvResponse
wkstaStatSessStarts
wkstaStatSessFails
wkstaStatUses
wkstaStatUseFails
wkstaStatAutoRecs

comStatNumNetIOs {common 5}
The number of network I/O operations submitted on this node.
SYNTAX Counter
ACCESS read-only

comStatFiNetIOs {common 6}
The number of network I/O operations on this node that failed issue.
SYNTAX Counter
ACCESS read-only

comStatFcNetIOs {common 7}
The number of network I/O operations on this node that failed completion.
SYNTAX Counter
ACCESS read-only

Server Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.lanmanager.lanmgr-2.server (1.3.6.1.4.1.77.1.2)

svDescription {server 1}
A comment describing the server.
SYNTAX DisplayString (size (0..255))
ACCESS read-write

svSvcNumber {server 2}
The number of network services installed on the server.
SYNTAX INTEGER
ACCESS read-only

svSvcTable {server 3}
A list of service entries describing the network service installed on the server.
SYNTAX SEQUENCE OF SvSvcEntry
ACCESS not-accessible

svSvcEntry {svSvcTable 1}
The names of the network services installed on the server.
SYNTAX SvSvcEntry
ACCESS read-only

svSvcName {svSvcEntry 1}
The name of a Windows NT network service.
SYNTAX DisplayString (size (1..15))
ACCESS read-only

svSvcInstalledState {svSvcEntry 2}
The installation status of a network.
SYNTAX INTEGER {
    uninstalled(1),
    install-pending(2),
    uninstall-pending(3),
    installed(4)
    }
ACCESS read-only

svSvcOperatingState {svSvcEntry 3}
The operating status of a network service.
SYNTAX INTEGER {
active(1),
continue-pending(2),
pause-pending(3),
paused(4)
}
ACCESS read-only

svSvcCanBeUninstalled {svSvcEntry 4}
Indicates whether the network service specified by this entry can be removed.
SYNTAX INTEGER {
cannot-be-uninstalled(1),
can-be-uninstalled(2)
}
ACCESS read-only

svSvcCanBePaused {svSvcEntry 5}
Indicates whether the network service specified by this entry can be paused.
SYNTAX INTEGER {
cannot-be-paused(1),
can-be-paused(2)
}
ACCESS read-only

svStatOpens {server 4}
The total number of files that were opened on the server.
SYNTAX Counter
ACCESS read-only

svStatDevOpens {server 5}
The total number of communication devices that were opened on the server.
SYNTAX Counter
ACCESS read-only

svStatQueuedJobs {server 6}
The total number of print jobs that were spooled on the server.
SYNTAX Counter
ACCESS read-only

svStatSOpens {server 7}
The number of sessions that were started on the server.
SYNTAX Counter
ACCESS read-only

```
svStatErrorOuts {server 8}
    The number of sessions disconnected because of an error on the server.
    SYNTAX Counter
    ACCESS read-only
svStatPwErrors {server 9}
    The number of password violations encountered on the server.
    SYNTAX Counter
    ACCESS read-only
svStatPermErrors {server 10}
    The number of access-permission violations encountered on the server.
    SYNTAX Counter
    ACCESS read-only
svStatSysErrors {server 11}
    The number of system errors encountered on the server.
    SYNTAX Counter
    ACCESS read-only
svStatSentBytes {server 12}
    The number of bytes sent by the server.
    SYNTAX Counter
    ACCESS read-only
svStatRcvdBytes {server 13}
    The number of bytes received by the server.
    SYNTAX Counter
    ACCESS read-only
svStatAvResponse {server 14}
    The mean number of milliseconds it took the server to process a workstation I/O
    request (for example, the average time an NCB sat at the server).
    SYNTAX INTEGER
    ACCESS read-only
svSecurityMode {server 15}
    The type of security running on the server.
    SYNTAX INTEGER{
        share-level(1),
        user-level(2)
        }
    ACCESS read-only
```

svUsers {server 16}
The number of concurrent users the server can support.
SYNTAX INTEGER
ACCESS read-only

svStatReqBufsNeeded {server 17}
The number of times the server requested allocation of additional buffers.
SYNTAX Counter
ACCESS read-only

svStatBigBufsNeeded {server 18}
The number of times the server needed but could not allocate a big buffer while processing a client request.
SYNTAX Counter
ACCESS read-only

svSessionNumber {server 19}
The number of sessions on the server.
SYNTAX INTEGER
ACCESS read-only

svSessionTable {server 20}
A list of session entries corresponding to the current sessions that clients have with the server.
SYNTAX SEQUENCE OF SvSessionEntry
ACCESS read-only

svSessionEntry {svSessionTable 1}
A session that is currently established on the server.
SYNTAX SvSessionEntry
ACCESS read-only

svSesClientName {svSessionEntry 1}
The name of the remote computer that established the session.
SYNTAX DisplayString (size (1..15))
ACCESS read-only

svSesUserName {svSessionEntry 2}
The name of the user account that established the session on the remote computer.
SYNTAX DisplayString (size (1..20))
ACCESS read-only

svSesNumConns {svSessionEntry 3}
The number of connections to server resources that are active in the current session.
SYNTAX INTEGER
ACCESS read-only

svSesNumOpens {svSessionEntry 4}
The number of files, devices, and pipes that are open in the current session.
SYNTAX INTEGER
ACCESS read-only

svSesTime {svSessionEntry 5}
The length of time, in seconds, since the current session began.
SYNTAX Counter
ACCESS read-only

svSesIdleTime {svSessionEntry 6}
The length of time, in seconds, that the session has been idle.
SYNTAX Counter
ACCESS read-only

svSesClientType {svSessionEntry 7}
The type of client that established the session.
SYNTAX INTEGER {
down-level(1),
dos-lm(2),
dos-lm-2(3),
os2-lm-1(4),
os2-lm-2(5),
dos-lm-2-1(6),
os2-lm-2-1(7),
afp-1-1(8),
afp-2-0(9),
NT-3-1(10)
}
ACCESS read-only

svSesState {svSessionEntry 8}
The state of the current session. (Setting the state of an active session to **deleted** with **netSessionDel** deletes the client session. The session state cannot be set to **active**.)
SYNTAX INTEGER{
active(1),
deleted(2)
}
ACCESS read-write

svAutoDisconnects {server 21}
The number of sessions that the server automatically disconnected because of inactivity.
SYNTAX INTEGER
ACCESS read-only

svDisConTime {server 22}
The number of seconds the server waits before disconnecting an idle session.
SYNTAX INTEGER
ACCESS read-write

svAuditLogSize {server 23}
The maximum size, in kilobytes, of the server's audit log.
SYNTAX INTEGER
ACCESS read-write

svUserNumber {server 24}
The number of users who have accounts on the server.
SYNTAX INTEGER
ACCESS read-only

svUserTable {server 25}
A table of active user accounts on the server.
SYNTAX SEQUENCE OF SvUserEntry
ACCESS not-accessible

svUserEntry {svUserTable 1}
A user account on the server.
SYNTAX SvUserEntry
ACCESS not-accessible

svUserName {svUserEntry 1}
The name of a user account.
SYNTAX DisplayString (size (1..20))
ACCESS read-only

svShareNumber {server 26}
The number of shared resources on the server.
SYNTAX INTEGER
ACCESS read-only

svShareTable {server 27}
A table of the shared resources on the server.
SYNTAX SEQUENCE OF svShareEntry
ACCESS not-accessible

svShareEntry {svShareTable. 1}
A table corresponding to a single shared resource on the server.
SYNTAX svShareEntry
ACCESS not-accessible

svShareName {svShareEntry 1}
The name of a shared resource.
SYNTAX DisplayString (size (1..12))
ACCESS read-only

svSharePath {svShareEntry 2}
The local name of a shared resource.
SYNTAX DisplayString (size (1..255))
ACCESS read-only

svShareComment {svShareEntry 3}
A comment associated with a shared resource.
SYNTAX DisplayString (size (0..255))
ACCESS read-only

svPrintQNumber {server 28}
The number of printer queues on the server.
SYNTAX INTEGER
ACCESS read-only

svPrintQTable {server 29}
A table of the printer queues on the server.
SYNTAX SEQUENCE OF SvPrintQEntry
ACCESS not-accessible

svPrintQEntry {svPrintQTable 1}
A table entry corresponding to a single printer queue on the server.
SYNTAX SvPrintQEntry
ACCESS not-accessible

svPrintQName {svPrintQEntry 1}
The name of a printer queue.
SYNTAX DisplayString (size (1..12))
ACCESS read-only

svPrintQNumJobs {svPrintQEntry 2}
The number of jobs currently in a printer.
SYNTAX INTEGER
ACCESS read-only

Workstation Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.lanmanager.lanmgr-2.workstation
(1.3.6.1.4.1.77.1.3)

wkstaStatSessStarts {workstation 1}
The number of sessions the workstation initiated.
SYNTAX Counter
ACCESS read-only

wkstaStatSessFails {workstation 2}
The number of failed sessions the workstation had.
SYNTAX Counter
ACCESS read-only

```
wkstaStatUses {workstation 3}
    The number of connections the workstation initiated.
    SYNTAX Counter
    ACCESS  read-only
wkstaStatUseFails {workstation 4}
    The number of failed connections the workstation had.
    SYNTAX Counter
    ACCESS  read-only
wkstaStatAutoRecs {workstation 5}
    The number of sessions that were broken and then automatically reestablished.
    SYNTAX Counter
    ACCESS  read-only
wkstaErrorLogSize {workstation 6}
    The maximum size, in kilobytes, of the workstation error log.
    SYNTAX INTEGER
    ACCESS  read-write
wkstaUseNumber {workstation 7}
    This object will always return the value 0.
    SYNTAX INTEGER
    ACCESS  read-only

wkstaUseTable {workstation 8}
    SYNTAX SEQUENCE OF WkstaUseEntry
    ACCESS  not-accessible
wkstaUseEntry {wkstaUseTable 1}
    SYNTAX WkstaUseEntry
    ACCESS  not-accessible
useLocalName {wkstaUseEntry 1}
    SYNTAX DisplayString (size  (0..8))
    ACCESS  read-only
useRemote {wkstaUseEntry 2}
    SYNTAX DisplayString (size  (1..255))
    ACCESS  read-only
useStatus {wkstaUseEntry 3}
    SYNTAX INTEGER {
        use-ok(1),
        use-paused(2),
        use-session-lost(3),
        use-network-error(4),
        use-connecting(5),
        use-reconnecting(6)
         }
    ACCESS  read-only
```

Domain Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.lanmanager.lanmgr-2.domain (1.3.6.1.4.1.77.1.4)

domPrimaryDomain {domain 1}
The name of the primary domain to which the computer belongs.
SYNTAX DisplayString (size (1..15))
ACCESS read-only

domLogonDomain {domain 2}
SYNTAX DisplayString (size (1..15))
ACCESS read-only

domOtherDomainNumber {domain 3}
SYNTAX INTEGER
ACCESS read-only

domOtherDomainTable {domain 4}
SYNTAX SEQUENCE OF domOtherDomainEntry
ACCESS not-accessible

domOtherDomainEntry {domOtherDomainTable 1}
SYNTAX domOtherDomainEntry
ACCESS not-accessible

domOtherName {domOtherDomainEntry 1}
SYNTAX DisplayString (size (1..15))
ACCESS read-write

domServerNumber {domain 5}
SYNTAX INTEGER
ACCESS read-only

domServerTable {domain 6}
SYNTAX SEQUENCE OF domServerEntry
ACCESS not-accessible

domServerEntry {domServerTable 1}
SYNTAX domServerEntry
ACCESS not-accessible

domServerName {domServerEntry 1}
SYNTAX DisplayString (size (1..15))
ACCESS read-only

domLogonNumber {domain 7}
SYNTAX INTEGER
ACCESS read-only

domLogonTable {domain 8}
SYNTAX SEQUENCE OF DomLogonEntry
ACCESS not-accessible

domLogonEntry {domLogonTable 1}
SYNTAX DomLogonEntry
ACCESS not-accessible

domLogonUser {domLogonEntry 1}
SYNTAX Display String (size (1..20))
ACCESS read-only

domLogonMachine {domLogonEntry 2}
SYNTAX DisplayString (size (1..15))
ACCESS read-only

Microsoft DHCP Objects

Enterprises are defined in RFC 1155-SMI. Object Type is defined in RFC 1212. DisplayString is defined in RFC 1213.

DHCP MIB Parameters

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Dhcp.DhcpPar
(1.3.6.1.4.1.311.1.3.1)

ParDhcpStartTime {DhcpPar 1}
DHCP Server start time.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParDhcpTotalNoOfDiscovers {DhcpPar 2}
Indicates the number of discovery messages received.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfRequests {DhcpPar 3}
Indicates the number of requests received.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfReleases {DhcpPar 4}
Indicates the number of releases received.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfOffers {DhcpPar 5}
Indicates the number of offers sent.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfAcks {DhcpPar 6}
Indicates the number of acknowledgments sent.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfNacks {DhcpPar 7}
Indicates the number of negative acknowledgments sent.
SYNTAX Counter
ACCESS read-only

ParDhcpTotalNoOfDeclines {DhcpPar 8}
Indicates the number of declines received.
SYNTAX Counter
ACCESS read-only

DHCP Scope Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Dhcp.DhcpScope
(1.3.6.1.4.1.311.1.3.2)

ScopeTable {DhcpScope 1}
A list of subnets maintained by the server.
SYNTAX SEQUENCE OF ScopeTableEntry
ACCESS read-only

sScopeTableEntry {ScopeTable 1}
The row corresponding to a subnet.
SYNTAX ScopeTableEntry
ACCESS read-only

SubnetAdd {sScopeTableEntry 1}
The subnet address.
SYNTAX IpAddress
ACCESS read-only

NoAddInUse {sScopeTableEntry 2}
The number of addresses in use.
SYNTAX Counter
ACCESS read-only

NoAddFree {sScopeTableEntry 3}
The number of free addresses available.
SYNTAX Counter
ACCESS read-only

NoPendingOffers {sScopeTableEntry 4}
The number of addresses currently in the offer state — that is, those that are used temporarily.
SYNTAX Counter
ACCESS read-only

Microsoft WINS Objects

Enterprises are defined in RFC 1155-SMI. Object Type is defined in RFC 1212. DisplayString is defined in RFC 1213.

WINS Parameters

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Wins.Par
(1.3.6.1.4.1.311.1.2.1)

ParWinsStartTime {Par 1}
WINS start time.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastPScvTime {Par 2}
Most recent date and time at which planned scavenging took place. Planned scavenging happens at intervals specified in the Registry. Scavenging involves changing owned nonrenewed entries to the released state. Further, released records might be changed to extinct records, extinct records might be deleted, and revalidation of old replicas can take place.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastATScvTime {Par 3}
Most recent date and time at which scavenging took place as a result of administrative action.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastTombScvTime {Par 4}
Most recent date and time at which extinction scavenging took place.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastVerifyScvTime {Par 5}
Most recent date and time at which revalidation of old active replicas took place.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastPRplTime {Par 6}
Most recent date and time at which planned replication took place. Planned replication happens at intervals specified in the Registry.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastATRplTime {Par 7}
Most recent date and time at which administrator-triggered replication took place.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastNTRplTime {Par 8}
Most recent date and time at which network-triggered replication took place. Network-triggered replication happens as a result of an update notification message from a remote WINS.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastACTRplTime {Par 9}
Most recent date and time at which address change-triggered replication took place. Address change-triggered replication happens when the address of an owned name changes because of a new registration.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastInitDbTime {Par 10}
Most recent date and time at which the local database was generated statically from one or more data files.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParLastCounterResetTime {Par 11}
Most recent date and time at which the local counters were initialized to zero.
SYNTAX DisplayString (size (1..30))
ACCESS read-only

ParWinsTotalNoOfReg {Par 12}
Indicates the number of registrations received.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfQueries {Par 13}
Indicates the number of queries received.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfRel {Par 14}
Indicates the number of releases received.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfSuccRel {Par 15}
Indicates the number of releases that succeeded.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfFailRel {Par 16}
Indicates the number of releases that failed because the address of the requester did not match the address of the name.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfSuccQueries {Par 17}
Indicates the number of queries that succeeded.
SYNTAX Counter
ACCESS read-only

ParWinsTotalNoOfFailQueries {Par 18}
Indicates the number of queries that failed.
SYNTAX Counter
ACCESS read-only

ParRefreshInterval {Par 19}
Indicates the Renewal interval in seconds (sometimes called the refresh interval).
SYNTAX INTEGER
ACCESS read-only

ParTombstoneInterval {Par 20}
Indicates the Extinct interval in seconds.
SYNTAX INTEGER
ACCESS read-write

ParTombstoneTimeout {Par 21}
Indicates the Extinct timeout in seconds.
SYNTAX INTEGER
ACCESS read-write

ParVerifyInterval {Par 22}
Indicates the Verify interval in seconds.
SYNTAX INTEGER
ACCESS read-write

ParVersCounterStartVal_LowWord {Par 23}
Indicates the Low Word of the version counter that WINS should start with.
SYNTAX Counter
ACCESS read-write

ParVersCounterStartVal_HighWord {Par 24}
Indicates the High Word of the version counter that WINS should start with.
SYNTAX Counter
ACCESS read-write

ParRplOnlyWCnfPnrs {Par 25}
Indicates whether replication is allowed with nonconfigured partners. If not set to zero, replication will be done only with partners listed in the Registry (except when an update notification comes in).
SYNTAX INTEGER
ACCESS read-write

ParStaticDataInit {Par 26}
Indicates whether static data should be read in at initialization and reconfiguration time. Update of any MIB variable in the parameters group constitutes reconfiguration.
SYNTAX INTEGER
ACCESS read-write

ParLogFlag {Par 27}
Indicates whether logging should be done. Logging is the default behavior.
SYNTAX INTEGER
ACCESS read-write

ParLogFileName {Par 28}
Specifies the path to the log file.
SYNTAX DisplayString
ACCESS read-write

ParBackupDirPath {Par 29}
Specifies the path to the backup directory.
SYNTAX DisplayString
ACCESS read-write

ParDoBackupOnTerm {Par30}
Specifies whether WINS should perform a database backup upon termination. Values can be 0 (no) or 1 (yes). Setting this value to 1 has no meaning unless **ParBackupDirPath** is also set.

```
SYNTAX INTEGER {
   no(0),
   yes(1)
   }
ACCESS read-write
```

ParMigrateOn {Par 31}
Specifies whether static records in the WINS database should be treated as dynamic records during conflict with new name registrations. Values can be 0 (no) or 1 (yes).
SYNTAX INTEGER {
no(0),
yes(1)
}
ACCESS read-write

WINS Datafiles Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Wins.Datafiles
(1.3.6.1.4.1.311.1.2.4)

DFDatafilesTable {Datafiles 1}
A list of datafiles specified under the \Datafiles key in the Registry. These files are used for static initialization of the WINS database.
SYNTAX SEQUENCE OF DFDatafileEntry
ACCESS read-write

dDFDatafileEntry {DFDatafilesTable 1}
Datafile name.
SYNTAX DFDatafileEntry
ACCESS read-write

dFDatafileIndex {dDFDatafileEntry 1}
Used for indexing entries in the datafiles table. It has no other use.
SYNTAX INTEGER
ACCESS not-accessible

dFDatafileName {dDFDatafileEntry 2}
Name of the datafile to use for static initialization.
SYNTAX DisplayString
ACCESS read-write

WINS Pull Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Wins.Pull
(1.3.6.1.4.1.311.1.2.2)

PullInitTime {Pull 1}
Indicates whether pull should be done at WINS invocation and at reconfiguration. If any pull or push group's MIB variable is set, that constitutes reconfiguration.
SYNTAX INTEGER
ACCESS read-write

PullCommRetryCount {Pull 2}
Specifies the retry count in case of communication failure when doing pull replication. This is the maximum number of retries to be done at the interval specified for the partner before WINS stops for a set number of replication-time intervals before trying again.
SYNTAX INTEGER
ACCESS read-write

PullPnrTable {Pull 3}
A list of partners with which pull replication needs to be done.
SYNTAX SEQUENCE OF PullPnrEntry
ACCESS read-write

pPullPnrEntry {PullPnrTable 1}
The row corresponding to a partner.
SYNTAX PullPnrEntry
ACCESS read-write

PullPnrAdd {pPullPnrEntry 1}
The address of the remote WINS partner.
SYNTAX IpAddress
ACCESS read-write

PullPnrSpTime {pPullPnrEntry 2}
Specifies the specific time at which pull replication should occur.
SYNTAX DisplayString
ACCESS read-write

PullPnrTimeInterval {pPullPnrEntry 3}
Specifies the time interval for pull replication.
SYNTAX INTEGER
ACCESS read-write

PullPnrMemberPrec {pPullPnrEntry 4}
The precedence to be given to members of the special group pulled from the WINS. The precedence of locally registered members of a special group is more than any replicas pulled in.
SYNTAX INTEGER {
low(0),
high(1)
}
ACCESS read-write

PullPnrNoOfSuccRpls {pPullPnrEntry 5}
The number of times replication was successful with the WINS after invocation or reset of counters.
SYNTAX Counter
ACCESS read-only

PullPnrNoOfCommFails {pPullPnrEntry 6}
The number of times replication was unsuccessful with the WINS because of communication failure (after invocation or reset of counters).
SYNTAX Counter
ACCESS read-only

PullPnrVersNoLowWord {pPullPnrEntry 7}
The Low Word of the highest version number found in records owned by this WINS.
SYNTAX Counter
ACCESS read-only

PullPnrVersNoHighWord {pPullPnrEntry 8}
The High Word of the highest version number found in records owned by this WINS.
SYNTAX Counter
ACCESS read-only

WINS Push Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Wins.Push
(1.3.6.1.4.1.311.1.2.3)

PushInitTime {Push 1}
Indicates whether a push (that is, notification message) should be done at invocation.
SYNTAX INTEGER
ACCESS read-write

PushRplOnAddChg {Push 2}
Indicates whether a notification message should be sent when an address changes.
SYNTAX INTEGER
ACCESS read-write

PushPnrTable {Push 3}
A list of WINS partners with which push replication is to be initiated.
SYNTAX SEQUENCE OF pPushPnrEntry
ACCESS read-write

pPushPnrEntry {PushPnrTable 1}
The row corresponding to the WINS partner.
SYNTAX pPushPnrEntry
ACCESS read-write

PushPnrAdd {pPushPnrEntry 1}
Address of the WINS partner.
SYNTAX IpAddress
ACCESS read-write

PushPnrUpdateCount {pPushPnrEntry 2}
Indicates the number of updates that should result in a push message.
SYNTAX INTEGER
ACCESS read-write

WINS Cmd Group

The object name and object identifier for this group is:
iso.dod.internet.enterprises.microsoft.software.Wins.Cmd
(1.3.6.1.4.1.311.1.2.5)

CmdPullTrigger {Cmd 1}
This variable, when set, causes the WINS to pull replicas from the remote WINS server identified by the IP address.
SYNTAX IpAddress
ACCESS read-write

CmdPushTrigger {Cmd 2}
If set, causes WINS to push a notification message to the remote WINS server identified by the IP address.
SYNTAX IpAddress
ACCESS read-write

CmdDeleteWins {Cmd 3}
If set, causes all information pertaining to a WINS server (data records, context information) to be deleted from the local WINS server. Use this only when the owner-address mapping table is nearing capacity. Deleting all information pertaining to the managed WINS is not permitted.
SYNTAX IpAddress
ACCESS read-write

CmdDoScavenging {Cmd 4}
If set, causes WINS to do scavenging.
SYNTAX INTEGER {
    no(0),
    yes(1)
    }
ACCESS read-write

CmdDoStaticInit {Cmd 5}
If set, WINS performs static initialization using the file specified as the value. If 0 is specified, WINS performs static initialization using the files specified in the Registry (filenames can be read and written to using the Datafile table).
SYNTAX DisplayString
ACCESS read-write

CmdNoOfWrkThds {Cmd 6}
Sets the number of worker threads in WINS.
SYNTAX INTEGER (1..4)
ACCESS read-write

CmdPriorityClass {Cmd 7}
Sets the priority class of WINS to normal or high.
SYNTAX INTEGER {
normal(0),
high(1)
}
ACCESS read-write

CmdResetCounters {Cmd 8}
Resets the counters. Value is ignored.
SYNTAX INTEGER
ACCESS read-write

CmdDeleteDbRecs {Cmd 9}
If set, causes all data records pertaining to a WINS server to be deleted from the local WINS server. Only data records are deleted.
SYNTAX IpAddress
ACCESS read-write

CmdDRPopulateTable {Cmd 10}
Retrieves records of a WINS server whose IP address is provided. When this variable is set, the CmdDRDataRecordsTable is generated immediately.
SYNTAX IpAddress
ACCESS read-write

CmdDRDataRecordsTable {Cmd 11}
The table that stores the data records. The records are sorted lexicographically by name. The table is cached for a certain time (to save overhead on WINS). To regenerate the table, set the **CmdDRPopulateTable** MIB variable.
SYNTAX SEQUENCE OF CmdDRRecordEntry
ACCESS read-only

CmdDRRecordEntry {CmdDRDataRecordsTable 1}
Data record owned by the WINS server whose address was specified when **CmdDRPopulateTable** was set.
SYNTAX CmdDRRecordEntry
ACCESS read-write

CmdDRRecordName {cCmdDRRecordEntry 1}
Name in the record.
SYNTAX OCTET STRING (size(1..255))
ACCESS read-only

CmdDRRecordAddress {cCmdDRRecordEntry 2}
Address(es) of the record. If the record is a multihomed record or an internet group, the addresses are returned sequentially in pairs. Each pair comprises the address of the owner WINS server followed by the address of the computer or of the internet group member. The records are always returned in network byte order.
SYNTAX OCTET STRING
ACCESS read-only

CmdDRRecordType {cCmdDRRecordEntry 3}
Type of record as unique, multihomed, normal group, or internet group.
SYNTAX INTEGER {
unique(0),
normal_group(1),
special_group(2)
multihomed(3)
}
ACCESS read-only

CmdDRRecordPersistenceType {cCmdDRRecordEntry 4}
Persistence type of the record as static or dynamic.
SYNTAX INTEGER {
static(0),
dynamic(1)
}
ACCESS read-only

CmdDRRecordState {cCmdDRRecordEntry 5}
State of the record as active, released, or extinct.
SYNTAX INTEGER {
active(0),
released(1),
tombstone(2)
deleted(3)
}
ACCESS read-only

CmdWinsVersNoLowWord {Cmd 12}
The Low Word of the version number counter of the record.
SYNTAX INTEGER
ACCESS read-only

CmdWinsVersNoHighWord {Cmd 13}
The High Word of the version number counter of the record.
SYNTAX INTEGER
ACCESS read-only

MIB II Objects

This MIB is defined in RFC 1213. Windows NT does not implement the egp and snmp parameters, so they are not included in this appendix. No information is included in this appendix for the Transmission group because RFC 1213 has no objects for the group.

System Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.system (1.3.6.1.2.1.1)

sysDescr {system 1}
A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only

sysObjectID {system 2}
The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box" is being managed. For example, if vendor "Flintstones, Inc." was assigned the subtree 1.3.6.1.4.1.4242, the vendor could assign the identifier 1.3.6.1.4.1.4242.1.1 to its "Fred Router."
SYNTAX OBJECT IDENTIFIER
ACCESS read-only

sysUpTime {system 3}
The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
SYNTAX TimeTicks
ACCESS read-only

sysContact {system 4}
The textual identification of the contact person for this managed node, together with information on how to contact this person.
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-write

sysName {system 5}
An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-write

sysLocation {system 6}
The physical location of this node (for example, "telephone closet, 3rd floor").
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-write

sysServices {system 7}
A value that indicates the set of services that this entity primarily offers.

The value is a sum. This sum initially takes the value zero. For each layer, L, in the range 1 through 7, for which this node performs transactions, 2 raised to (L–1) is added to the sum. For example, a node that performs primarily routing· functions would have a value of 4 (2^(3–1)). In contrast, a node that is a host offering application services would have a value of 72 (2^(4–1) + 2^(7–1)).

In the context of the Internet suite of protocols, values should be calculated as follows:

1 physical (such as repeaters)
2 datalink/subnetwork (for example, bridges)
3 internet (such as IP gateways)
4 end-to-end (such as IP hosts)
5 session (for systems including OSI protocols)
6 presentation (for systems including OSI protocols)
7 applications (for example, mail relays)

SYNTAX INTEGER (0..127)
ACCESS read-only

Interfaces Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.interfaces (1.3.6.1.2.1.2)

ifNumber {interfaces 1}
The number of network interfaces (regardless of their current state) present on this system.
SYNTAX INTEGER
ACCESS read-only

ifTable {interfaces 2}

A list of interface entries. The number of entries is given by the value of ifNumber.

The Interfaces table contains information on the entity's interfaces. Each interface is thought of as being attached to a "subnetwork." This term should not be confused with "subnet," which refers to an addressing partitioning scheme used in the Internet suite of protocols.

SYNTAX SEQUENCE OF IfEntry
ACCESS not-accessible

ifEntry {ifTable 1}

An interface entry containing objects at the subnetwork layer and below for a particular interface.
SYNTAX IfEntry
ACCESS not-accessible

ifIndex {ifEntry 1}

A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
SYNTAX INTEGER
ACCESS read-only

ifDescr {ifEntry 2}

A textual string containing information about the interface. This string should include the name of the manufacturer, the product name, and the version of the hardware interface.
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only

ifType {ifEntry 3}

The type of interface, distinguished according to the physical/link protocol(s) immediately "below" the network layer in the protocol stack.

```
SYNTAX INTEGER {
    other(1),                  none of the following
    regular1822(2),
    hdh1822(3),
    ddn-x25(4),
    rfc877-x25(5),
    ethernet-csmacd(6),
    iso88023-csmacd(7),
    iso88024-tokenBus(8),
    iso88025-tokenRing(9),
    iso88026-man(10),
    starLan(11),
    proteon-10Mbit(12),
    proteon-80Mbit(13),
    hyperchannel(14),
    fddi(15),
    lapb(16),
    sdlc(17),
    ds1(18),                   T-1
    e1(19),                    european equiv. of T-1
    basicISDN(20),
    primaryISDN(21),           proprietary serial
    propPointToPointSerial(22),
    ppp(23),
    softwareLoopback(24),
    eon(25),                   CLNP over IP [11]
    ethernet-3Mbit(26),
    nsip(27),                  XNS over IP
    slip(28),                  generic SLIP
    ultra(29),                 ULTRA technologies
    ds3(30),                   T-3
    sip(31),                   SMDS
    frame-relay(32)
    }
ACCESS  read-only
```

ifMtu {ifEntry 4}

The size of the largest datagram that can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.

```
SYNTAX INTEGER
ACCESS  read-only
```

ifSpeed {ifEntry 5}
An estimate of the interface's current bandwidth in bits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.
SYNTAX Gauge
ACCESS read-only

ifPhysAddress {ifEntry 6}
The interface's address at the protocol layer immediately "below" the network layer in the protocol stack. For interfaces that do not have such an address (such as a serial line), this object should contain an octet string of zero length.
SYNTAX PhysAddress
ACCESS read-only

ifAdminStatus {ifEntry 7}
The desired state of the interface. The testing (3) state indicates that no operational packets can be passed.

```
SYNTAX INTEGER {
    up(1),        ready to pass packets
    down(2),
    testing(3)    in some test mode
    }
ACCESS  read-write
```

ifOperStatus {ifEntry 8}
The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed.

```
SYNTAX INTEGER {
    up(1),        ready to pass packets
    down(2),
    testing(3)    in some test mode
    }
ACCESS  read-only
```

ifLastChange {ifEntry 9}
The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.
SYNTAX TimeTicks
ACCESS read-only

ifInOctets {ifEntry 10}
The total number of octets received on the interface, including framing characters.
SYNTAX Counter
ACCESS read-only

ifInUcastPkts {ifEntry 11}
The number of subnetwork-unicast packets delivered to a higher-layer protocol.
SYNTAX Counter
ACCESS read-only

ifInNUcastPkts {ifEntry 12}
The number of non-unicast (that is, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
SYNTAX Counter
ACCESS read-only

ifInDiscards {ifEntry 13}
The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
SYNTAX Counter
ACCESS read-only

ifInErrors {ifEntry 14}
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
SYNTAX Counter
ACCESS read-only

ifInUnknownProtos {ifEntry 15}
The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.
SYNTAX Counter
ACCESS read-only

ifOutOctets {ifEntry 16}
The total number of octets transmitted out of the interface, including framing characters.
SYNTAX Counter
ACCESS read-only

ifOutUcastPkts {ifEntry 17}
The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
SYNTAX Counter
ACCESS read-only

ifOutNUcastPkts {ifEntry 18}
The total number of packets that higher-level protocols requested be transmitted to a non-unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
SYNTAX Counter
ACCESS read-only

ifOutDiscards {ifEntry 19}

The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
SYNTAX Counter
ACCESS read-only

ifOutErrors {ifEntry 20}

The number of outbound packets that could not be transmitted because of errors.
SYNTAX Counter
ACCESS read-only

ifOutQLen {ifEntry 21}

The length of the output packet queue (in packets).
SYNTAX Gauge
ACCESS read-only

ifSpecific {ifEntry 22}

A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.
SYNTAX OBJECT IDENTIFIER
ACCESS read-only

Address Translation Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.at (1.3.6.1.2.1.3)

Implementation of the Address Translation group is mandatory for all systems. However, this group is deprecated by MIB-II. That is, it is being included solely for compatibility with MIB-I nodes, and will most likely be excluded from MIB-III nodes. From MIB-II and onwards, each network protocol group contains its own address translation tables.

atTable {at 1}

The Address Translation tables contain the NetworkAddress to physical address equivalences. Some interfaces do not use translation tables for determining address equivalences (for example, DDN-X.25 has an algorithmic method); if all interfaces are of this type, then the Address Translation table is empty—that is, it has zero entries.
SYNTAX SEQUENCE OF AtEntry
ACCESS not-accessible

atEntry {atTable 1}
Each entry contains one NetworkAddress to physical address equivalence.
SYNTAX AtEntry
ACCESS not-accessible

atIfIndex {atEntry 1}
The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
SYNTAX INTEGER
ACCESS read-write

atPhysAddress {atEntry 2}
The media-dependent physical address. Setting this object to a null string (one of zero length) has the effect of invalidating the corresponding entry in the atTable object. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant atPhysAddress object.
SYNTAX PhysAddress
ACCESS read-write

atNetAddress {atEntry 3}
The NetworkAddress (for example, the IP address) corresponding to the media-dependent physical address.
SYNTAX NetworkAddress
ACCESS read-write

IP Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.ip (1.3.6.1.2.1.4)

ipForwarding {ip 1}

The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams, but IP hosts do not (except those source-routed via the host). For some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.

```
SYNTAX INTEGER {
   forwarding(1),          acting as a gateway
   not-forwarding(2)   NOT acting as a gateway
   }
ACCESS read-write
STATUS  mandatory
```

ipDefaultTTL {ip 2}

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity whenever a TTL value is not supplied by the transport layer protocol.

SYNTAX INTEGER
ACCESS read-write

ipInReceives {ip 3}

The total number of input datagrams received from interfaces, including those received in error.

SYNTAX Counter
ACCESS read-only

ipInHdrErrors {ip 4}

The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

SYNTAX Counter
ACCESS read-only

ipInAddrErrors {ip 5}

The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
SYNTAX Counter
ACCESS read-only

ipForwDatagrams {ip 6}

The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter will include only those packets that were Source-Routed via this entity, and the Source-Route option processing was successful.
SYNTAX Counter
ACCESS read-only

ipInUnknownProtos {ip 7}

The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
SYNTAX Counter
ACCESS read-only

ipInDiscards {ip 8}

The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
SYNTAX Counter
ACCESS read-only

ipInDelivers {ip 9}

The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
SYNTAX Counter
ACCESS read-only

ipOutRequests {ip 10}

The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
SYNTAX Counter
ACCESS read-only

ipOutDiscards {ip 11}

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
SYNTAX Counter
ACCESS read-only

ipOutNoRoutes {ip 12}

The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this "no-route" criterion, which includes any datagrams that a host cannot route because all of its default gateways are down.
SYNTAX Counter
ACCESS read-only

ipReasmTimeout {ip 13}

The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
SYNTAX INTEGER
ACCESS read-only

ipReasmReqds {ip 14}

The number of IP fragments received that needed to be reassembled at this entity.
SYNTAX Counter
ACCESS read-only

ipReasmOKs {ip 15}

The number of IP datagrams successfully reassembled.
SYNTAX Counter
ACCESS read-only

ipReasmFails {ip 16}

The number of failures detected by the IP reassembly algorithm (for whatever reason, such as timed out or errors). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
SYNTAX Counter
ACCESS read-only

ipFragOKs {ip 17}

The number of IP datagrams that have been successfully fragmented at this entity.
SYNTAX Counter
ACCESS read-only

ipFragFails {ip 18}
The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set).
SYNTAX Counter
ACCESS read-only

ipFragCreates {ip 19}
The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
SYNTAX Counter
ACCESS read-only

ipAddrTable {ip 20}
The table of addressing information relevant to this entity's IP addresses.
SYNTAX SEQUENCE OF IpAddrEntry
ACCESS not-accessible

ipAddrEntry {ipAddrTable 1}
The addressing information for one of this entity's IP addresses.
SYNTAX IpAddrEntry
ACCESS not-accessible

ipAdEntAddr {ipAddrEntry 1}
The IP address to which this entry's addressing information pertains.
SYNTAX IpAddress
ACCESS read-only

ipAdEntIfIndex {ipAddrEntry 2}
The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
SYNTAX INTEGER
ACCESS read-only

ipAdEntNetMask {ipAddrEntry 3}
The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
SYNTAX IpAddress
ACCESS read-only

ipAdEntBcastAddr {ipAddrEntry 4}
The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
SYNTAX INTEGER
ACCESS read-only

ipAdEntReasmMaxSize {ipAddrEntry 5}
The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.
SYNTAX INTEGER (0..65535)
ACCESS read-only

ipRouteTable {ip 21}
This entity's IP Routing table.
SYNTAX SEQUENCE OF IpRouteEntry
ACCESS not-accessible

ipRouteEntry {ipRouteTable 1}
A route to a particular destination.
SYNTAX IpRouteEntry
ACCESS not-accessible

ipRouteDest {ipRouteEntry 1}
The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.
SYNTAX IpAddress
ACCESS read-write

ipRouteIfIndex {ipRouteEntry 2}
The index value that uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
SYNTAX INTEGER
ACCESS read-write

ipRouteMetric1 {ipRouteEntry 3}
The primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
SYNTAX INTEGER
ACCESS read-write

ipRouteMetric2 {ipRouteEntry 4}
An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
SYNTAX INTEGER
ACCESS read-write

ipRouteMetric3 {ipRouteEntry 5}
An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
SYNTAX INTEGER
ACCESS read-write

ipRouteMetric4 {ipRouteEntry 6}
An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
SYNTAX INTEGER
ACCESS read-write

ipRouteNextHop {ipRouteEntry 7}
The IP address of the next hop of this route. (In the case of a route bound to an interface that is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)
SYNTAX IpAddress
ACCESS read-write

ipRouteType {ipRouteEntry 8}
The type of route. The values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively disassociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object.

```
SYNTAX INTEGER {
   other(1),      none of the following
   invalid(2),    an invalidated route
   direct(3),        route to directly connected (sub-)network
   indirect(4)    route to a non-local host/network/sub-network
   }
ACCESS read-write
```

ipRouteProto {ipRouteEntry 9}

The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.

SYNTAX INTEGER {
other(1), none of the following
local(2), non-protocol information, such as manually configured entries
netmgmt(3), set via a network management protocol
icmp(4), obtained via ICMP, for example, Redirect;
the remaining values are all gateway routing protocols
egp(5),
ggp(6),
hello(7),
rip(8),
is-is(9),
es-is(10),
ciscoIgrp(11),
bbnSpfIgp(12),
ospf(13),
bgp(14)
}
ACCESS read-only

ipRouteAge {ipRouteEntry 10}

The number of seconds since this route was last updated or otherwise determined to be correct. No semantics of "too old" can be implied except through knowledge of the routing protocol by which the route was learned.

SYNTAX INTEGER
ACCESS read-write

ipRouteMask {ipRouteEntry 11}

Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belongs to a class A, B, or C network, and then using the corresponding mask.

network	**mask**
class A	255.0.0.0
class B	255.255.0.0
class C	255.255.255.0

If the value of the ipRouteDest is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. All IP routing subsystems implicitly use this mechanism.
SYNTAX IpAddress
ACCESS read-write

ipRouteMetric5 {ipRouteEntry 12}
An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
SYNTAX INTEGER
ACCESS read-write

ipRouteInfo {ipRouteEntry 13}
A reference to MIB definitions specific to the particular routing protocol that is responsible for this route, as determined by the value specified in the route's ipRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.
SYNTAX OBJECT IDENTIFIER
ACCESS read-only

ipNetToMediaTable {ip 22}
The IP Address Translation table used for mapping from IP addresses to physical addresses.
SYNTAX SEQUENCE OF IpNetToMediaEntry
ACCESS not-accessible

ipNetToMediaEntry {ipNetToMediaTable 1}
Each entry contains one IpAddress to "physical" address equivalence.
SYNTAX IpNetToMediaEntry
ACCESS not-accessible

ipNetToMediaIfIndex {ipNetToMediaEntry 1}
The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
SYNTAX INTEGER
ACCESS read-write

ipNetToMediaPhysAddress {ipNetToMediaEntry 2}
The media-dependent physical address.
SYNTAX PhysAddress
ACCESS read-write

ipNetToMediaNetAddress {ipNetToMediaEntry 3}
The IpAddress corresponding to the media-dependent physical address.
SYNTAX IpAddress
ACCESS read-write

ipNetToMediaType {ipNetToMediaEntry 4}

The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

```
SYNTAX INTEGER {
    other(1),           none of the following
    invalid(2),       an invalidated mapping
    dynamic(3),
    static(4)
    }
ACCESS  read-write
```

ipRoutingDiscards {ip 23}

The number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free up buffer space for other routing entries.

SYNTAX Counter
ACCESS read-only

ICMP Parameters

The object name and object identifier for this group is:

iso.org.dod.internet.mgmt.mib-2.icmp   (1.3.6.1.2.1.5)

icmpInMsgs {icmp 1}

The total number of ICMP messages that the entity received. Note that this counter includes all those counted by icmpInErrors.

SYNTAX Counter
ACCESS read-only

icmpInErrors {icmp 2}

The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

SYNTAX Counter
ACCESS read-only

icmpInDestUnreachs {icmp 3}

The number of ICMP Destination Unreachable messages received.

SYNTAX Counter
ACCESS read-only

icmpInTimeExcds {icmp 4}
The number of ICMP Time Exceeded messages received.
SYNTAX Counter
ACCESS read-only

icmpInParmProbs {icmp 5}
The number of ICMP Parameter Problem messages received.
SYNTAX Counter
ACCESS read-only

icmpInSrcQuenchs {icmp 6}
The number of ICMP Source Quench messages received.
SYNTAX Counter
ACCESS read-only

icmpInRedirects {icmp 7}
The number of ICMP Redirect messages received.
SYNTAX Counter
ACCESS read-only

icmpInEchos {icmp 8}
The number of ICMP Echo (request) messages received.
SYNTAX Counter
ACCESS read-only

icmpInEchoReps {icmp 9}
The number of ICMP Echo Reply messages received.
SYNTAX Counter
ACCESS read-only

icmpInTimestamps {icmp 10}
The number of ICMP Timestamp (request) messages received.
SYNTAX Counter
ACCESS read-only

icmpInTimestampReps {icmp 11}
The number of ICMP Timestamp Reply messages received.
SYNTAX Counter
ACCESS read-only

icmpInAddrMasks {icmp 12}
The number of ICMP Address Mask Request messages received.
SYNTAX Counter
ACCESS read-only

icmpInAddrMaskReps {icmp 13}
The number of ICMP Address Mask Reply messages received.
SYNTAX Counter
ACCESS read-only

icmpOutMsgs {icmp 14}
The total number of ICMP messages that this entity attempted to send. This counter includes all those messages counted by icmpOutErrors.
SYNTAX Counter
ACCESS read-only

icmpOutErrors {icmp 15}
The number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error that contribute to this counter's value.
SYNTAX Counter
ACCESS read-only

icmpOutDestUnreachs {icmp 16}
The number of ICMP Destination Unreachable messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutTimeExcds {icmp 17}
The number of ICMP Time Exceeded messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutParmProbs {icmp 18}
The number of ICMP Parameter Problem messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutSrcQuenchs {icmp 19}
The number of ICMP Source Quench messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutRedirects {icmp 20}
The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
SYNTAX Counter
ACCESS read-only

icmpOutEchos {icmp 21}
The number of ICMP Echo (request) messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutEchoReps {icmp 22}
The number of ICMP Echo Reply messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutTimestamps {icmp 23}
The number of ICMP Timestamp (request) messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutTimestampReps {icmp 24}
The number of ICMP Timestamp Reply messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutAddrMasks {icmp 25}
The number of ICMP Address Mask Request messages sent.
SYNTAX Counter
ACCESS read-only

icmpOutAddrMaskReps {icmp 26}
The number of ICMP Address Mask Reply messages sent.
SYNTAX Counter
ACCESS read-only

TCP Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.tcp (1.3.6.1.2.1.6)

Instances of object types that represent information about a particular TCP connection are transient; they persist only as long as the connection in question.

tcpRtoAlgorithm {tcp 1}
The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
SYNTAX INTEGER {

```
    other(1),        none of the following
    constant(2),     a constant rto
    rsre(3),         MIL-STD-1778, Appendix B
    vanj(4)          Van Jacobson's algorithm [10]
    }
```

ACCESS read-only

tcpRtoMin {tcp 2}
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
SYNTAX INTEGER
ACCESS read-only

tcpRtoMax {tcp 3}
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
SYNTAX INTEGER
ACCESS read-only

tcpMaxConn {tcp 4}
The limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
SYNTAX INTEGER
ACCESS read-only

tcpActiveOpens {tcp 5}
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
SYNTAX Counter
ACCESS read-only

tcpPassiveOpens {tcp 6}
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
SYNTAX Counter
ACCESS read-only

tcpAttemptFails {tcp 7}
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
SYNTAX Counter
ACCESS read-only

tcpEstabResets {tcp 8}
The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
SYNTAX Counter
ACCESS read-only

tcpCurrEstab {tcp 9}
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
SYNTAX Gauge
ACCESS read-only

tcpInSegs {tcp 10}

The total number of segments received, including those received in error. This count includes segments received on currently established connections.
SYNTAX Counter
ACCESS read-only

tcpOutSegs {tcp 11}

The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
SYNTAX Counter
ACCESS read-only

tcpRetransSegs {tcp 12}

The total number of segments retransmitted—that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
SYNTAX Counter
ACCESS read-only

tcpConnTable {tcp 13}

A table containing TCP connection-specific information.
SYNTAX SEQUENCE OF TcpConnEntry
ACCESS not-accessible

tcpConnEntry {tcpConnTable 1}

Information about a particular current TCP connection. An object of this type is transient—it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state.
SYNTAX TcpConnEntry
ACCESS not-accessible

tcpConnState {tcpConnEntry 1}

The state of this TCP connection.

The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to set this object to any other value.

If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection.

As an implementation-specific option, an RST segment may be sent from the managed node to the other TCP endpoint. (However, RST segments are not sent reliably.)

```
    SYNTAX INTEGER {
        closed(1),
        listen(2),
        synSent(3),
        synReceived(4),
        established(5),
        finWait1(6),
        finWait2(7),
        closeWait(8),
        lastAck(9),
        closing(10),
        timeWait(11),
        deleteTCB(12)
    }
    ACCESS  read-write
tcpConnLocalAddress {tcpConnEntry 2}
    The local IP address for this TCP connection. In the case of a connection in the
    LISTEN state that is willing to accept connections for any IP interface
    associated with the node, the value 0.0.0.0 is used.
    SYNTAX IpAddress
    ACCESS  read-only
tcpConnLocalPort {tcpConnEntry 3}
    The local port number for this TCP connection.
    SYNTAX INTEGER (0..65535)
    ACCESS  read-only
tcpConnRemAddress {tcpConnEntry 4}
    The remote IP address for this TCP connection.
    SYNTAX IpAddress
    ACCESS  read-only
tcpConnRemPort {tcpConnEntry 5}
    The remote port number for this TCP connection.
    SYNTAX INTEGER (0..65535)
    ACCESS  read-only
tcpInErrs {tcp 14}
    The total number of segments received in error (such as, bad TCP checksums).
    SYNTAX Counter
    ACCESS  read-only
tcpOutRsts {tcp 15}
    The number of TCP segments sent containing the RST flag.
    SYNTAX Counter
    ACCESS  read-only
```

UDP Parameters

The object name and object identifier for this group is:
iso.org.dod.internet.mgmt.mib-2.udp (1.3.6.1.2.1.6)

udpInDatagrams {udp 1}
The total number of UDP datagrams delivered to UDP users.
SYNTAX Counter
ACCESS read-only

udpNoPorts {udp 2}
The total number of received UDP datagrams for which there was no application at the destination port.
SYNTAX Counter
ACCESS read-only

udpInErrors {udp 3}
The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
SYNTAX Counter
ACCESS read-only

udpOutDatagrams {udp 4}
The total number of UDP datagrams sent from this entity.
SYNTAX Counter
ACCESS read-only

udpTable {udp 5}
A table containing UDP listener information.
SYNTAX SEQUENCE OF UdpEntry
ACCESS not-accessible

udpEntry {udpTable 1}
Information about a particular current UDP listener.
SYNTAX UdpEntry
ACCESS not-accessible

udpLocalAddress {udpEntry 1}
The local IP address for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
SYNTAX IpAddress
ACCESS read-only

udpLocalPort {udpEntry 2}
The local port number for this UDP listener.
SYNTAX INTEGER (0..65535)
ACCESS read-only

APPENDIX B

Major Revision to Windows NT Messages

The "Windows NT Debugger" section of Chapter 2, "Windows NT Executive Messages," in the *Windows NT Messages* book has been updated to reflect using the new debugging tools included in the Windows NT Workstation and Windows NT Server version 3.51 release. However, the information in that section on configuring the target computer for remote debugging is still valid. Our next release of the *Windows NT Resource Kit* will contain a merged document. The first two major sections in that chapter remain unchanged.

Windows NT Debugger

WINDBG.EXE, the utility used for reading dump files and Kernel debugging under Windows NT 3.5, has been replaced under version 3.51 with a set of utilities that automatically read and interpret dump files. They also aid in sending dump files to support personnel for advanced analysis. These utilities simplify the process of dealing with Kernel dump files. For those cases where a local debug is necessary, the KD debuggers (I386KD.EXE, ALPHAKD.EXE, MIPSKD.EXE, and PPCKD.EXE) are still available.

This section discusses how to use the new utilities and provides instructions for configuring the KD debuggers for local debugging.

Terminology

This section defines some common terms and procedures that you should be familiar with before debugging Kernel errors.

Symbols and Symbol Trees

Usually, when code is compiled to create executable files, either of two different versions of the executables can be created: a debug (also known as checked) version or a non-debug (also known as free) version. The checked version contains extra code that enables a developer to debug problems, but this means a larger and possibly slower executable file. The free version of the executable is smaller and runs at a normal speed, but cannot be debugged.

In Windows NT, we combine the speed and smaller size of free versions with the debugging capabilities of the checked versions. The executable itself is in the free version. However, all executables, drivers, dynamic-link libraries, and other program files in Windows NT have a corresponding "symbol" file, which contains the debug code that is normally part of the checked file. These symbol files are stored on the Windows NT CD, in the \SUPPORT\DEBUG\platform\SYMBOLS directories, where *platform* is I386, ALPHA, MIPS, or PPC. Within each \SYMBOLS directory, there is one directory for each type of file (.EXE, .DLL, .SYS, etc.). This structure is referred to as a *symbol tree*. The following directories exist in a standard symbol tree:

Directory	Contains symbols for
ACM	MSACM files
COM	.COM executable files
CPL	Control Panel applets
DLL	Dynamic-Link Libraries (.DLL files)
DRV	.DRV driver files
EXE	.EXE executable files
SCR	Screen Saver files
SYS	.SYS driver files

All of the utilities used to debug Windows NT or interpret dump files require a symbol tree available containing the symbol files for the version of Windows NT you were running at the time of the crash. Some utilities (such as Dr. Watson) expect the \SYMBOLS directory to be on your hard drive, in the *systemroot* directory. Other utilities allow you to specify the path to the \SYMBOLS directory as a command line option or in a dialog box. Some of the utilities described in this section allow you to specify multiple directories separated by semicolons (;) in a symbol path, much like the syntax for the PATH environment variable.

Target Computer

The term *target computer* refers to the computer on which the STOP error actually occurs. This computer is the one that needs to be debugged. It can be a computer on the local network or a computer that you dial in to using a modem.

Host Computer

The term *host computer* refers to the computer on which you run the debugger. This computer is always local and should be running a version of Windows NT that is at least as recent as the one on the target computer. It can use a later version of Windows NT, although that introduces some complications when setting up the debugger.

Dealing with Memory Dump Files

Included on the Windows NT Server and Windows NT Workstation version 3.51 CDs are three new utilities for dealing with dump files: DUMPCHK, DUMPFLOP, and DUMPEXAM. DUMPEXAM is the most important of these utilities from a debugging standpoint, but the others can be useful as well. All three utilities are on the Windows NT Server and Windows NT Workstation CDs in the \SUPPORT\DEBUG\platform directories, where *platform* is I386, ALPHA, MIPS, or PPC.

DUMPFLOP.EXE

DUMPFLOP.EXE is a command-line utility that you can use to write a dump file in segments to floppy disks, so it can be sent to a support engineer. This is rarely the most efficient way to send a dump file, but it is sometimes the only way. DUMPFLOP compresses the information it writes to the floppy disks, using the compression algorithm used by the NTFS file system, so a 32-MB dump file will generally fit onto 10 floppy disks, rather than 20 or more as you might expect. DUMPFLOP does not require access to symbols.

To store the crash dump onto floppy disks, use DUMPFLOP with the following command-line syntax:

dumpflop *[options] <CrashDumpFile> [<Drive>:]*

To assemble a crash dump from floppy disks, use DUMPFLOP with the following command-line syntax:

dumpflop *[options] <Drive>: [<CrashDumpFile>]*

In either case, the options are as follows:

-?
Displays the command syntax.

-p
Only prints the crash dump header on an assemble operation.

-v
Shows compression statistics.

-q
Formats the floppy when necessary during a store operation; also overwrites the existing crash dump file during an assemble operation.

If executed with no parameters, DUMPFLOP attempts to find a memory dump in the \systemroot directory (the default location for creating a memory dump) and writes it to floppy disks on the A drive.

DUMPCHK.EXE

DUMPCHK.EXE is a command-line utility that you can use to verify that a dump file has been created correctly. DUMPCHK does not require access to symbols.

DUMPCHK has the following command line parameters:

dumpchk *[options] CrashDumpFile*

where the options are as follows:

-?
Displays the command syntax.

-p
Prints the header only (with no validation).

-v
Specifies verbose mode.

-q
Performs a quick test.

DUMPCHK displays some basic information from the dump file and then verifies all the virtual and physical addresses in the memory dump. If any errors are found in the dump file, it reports them. The following is an example of the output of a DUMPCHK command:

```
Filename . . . . . . .memory.dmp
Signature. . . . . . .PAGE
ValidDump. . . . . . .DUMP
MajorVersion . . . . .free system
MinorVersion . . . . .807
DirectoryTableBase . .0x00030000
PfnDataBase. . . . . .0xffb7e000
PsLoadedModuleList . .0x80196d40
PsActiveProcessHead. .0x80196c38
MachineImageType . . .i386
NumberProcessors . . .1
BugCheckCode . . . . .0xc000021a
BugCheckParameter1 . .0xe17b7b68
BugCheckParameter2 . .0xc0000005
BugCheckParameter3 . .0x00000000
BugCheckParameter4 . .0x00000000

ExceptionCode. . . . .0x80000003
ExceptionFlags . . . .0x00000001
ExceptionAddress . . .0x8015f015

NumberOfRuns . . . . .0x3
NumberOfPages. . . . .0x3f9e
Run #1
  BasePage . . . . . .0x1
  PageCount. . . . . .0x9e
Run #2
  BasePage . . . . . .0x100
  PageCount. . . . . .0xec0
Run #3
  BasePage . . . . . .0x1000
  PageCount. . . . . .0x3040

**************
**************--> Validating the integrity of the PsLoadedModuleList
**************

**************
**************--> Performing a complete check (^C to end)
**************
**************
**************--> Validating all physical addresses
**************
**************
**************--> Validating all virtual addresses
**************
```

In this example, the most important information (from a debugging standpoint) is the following:

```
MajorVersion . . . . .free system
MinorVersion . . . . .807
MachineImageType . . .i386
NumberProcessors . . .1
BugCheckCode . . . . .0xc000021a
BugCheckParameter1 . .0xe17b7b68
BugCheckParameter2 . .0xc0000005
BugCheckParameter3 . .0x00000000
BugCheckParameter4 . .0x00000000
```

This information can be used to determine what STOP error occurred and, to a certain extent, what version of Windows NT was in use.

DUMPEXAM.EXE

DUMPEXAM.EXE is a command-line utility that examines a memory dump file, extracts information from it, and writes it to a text file. This text file can then be used by support personnel to determine the cause of the STOP error. In many cases, the analysis provided by DUMPEXAM provides enough information for support personnel to determine the cause of the error, without direct access to the dump file.

Three files are required to run DUMPEXAM, and they all must be in the same directory. You can find them on the Windows NT Server or Windows NT Workstation CD in the directory \SUPPORT\DEBUG\platform, where *platform* is I386, ALPHA, MIPS, or PPC. The first two files are:

- DUMPEXAM.EXE
- IMAGEHLP.DLL

The third file is one of the following, depending on the type of computer on which the dump file was generated:

- KDEXTX86.DLL
- KDEXTALP.DLL
- KDEXTMIP.DLL
- KDEXTPPC.DLL

If you have not applied any hotfixes or service packs to Windows NT 3.51, and the memory dump file you want to examine is in the location specified in the Recovery dialog box in the System option in Control Panel, then you can simply run DUMPEXAM directly off the CD with no parameters. This creates a text file called MEMORY.TXT, located in the same directory as the MEMORY.DMP file, that contains information extracted from the dump file.

You can also use DUMPEXAM to examine dump files created on computers running earlier versions of Windows NT. However, it will only run on a system running Windows NT 3.51, so you will need to move the dump file or access it over the network. Additionally, you will need to replace the KDEXT*.DLL files listed above with copies from the version of Windows NT that was running on the trapping (or target) system. These files contain debug information specific to that version of Windows NT.

The syntax for DUMPEXAM is as follows:

dumpexam *[options] [CrashDumpFile]*

where

-?
Displays the command syntax.

-v
Specifies verbose mode.

-p
Prints the header only.

-f ***filename***
Specifies the output file name.

-y ***path***
Sets the symbol search path.

You need to specify the dump file path (using the **-f** option) only if you have moved the dump file.

You need to specify the symbol search path (using the **-y** option) only if you are using an alternate symbol path. The symbol path for DUMPEXAM can contain several directories, separated by semicolons(;). These directories are searched in the order in which they are listed, so you should list directories with the most recently installed hotfixes or service packs first.

Examples

In our first example, the memory dump was created on a computer with Windows NT Workstation 3.51 and no service packs. The symbols are all in the directory C:\SYMBOLS. The dump file is in the directory C:\DUMP and is called MACHINE1.DMP. The command line reads as follows:

```
dumpexam -y c:\symbols c:\dump\machine1.dmp
```

The results of the exam will be in *systemroot*\MEMORY.TXT.

In the next example, the memory dump was created on a DEC Alpha computer running Windows NT Server 3.5, with Service Pack 2 installed. The Service Pack 2 symbols are in D:\SP2\SYMBOLS. The Windows NT Server 3.5 symbols are on the product CD, which is in the E drive. The dump file MEMORY.DMP, is in D:\TEMP. The output file is to be put in the same directory as the dump file. The command line reads as follows:

```
dumpexam -y d:\sp2\symbols;e:\support\debug\alpha -f d:\temp\memory.txt
d:\temp\memory.dmp
```

Setting Up for Local and Remote Debugging

Configuring a Windows NT computer so it can be used to debug another computer, either over a local null modem cable or over a modem, requires you to carry out the following procedures:

- Set up a symbol tree
- Set up the debugger
- Start the debugger

The following instructions assume that you have already configured the target computer for remote debugging and set up the hardware, following the instructions under the “Windows NT Debugger”section of Chapter 2, “Windows NT Executive Messages,” in *Windows NT Messages.*

Setting Up a Symbol Tree

The Windows NT Server and Windows NT Workstation 3.51 CDs come with symbol trees already created. They are in \SYMBOLS directories on the CD under \SUPPORT\DEBUG\platform, where *platform* is I386, ALPHA, MIPS, or PPC. If you have not installed any service packs or hotfixes and do not have a multiprocessor system, then you might need only to specify the path to the correct symbols directory on the CD, or copy that directory to *systemroot* and use this as the symbol path.

If you have installed service packs or hotfixes to Windows NT, you must construct a symbol tree.

▸ To construct a symbol tree

1. Copy the correct tree from the \SUPPORT directory on the CD to your hard drive.
2. Copy the symbols for the updates you have applied into this tree in the order that you applied the updates, so that the later versions overwrite the earlier versions.

Note Some of the utilities mentioned earlier in this section allow you to specify multiple symbols directories in a symbol path. You can establish separate directories for the symbols accompanying updates and Service Packs if you are using these utilities, rather than overwrite files in the single symbol tree. However, the KD debuggers require all the symbols in one path.

3. If you are using KD debuggers to debug a multiprocessor or a single processor system using a special HAL, you must rename some of the symbol files.

The KD debuggers always load the files named NTOSKRNL.DBG for Kernel symbols and HAL.DBG for HAL symbols, so you need to determine which Kernel and HAL you are using and rename the associated files to these filenames. (This procedure is not necessary if you are using the DUMPEXAM utility described earlier. It detects which Kernel and HAL files are needed and loads the correct ones.)

If you have a computer with a multiprocessor, you need only rename NTKRNLMP.DBG to NTOSKRNL.DBG. These files are in the \EXE subdirectory of the symbol tree.

If your computer uses a special HAL, there are a number of possibilities. The following tables list the possible HAL files for each hardware platform. These tables list the actual name of the .DLL file as it exists on the CD and the uncompressed size of the file in bytes. Each .DLL file has a corresponding .DBG file, which is in the \DLL sub-directory of the symbol tree. Determine which HAL you are using and rename the associated .DBG file to HAL.DBG. If you are not sure which HAL you are using, compare the file size in the table with the HAL.DLL file on the target system. The HAL.DLL file can be found in *systemroot*\SYSTEM32.

HAL files for I386 systems

Filename	Uncompressed Size (bytes)	Description
HAL.DLL	48,416	Standard HAL for Intel systems
HAL486C.DLL	47,376	HAL for 486 c step processor
HALAPIC.DLL	63,616	Uniprocessor version of HALMPS.DLL
HALAST.DLL	46,416	HAL for AST SMP systems
HALCBUS.DLL	79,776	HAL for Cbus systems
HALMCA.DLL	45,488	HAL for MCA-based systems (PS/2 and others)
HALMPS.DLL	65,696	HAL for most Intel multiprocessor systems
HALNCR.DLL	79,392	HAL for NCR SMP machines
HALOLI.DLL	40,048	HAL for Olivetti SMP machines
HALSP.DLL	52,320	HAL for Compaq Systempro
HALWYSE7.DLL	40,848	HAL for Wyse7 systems

HAL files for DEC Alpha systems

Filename	Uncompressed Size (bytes)	Description
HAL0JENS.DLL	56,800	Digital DECpc AXP 150 HAL
HALALCOR.DLL	69,120	Digital AlphaStation 600 Family
HALAVANT.DLL	66,752	Digital AlphaStation 200/400 Family HAL
HALEB64P.DLL	70,528	Digital AlphaPC64 HAL
HALGAMMP.DLL	72,896	Digital AlphaServer 2x00 5/xxx Family HAL
HALMIKAS.DLL	67,040	Digital AlphaServer 1000 Family Uniprocessor HAL
HALNONME.DLL	65,376	Digital AXPpci 33 HAL
HALQS.DLL	65,088	Digital Multia MultiClient Desktop HAL
HALSABMP.DLL	72,736	Digital AlphaServer 2x00 4/xxx Family HAL

HAL files for MIPS systems

Filename	Uncompressed Size (bytes)	Description
HALACR.DLL	43,648	ACER HAL
HALDTI.DLL	68,288	DESKStation Evolution
HALDUOMP.DLL	41,728	Microsoft-designed dual MP HAL
HALFXS.DLL	42,016	MTI with a r4000 or r4400
HALFXSPC.DLL	42,176	MTI with a r4600
HALNECMP.DLL	44,736	NEC dual MP
HALNTP.DLL	116,000	NeTpower FASTseries
HALR98MP.DLL	127,232	NEC 4 processor MP
HALSNI4X.DLL	95,520	Siemens Nixdorf UP and MP
HALTYNE.DLL	68,032	DESKstation Tyne

HAL files for PPC Systems

Filename	Uncompressed Size (bytes)	Description
HALCARO.DLL	169,504	HAL for IBM-6070
HALEAGLE.DLL	206,208	HAL for Motorola PowerStack and Big Bend
HALFIRE.DLL	136,576	Hal for Powerized_ES, Powerized_MX, and Powerized_MX MP
HALPOLO.DLL	169,152	HAL for IBM-6030
HALPPC.DLL	169,184	HAL for IBM-6015
HALWOOD.DLL	95,616	HAL for IBM-6020

In some cases, you might have a HAL file that was supplied by your computer manufacturer. If so, you need to obtain symbols for these files from the manufacturer, rename that symbol file to HAL.DBG, and place it in the \DLL subdirectory of the symbol tree. For example, Compaq provides updated HAL files for their Proliant systems. This also applies if you have drivers from third party sources; obtain symbols from the original source and put them in the appropriate directory.

Setting Up the Debugger

To set up the debugger, first ensure that you have the correct files available. These files should be copied from the \SUPPORT\DEBUG\platform directory to a debug directory on the hard drive, where *platform* matches the platform of the host computer. If you are debugging Windows NT 3.1 or 3.5 from a Windows NT 3.51 computer, copy the files from a CD containing the version of Windows NT on the target computer. The following files are necessary for Kernel debugging:

- *platform*KD.EXE

  Where *platform* matches the platform of the target computer. The files are from the following list:

  - ALPHAKD.EXE
  - I386KD.EXE
  - MIPSKD.EXE
  - PPCKD.EXE
- IMAGEHLP.DLL
- KDEXT*platform*.DLL

  Where *platform* matches the platform of the target computer. The files are from the following list:

  - KDEXTALP.DLL
  - KDEXTX86.DLL
  - KDEXTMIP.DLL
  - KDEXTPPC.DLL

Once you have set up the symbol tree and copied the necessary files to it, use a batch file or command line to set the following environment variables:

Variable	Purpose
_NT_DEBUG_PORT	COM port being used for debugging on host
_NT_DEBUG_BAUD_RATE	Max baud rate for debug port, 9600 for modems, 19200 for null modem serial cables
_NT_SYMBOL_PATH	Path to symbols directory
_NT_LOG_FILE_OPEN	Optional, can be used to list name of file to write a log of the debug session

Once these environment variables have been set, you can start the Kernel debugger.

Starting the Debugger

The Kernel debuggers are started from the command line, using the name of the executable as the command. They support the following command-line options:

-b

Causes the debugger to stop execution on target computer as soon as possible, by causing a debug breakpoint (INT 3).

-c

Causes the debugger to request a resync on connect. Resynchronization ensures that the host and target computers are communicating in sequence.

-m

Causes the debugger to monitor modem control lines. The debugger is only active when the CD (carrier detect) line is active; otherwise, the debugger is in terminal mode.

-n

Causes symbols to be loaded immediately, rather than in a deferred mode.

-v

Verbose mode; displays more information about such things as when symbols are loaded.

-x

Causes the debugger to break in when an exception first occurs, rather than letting the application or module that caused the exception deal with it.

The most commonly used switches are **-v** (verbose) and **-m** (for modem debugging).

Generally, the best way to start the debugger is to create a batch file with the necessary commands to set the environment variables followed by the command to start the correct KD debugger.

If the host computer is on a network, you might choose to use the REMOTE.EXE utility included with the *Windows NT Resource Kit* to start the debugger. REMOTE.EXE is a server/client utility that provides remote network access via named pipes to applications that use STDIN and STDOUT for input and output. This allows users at other computers on the network to connect to your Kernel debugging session and either view the debugging information or enter commands themselves. The syntax for starting the server end of the remote session is as follows:

remote /s "*command*" *Unique_Id* [**/f** *foreground_color***|/b** *background_color*]

For example:

```
REMOTE /S "i386kd -v" debug
```

The server session is ended with @K.

To interact with this session from some other computer, use the **remote /c** command. The syntax of this command is as follows:

remote /c *ServerName Unique_Id* [**/l** *lines_to_get*|**/f** *foreground_color*|**/b** *background_color*]

To exit from the remote session, leaving the debugger running on the remote system, use @Q.

For example, if a session with id **debug** had been started on the computer \\Server1 by using the **remote /s** command, you could connect to it with the command

```
REMOTE /C server1 debug
```

For more information on using the remote command, see the RKTOOLS. HLP file on the *Windows NT Resource Kit* CD.

Examples

Let us suppose the following:

- Debugging needs to take place over a null modem serial cable on COM2.
- The symbols are on a CD on the E drive.
- A log file called DEBUG.LOG is to be created in C:\TEMP.

A sample batch file might be as follows:

```
REM Local debugging batch file
set _NT_DEBUG_PORT=com2
set _NT_DEBUG_BAUD_RATE=19200
set _NT_SYMBOL_PATH=e:\support\debug\i386\symbols
SET _NT_LOG_FILE_OPEN=c:\temp\debug.log
remote /s "i386kd -v" debug
```

The last line of the batch file uses the REMOTE utility to start the debugger. This lets people on Windows NT computers who are networked to the host computer (and who have a copy of REMOTE.EXE) connect to the debug session using the following command:

remote /c *computername* **debug**

where *computername* is the name of the host computer.

To allow remote debugging, begin with the batch file in the previous example, change the baud rate to 9600, and add the **-m** switch to the last line. The result is as follows:

```
REM remote debugging batch file
set _NT_DEBUG_PORT=com2
set _NT_DEBUG_BAUD_RATE=9600
set _NT_SYMBOL_PATH=e:\support\debug\i386\symbols
SET _NT_LOG_FILE_OPEN=c:\temp\debug.log
remote /s "i386kd -v -m" debug
```

The batch file should be executed from the directory that contains the debugger files.

When you start the debugger, one of two screens appears, depending upon whether you are doing local debugging or remote debugging.

When doing local debugging, the following screen appears:

```
**************************************
***********     REMOTE    ************
***********     SERVER    ************
**************************************
To Connect: Remote /C BANSIDHE debug

Microsoft(R) Windows NT Kernel Debugger
Version 3.5
(C) 1991-1994 Microsoft Corp.

Symbol search path is:
KD: waiting to connect...
```

Once at this screen, you can use CTRL+C to break in to the target computer, if it is still running. If the target is currently stopped at a blue screen, you will most likely break in automatically. If you have any problems, try using a CTRL+R to force a resync between the host and target computers.

If you are doing remote debugging, the same screen appears, with the following extra line:

```
KD: No carrier detect - in terminal mode
```

In this case, the debugger is in terminal mode, and you can issue any of the standard AT commands to your modem. Begin by sending commands to disable hardware compression, flow control, and error correction. These commands will vary from modem to modem, so consult your modem documentation. Once you connect to the target system and have a carrier detect signal, you are returned to the debugger.

APPENDIX C

Minor Revisions to Existing Resource Kit Books

The *Microsoft Windows NT Resource Kit* for Windows NT Workstation and Windows NT Server Version 3.51 contains slightly updated editions of the version 3.5 set of four volumes. For those customers who already have the version 3.5 set and will only receive this *Windows NT Update 1* book, we are including here a list of the changes that were made when we reprinted the books for this current version.

Resource Guide

The following changes were made in the *Windows NT Resource Guide*:

- Introduction
    - page *xxiii*, second item in the second bulleted list, Delete the phrase "and disks."
    - page *xxvi*, first two paragraphs under the section "Resource Kit Compact Disc," Replace them with the following paragraph:

      The compact disc (CD) that accompanies the *Windows NT Resource Kit* contains utilities that apply to information in both the *Windows NT Resource Guide* and the *Windows NT Networking Guide*. This CD includes a collection of information resources, tools, and utilities that can make networking and working with Windows NT even easier. The Windows NT Messages database and the utilities for *Optimizing Windows NT* are also included on the *Windows NT Resource Kit* CD.
    - page *xxix*, both bulleted items at the top of the page, Delete the phrase "or first floppy disk."
- Chapter 5, "Windows NT File Systems and Advanced Disk Management"
    - page 189, first paragraph, Add quotation marks before and after the following path statement, "D:\WORD FOR WINDOWS\WINWORD.EXE."
    - page 205, first paragraph under the section "Disk Striping with Parity," Replace the phrase "multiple single points" with "against a single point."
    - page 205, second paragraph under the section "Disk Striping with Parity," Delete the following phrase, "(that is, CD-ROMs)."

- Chapter 6, "Printing"
  - page 215, Delete the following sentence at the end of the page:

    Included with this resource kit is a PRINTER.INF file you can modify to install newly released .PPD files.
  - page 216, Table 6.2, Switch the order of the two data types (RAW [FF Auto] and RAW [FF Appended]) in the first column. Do not switch the order of the text in the second and third columns.
  - page 229, Figure 6.7, In the WINPRINT.DLL box, add a fifth datatype, JOURNAL surrounded by a box. In the SFMPSPRT.DLL box, change PSCRIPT to PSCRIPT1.
  - page 230, second paragraph after the bulleted list, Replace [FF Auto] with [FF Appended] and vice versa.
  - page 235, screen shot of Available AppleTalk Printing Devices, Remove the three entries that have PCL in their name.
  - page 235, first sentence in last paragraph, Delete the word "printers" and replace it with "print devices."
  - page 235, after the last paragraph, Add the following new paragraph:

    Some print devices process non-PostScript® print jobs incorrectly if they receive those jobs over AppleTalk®. Also, some print devices process PostScript jobs incorrectly if those jobs contain binary data and arrive over any protocol other than AppleTalk. These problems result from restrictions in certain print devices; they do not indicate that the Windows NT Server print server is transmitting the jobs incorrectly.
  - page 238, second paragraph after the screen shot, Change the two instances of the sample IP address to "11.22.33.44."
  - page 239, after the paragraph following the Note, Add the following new paragraph:

    When you use the **LPR** command to send print jobs to a Windows NT Server print server, the name of the printer is the text in the Print Name field of the Printer Properties dialog box; it is not the text in the Share Name field.
  - page 241, Table 6.3, Change the asterisks (*) in the fourth row to the superscript footnote symbol 1 (^{1}).
  - page 241, Table 6.4, Change "PSCRIPT^1" in the second row to "PSCRIPT1." Change the three instances of "No1" in the fourth row to "No^1."
  - page 242, first sentence in second paragraph, Replace it with the following sentence:

    When a Windows-based application running on a Windows NT Workstation (or client) computer sends a job over the network to a printer established by the Connect To Printer command, it uses the graphics engine to create a fully rendered job, with data type RAW.

  - page 242, first sentence in fourth paragraph, Change "Windows NT Workstation" to "Windows NT Workstation (or client)" and "Connect To" to "Create Printer."
  - page 247, last paragraph, Change the paragraph to a **Note** format to give it more emphasis, add the word :"**Note**," delete the first two words, "Note that," and change the third word, "the," to "The."
- Chapter 14, "Registry Value Entries"
  - Entire chapter, See the REGENTRY.HLP file on the *Windows NT Resource Kit* CD for the latest additions and changes to the Registry values.
  - page 448, first paragraph under the section "Linkage Subkey Entries for Network Componenets," Change the referenced chapter number from "11" to "10."
  - page 449, last paragraph at the bottom of the page, Change the referenced chapter number from "11" to "10."
  - page 521, third paragraph under the section "Remote Access Service (RAS) Entries," Replace it with the following sentence:

    For information on Remote Access configuration files and other parameters, see Appendix B, "Migrating from Earlier Versions of the Remote Access Service," in the *Windows NT Remote Access Service* book, which comes as part of the Windows NT Server product documentation. This book is also included in the "Books Online" part of Windows NT Server.
- Appendix D, "Hardware Compatibility List," Entire chapter, See the online Help version on the *Windows NT Resource Kit* CD for the latest additions and changes to the list of computers and peripherals that have been tested for compatibility with Windows NT 3.51 and passed.

Networking Guide

The following changes were made in the *Windows NT Networking Guide*:

- Introduction, page *xix*, last paragraph before bulleted list, Delete the following portion of that paragraph and add a period after the remaining "(CD):"

  ...and in a single set of 3.5-inch floppy disks. (The CD is bound into the back cover of the *Windows NT Resource Guide*, and the floppy disks are available upon request from MS-Press.)

- Chapter 8, “Client-Server Connectivity on Windows NT”
    - page 115, Figure 8.1, Due to legal restrictions, change the two instances of “Net-library” to “Network Library.”
    - page 116, last sentence in next-to-the-last paragraph, Due to legal restrictions, change the one instance of “Net-Library” to “Network Library.”
    - page 118, scattered throughout that page, Due to legal restrictions, change the eleven instances of “Net-Library” to “Network Library,” and the six instances of “Net-Libraries” to “Network Libraries.”
    - page 119, scattered throughout that page, Due to legal restrictions, change the nine instances of “Net-Library” to “Network Library,” and the three instances of “Net-Libraries” to “Network Libraries.”
    - page120, scattered throughout that page, Due to legal restrictions, change the five instances of “Net-Library” to “Network Library,” and the one instance of “Net-Libraries” to “Network Libraries.”
    - page 121, scattered throughout that page, Due to legal restrictions, change the four instances of “Net-Library” to “Network Library.”
    - page 122, scattered throughout that page, Due to legal restrictions, change the seven instances of “Net-Library” to “Network Library,” and the one instance of “Net-Libraries” to “Network Libraries.”
    - page 123, scattered throughout that page, Due to legal restrictions, change the ten instances of “Net-Library” to “Network Library,” and the one instance of “Net-Libraries” to “Network Libraries.”
    - page 124, scattered throughout that page, Due to legal restrictions, change the seven instances of “Net-Library” to “Network Library.”
    - page 125, Table 8.1, Due to legal restrictions, change the three instances of “Net-Library” to “Network Library,” and the one instance of “Net-Libraries” to “Network Libraries.”
- Chapter 9, “Using Remote Access Service,” See the preceding Appendix A, “Major Revisions to the Windows NT Networking Guide,” for an updated version of that chapter.
- Chapter 10, “Overview of Microsoft TCP/IP for Windows NT,” page 162, Step 5., Replace the directory name “**\advsys**” with the new name “**\bussys**.”
- Chapter 12, “Networking Concepts for TCP/IP”
    - page 202, under the section “NetBIOS over TCP/IP and Name Resolution,” Change the two instances of “NBT” to “NetBT.”
    - page 203, in the first three paragraphs, Change the six instances of “NBT” to “NetBT.”
    - page 218, last paragraph on the page, Change the letter of the referenced appendix from “A” to “B.”

- Chapter 13, "Installing and Configuring DHCP Servers"
  - page 226, Step 1, Delete the word "Known" from the dialog box name.
  - page 226, Step 2, Replace "in which" with "to which."
  - page 228, Step 6, Replace "seconds" with "minutes."
  - page 249, first paragraph after the Caution, Replace "15 minutes" with "60 minutes."
  - page 254, under **BackupInterval**, Replace "15 minutes" with "60 minutes."
  - page 256, in the Registry key example, Delete "\current" and add "Server" after "DHCP." The new key example should then read as follows:

    ```
    ...SYSTEM\currentcontrolset\services\DHCPServer\Parameter\<option#
    >
    ```
- Chapter 14, "Installing and Configuring WINS Servers"
  - page 265, Note at the bottom of the page, Change the letter of the referenced appendix from "A" to "B."
  - page 266, fourth item in the bulleted list, Replace it with the following sentence:

    The ability for clients running Windows NT and Windows for Workgroups on a Windows NT Server network to browse domains on the far side of a router without a local domain controller being present on the other side of the router.
  - page 275, Step 3, Description of Renewal Interval, Change "five hours" to "96 hours (4 days)."
  - page 275, Step 3, Description of Extinction Interval, Add "The" before the beginning of the last sentence. Add an additional sentence as follows:
    The minimum cannot be less than the renewal interval.
  - page 275, Step 3, Description of Extinction Timeout, Add "The" before the beginning of the last sentence.
  - page 275, Step 3, Description of Verify Interval, Delete the extra period before the last sentence. Change the last sentence to read as follows:

    The maximum allowable value is 576 hours (24 days).
  - page 275, Step 4, Close up space before "Initial Replication."
- Chapter 21, "Setting Up Internet Servers and Clients on Windows NT Computers," page 389, last line under the section "Publishing Tools," Delete the phrase "and the Telnet Server." Add the word "and" before the phrase "the WAIS toolkit" and a period after "toolkit."

- Chapter 22, "Remote Access Service and the Internet," See the preceding Appendix A, "Major Revisions to the Windows NT Networking Guide," for an updated version of the "Installing a Simple Internet Router that Uses PPP" section.
- Appendix B, "MIB Object Types for Windows NT," See the preceding Appendix A, "Major Revisions to the Windows NT Networking Guide," for an updated version of that appendix.

Windows NT Messages

The following changes were made in *Windows NT Messages*:

- Welcome
  - page *ix*, first sentence under the section "Setting Up, Starting, and Quitting the Messages Database," Delete the phrase "floppy disks or" and italicize the book title "*Windows NT Resource Kit*."
  - page *ix*, after the first sentence under the section "Setting Up, Starting, and Quitting the Messages Database," Add the following sentence:

    If you want to wait and install it at a later time, you may use a separate Messages database Setup program that is located under the \WINNTMSG directory.
  - page *ix* - *x*, Delete the entire procedure "**To set up the Messages database from floppy disks**."
  - page *x*, in the procedure title, Delete the phrase "**from the compact disc**."
  - page *xii*, first paragraph after the bulleted list, Delete the phrase "floppy disks or" and italicize the book title "*Windows NT Resource Kit*."
  - page *xii*, last sentence in the Important notice, Delete the phrase "floppy disks or" and italicize the book title "*Windows NT Resource Kit*."
- Chapter 2, "Windows NT Executive Messages," See the preceding Appendix B, "Major Revision to Windows NT Messages," for an updated version of the "Windows NT Debugger" section.

Optimizing Windows NT

The following changes were made in *Optimizing Windows NT*:

- Introduction
  - page *xxiii*, second line of first paragraph, Replace the phrase "initial release of Windows NT 3.5" with the phrase "initial release of Windows NT 3.1 and the subsequent release of Windows NT 3.5."
  - page *xxiii*, first line of third paragraph, Replace the phrases "floppy disk (or CD-ROM)" with "CD" and "this book" with "the *Windows NT Resource Kit*."
  - page *xxiii*, near the end of third paragraph, Replace the phrase "floppy disk" with "CD."
- Chapter 1, "How to Optimize Windows NT"
  - page 5, last line of first paragraph, Replace the phrases "floppy disk" with "CD" and "this book" with "the *Windows NT Resource Kit*."
  - page 6, second line of first paragraph, Replace the phrases "floppy disk" with "CD" and "this book" with "the *Windows NT Resource Kit*."
- Appendix C, "Using Response Probe," page 621, last sentence in first paragraph, Replace the phrases "floppy disk" with "CD" and "this book" with "the *Windows NT Resource Kit*."

APPENDIX D

Security In a Software Development Environment

Windows NT provides a number of different "environment subsystems," such as the Windows subsystem, the POSIX subsystem, and the OS/2 subsystem. Each of these subsystems presents a set of application programming interfaces (APIs). These subsystems are built using an underlying set of programming interfaces and mechanisms that are primarily used only in the development of the operating system and operating system components (such as device drivers and environment subsystems). These underlying mechanisms are not designed to be used in the development of applications, such as word processors or database server packages, and so generally are of little interest to a security administrator. However, this is not always the case, and in some circumstances these mechanisms are of vital interest to security administrators.

A typical shrink-wrapped product from a reputable manufacturer uses only the programming features explicitly provided for application development. However, what do you really know about a shareware program downloaded from a public network server? It might try to take advantage of some of the mechanisms in Windows NT that are not intended to be used by application programmers — either for beneficial uses, or maybe to introduce a Trojan Horse or virus program into your system. This might also be true if you purchase software from a company more interested in exploiting every bell and whistle, rather than producing quality products using published interfaces and mechanisms. Even your own developers, if your company does its own in-house software development, could use these mechanisms in their programs. As you can see, there are situations where understanding some of these underlying mechanisms and being able to monitor their use is vitally important.

This document helps you to understand some of Windows NT's underlying and internal APIs and mechanisms. It also provides information that can be used by a security administrator to monitor these mechanisms and to interpret the log files generated as a result of this monitoring. This information is, necessarily, quite technical in nature, being roughly equivalent to programmer documentation. In fact, the information in this document might also prove to be useful background for anyone wishing to write some automated security monitoring tools.

User Rights

The following rights can be assigned to user accounts through the Windows NT Win32 application programming interface. Security event log entries that record the assignment and use of privileges refer to the privileges using the name shown in parentheses.

Create a token object (SeCreateTokenPrivilege)
This right allows a process to create access tokens. Only the Local Security Authority can do this. By default, no account has this privilege. Use of this right is not auditable. For C2 certification, it is recommended that it not be assigned to any user.

Debug programs (SeDebugPrivilege)
This right allows a user to debug various low-level objects such as threads. By default, the Administrators account has this privilege. Use of this right is not auditable. For C2 certification, it is recommended that it not be assigned to any user, including system administrators.

Generate security audits (SeAuditPrivilege)
This right allows a process to generate security audit log entries. By default, no account has this privilege. Use of this right is not auditable. For C2 certification, it is recommended that it not be assigned to any user.

Audit Record Format

The format and contents of the audit event records are based on the design of Event Viewer. Event Viewer uses information from the Registry to locate message files and to determine how to present the information in an event record.

Event Viewer expects a number of *event source modules* to be defined as part of the security audit log information in the Registry. At least one event source module must be provided by each product that generates audit event records. For example, if a mail product is installed, that product's installation procedure needs to add its event source module information to the security log information in the Registry. A special event source module shipped with Windows NT contains default information, so that information does not have to be replicated in other event source modules.

The information defined for event source modules includes:

- Event Message File. This file contains the displayable strings for each audit event record. It includes parameter substitution markers to be replaced at viewing time with Unicode strings logged in the event record.

  Only the event source module shipped with Windows NT should define an event message file. This single event message file serves as the default for other event source modules.
- Category Message File. Categories are discussed in "Elements of an Event Record," later in this document. Only the security event source module shipped with Windows NT should define a category message file. This single category message file serves as the default for other event source modules. In Windows NT version 3.51, this file is not actually used for auditing.
- Parameter Message File. The parameter message file is used to provide object type-specific access names. Each security event source module should (but does not have to) provide a parameter message file. If object type-specific access names are not provided by an event source module, then default names will be used (such as "Specific Access Bit 0").

When Event Viewer is asked to display an audit record, it uses the event source module name and event ID from the record to retrieve a message string for that event. This string can include parameter substitution markers and other format characters that are interpreted and acted upon by a call to FormatMessage(). For example, the string for a successful logon audit might look like:

```
Successful Logon: \n\t\tUser Name:\t%1 \n\t\tDomain:\t%2
```

Notice that this message string includes two parameter substitution markers (%1 and %2). These parameter strings are obtained from the event record. So, if Administrator logged on to a computer named ACCTG, an event record containing those two strings would be recorded. The corresponding event record in Event Viewer would look like this:

```
Successful Logon:
        User Name:  Administrator
        Domain: ACCTG
```

Before Event Viewer formats the entire message string, it must format the individual parameter strings received in the event record. In the preceding example, the parameter strings needed no formatting. In the case of an audit generated when a file is opened for WRITE_DATA and WRITE_DAC, however, the event message might be:

```
Object Open:\n\t\tObject Type:\t%1\n\t\tObject
Name:\t%2\n\t\tAccesses:\t%3
```

and parameter strings received in the audit record might be:

Parameter string 1: “File”

Parameter string 2: “C:\accounting\payroll\hours_worked.dat”

Parameter string 3: “%%972\n\t\t\t\t%%1032”

The "%%" directive tells Event Viewer to look up and substitute the message specified by the number following the directive from the parameter message file for the event source module. Assuming message numbers 972 and 1032 in the message file are "Write DAC" and "Write Data" respectively, the third string will be changed to:

```
Write DAC\n\t\t\tWrite Data
```

This would cause the resultant display by Event Viewer to look like:

```
Object Open:
        Object Type:File
        Object Name:C:\accounting\payroll\hours_worked.dat
        Accesses:    Write Dac
                     Write Data
```

(This example is for illustrative purposes only and does not correspond to an actual event-record type.)

Tight Security for Shared Objects

As shipped and installed, Windows NT is configured to provide a high degree of ease of use. In some cases, this ease of use can be seen as a security threat. This is particularly true of “denial of service” attacks, in which a user is able to deny others the use of various parts of the system. There are a number of components of the underlying mechanisms of Windows NT that may be affected in this manner by anyone with the programming knowledge to locate and manipulate them.

A highly security-conscious system administrator might choose to trade this ease of use for added security. It is impossible to enumerate all the ways in which this tradeoff might be seen or experienced by each user or application. However, you can expect that the biggest area of impact will be for users that redefine system-wide resource attributes, such as the attributes of COM1: or of printers. In general, by tightening base security, you must accept that these shared resources will be administered only by system administrators.

To strongly protect shared objects, use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Session Manager
Name:	ProtectionMode
Type:	REG_DWORD
Value:	1

If this value does not exist, or is set to anything other than one (1), then standard protection is applied to these objects.

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Auditing

This section describes special cases of auditing that might be of interest to administrators of high-level security installations.

Auditing Backup and Restore Activities

When files are being backed up, Windows NT checks to ensure that the user performing the backup has the Back Up Files and Directories special right each time the backup program attempts to copy a file to the backup media. In the same way, Windows NT checks for the Restore Files and Directories right for each file that is being restored from backup media. Obviously, if Windows NT were to record an audit event each time those rights were invoked, thousands of events would be recorded during a routine backup. Because this would flood the security log with event records that most often would be of little value for maintaining system security, Windows NT does not normally record audit events for the use of these rights, even when success auditing of Use of User Rights is enabled in the system user rights policy.

To audit the use of these rights, use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\System
Key:	\CurrentControlSet\Control\Lsa
Name:	FullPrivilegeAuditing
Type:	REG_BINARY
Value:	1

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Note The *use* of the following rights is never audited, even when the FullPrivilegeAuditing Registry entry is set to 1. However, the *assignment* of these rights, during logon, is audited.

- Bypass traverse checking (SeChangeNotify)
- Generate security audits (SeAuditPrivilege)
- Create a token object (SeCreateTokenPrivilege)
- Debug programs (SeDebugPrivilege)
- Create a new security context for a new logon (AssignPrimaryToken)

Managing Auditing of Particular Objects

In addition to letting you audit system-wide events (such as users logging on), Windows NT gives you the ability to record such events as whether a specific user fails to open a given object (such as a file or printer) for a particular type of access.

Note Only files and directories in NTFS partitions can be audited, and it is only access that is auditable, not intent. In other words, the audit log records will show that a particular user opened a specific file or directory; it will not tell you what the user's intent was. Copying a file, reading a file, or viewing a file's attributes all write the same set of audit records to the log.

To be able to audit object access in this way, you must first use the Audit Policy dialog of User Manager to enable auditing of file and object access events. You can enable auditing of success or failure events, or both. This establishes the global object-access auditing policy for the system. The global policy determines whether object-specific auditing will occur at all; to record access events for a particular object, you must also specify the type of auditing to be performed for that object. File Manager lets you set up auditing for files and directories, Print Manager lets you configure auditing for printers, and Registry Editor lets you specify auditing for Registry entries.

In a sense, object-access auditing works like a building's electrical system. You can turn on and off switches for lamps throughout the building, but if the master circuit breaker is off, no lamps will actually turn on. On the other hand, if the master circuit breaker is on, then only those lamps whose switches are in the on position will light up.

Because the security log is limited in size, and because a large number of routine audit records can make it difficult to find records that suggest a security problem, you should carefully consider how you will audit object access. Generating too many audit records might require you to review and clear the security log more often than is practical. On the other hand, judicious use of object-access auditing can be invaluable in helping you identify areas where your security policy should be tightened or even where a security breach has been attempted successfully or unsuccessfully.

For example, if you use permissions to control users' access to sensitive files and directories, you should enable auditing of those users' access to those files and directories to ensure that the permissions are working as expected.

If a directory has a list of users whose access to the directory is to be audited, a new file added to the directory will inherit the auditing list from the directory. You can ensure that Windows NT Workstation will record access to new files by making sure the new files are placed in directories with auditing lists.

Note Only new files and directories inherit auditing lists from the directory in which they are created. To ensure that access to existing files will be audited, be sure to select both Replace Auditing On Subdirectories and Replace Auditing On Existing Files in the Directory Auditing dialog box when creating a directory auditing list.

For procedures for managing access auditing for files and directories, see the "File Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide*. For procedures for managing access auditing for printers, see the "Print Manager" chapter in the Windows NT Workstation or Windows NT Server *System Guide*. For information about auditing access to Registry keys, see the online Help for Registry Editor and Part IV, "Windows NT Registry," in the *Windows NT Resource Guide*.

Base Object Auditing

In addition to Files, Registry Keys, and Printers, Windows NT has a number of objects that are not generally visible to or known by a typical user. Application programmers or people writing I/O device drivers might have learned about these objects in software development or device driver development kits. Normal interactive users, however, have no direct ability to affect these objects except as intended by Windows NT.

Generally speaking, these objects are used by Windows NT in a manner that makes auditing their use not very interesting. In fact, doing so can introduce so many audit entries into the security log that locating real security problems becomes considerably more difficult.

However, in some situations, it might be desirable to audit accesses to base objects. For example, where custom applications are being developed, the “users” are not just the people that interactively log on, but also the programmers who are developing applications. These programmers might be able to directly access the base objects.

Note It is only access that is auditable, not intent. In other words, the audit log records will show that a particular user opened an object; it will not tell you what the user’s intent was.

To audit the use of base objects, first set your system’s audit policy to audit successful and/or failed object accesses, and then use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Lsa
Name:	AuditBaseObjects
Type:	REG_DWORD
Value:	1

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

Accesses to shared base objects appear in the security log as Object Access events, like those for Files, Registry Keys, and Printers, but with different object type names and access names. For a full description of each of the base object types and their access types, refer to the Microsoft Software Developer’s Network (MSDN). To receive MSDN level 2, call 800-759-5474.

When the Security Log Is Full

If you have set the security log either to "Overwrite Events Older than *n* Days" or "Do Not Overwrite Events (Clear Log Manually)", you might want to prevent auditable activities while the log is full and no new audit records can be written. To do so, use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Value:	1

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

If Windows NT halts as a result of the security log becoming full, the system must be restarted and reconfigured to restore it to high-level security. When Windows NT restarts, the Security log is full and so no auditable actions are recorded until the Security log is cleared.

To recover when Windows NT halts because it cannot generate an audit event record

1. Restart the computer and log on using an account in the Administrators group.
2. Use Event Viewer to clear all events from the Security log, archiving the currently logged events. For details, see the "Event Viewer" chapter in the Windows NT Workstation or Windows NT Server *System Guide.*
3. Use the Registry Editor to delete and replace value entry **CrashOnAuditFail**, with data type **REG_DWORD** and value **1**, under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa (as described earlier in this section).
4. Exit, and then restart the computer.

Interpreting the Security Log

When you view the security log, you can use filters to specify criteria for the records you want to view. For example, you can choose to view events recorded by a particular source within a range of dates.

If you need a more complex analysis of the information in the security log, you can save the security log in one of two text formats. The information can then be imported into an analysis tool (such as a spreadsheet). See the "Event Viewer" chapter in the Windows NT Workstation or Windows NT Server *System Guide* for more information about using security log data archived in a text format.

Elements of an Event Record

All event-log records, regardless of type, consist of a header containing standard information, a description that varies depending on the event type, and (optionally) additional data. Most security log entries consist of the header and a description.

The event-record header contains the following information:

Date The date the event occurred.

Time The (local) time the event occurred.

User The username of the user on whose behalf the event occurred. This is the client ID if the event was actually caused by a server process, or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs.

Computer The name of the computer where the event occurred. (Event Viewer can be used to view event logs on other Windows NT computers on a network.)

Event ID A unique number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 562 is the ID of the event that occurs when a new object handle is created, and so the first line of the description of such an event is "Handle Allocated."

Source The name of the system component that actually recorded the event in the security log. Usually, this is Security, indicating that it is the result of Windows NT security auditing. Applications can also define their own auditable events that can be recorded in the security log.

Type Either Success Audit or Failure Audit, indicating whether the audit is a record of a successful or failed attempt. In Event Viewer's normal list view, these are represented by a key or a lock, respectively.

Category A classification of the event by the event source. For security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in the User Manager Audit Policy dialog.

The format and contents of the description that appears with these items vary with the event category. The various event categories are discussed later, under "Audit Categories."

Identifying the User Behind the Action

The security log identifies the user account that caused each recorded event to happen. In some cases, more than one account is actually involved because of the client-server design of Windows NT. This design makes it possible for one process (called a server process) to perform actions on behalf of another process (called the client process).

When the server process is acting on behalf of the client, Windows NT security treats it as though it were the client process. The server process is not allowed to access objects that are off limits to the client.

Also, the audit records for events performed by a server impersonating a client identify the "user" that "owns" the server process as the primary user (typically identified as SYSTEM), and the user responsible for starting the client process as the client user. When there is no impersonation taking place, the primary user is the actual user who started the process that caused the audited event to occur. Most often, this is the user who is actually logged on to the computer, although sometimes it can be SYSTEM.

Process IDs

Primary IDs and impersonation IDs provide enough information for many security administrators because they show who is performing auditable actions. However, in some cases, an operator might want to see what is going on at a process-by-process level of detail. If detailed tracking auditing is enabled, the security log shows when a new process is created (such as when an application program begins execution). Each process is assigned its own, globally unique process ID, which is included in all records of events caused by that process, to the point at which the process ends.

This information can be correlated with specific audit event records to see which user account is being used to perform auditable actions and which program was being run. Process IDs are included in audit event records regardless of whether process-level tracking is enabled. However, process IDs are useful only if process-level tracking is enabled.

Note Because of the way impersonation works, it is impossible to know what the process ID of a client is at audit time. In fact, a single access token can actually be used by several processes simultaneously. For this reason, process IDs can only be displayed by audits generated by the Kernel.

Handle IDs

When a particular operation consists of multiple actions, Windows NT assigns an *operation ID* to each so you can properly associate the separate actions with the operation. This operation ID is unique only to the process performing the operation. Furthermore, to help you track how a process accesses a particular object, each object is identified by a *handle ID*. Typically a new handle is allocated immediately after a file is opened, and then closed when the file is closed. If the handle ID refers to a Kernel object, the handle ID is unique only to the process to which the handle belongs. If the handle ID refers to an object managed by a protected server, the handle ID is unique across all processes.

The handle ID enables the audit to be associated with future audits. For example, when a file is opened the audit information indicates the handle ID assigned. When that handle is closed another audit event record is generated which also includes the handle ID. This allows you to determine the entire span of time the file was open, which can be useful when attempting to assess damage following a security breach.

There are two types of handle IDs, often called Kernel object handle IDs and protected server object handle IDs. Handle IDs to Kernel objects are unique only to the process to which the handle belongs. As a result, two processes can have a handle with an ID of 35, for example; they are distinguished by the process ID associated with them. Handle IDs to protected servers on the other hand, come from a single ID space and are unique across all processes.

Audit Event Record Contents and Meaning

This section describes the contents and meaning of each audit event record.

Common Event Record Data

Audit event records include header information that is present in all event records. The following list describes this common information.

- The time the event was generated.
- The SID of the subject that caused the event to be generated. If possible, Event Viewer translates this SID to an account name for display. The SID is the impersonation ID if the subject is impersonating a client, or the primary ID if the subject is not impersonating.
- The name of the system component or module that submitted the event. For security audits this is always Security.
- The module-specific ID of the specific event.
- The event type, either Success Audit or Failure Audit.
- The event category, used to group related events such as logon audits, object access audits, and policy change audits.

When an event is displayed in detail, this information is displayed at the top of that window. The following is an example of how this information is displayed:

```
Date:        9/8/92           Event ID:    172
Time:        10:32:11 AM      Source:      Security
User:        Administrator    Type:        Failure Audit
Computer:    ACCTG            Category:    Logon/Logoff
```

Audit Categories

Audit event records are divided into auditing *categories*. These categories are displayed by Event Viewer and allow a user to visually distinguish or automatically filter audit events of interest. These audit categories are listed in the following table, and discussed in detail in the Audit Categories Help file (AUDITCAT.HLP).

Category	**Description**
System Event	Events in this category indicate that something affecting the security of the entire system or of the audit log has occurred.
Logon/Logoff	Events in this category describe a single successful or unsuccessful logon or logoff. Included in each logon description is an indication of what type of logon was requested/performed (for example, interactive, network, or service).
Object Access	Events in this category describe both successful and unsuccessful accesses to protected objects.
Privilege Use	Events in this category describe both successful and unsuccessful attempts to use privileges. The Privilege Use category also covers a special case of informing when some special privileges are assigned. These special privileges are only audited when they are assigned, not when they are used.
Account Management	Events in this category describe high-level changes to the security account database, such as the creation of a user account or a change in group membership. There can also be a finer granularity of auditing performed at the object level under the Object Access category.
Policy Change	Events in this category describe high-level changes in security policy, such as the assignment of privileges or changes in the audit policy. There can also be a finer granularity of auditing performed at the object level under the Object Access category.
Detailed Tracking	Events in this category provide detailed subject tracking information, such as program activation, some forms of handle duplication and indirect object accesses, and process exit.

APPENDIX E

Domain Planning for Your Enterprise

The descriptions of other companies' products in this appendix are provided only as a convenience to the reader. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this appendix should not be interpreted as a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Overview

The information in this appendix supersedes the paper, "*Microsoft Windows NT Enterprise Planning Guide: Windows NT Domains and Domain Strategies*," which was written for Windows NT Advanced Server 3.1. This appendix covers the enhancements to domains and domain planning for Windows NT Server version 3.5 and 3.51.

This planning guide provides in-depth information on the implementation of Microsoft Windows NT Server 3.51, with a focus on domains and domain strategies. It is intended for networking groups who are going to implement a networking solution and may need assistance in planning the design and implementation of domains. The goal of this document is to provide an understanding of the various domain models, the business and technical reasons for selecting one model as opposed to the others, as well as the advantages and tradeoffs associated with each of the domain models.

This guide discuss the following topics:

Impact of New Features

Enhancements introduced in Windows NT Server 3.5/3.51 may impact the domain model selection as capacity and throughput increase.

Review of Important Concepts

The purpose of this section is to provide a summary of the key concepts and features available within Windows NT Server that allow the implementation of domain structures.

Planning for Your Domain Model

There are several areas that can influence the type of domain model you choose and the placement of backup domain controllers. This section covers the management, location, and replication areas that should be taken into consideration.

Putting it all Together: Selecting Your Domain Model

Once the key concepts of domains are presented, the selection of a domain model is explored. This section covers the questions that a networking group should answer in order to determine the right domain model for the organization.

Case Study: Microsoft Corporation Worldwide Network

Microsoft's domain model is presented here to show the flexibility of the Windows NT domain model. The Microsoft domain model serves over 150 sites in 52 countries and uses the multiple master domain model.

Reference Materials

A further reading list is presented as reference material.

Related Topics: What you should already know

You should already be familiar with the following manuals and concepts:

- *Microsoft Windows NT Server Concepts and Planning Guide*
- *Microsoft Windows NT Server Installation Guide*
- *Microsoft Windows NT Resource Kit*
  - Network Security and Administration:
    Windows NT Networking Guide, Volume 2, Chapter 4
  - User Accounts Communication over Servers: Identification and Authentication:
    Windows NT Networking Guide, Volume 2, Chapter 4

Impact of New Features

Microsoft Windows NT Server version 3.5/3.51 includes many performance and product improvements. This section lists the enhancements that impact domain planning and enterprise issues.

More Users Possible In a Single Domain

Windows NT Advanced Server 3.1 had a recommended limit of 10,000 users per domain. Beginning with Windows NT Server version 3.5, performance improvements, combined with the more powerful hardware now available, have significantly increased the number of users per domain. Now, as many as 40,000 user accounts can be supported in a single domain, and well in excess of 100,000 users using multiple master domains. The maximum recommended size of the Security Accounts Manager (SAM) database file (40 MB) is the determining factor for the number of users. This appendix provides job aids to assist you in calculating the size of the file, and therefore the number of user, machine, and group accounts.

Faster Logon Processing

More logons can be processed in a shorter span of time. The new encryption method for user account records is more than 100 times faster than the algorithm used for Windows NT Advanced Server 3.1. The new method significantly decreases the number of BDCs(backup domain controllers) required to support the early morning logon crowd.

Servers Dedicated to Specialized Tasks

With the introduction of non-domain controller servers in Windows NT Server 3.5, no longer do all servers need to be involved in authentication of accounts and replication of the SAM. The network administrator can dedicate a server to a specific task or function rather than sharing its processing capacity with its primary task and administrative tasks. Because these servers rarely had free time to process replications due to the heavy processing load of business operations, the non-domain controller server results in faster replication.

Because a non-domain controller server has less overhead than either a primary domain controller (PDC) or a backup domain controller (BDC), and is fully fault tolerant, it is an excellent platform for an applications server, running applications, such as SQL Server and SNA Server. These non-domain servers have Windows NT Workstation security but contain all of the server software, which means they can take advantage of such features as:

- Supporting up to 256 simultaneous RAS connections
- Advanced Fault Tolerance (disk mirroring/duplexing, RAID 5)
- Macintosh® access to Windows NT Server File and Print Services
- Being a Remoteboot Server that supports MS-DOS and Windows 3.*x* clients

Faster Replication

In Windows NT Server 3.5, synchronization of the User Account database was changed to better suit wide area networks (WANs) and to increase performance. In addition, each BDC can now support up to 2000 users. Since BDCs can help spread the load of logon authentication and replication, replication time will decrease in many organizations due to the following factors:

- The new algorithm for replication ensures that only 10 BDCs are contacted at a time, in a round-robin fashion. The entire domain accomplishes synchronization faster because not all BDCs are vying for updates at the same time.
- The PDC knows all of the replication levels of each of the BDCs, and sends only the information that each BDC needs for replication. This speed of replication reduces the need for and use of full synchronization.
- A full synchronization of the user account database is no longer necessary when the PDC of the domain changes, if the PDC and the BDC are both running Windows NT Server version 3.5/3.51. This is because the PDC keeps track of the synchronization level of each BDC, which allows the PDC to control the rate of partial synchronizations.
- The encryption format of the mailslot messages for user account database changes has been improved, making the messages 100 times faster, while maintaining security.

Network Traffic Regulation

The network administrator has new settings to control the amount of account replication traffic over the WAN or RAS. Windows NT Server version 3.5/3.51 now has a parameter for BDCs, called **ReplicationGovernor**, that defines both the size of the data transferred on each call to the PDC and the frequency of those calls. Adjusting the **ReplicationGovernor** percentage affects both the amount of traffic sent and the frequency of sending the information.

The **ReplicationGovernor** parameter trades off the ability to regulate network traffic with the time it takes to complete replication by:

- Reducing the size of the buffer used on each call from the BDC to the PDC, ensuring that a single call does not consume the WAN link for too long.
- Causing Net Logon to essentially "sleep" between calls, allowing other applications to access the WAN link between calls to the PDC.

The NetLogon service can now be paused on any Windows NT Server version 3.5/3.51 machine, including the PDC of a domain. When paused, the NetLogon service will not be the target of any pass-through authentication, allowing the machine to be available for other purposes. For example, one might pause the NetLogon service on the PDC of the domain to allow it to replicate to more BDCs. Both the PDC and BDC must be running Windows NT Server version 3.5/3.51 in order to take advantage of this improvement.

Review of Important Concepts

To engage in a technical discussion of domain implementation, it is first necessary to understand basic domain concepts—accounts, servers, and domains —and the interaction between these components.

The basic unit of security and centralized administration in Windows NT is the *domain*, a logical grouping of servers and workstations. A Windows NT network consists of one or more domains and can be contained at one site or span different sites. The minimum requirement for a domain is one server running Windows NT Server, which serves as the Primary Domain Controller and stores the master copy of the domain's user and group database. Optionally, a domain can include other servers running Windows NT Server acting as Backup Domain Controllers, Windows NT Server computers serving as standard servers, LAN Manager 2.*x* servers, Windows NT Workstation clients, and other clients, such as those running Windows® for Workgroups and MS-DOS®.

The following topics are summarized here for your convenience; other pertinent concepts are covered in other Windows NT Server materials.

- Accounts
- Groups
- Server Roles
- Domain Models

Accounts

Windows NT security requires users to be identified to the system. Therefore, each person who regularly uses the network must have a user account on a domain in the network. Guest access may be allowed for users without user accounts who need limited access to the network. User accounts are also subdivided into two types: *global user accounts* and *local user accounts*. Most or all user accounts you create will be global user accounts.

User Accounts

In order to identify users to the system, an administrator creates user accounts by assigning user names to new user accounts. When this happens, Windows NT generates a security identifier (SID) for each new account. Each user account SID uniquely identifies the user, regardless of when or where the account was created. This information is stored in the Security Accounts Manager (SAM) database in the Windows NT Registry and includes such data as:

- The user name that identifies an individual account.
- The account's password.
- Groups of which the account is a member.
- Initialization information, including home directory and logon script.
- Restrictions on how the user can use the network.

Each user account requires approximately 1K in the SAM. The database is located on the PDC for the domain or on a PDC in the master domain. The password information for the account is stored doubly encrypted for security purposes.

Regardless of the domain model selected, an administrator only needs to define a user account *once*. Windows NT Server 3.5/3.51 allows a user to maintain a single user account to gain access to the domain, including other servers in the domain. If trust relationships are established, that single user account can also gain access to servers in other domains that trust the account domain.

On a regular basis, the user account database is replicated between the PDCs and all BDCs in the domain. The replication allows the logon process to be handled by the PDC or any BDC, which will increase throughput and help eliminate bottlenecks during the logon process.

Machine Accounts

When a workstation, server, or BDC is added to a domain, Windows NT generates an account for the machine name. The machine accounts serve various purposes, including linking BDCs with the PDC and pairing up the trusting and trusted domains. Each machine account requires approximately 0.5K in the SAM.

Groups

To simplify administration of user accounts which have similar resource needs, the administrator can categorize the user accounts into *groups*, which makes granting access rights and resource permissions easier. Instead of performing many individual actions to grant certain rights or permissions, the administrator can perform a single action that gives a group that right or permission to all the present and future members of that group. Group accounts are also stored in the SAM. The size of a group account may vary, based on the number of user accounts associated with the group. A good rule of thumb is that each group account requires 4K in the SAM.

Windows NT Server provides built-in *local* groups, and the ability to create custom *global* groups. Adding a user to a predefined group provides the user with all the access rights and privileges of that group. Changing access rights is a simple task; changing the rights of the group will automatically change the rights of all group members. Administrators should use built-in groups whenever possible.

For a complete discussion of groups, see Chapter 3, “How Network Security Works, in the *Windows NT Server Concepts and Planning Guide.*

Local Groups

Local groups define permissions to resources only within the domain in which the local group exists. Hence, the term “local” defines the scope of the resource permissions granted to users within the group. Local groups may contain users and global groups from the local domain (but not other local groups), as well as users and global groups from trusted domains. However, a local group can only be assigned permissions and rights in its home domain.

Not only are local groups an effective way of collectively assigning user rights and permissions for a set of users within the home domain, but they can be used to gather together numerous global groups and users from other domains. This allows an administrator to change access to domain resources globally with a single modification to the local group permissions.

The best group strategy to implement in the multiple master domain model is to create local groups in the resource domains. Those local groups will hold the global groups from the account domains.

Global groups

Global groups can be thought of as groups that can be used in other domains. In fact, global groups, since they have no user rights associated with them, are powerless until they are assigned to a local group or to a user right. Note that global groups defined in a domain can be "exported" to Windows NT Workstations in that domain. Windows NT Workstations support local groups and can, therefore, make use of global groups defined in either the Workstation's own domain or from other domains.

A global group may only contain user accounts that are locally defined in the domain in which the global group exists. By using trust relationships, users within a global group can access resources outside of their locally defined domain. Global groups are quite suitable, therefore, for large, multi-domain networks. Global groups can provide an inclusive list of all user accounts within a domain that require a particular type of access to resources that exist within another domain.

An administrator will have to create multiple global groups (in each master domain) to accommodate all the users in the network. It might help to distribute the users among the master domains according to organization within the company rather than alphabetically.

How Many User Accounts in a Domain?

A domain consists of user accounts, machine accounts, and group accounts, both built-in and custom. Each of these objects occupies space in the SAM file. The practical limit for the size of the SAM file depends on the type of computer processor and amount of memory available in the machine being used to administer the domain. Microsoft has successfully tested SAM files in excess of 40MB and recommends 40MB as the upper limit (larger SAM files may take several minutes to load into memory for administration purposes). Different types of objects require different amounts of space in the SAM file:

Object	Space Used
user account	1K
machine account	0.5K
group account	4K

For a single domain, here are some examples of how objects might be distributed:

	User Accounts (1K per account)	Machine Accounts (0.5K per account)	Group Accounts (4K per account)	Total SAM size
1 workstation per user	2,000	2,000	30	3.12 MB
2 workstations per user	5,000	10,000	100	10.4 MB
2 users per workstation	10,000	5,000	150	13.1 MB
1 workstation per user	25,000	25,000	200	38.3 MB
1 workstation per user	26,000	26,000	250	40 MB
1 workstation per user	40,000	0	0	40 MB

Note that these numbers can be applied to domains that comprise a single master and multiple master domain.

Server Roles

In a client-server networking environment, there are client workstations and servers which perform special tasks. The types of roles a server can fill under Windows NT Server 3.5/3.51 are described in this section, which begins with the minimum requirements for a Windows NT Server domain.

Primary Domain Controller

The minimum requirement for a domain is one server running Windows NT Server 3.5/3.51, which acts as the *Primary Domain Controller* (PDC), and stores the master copy of the domain's user and group security accounts database (SAM).

A domain has only one PDC.

Backup Domain Controller

A domain may have any number of Backup Domain Controllers (BDCs) running Windows NT Server. While not required, one or more backup domain controllers in a domain provide load balancing and fault tolerance. A BDC contains a copy of the domain's or master domain's SAM and can be used to authenticate user logons to help spread the load of logon request processing. The SAM is replicated to all the Backup Domain Controllers in the domain. If the PDC goes down, a BDC may be promoted to the PDC. The administrator should consider having as many Backup Domain Controllers as needed to process a high volume of logon activity at the desired performance levels. Each BDC can support up to 2000 user accounts.

Servers (non-domain controllers)

Servers dedicated for other uses can also run Windows NT Server software, but function as neither a primary nor backup domain controller. These servers can be standalone workstations, may participate in a domain as a file or application server, or may house BackOffice components. These servers do not participate in the replication of the user and group database, or the logon authentication process.

Some reasons for implementing non-domain servers are:

- The server must perform business-critical tasks or services, and should not spend any resources authorizing user logon requests or replicating the user database.
- The administrator for this type of server might not be allowed administrator rights for the rest of the domain.
- The server might be moved to another domain in the future.
- A non-domain server can be used to administer the domain server.

Just like a Windows NT Workstation version 3.5/3.51, the server will have its own security accounts database which it will use for User level security. Like the workstation, the server will be able to join a domain and use the domain's SAM to assign permissions to its own shared resources. If the network does not have a domain, the Windows NT Server can create or become a member of a workgroup just like Windows NT Workstations or Windows for Workgroups systems.

Domain Models and Windows NT Server Directory Services

Windows NT Server includes directory services that provide single network logon, single point of administration, and replication functions. These services simplify the management and use of a Windows NT Server-based network.

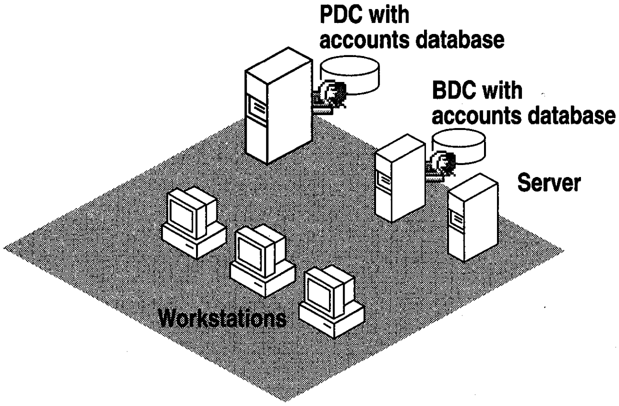
Windows NT Server Directory Services are based upon the configuration and use of Windows NT Server *domains*. Domains are logical groupings of multiple Windows NT Server-based computers that allow them to be managed and used as a single unit. They are the building blocks of Windows NT Server's Directory Services. Using domains, administrators create one user account for each user. That account includes user information, group memberships, and security policy information and is the central point of user administration. Users then log on once to the domain, not to the individual servers in the domain.

A *domain model* is a grouping of one or more domains, with administration and communications links between the domains (called trust relationships), arranged for the purpose of user and resource management.

Once logged on, users can access all the resources they have rights to access including files, directories, servers, applications, and printers. Windows NT Server Directory Services allow the administrator to maintain one user account for each user regardless of the number of servers in the distributed system. Users log on only once to gain access to all the different files, printers, and other network resources they need to use.

Single Domain Model

As the name implies, this configuration consists of one domain. There is one primary domain controller with potentially multiple backup domain controllers.



Single Domain Model

In a single domain network, network administrators can always administer all network servers, because the ability to administer servers is at the domain level.

The single domain model is an appropriate choice for organizations that require both centralized management of user accounts and the simplest domain model for ease of administration.

Trust Relationships

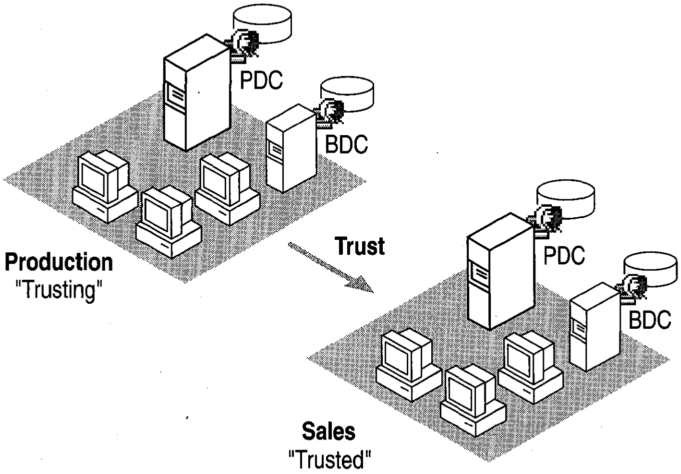
Windows NT Server domain models are extensible and flexible. The single domain model is the building block; *trust relationships* between domains allow network designers to implement the most appropriate design for their enterprise.

A trust relationship is an administration and communications link between two Windows NT Server domains. Domains use established trust relationships to share account information and validate the rights and permissions of users and global groups residing in the trusted domain. A user has only one user account in one domain yet can access all servers on the network.

Trust relationships are simple to initiate and administer with Windows NT Server User Manager for Domains. Windows NT Server domain models make use of trust relationships to facilitate:

- Centralized administration in multiple domain models.
- Simplified administration by combining two or more domains into a single administrative unit.
- The ability for users to log on from domains where they don't have accounts.
- The ability for users from one domain to be permitted to use resources in another domain, even if they do not have a user account in the resource domain.

- Increased number of user accounts in a master domain by locating machine and resource accounts in other domains.
- A domain structure to serve a large organization, for example 100,000 users.

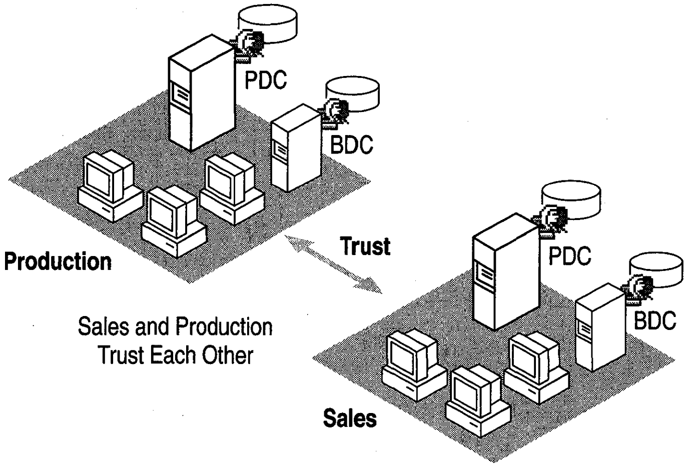


A One-way Trust Relationship: Production trusts Sales. Sales can access resources and accounts in the Production domain.

The "trusting" domain allows the remote user accounts and global groups in the "trusted" domain to use the resources of the trusting domain. Consider, for example, giving your neighbor a house key: you are "trusting" of your neighbor; your neighbor is the "trusted" one.

In a two domain example, where one is an account domain and the other is a resource domain, the only way that a one-way trust relationship makes sense is that the account domain is the trusted domain, and its users can use the resources in the resource domain (which is the trusting domain).

A two-way trust is two one-way trusts; both domains trust each other equally. This allows users to log on from either domain to the domain that contains their account. Using this implementation, each domain can have both accounts and resources, and remote user accounts and global groups may be used from either domain to grant rights and permissions to resources in either domain. In other words, both domains are trusted domains.



Two-way Trust Relationships

Depending on the goals of a domain model, one-way and two-way trust relationships can be used.

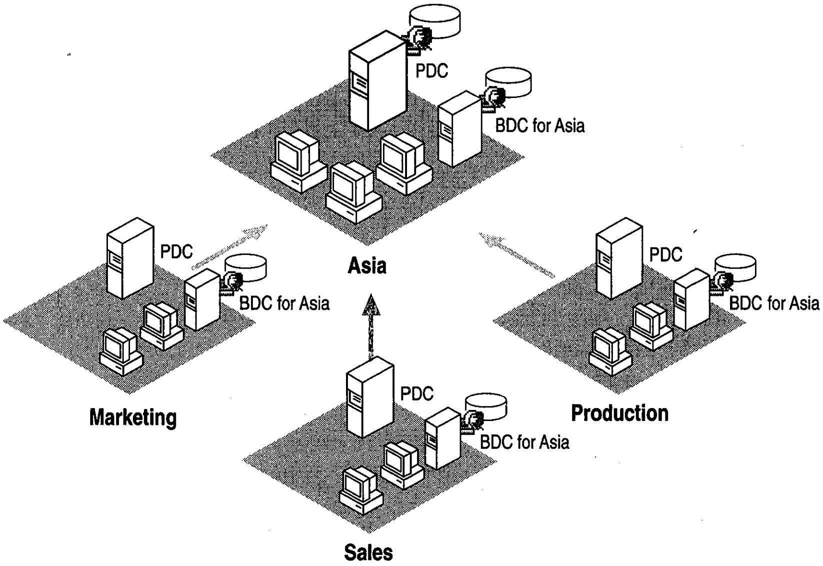
A domain can make use of up to 128 incoming trust relationships and an unlimited number of outgoing trust relationships.

Trust relationships are easily established and maintained with the User Manager for Domains administrative tool. Trust relationships are not transitive. If Domain A trusts Domain B, and Domain B trusts Domain C, Domain A does not automatically trust Domain C. This is so that administrators can explicitly control access to each domain.

Single Master Domain Model

The single master domain model is comprised of several domains, one of which acts as the central administrative unit for user accounts. All user and machine accounts are defined in this "master" domain and all users log on to their accounts in the master domain. Resources, such as printers and file servers, are located in the other domains. Each *resource* domain establishes a one-way trust with the master (account) domain, enabling users with accounts in the master domain to use resources in all the other domains. The network administrator can manage the entire multi-domain network, as well as its users and resources, by managing only a single domain.

The master account domain is also referred to as a *first-tier domain;* resource domains are also referred to as *second-tier domains.*



Single Master Domain Model

The benefit of the single master domain model is in its flexibility of administration. For example, in a network requiring four domains, it might at first seem most obvious to create four separate user account databases, one for each domain. By putting all user accounts in a single database on one of the domains and then implementing one-way trust relationships between these domains, you can consolidate administration of user and machine accounts. You can also administer all resources or delegate these to local administrators. And users have only one logon name and one password to get access to resources in any of the domains.

This model balances the requirements for account security with the need for readily available resources on the network, because users are given permission to resources based on their master domain logon identity.

The single master domain model is particularly suited for:

- Centralized account management. User accounts can be centrally managed; add/delete/change user accounts from a single point.
- Decentralized resource management or local system administration capability. Department domains can have their own administrators, who manage the resources in the department.
- Resources can be grouped logically, corresponding to local domains.

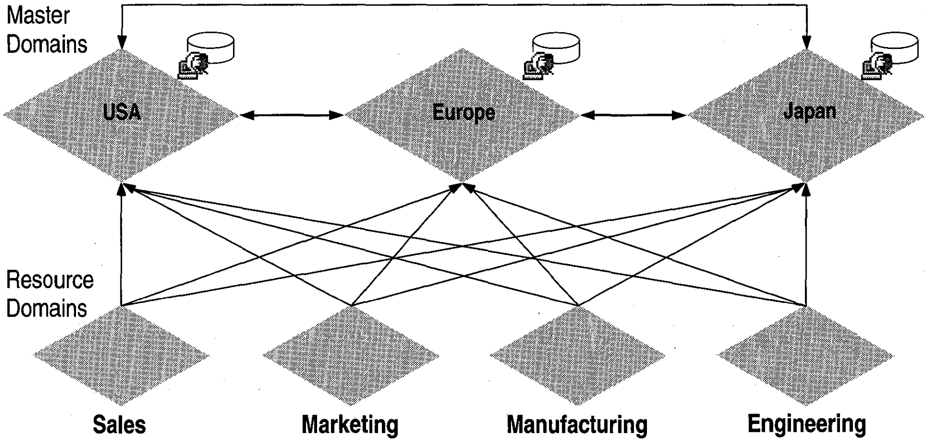
Additional Notes About the Single Master Domain Model

- Small offices/departments should not automatically be assigned to separate second-tier domains. Instead, they should be part of larger, adjacent resource domains. Keep the number of second-tier domains as small as possible.
- The single master domain model requires consideration in the placement of BDCs. Consider the following:
  - Resource domains that have a WAN connection to the master account domain controller should consider an on-site BDC for local authentication so that accounts can log on in the event that the WAN link becomes unavailable.
  - Resource domains that have a LAN connection to the master account domain controller do not require an on-site BDC.

Multiple Master Domain Model

With the multiple master domain model, there are two or more single master domains. Like the single master domain model, the master domains serve as account domains, with every user and machine account created and maintained on one of these master domains. A company's MIS groups can centrally manage these master domains. As with the single master domain model, the other domains on the network are called resource domains; they don't store or manage user accounts but do provide resources such as shared file servers and printers to the network.

In this model, every master domain is connected to every other master domain by a two-way trust relationship. Each resource domain trusts every master domain with a one-way trust relationship. The resource domains can trust other resource domains, but are not required to do so. Because every user account exists in one of the master domains, and since each resource domain trusts every master domain, every user account can be used on any of the master domains.



In this example, there is one machine account for each user account. Therefore, each master domain can contain as many as 26,000 user accounts. Users log on to the domain that contains their account. Each master domain contains one PDC and at least one BDC per 2000 user accounts to validate user logons and provide fault tolerance. The multiple master domain model incorporates all the features of a single master domain, and in addition accommodates:

- Organizations of more than 40,000 users. The multiple master domain model is scalable to networks with any number of users.
- Mobile users. Users can log on from anywhere in the network, anywhere in the world.

- Centralized or decentralized administration schemes.
- Organizational needs. Domains can be configured to mirror specific departments or internal company organizations.

Domain Models — Flexibility for Your Organization

Windows NT Server Directory Services and the Windows NT Server multiple domain structure provide the capability and scalability to accommodate any organization. This capability is provided with the Windows NT Server product; no special add-on products are needed.

The three domain models—single domain, single master domain, and multiple master domain—combined with trust relationships, allow for the flexibility needed for different organizations. Specifically, you can accommodate:

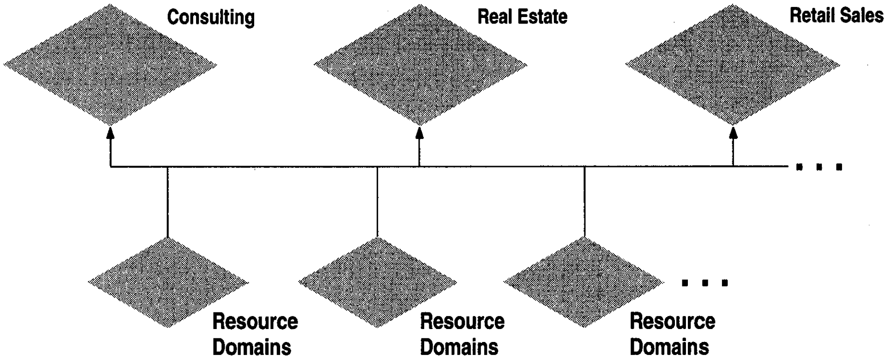
- Organizations with many small branch offices.
- Large organizations.
- Security for sensitive information.

In addition, expansion is easy. Offices can start out with separate domains and can link to each other later or can be added to existing domains.

There are many ways to implement your domain model. The following examples illustrate just some of the flexibility of domains.

Multiple Independent Lines of Business

Consider a corporation with fairly independent lines of business, perhaps a consulting business, a real estate business, and a retail sales business. Each division has its own marketing, sales, and data processing groups. However, at the center of the firm is a small group focused on functional services, such as accounting, finance, and human resources. For the most part, users in a division only need access to resources in that division (very much like a master domain scenario); however, there are instances, particularly in the central division, in which an employee will need access to resources in another division; thus the need to link the master domains together.

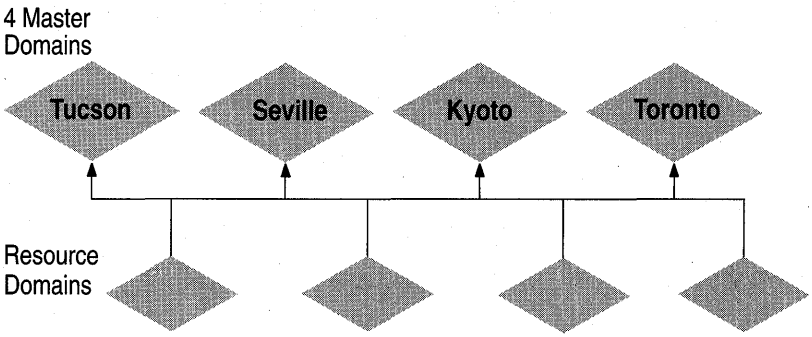


Multiple Master Domain: Multiple Independent Lines of Business

A multiple master domain was selected over a single master domain model because of the lack of a data processing staff in the central division. The domain model, then, can be constructed to acknowledge the data processing autonomy of divisions as it exists.

A Large Organization

This example is of a very large firm with approximately 100,000 employees in multiple locations. By using master domains, the number of users per master domain can go up to at least 26,000. To accommodate this scenario, the company can create a minimum of four master domains with approximately 25,000 user accounts and machine accounts each. If there are significantly fewer machine accounts, three master domains with a maximum of 40,000 user accounts each can be created.

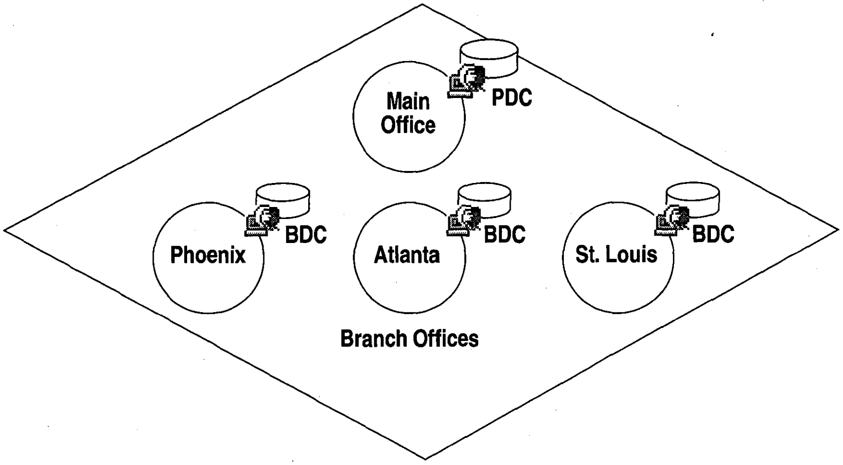


Multiple Master Domain for a 100,000-User Organization

The domain a user is defined in could be based on any grouping or sequencing such as alphabetical, divisional, departmental, or physical location. Which domain a user is defined in is unimportant since a trust relationship exists between each resource domain and each of the master domains.

Branch Offices

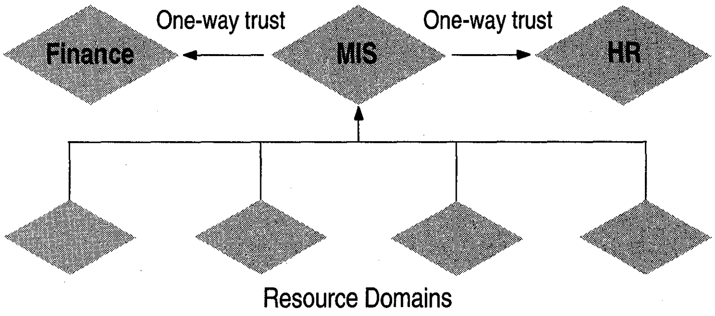
In a branch office scenario, a single domain or single master domain can be employed in most situations. Assuming that the branch office is linked to the PDC by means of a communications link or modem, a BDC would be the onsite server. The BDC handles local authentication as well as local file and print services. A second BDC can be added for fault tolerance.



Branch Office: A single domain provides connectivity; one on-site BDC per branch is required.

Secure Domains

In the multiple master domain model, all master domains are linked to each other by trust relationships so that users in all domains can access resources in any domain. However, in many organizations some departments have confidential information, such as financial records or human resources files. In this case, most of the organization can be served by a single master domain. Finance and HR have their own domains. They are trusted by the master MIS domain, but they do not trust other domains. This means that Finance and HR can access MIS resources, but their resources remain secure.



Secure Domains: Finance and HR domains can access resources in the rest of the organization, but other users cannot access their resources.

Planning for Your Domain Model

The domain model you select is based on the number of users in the organization and how you want to manage your organization. In addition, topology and location considerations will influence how domains are specifically implemented and where different resources are physically located.

Designing and building a domain strategy can be a challenging task, since there are few limits in the Windows NT software itself to dictate decision points. Other aspects of the computing environment must be considered to provide guidelines for the choices and decisions needed. This section presents a number of assumptions about the computing environment and discusses the domain models that apply.

- Even though Windows NT Server implies no limits on the number of users or sessions that can be supported by a single server, the hardware of the server does. The system needs resources to support users logging on. Unless otherwise noted, this paper assumes that the Windows NT Server computer being used as a PDC is a minimum 486/33 class machine with 32 MB of physical RAM memory, and a 1-GB hard disk. The test conditions included base Windows NT Server services, moderate file and print activity, RAS, Microsoft SNA Server, and Microsoft SQL Server.
- Real-life limits of the Windows NT Server system are beyond the simple capacity of the server. There are certain user expectations that must be satisfied, some under extremely harsh computing environments.
- The process of design and selection is recursive. Decisions made earlier in the process must be verified in light of information available later in the process. Therefore, you should anticipate making several passes through the process until all decisions match with the information available at all steps.

Management and Administration Considerations

Windows NT allows you to centrally or decentrally manage user accounts for your organization. With centralized management, there is usually one SAM and therefore one master domain where all user account information is stored. Users are defined once on the network and given permissions to resources based on their logon identity in the central user database. The single domain model and single master domain models are centrally managed. A multiple master domain model can also be managed centrally by adding designated administrators to the appropriate Domain Admin groups.

With decentralized management, there is more than one SAM containing information about different user accounts in the organization. You can create trust relationships to enable domains to access resources in other domains. The multiple master domian model and the single domian models can make use of decentralized management.

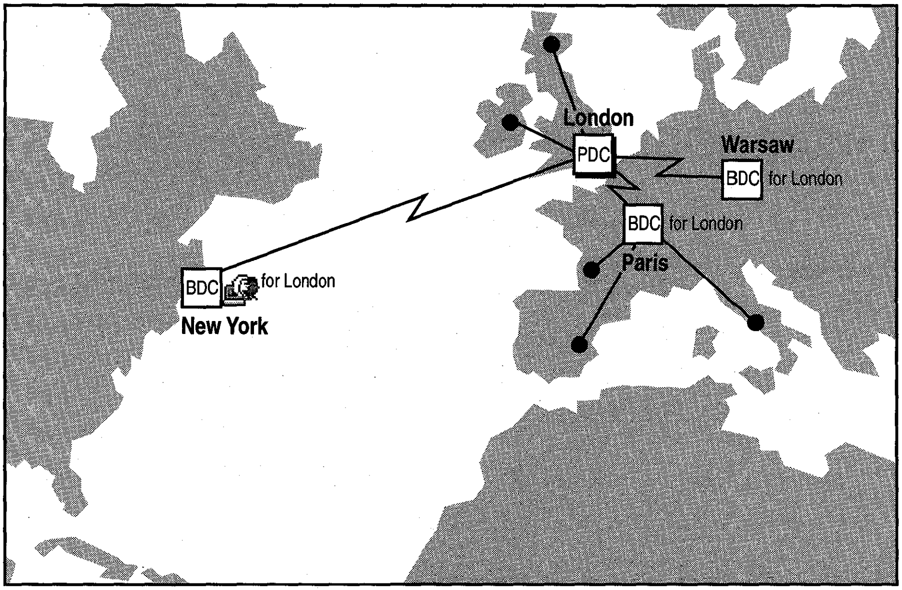
In addition, in planning for your domain model, you'll need to establish administrative policies and procedures for:

- Managing and monitoring domain(s) and accounts.
- Managing and monitoring resources.
- Establishing addressing and naming conventions.

Location Considerations

The most important location considerations are where to locate BDCs that will act as account logon servers and how to plan account replication traffic across WAN links. If your WAN speed or bandwidth is too low, you will want to arrange for logon to occur at a local backup domain controller.

Think of your networked organization in terms of sites. A site is a well-connected LAN—it may be separated by fast links such as bridges and routers, but not asynchronous (WAN) links such as T1, 56K, or ISDN. In most cases, sites correspond to physical locations such as Seattle, Paris, New York, and so on. Is your networked organization one location (a well-connected LAN), or does it consist of several locations connected by WAN links?



WAN Connectivity

The physical distribution of BDCs is determined by several factors: line speed, link reliability, administrative access, protocol, user authentication requirements, the number of users to be supported at a site, and locally available resources.

The preceding diagram represents a part of the network topology that one of these domains will have to service. There are several networked hub sites out of London that would be part of a CentralEurope domain.

This diagram also shows that the European PDCs reside in London, the main hub to all of Europe. The European PDCs will then replicate to each of their European backup domain controllers at each site, including New York. The CentralEurope PDC replicates all changes to the CentralEurope BDCs. These changes include anything from a user password change to adding accounts or groups.

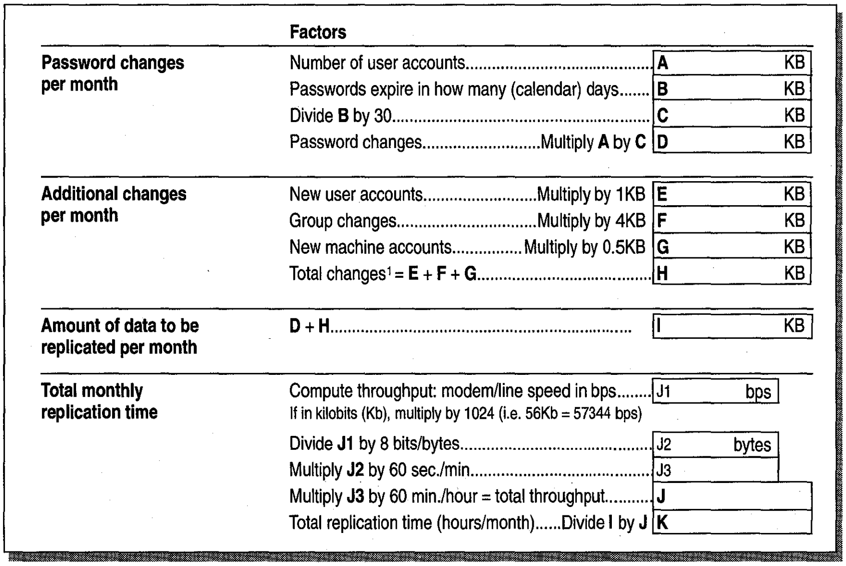
Replication over WAN and RAS

Consideration should be given to the amount of traffic that replication places on the WAN or a RAS dial-up line. In particular, avoid doing full synchronization across WAN links. Full synchronizations are required when first setting up a new PDC or bringing a new location online. Full synchronizations are also initiated when more than 2000 changes happen to user/groups within a short period of time (less than one hour). This is configurable by increasing the size of the change log. If you anticipate high change activity, you may wish to increase the value of this parameter.

Calculating Replication Times

An important part of administration is managing the amount of network traffic so that response time remains acceptable. When the PDC is located across a WAN or modem link, you can estimate the amount of traffic and time needed to replicate SAM changes to and from the PDC and then schedule this traffic to meet the needs of the site. The following chart helps you calculate the time needed for replication:

Job Aid 1: Calculate Monthly Replication Time Microsoft Windows NT Server



	Factors		
Password changes per month	Number of user accounts..	A	KB
	Passwords expire in how many (calendar) days.......	B	KB
	Divide **B** by 30...	C	KB
	Password changes...........................Multiply **A** by **C**	D	KB
Additional changes per month	New user accounts..........................Multiply by 1KB	E	KB
	Group changes................................Multiply by 4KB	F	KB
	New machine accounts................Multiply by 0.5KB	G	KB
	Total changes[1] = **E** + **F** + **G**.......................................	H	KB
Amount of data to be replicated per month	**D** + **H**..	I	KB
Total monthly replication time	Compute throughput: modem/line speed in bps........ If in kilobits (Kb), multiply by 1024 (i.e. 56Kb = 57344 bps)	J1	bps
	Divide **J1** by 8 bits/bytes..	J2	bytes
	Multiply **J2** by 60 sec./min...	J3	
	Multiply **J3** by 60 min./hour = total throughput..........	J	
	Total replication time (hours/month)......Divide **I** by **J**	K	

[1] If user, group, and machine changes cannot be predicted, use 5% of **D** as an estimate.

Putting it all Together: Selecting Your Domain Model

For ease of administration, the preferred domain model is the single domain model. If the single domain model cannot be used, the second choice should be the single master domain model. If neither of these is available, an administrator can use trust relationships to centralize all user administration into a single domain, eliminating the need to administer each domain separately.

Tools and Checklists

Domain Selection Matrix

This section discusses various tools and checklists useful in selecting your domain model.

It is useful to view the characteristics of the domain models side by side, to match the characteristics and benefits of each implementation model to the needs of your organization. If the needs of your organization change over time, you can review this matrix to determine if the optimal implementation model should change. Conversely, if you have established an implementation model already, you might review this chart to see which additional benefits or trade-off decisions are related to an alternative domain model strategy.

Domain Selection Matrix

Domain Attribute	Single Domain	Single Master Domain	Multiple Master Domain	Independent Single Domains w/Trust relationships
less than 40,000 users/domain	x	x		
more than 40,000 users/domain			x	
centralized account management	x	x	x[1]	
centralized resource management	x			
decentralized account management			x[1]	x
decentralized resource management		x	x	x
central MIS	x	x	x	
no central MIS				x

[1] It is possible to have either centralized or decentralized account management under the multiple master domain model.

Location Considerations Checklist

- Where will users log on? Ensure adequate access to an authenticating BDC.
- Do users need to be able to log on from more than one location? If so, their account cannot be tied to that location, implying a single master domain or multiple master domain model.
- What are the availability requirements?
- Does a user need to be able to log on if the WAN to the central location is down (for example, if all data is central and no local processing can be done)?
- How fast are the WAN links? The speed of the links needed between locations should be determined by the usage of resources across the links, and also the frequency of changes to user/group settings.

Hardware Requirements

When selecting a computer for use as a PDC or BDC, use the following hardware guidelines:

PDC/BDC Hardware Requirements

SAM file size	Number of User accounts[1]	Minimum CPU Needed	Required RAM[2]
5 MB	up to 3000	486DX/33	32 MB
10 MB	7500	486DX/66	32 MB
15 MB	10,000	Pentium, MIPS, Alpha AXP	48 MB
20 MB	15,000	Pentium, MIPS, Alpha AXP	64 MB
30 MB	20,000 - 30,000	Pentium, MIPS, Alpha AXP	128 MB
40 MB	30,000 - 40,000	Pentium, MIPS, Alpha AXP	166 MB

[1] User account numbers are approximate. The exact SAM file size is dependent on the number of user accounts, machine accounts, and group accounts.

[2] RAM memory should equal at least 2.5 times the size of the SAM

For more information, refer to the *Large Domain Testing Overview* document, available from Microsoft Product Support services.

How Many Domains Are Needed?

As described earlier, the number of users in a domain is a function of the size of the SAM database. The following chart can help you determine the number of domains you need. Note that the single domain and single master domain models can accommodate at least 26,000 user accounts if both user accounts and machine accounts are stored in the SAM database.

Job Aid 2: Calculate Number of Master Domains Microsoft Windows NT Server

	Factors			
Calculate SAM database size	Number of users	Multiply by 1KB	**A**	KB
	Number of machines (workstations, servers, printers, etc.)	Multiply by 0.5KB	**B**	KB
	Number of custom groups	Multiply by 4KB	**C**	KB
	Built-in local groups		**D**	**44** KB
	Total SAM size	**A** + **B** + **C** + **D** =	**E**	KB
	Convert SAM size to MB	Multiply **E** by .001024	**F**	MB

Minimum # of domains = **F** / 40[1] ____________
(round up to next whole number)

[1] Maximum recommended SAM database size is 40MB

How Many BDCs Are Needed?

The ratio of workstations to servers in a domain is a way of maintaining a level of responsiveness during the logon process. Additional backup domain controllers (also called domain servers) allow for more users to log on simultaneously. One BDC can support up to 2000 users.

The server configuration in this table is a 486/66 with 32 MB of RAM, running Windows NT Server.

BDCs per Number of User Accounts

Number of workstations	Number of BDC Servers
10	1
100	1
500	1
1,000	1
2,000	1
5,000	2
10,000	5
20,000	10
30,000	15

Consider performing the initial setup of all BDCs on-site or over high speed links, because each new BDC will need a full synchronization with the PDC. At many companies, BDCs are set up at the same site as the PDC and then shipped to the intended location. This is the most efficient alternative for sites that have only low-speed or RAS access.

Planning for Future Versions of Windows NT Server

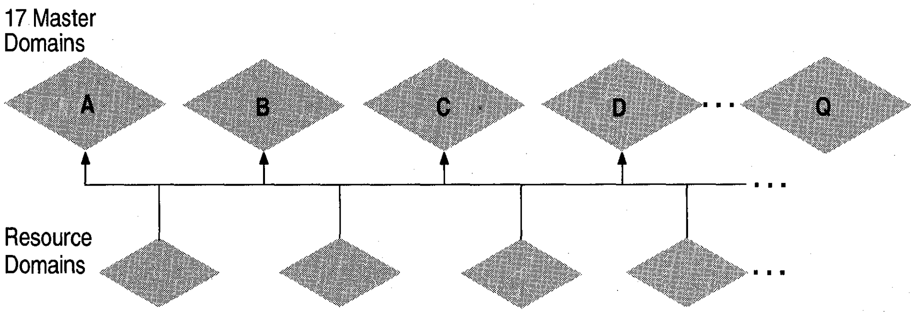
The next major release of the Windows NT operating platform, code-named "Cairo," will further enhance the Windows NT Server Directory Services model. This model will provide a hierarchical structure scaling easily from small to large organizations. All domain controllers will hold master copies of the SAM database.

To accommodate phased migration, the design of the Cairo domain model will allow interoperability with existing Windows NT domains from day one. Windows NT domain accounts can be migrated to Cairo as business needs dictate.

Case Study: Microsoft Corporation Worldwide Network

Microsoft currently has approximately 16,000 user accounts and 35,000 network nodes worldwide. The Microsoft staff is evenly divided: approximately one half of the employees are located at or near the Redmond, Washington, campus, and the other half are distributed among approximately 150 sites in 52 countries. All sites require full access to information and electronic mail.

In order to fulfill the goals of worldwide access to corporate information and to demonstrate its commitment to Windows NT Server technology, Microsoft designed its worldwide network around the Window NT domain structure.



A Multiple Master Domain Model

The goals of Microsoft's worldwide domain strategy include:

- Optimum availability to all Microsoft sites.
- Centralized support and administration.
- The ability to recover from an extended WAN link interruption without requiring a full synchronization of the SAM to the PDC.

In order to meet these goals, the Microsoft International Technology Group (ITG) implemented a multiple master domain model, using a relatively small number of master user domains (first tier) administered by Microsoft ITG, using DHCP to compensate for the use of slow WAN links, and using PDCs and BDCs strategically placed to provide optimum availability and performance. The multiple master domain model was selected when Windows NT Advanced Server 3.1 was installed, and the model was not modified when the company upgraded to Windows NT Server 3.5.

Many sites are connected to the network by (slower) 64K links. These are not yet cost-effective to upgrade or, in some cases, an upgrade is not available for that specific location. ITG provides administration of any second-tier domain that is so requested.

Microsoft ITG worked to keep the number of master user domains as small as possible in order to:

- Keep administration centralized.
- Make global groups feasible.
- Require few specialized administrative tools.

Microsoft ITG chose to limit the number of departmental, site, and developer server domains because it is easier to divide large domains in the future than try and combine many small ones into a larger domain. For example, there is one ITG-NETWORKS domain. All servers for the Corporate Networks department are maintained in this one domain.

Implementation

Again, Microsoft employs the multiple master domain strategy. Because every user and global group account in the company exists in one of the master user domains, and because all the domains in the company trust every master user domain, every user and global group account in the company is functional in all domains.

In all cases, ITG has full administrative permissions on all the domains in the model. This is so that all domain controllers can be backed up and restored, and updated with current builds and new system configuration files.

There are some disadvantages to this model. The most challenging issue is administration of individualized global groups. Creation and administration of global groups becomes impractical to manage unless it can be done based on a database against which data can be compared. This allows for an automatic update if an individual no longer requires membership in that group. ITG provides global groups based on department accounts, and updates membership based on HR records. Additional global groups are reviewed on a case-by-case basis. Users are added to a master user domain based on their current geographic location. If a user moves to a different site within Microsoft (for example, Redmond to Northern Europe), he/she will be removed and added to the appropriate master user domain.

Windows for Workgroup-based systems belong to a second-tier domain to ensure that they have full access to the domain model. They use their account on the master user domain and use the second-tier domain as their workgroup. This allows them to access servers in the domain that are using Windows NT security.

All Windows NT Server-based systems running Remote Access Services (RAS) are located in a second-tier domain. Because there is a trust relationship between all the domains in the corporate model, a user can dial into any RAS server anywhere in the model without needing additional administration.

Administration

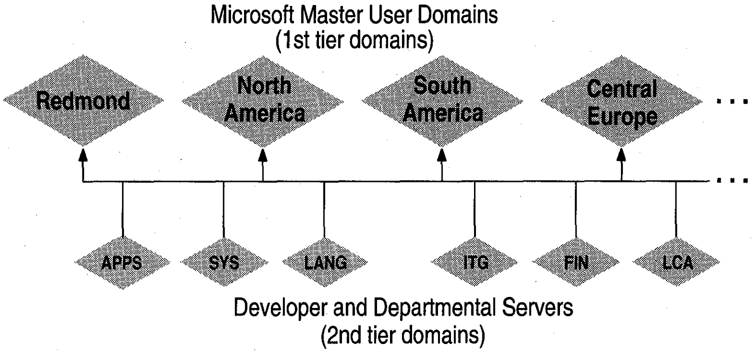
ITG has sole authority to establish a trust relationship between the master domains and another domain on the Microsoft corporate network. ITG has administrative ability on all servers running Windows NT Server in a trust relationship within the Microsoft domains structure.

Microsoft ITG uses the following criteria to establish a trust relationship with a second-tier domain:

- Any product development group is eligible to create one second-tier domain with trust relationships to the Master User Domains, until every defined development business unit has a second-tier domain. For example, Apps-Word, Apps-Excel, Sys-WFW, or Sys-WinNT.
- Every non-Redmond campus site is eligible to create one resource domain with trust relationships with the Master User Domains. For example: USA-Atlanta, USA-Chicago, FRA-Paris, GER-Munich, and every site city name.
- ITG uses a standard administrative account that is part of the second-tier Domain Administrators group. This allows ITG to perform administrative duties and assist the domain administrator when needed. It also allows ITG to perform backups of the servers in the domain.

The Microsoft Worldwide Domain Model

The master user account domains contain all the user accounts for the entire domain structure worldwide. Master user domain names represent the geographic location of users to assist in distribution of backup domain controllers.



Microsoft Domain Model

Two categories of administration are acknowledged at Microsoft. ITG is solely responsible for administration of some domains. Other domains are jointly administered by ITG and specific user groups, such developers, sites, and others. Domain administration permissions can be given to a group of users within their second-tier domain. ITG retains the option of allowing any of the departmental server domains to have their own domain administrators and ITG administration.

Domain Controller Locations

ITG provides master user domains (first-tier) that are used by a specific set of sites. The name and size of these master user domains are determined by geographic limitations, network topology, and the number of accounts to be supported. The PDC for the master user domains for Redmond, NorthAmerica, and SouthAmerica, are located in Redmond. Others are located near the constituent user population where local data centers provide administrator resources. A BDC for the master user domain is located at each respective remote site for authentication of accounts at that site.

The European master user domain PDCs are physically located in England, with a BDC for the appropriate European master user domain located in each respective European site.

A BDC for the global master user domain is also physically located at each network hub site worldwide.

Special Domain Considerations

Microsoft maintains two domains that, due to business security reasons, have restricted access to or from the other domains.

- The Microsoft Human Resources group, because of the confidential nature of its information, maintains a secure network with its master domain isolated from the other domains on the network. It is also separately wired so that it is not physically connected to the other network.
- Microsoft created a separate master domain for use by its vendors. Servers in the Vendor domain are used as "drop off" points for vendors. Regular Microsoft employees can access the domain via a one-way trust relationship, but vendors are restricted to the Vendor domain.

WAN Protocols

On the Microsoft corporate network, TCP/IP is used by Windows NT Server to forward authentication requests between domain controllers across a WAN. Every server in the master user domain can process logon requests from the domain's user accounts.

DHCP/WINS

Every server in the corporate domain model runs TCP/IP. Adding DHCP to Microsoft's network has significantly reduced administrative overhead for WAN management because individual machine TCP/IP addresses are configured automatically by DHCP.

Naming Conventions

Microsoft devised a naming convention for the corporate domain structure to provide a consistent interface to the worldwide user community. The naming convention for second-tier domains is based on geographic location (USA-Atlanta), business (ITG-Networks), or development group (Apps-Word).

Master User Domains (1st Tier)

Redmond	SouthernEurope	FarEast	SouthAmerica
NorthernEurope	NorthAmerica	MiddleEast	SouthPacific
CentralEurope	Africa		

Departmental and Site Resource Domains (2nd Tier)

SYS-WINNT	APPS-EXCEL	ITG-SQL	PSS-LP
SYS-MSDOS-WIN	APPS-WORD	ITG-NETWORKS	PSS-BP
SYS-BUSINESS	APPS-POWERPOINT	ITG-APPS	PSS-RWG
SYS-HARDWARE	AT-RESEARCH	ITG-DEVELOPMENT	USA-DENVER
SYS-MARKETING	APPS-MULTIMEDIA	FIN-ACCTSVRS	USA-ATLANTA
OPS-MSPRESS	FRA-PARISEHQ	GER-MUNICH	SWI-NYON
OPS-FACILITIES	AUT-VIENNA	GER-BERLIN	POL-WARSAW

The preceding list is a sample of some of the domains currently established. The general rule is to use *{division}-{department}*. Encompassing the largest practical group is an additional guiding factor in establishing the domain name.

Site domains are determined by *{country code}-{city name}*. Every site is permitted one resource domain in the corporate domain model.

Reference Materials

The following sections provide further reading material.

Frequently Asked Questions – Domains and SIDs

What is so special about the SID of the domain?
Once you decide to install Windows NT Server in a particular domain, you are committed to that domain. This is because of the domain's SID. Installing Windows NT Server creates an account database that contains the domain's SID. This SID is used for all accounts in the domain.

How do I change domain names?
You will need to reinstall Windows NT Server on the PDC and all BDCs. Because the domain's SID (rather than the domain's name) uniquely identifies the domain, the administrator can change the domain's name if the need arises. The new name is simply associated with the existing SID.

The PDC's domain name must be changed first. Then the domain name in all the other computers in the domain must be changed to the new domain name. The only way a machine can be separated from its domain's SID is through a reinstallation. This means that to change a domain's SID, the administrator must reinstall Windows NT Server.

Do all user SIDs change when the domain name changes?
No SIDs will change at all. Only the domain name changes.

Can users of the changed domain still access resources on other machines?
Yes, in the same domain. However, all existing trust relationships will be broken and will require reestablishment with the new domain name. As a result, all access rights associated with users from the trusted domain will also need to be reestablished.

Backup Domain Controller over a RAS Link

A Backup Domain Controller (BDC) can be connected to a remote domain using Windows NT Server's Remote Access Service (RAS) and a modem connection.

Using a RAS-connected BDC as a PDC

If the RAS-connected BDC is ever expected to be promoted to Primary Domain Controller (PDC) while it is remotely connected to the domain, this BDC should be set up as a dial-out-only RAS client (RAS is not running on this computer). If you promote the RAS-connected client, NetLogon stops, changes roles, and restarts. RAS is dependent on NetLogon, so when NetLogon stops, you would lose your connection. By having just the RAS client dial-out services on this remote BDC, it can function as a PDC because that functionality does not depend on NetLogon running constantly. If neither the RAS server (which could also be a BDC) nor the RAS-connected BDC are expected to ever serve as PDC, this is not an issue. A RAS-connected BDC that has been promoted to PDC functions as it should, but possibly with slower response time, depending on line speed.

Partial Synchronization with a RAS-connected BDC

If a remote site has a RAS-connected BDC that dials in nightly to do a partial synchronization of any changes, and on some days 2000 changes are made to the SAM/LSA database, then the default ChangeLogSize should be increased. This may be necessary if any BDC has been off-line while a lot of changes have occurred, or else this BDC may be forced to do a full synchronization of the database. If minimal changes (for example, fewer than 2000) occur during the time the RAS BDC or any BDC does not have a physical connection to the PDC, then the default size is sufficient. If an administrator begins to notice any BDCs doing full synchronizations, it could be that many changes are occurring and the ChangeLogSize needs to be increased. The default ChangeLogSize is 64K which is approximately 2000 changes.

Pass-Through Authentication

When a user logs on to a domain in which trust relationships are established between domains, the account is verified by the process of *pass-through authentication.* Pass-through authentication makes it possible for users to log on from machines or domains in which they have no account. With pass-through authentication, a user can have an account on only one domain and still access the entire network—including all its trusted domains.

When a user logs on to a resource (trusting) domain, an access token containing the user's SID will be passed on to the account (trusted) domain. Authentication of both the user's identity and password will actually take place within the account domain, hence the name pass-through authentication. This mechanism effectively allows a user to have an account in only one domain and yet access the entire network using trusted domains.

For example, in a large network consisting of several domains linked by trust relationships, a user can log on at a machine in Domain A and be verified by the user accounts database in Domain B.

Pass-through authentication occurs under one of these circumstances:

- At initial logon from a workstation when a user is logging on to a trusted domain.
- When accessing a resource in a trusting domain.

It does not matter where the users are physically located. It only matters where their accounts reside. As long as a user has an account in the trusted domain, the user can log on from anywhere in any domain, provided that the domain is connected by a trust to the account domain. In other words, users can log on from any trusting domain as long as they log on to the trusted account domain.

For more information on pass-through authentication and how accounts are actually verified, see the *Windows NT Resource Kit, Volume 2: Windows NT Networking Guide.*

Suggested Domain Naming Conventions

It is recommended that domain names not change frequently. Changing domain names requires the *reinstallation* of every server that belongs to the domain whose name has been changed. For clarity, domain names should be reflective of the general business areas they serve.

Group Naming/Assignment Conventions

For the XYZ Corporation, a global group will be defined for every Resource Domain that includes all of the users who use that domain as their primary resource base. For both models, global groups will be created for all departments/locations and the members of each department will automatically be made members of their department groups. The group name should be reflective of the domain and the department (XYZ-UK). Other groups may be created for job categories (XYZ-UK-MANAGERS).

Username Conventions

Ideally one user ID/password would allow access to all of a user's resources. If you want to take advantage of Microsoft's Client Services for NetWare®, in which the Windows NT username and password is passed through to NetWare, then set up the user account on NetWare with the same account name and password as in Windows NT. If there is no capability to send the user's password to other systems (such as Banyan® Vines®, or some databases), the next best thing is to at least have a consistent full name property within each company organization.

Index

IMPORTANT—READ CAREFULLY BEFORE OPENING SOFTWARE PACKET(S). By opening the sealed packet(s) containing the software, you indicate your acceptance of the following Microsoft License Agreement.

MICROSOFT LICENSE AGREEMENT

(Resource Kit Companion Disks)

This is a legal agreement between you (either an individual or an entity) and Microsoft Corporation. By opening the sealed software packet(s) you are agreeing to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, promptly return the unopened software packet(s) and any accompanying written materials to the place you obtained them for a full refund.

MICROSOFT SOFTWARE LICENSE

1. GRANT OF LICENSE. Microsoft grants to you the right to use one copy of the Microsoft software program included with this book (the "SOFTWARE") for your internal use. The SOFTWARE is in "use" on a computer when it is loaded into the temporary memory (i.e., RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer.

2. COPYRIGHT. The SOFTWARE is owned by Microsoft or its suppliers and is protected by United States copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE like any other copyrighted material (e.g., a book or musical recording). You may not copy the written materials accompanying the SOFTWARE.

3. OTHER RESTRICTIONS. You may not rent or lease the SOFTWARE, but you may transfer the SOFTWARE and accompanying written materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement. You may not reverse engineer, decompile, or disassemble the SOFTWARE. If the SOFTWARE is an update or has been updated, any transfer must include the most recent update and all prior versions.

DISCLAIMER OF WARRANTY

The SOFTWARE (including instructions for its use) is provided "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT FURTHER DISCLAIMS ALL IMPLIED WARRANTIES INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE OR AGAINST INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE AND DOCUMENTATION REMAINS WITH YOU.

IN NO EVENT SHALL MICROSOFT, ITS AUTHORS, OR ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION, EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

U.S. GOVERNMENT RESTRICTED RIGHTS

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software — Restricted Rights 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

If you acquired this product in the United States, this Agreement is governed by the laws of the State of Washington.

Should you have any questions concerning this Agreement, or if you desire to contact Microsoft Press for any reason, please write:
Microsoft Press, One Microsoft Way, Redmond, WA 98052-6399.

Microsoft® Windows NT™ Resource Kit

Version 3.51 Update

Update for Owners of the Windows NT Resource Kit Version 3.5

CD INCLUDED

New Utilities on the Resource Kit Update CD Include:

- Scripting languages PERL5 and REXX for Windows NT
- New Internet server software, including WEB, HCT, and Gopher
- Internet and TCP/IP services and tools, including Mail Server, a Simple Mail Transport Protocol (SMTP) and Post Office Protocol (POP) server

MICROSOFT® WINDOWS NT™

U.S.A.	**$39.95**
U.K.	£37.49 [V.A.T. included]
Canada	$53.95

[*Recommended*]

This Update for Owners of the WINDOWS NT RESOURCE KIT, Version 3.5 Covers New Features in Version 3.51 and the PowerPC® Version of Windows NT

The WINDOWS NT UPDATE provides owners of the WINDOWS NT RESOURCE KIT, version 3.5, with the information and tools they need to update their kits to version 3.51. This volume covers the features that are new to Windows NT version 3.51 and updates and corrects the four main volumes in the Resource Kit. It also contains an updated version of the Resource Kit CD, which includes many new utilities, technical updates of the main utilities, and support for the PowerPC. To use this update effectively, you must have the four-volume WINDOWS NT RESOURCE KIT for version 3.5. If you do not, you should purchase the full WINDOWS NT RESOURCE KIT for version 3.51.

Inside This Book, You'll Find New Technical and Support Information Covering:

- The enhanced Setup program in version 3.51 of Windows NT Workstation and Windows NT Server, including a discussion of the Resource Kit utilities designed to make installation easier
- Security and the issues that administrators of computers and computer networks face every day, including a full discussion of the C2CONFIG utility on the Resource Kit CD, which helps configure a computer system that complies with the Federal requirements for C2-level security certification
- Internet services and security, including a discussion of the Resource Kit utilities that make Windows NT Server an excellent platform for Internet information providers
- Troubleshooting tips for version 3.51

ISBN 1-55615-929-3

90000

Microsoft Press

Operating Systems/Windows NT