
Microsoft®
Windows™ for Workgroups
Resource Kit
Addendum for Version 3.11

Complete Technical Information
for the Support Professional
for Microsoft Windows for Workgroups
Version 3.11

Microsoft Corporation

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.

© 1993 Microsoft Corporation. All rights reserved.

Printed in the United States of America. 1 2 3 4 5 6 7 8 9

Microsoft, MS, and MS-DOS are registered trademarks and Windows, the Windows logo, Windows NT and Microsoft At Work are trademarks of Microsoft Corporation.

Document No. 0030-54303

3+ is a registered trademark of 3Com Corporation. 3+Open is a trademark of 3Com Corporation. 3+Share is a registered trademark of 3Com Corporation. 3Com is a registered trademark of 3Com Corporation. ArcNet is a registered trademark of Datapoint Corporation. AS/400 is a registered trademark of International Business Machines Corporation. Banyan is a registered trademark of Banyan Systems, Inc. COMPAQ is a registered trademark of Compaq Computer Corporation. CompuServe is a registered trademark of CompuServe, Inc. DCA is a registered trademark of Digital Communications Associates, Inc. DEC is a registered trademark of Digital Equipment Corporation. DeskJet is a registered trademark of Hewlett-Packard Company. Epson is a registered trademark of Seiko Epson Corporation, Inc. EtherExpress is a trademark of Intel Corporation. EtherLink is a registered trademark of 3Com Corporation. Everex is a trademark of Everex Systems, Inc. ExecJet is a registered trademark of International Business Machines Corporation. GENie is a trademark of General Electric Corporation. Hercules is a registered trademark of Hercules Computer Technology, Inc. Hewlett-Packard is a registered trademark of Hewlett-Packard Company. IBM is a registered trademark of International Business Machines Corporation. Intel is a registered trademark of Intel Corporation. Kodak is a registered trademark of Eastman Kodak Company. LaserJet is a registered trademark of Hewlett-Packard Company. Linotronic is a trademark of Linotype AG and its subsidiaries. Logitech is a trademark of Logitech, Inc. Lotus is a registered trademark of Lotus Development Corporation. Lotus Notes is a registered trademark of Lotus Development Corporation. Mac is a registered trademark of Apple Computer, Inc. Macintosh is a registered trademark of Apple Computer, Inc. Micro Channel is a registered trademark of International Business Machines Corporation. NEC is a registered trademark of NEC Corporation. NetWare is a registered trademark of Novell, Inc. Novell is a registered trademark of Novell, Inc. Okidata is a registered trademark of Oki America, Inc. Olivetti is a registered trademark of Ing. C. Olivetti. Operating System/2 and OS/2 are registered trademarks of International Business Machines Corporation. OS/400 is a registered trademark of International Business Machines Corporation. PaintJet is a registered trademark of Hewlett-Packard Company. Panasonic is a registered trademark of Matsushita Electric Co., Ltd. Pathworks is a trademark of Digital Equipment Corporation. PC/XT is a trademark of International Business Machines Corporation. Personal Computer AT is a registered trademark of International Business Machines Corporation. Personal Computer XT is a trademark of International Business Machines Corporation. Personal System/1 is a trademark of International Business Machines Corporation. Personal System/2 is a registered trademark of International Business Machines Corporation. Philips is a registered trademark of Philips International B.V. PostScript is a registered trademark of Adobe Systems, Inc. Quietwriter is a registered trademark of International Business Machines Corporation. Rumba is a registered trademark of Wall Data Incorporated. SatisFAXtion is a registered trademark of Intel Corporation. Sound Blaster is a trademark of Creative Technology Ltd. Sound Blaster Pro is a trademark of Creative Technology Ltd. Stacker is a trademark of STAC Electronics. PC-NFS is a registered trademark of Sun Microsystems, Incorporated. System/360 is a trademark of International Business Machines Corporation. TCS is a registered trademark of Eurotherm International P.L.C. Tektronix is a registered trademark of Tektronix, Inc. Texas Instruments is a registered trademark of Texas Instruments, Inc. ThinkJet is a registered trademark of Hewlett-Packard Company. TokenExpress is a trademark of Intel Corporation. Toshiba is a registered trademark of Kabushiki Kaisha Toshiba. Triumph is a registered trademark of Triumph Adler AG. TrueType is a registered trademark of Apple Computer, Inc. Tulip is a registered trademark of Tulip Computers International, BV. Unisys is a registered trademark of Unisys Corporation. Vectra is a registered trademark of H-P Company. Video Seven is a trademark of Headland Technology, Inc. VINES is a registered trademark of Banyan Systems, Inc. VMS is a registered trademark of Digital Equipment Corporation. WANG is a registered trademark of Wang Laboratories. Western Digital is a trademark of Western Digital Corporation. WYSE is a registered trademark of Wyse Technology. Xerox is a registered trademark of Xerox Corporation. XGA is a registered trademark of International Business Machines Corporation. XT is a trademark of International Business Machines Corporation. Zenith is a registered trademark of Zenith Data Systems Corporation.

All other trademarks, marked and not marked, are the property of their respective owners.

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 ("Agreement").

MICROSOFT LICENSE AGREEMENT.
(Microsoft Windows for Workgroups Resource Kit, version 3.11)

This is a legal agreement between you (either an individual or an entity), and Microsoft Corporation. **By opening the enclosed sealed disk package(s) and/or by using the SOFTWARE 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 disk package(s) and the accompanying items (including printed materials and binders or other containers) to the place you obtained them for a full refund.**

MICROSOFT SOFTWARE LICENSE

1. **GRANT OF LICENSE.** This Agreement permits you to make and use copies of the enclosed Microsoft software program (the "SOFTWARE") for your internal use only provided that (a) the SOFTWARE is not modified in any way and (b) you maintain the copyright notice on all copies of the SOFTWARE.

2. **COPYRIGHT.** The SOFTWARE (including any images, "applets", photographs, animations, video, audio, music, and text incorporated into 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 printed materials accompanying the SOFTWARE.

3. **OTHER RESTRICTIONS.** You may not rent or lease the SOFTWARE, but you may transfer the SOFTWARE and accompanying printed 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.

4. **DUAL MEDIA SOFTWARE.** If the SOFTWARE package contains both 3.5" and 5.25" disks, then you may use only the disks appropriate for your single-user computer. You may not use the other disks on another computer or loan, rent, lease, or transfer them to another user except as part of the permanent transfer (as provided above) of all SOFTWARE and printed materials.

LIMITED WARRANTY

NO WARRANTIES. To the maximum extent permitted by applicable law, Microsoft expressly disclaims any warranty for the SOFTWARE. The SOFTWARE and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability or fitness for a particular purpose. The entire risk arising out of use or performance of the SOFTWARE remains with you.

CUSTOMER REMEDIES. Microsoft's entire liability and your exclusive remedy shall not exceed the price paid for the SOFTWARE.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall Microsoft or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profit, business interruption, loss of business information, or any other pecuniary loss) arising out of the use or inability to use this Microsoft product, even if Microsoft has been advised of the possibility of such damages. Because some states/jurisdictions 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 at 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.

If you acquired this product in Canada, this Agreement is governed by the laws of the Province of Ontario, Canada. Each of the parties hereto irrevocably attorns to the jurisdiction of the courts of the Province of Ontario and further agrees to commence any litigation which may arise hereunder in the courts located in the Judicial District of York, Province of Ontario.

If this product was acquired outside the United States, then local law may apply.

Should you have any questions concerning this Agreement, or if you desire to contact Microsoft for any reason, please contact the Microsoft subsidiary serving your country, or write: Microsoft Customer Sales and Service/One Microsoft Way/Redmond, WA 98052-6399.

Si vous avez acquis votre produit Microsoft au CANADA, la garantie limitée suivante vous concerne :

GARANTIE LIMITÉE

EXCLUSION DE GARANTIES. Microsoft renonce entièrement à toute garantie pour le LOGICIEL. Le LOGICIEL et toute autre documentation s'y rapportant sont fournis « comme tels » sans aucune garantie quelle qu'elle soit, expresse ou implicite, y compris, mais ne se limitant pas aux garanties implicites de la qualité marchande ou un usage particulier. Le risque total découlant de l'utilisation ou de la performance du LOGICIEL est entre vos mains.

RECOURS DU CLIENT. La seule obligation de Microsoft et votre recours exclusif n'excéderont pas le prix payé pour le LOGICIEL.

ABSENCE DE RESPONSABILITÉ POUR LES DOMMAGES INDIRECTS. Microsoft ou ses fournisseurs ne pourront être tenus responsables en aucune circonstance de tout dommage quel qu'il soit (y compris mais non de façon limitative les dommages directs ou indirects causés par la perte de bénéfices commerciaux, l'interruption des affaires, la perte d'information commerciale ou toute autre perte pécuniaire) résultant de l'utilisation ou de l'impossibilité d'utilisation de ce produit, et ce, même si la société Microsoft a été avisée de l'éventualité de tels dommages. Certains états/juridictions ne permettent pas l'exclusion ou la limitation de responsabilité relative aux dommages indirects ou consécutifs, et la limitation ci-dessus peut ne pas s'appliquer à votre égard.

La présente Convention est régie par les lois de la province d'Ontario, Canada. Chacune des parties à la présente reconnaît irrévocablement la compétence des tribunaux de la province d'Ontario et consent à instituer tout litige qui pourrait découler de la présente auprès des tribunaux situés dans le district judiciaire de York, province d'Ontario.

Au cas où vous auriez des questions concernant cette licence ou que vous désiriez vous mettre en rapport avec Microsoft pour quelque raison que ce soit, veuillez contacter la succursale Microsoft desservant votre pays, dont l'adresse est fournie dans ce produit, ou écrire à : Microsoft Customer Sales and Service, One Microsoft Way, Redmond, Washington 98052-6399.

Contents

Microsoft Software License Agreement..... iii

Welcome **ix**

About the Windows for Workgroups Resource Kit Addendum for
Version 3.11xi
About the Windows for Workgroups Resource Kit for Version 3.1 xiii
Conventions in This Manualxv

Part 1 Technical Overview

Chapter 1

Windows for Workgroups 3.11 Architecture **1-1**

Differences from Windows for Workgroups 3.1..... 1-3
Networking Component Enhancements 1-5
32-Bit Disk Access 1-12
32-Bit File Access 1-20
Windows for Workgroups 3.11 Boot Sequence 1-33
Driver Configuration Changes from Windows for Workgroups 3.10..... 1-36
Network Browsing 1-41
Enhanced MS-DOS Drivers and Utilities..... 1-46

Part 2 Installation and Setup

Chapter 2

Windows for Workgroups 3.11 Installation and Setup **2-1**

About Windows for Workgroups 3.11 Setup 2-3
Windows for Workgroups Network Support 2-3
Windows for Workgroups 3.11 Setup Options 2-6
Last Known Clean Configuration Files 2-8
Defining Default Workgroups for Users with WRKGRP.INI 2-9
Support for MS-DOS 6 Multi-Config Installation 2-11
Removing Mail, Schedule+, and Microsoft At Work Fax from Windows for
Workgroups Setup 2-15
Quick Windows for Workgroups Installations 2-16

Chapter 3	Windows for Workgroups 3.11 Files	3-1
	About the Windows for Workgroups 3.11 Files.....	3-2
	WIN.COM	3-2
	The Core Files	3-3
	Setup-related Files, Driver Files, Fonts, and International Support Files.....	3-3
	MS-DOS Support Components of Windows for Workgroups 3.11	3-13
	Windows for Workgroups 3.11 Applications, Setup, and Other Files	3-15
	Network Files Used for Microsoft Windows Network.....	3-20
	Minimizing Files Necessary for Windows for Workgroups 3.11.....	3-24
Chapter 4	The Windows for Workgroups 3.11 Initialization Files	4-1
	About the Initialization Files	4-2
	SYSTEM.INI: System Initialization File.....	4-6
	MSMAIL.INI: Microsoft Mail Initialization File.....	4-21
	EFAQPUMP.INI: Microsoft At Work Fax Settings Initialization File	4-22
Chapter 5	The Windows for Workgroups 3.11 Security Control Enhancements	5-1
	Configurable Peer Networking	5-2
	Administrator-Defined Password Settings.....	5-5
	Support for Windows NT Security Features	5-7
	Implementing Windows for Workgroups 3.11 Security Controls.....	5-10
	Auditing of Network Events.....	5-19

Part 3 Network Integration

Chapter 6	Windows for Workgroups 3.11 Network Protocols	6-1
	Windows for Workgroups 3.11 Protocol Support	6-2
	NetBEUI	6-2
	NWLink: 32-bit IPX/SPX-Compatible Transport	6-3
	Microsoft TCP/IP for Windows for Workgroups.....	6-7
	Microsoft Data Link Control Protocol for Windows for Workgroups	6-26
Chapter 7	Integrating with Windows NT and Windows NT Advanced Server	7-1
	Overview of Support for Integrating Workgroups 3.11 with Windows NT.....	7-2
	Enhanced Security Features in a Windows NT Environment	7-4
	Remote Access Services Client	7-6

Chapter 8	<i>Integrating with Novell NetWare</i>	8-1
	Overview of Enhancements to Novell NetWare Support.....	8-3
	Installing Support for Novell NetWare	8-4
	Workstation Configuration Files	8-21
	32-Bit IPX/SPX-Compatible Transport with NetBIOS.....	8-25
	NetBIOS Services over IPX	8-28
	Specific Novell NetWare Issues	8-29
	Sample Files for Configuration Scenarios	8-31
	NDIS 2.0 Protocols on ODI Drivers.....	8-39
 Chapter 9	 <i>Integrating with Other Networks</i>	 9-1
	Summary of Network Support.....	9-2
	Microsoft LAN Manager	9-4
	Banyan VINES	9-4
	DEC PATHWORKS	9-6
	Windows 3.1-compatible Networks	9-7

Part 4 Using Windows for Workgroups 3.11

Chapter 10	<i>Microsoft At Work Fax</i>	10-1
	Overview of Microsoft At Work Fax Software.....	10-2
	Sharing a Fax Modem Over the Network.....	10-5
	Using the Advanced Dialing Feature.....	10-7
	Using Security	10-10

Part 5 Configuring Windows for Workgroups 3.11

Chapter 11	<i>Tips for Optimizing Windows for Workgroups 3.11</i>	11-1
	Overview of Tips for Optimizing and Configuring.....	11-2
	General Configuration Guidelines.....	11-2
	Optimizing 32-bit File Access.....	11-7
	Using Windows for Workgroups 3.11 as a Client Only.....	11-8
	Using Windows for Workgroups 3.11 as a Client and Peer Server	11-12
	Using Windows for Workgroups 3.11 as a “Dedicated” server	11-13

Chapter		
12	Windows for Workgroups 3.11 Configuration Tips	12-1
	Overview of Configuration Tips.....	12-2
	Tips for Sharing Resources.....	12-2
	Windows for Workgroups Mail and Schedule+ Tips	12-3
	Miscellaneous Configuration Tips.....	12-13

Part 6 Troubleshooting Windows for Workgroups 3.11

Chapter		
13	Troubleshooting Windows for Workgroups 3.11	13-1
	Troubleshooting Tools for Windows for Workgroups	13-4
	Creating a Clean Configuration for Troubleshooting	13-9
	Network Adapter Card Settings.....	13-10
	Installation	13-13
	How to Troubleshoot Network Connection Problems.....	13-17
	Real Mode Network.....	13-27
	Architecture and Configuration	13-30
	Interoperability with LAN Manager, Windows NT, and Windows NT Advanced Server.....	13-31
	Interoperability with Novell NetWare	13-33
	Interoperability with Banyan VINES	13-37
	Interoperability with SunSelect PC-NFS	13-39
	Performance Enhancements.....	13-39
	Other New Features	13-45
	Microsoft At Work PC Fax	13-46
	Remote Access Service (RAS) Client	13-48

Part 7 Additional Information

Appendix		
A	Additional Support Information	A-1
	Getting Answers to Your Technical Questions	A-2
	Sources for Support Information	A-4
	Microsoft KnowledgeBase	A-11
	Microsoft CompuServe Forums	A-18
	Obtaining New and Updated Drivers and Information Electronically	A-20

Index	1
--------------	----------

Welcome

Welcome to the *Windows™ for Workgroups Resource Kit Addendum for Version 3.11*. This manual is an addendum guide to the *Windows for Workgroups Resource Kit for Version 3.1* and is designed for people who are, or who want to become, expert users of Microsoft® Windows™ for Workgroups version 3.11.

As an addendum, the *Windows for Workgroups Resource Kit Addendum for Version 3.11* covers only new and changed information originally covered in the *Windows for Workgroups Resource Kit for Version 3.1*. While it is not absolutely necessary to have the *Windows for Workgroups Resource Kit for Version 3.1*, it is helpful to have it available as a reference for information and topics not covered in the addendum.

The *Windows for Workgroups Resource Kit* presents a detailed, easy-to-read technical view of Windows for Workgroups, so that you can better manage how Windows for Workgroups is used at your site. The *Windows for Workgroups Resource Kit* also contains specific information for system administrators who are responsible for installing, managing, and integrating Windows for Workgroups in a network or multi-user environment.

This introductory chapter presents three kinds of information you can use to get started:

- The first section outlines the contents of the *Windows for Workgroups Resource Kit Addendum for Version 3.11*, so you can quickly find technical details about specific elements of Microsoft Windows for Workgroups 3.11.
- The second section contains an overview of the conventions used to present information in the *Windows for Workgroups Resource Kit Addendum for Version 3.11*.
- The third section presents a series of troubleshooting flowcharts, so you can quickly find details and procedures for solving problems you might have installing or running Windows for Workgroups.

The *Windows for Workgroups Resource Kit* is a technical supplement to the documentation that is included in your Windows for Workgroups product and does not replace that information as the source for learning how to use Windows for Workgroups features and Windows-based applications.

Contents

About the Windows for Workgroups Resource Kit Addendum for
Version 3.11 xi
About the Windows for Workgroups Resource Kit for Version 3.1 xiii
Conventions in This Manual.....xv
 Document Conventions xvi
 Syntax Conventions..... xvii

About the Windows for Workgroups Resource Kit Addendum for Version 3.11

This addendum guide is organized in seven parts that provide specific details about the Windows for Workgroups 3.11 architecture, installation and setup, integration with other networks, use of new features, configuration tips, and troubleshooting. Information is provided on new or changed topics from Windows for Workgroups version 3.1. Any information present in the *Windows for Workgroups Resource Kit Addendum for Version 3.11* that is also covered in the *Windows for Workgroups Resource Kit for Version 3.1* supercedes the information for version 3.1.

Part 1: Technical Overview

- **Chapter 1, “Windows for Workgroups 3.11 Architecture,”** describes the architecture used by Windows for Workgroups version 3.11 and discusses the components and enhancements that differentiate it from Windows for Workgroups version 3.1.

Part 2: Installation and Setup

- **Chapter 2, “Windows for Workgroups 3.11 Installation and Setup,”** contains a discussion of the Windows for Workgroups 3.11 Setup program, details about setting up Windows for Workgroups Setup options, and specific tips for installing and customizing the setup of Windows for Workgroups 3.11.
- **Chapter 3, “Windows for Workgroups 3.11 Files,”** describes the purpose for each file installed by Windows for Workgroups 3.11 in the WINDOWS directory and the Windows SYSTEM subdirectory.
- **Chapter 4, “Windows for Workgroups 3.11 Initialization Files,”** describes the new or changed entries in several Windows for Workgroups initialization files, including SYSTEM.INI, MSMAIL.INI, and EFAXPUMP.INI, and explains how you can change entries in these files.
- **Chapter 5, “Windows for Workgroups 3.11 Security Control Enhancements,”** describes the security control enhancements that are present in Windows for Workgroups 3.11 and discusses the administrator configuration utility, ADMINCFG.EXE, which can be used by administrators to control peer networking functionality and define password settings.

Part 3: Network Integration

- **Chapter 6, “Integrating with Other Protocols,”** contains information about protocols supported by Windows for Workgroups 3.11 and discusses specific configuration tips.
- **Chapter 7, “Integrating with Windows NT and Windows NT Advanced Server,”** contains information about integrating Windows for Workgroups with Windows NT and Windows NT Advanced Server. Topics covered include enhanced security support available from Windows NT and Windows NT Advanced Server, and using the Remote Access Services client to remotely access shared network resources.
- **Chapter 8, “Integrating with Novell NetWare,”** contains information about integrating Windows for Workgroups with Novell NetWare. Topics covered include installing and configuring Windows for Workgroups in a NetWare environment, support for the 32-bit IPX/SPX compatible transport, support for the 32-bit NetBIOS driver, specific NetWare issues, information about using the ODINSUP driver to support using NDIS 2 network transport protocols with ODI drivers, and sample configuration files for different NetWare installation scenarios.
- **Chapter 9, “Integrating with Other Networks,”** contains information about integrating Windows for Workgroups with other networks including Banyan VINES, Sun PC-NFS, DEC Pathworks, and Windows 3.1-compatible networks. Topics covered include special configuration issues and a summary of the network support provided for the other networks discussed.

Part 5: Using Windows for Workgroups 3.11

- **Chapter 10, “Microsoft At Work Fax,”** discusses the Microsoft At Work fax software provided with Windows for Workgroups 3.11. Topics covered include sharing a fax modem over the network, using the advanced dialing feature, and using security mechanisms supported by Microsoft At Work fax.

Part 6: Configuring Windows for Workgroups 3.11

- **Chapter 11, “Tips for Optimizing Windows for Workgroups 3.11,”** contains information about optimizing Windows for Workgroups 3.11 when used as a client only, as a client and peer network server, and as a “dedicated” server that is only sharing resources.

- **Chapter 12, “Windows for Workgroups 3.11 Configuration Tips,”** provides tips for configuring Windows for Workgroups 3.11. Topics covered include tips for sharing resources, tips for configuring Mail and Schedule+, along with several miscellaneous configuration tips.

Part 6: Troubleshooting Windows for Workgroups

- **Chapter 13, “Troubleshooting Windows for Workgroups 3.11,”** provides specific information for troubleshooting problems with Windows for Workgroups 3.11, showing the key steps for isolating and solving common problems.

Part 7: References, Resources, and Appendixes

This part of the *Windows for Workgroups Resource Kit Addendum for Version 3.11* contains appendixes describing additional sources for support information, and an index cross referenced with the *Windows for Workgroups Resource Kit for Version 3.1*.

About the Windows for Workgroups Resource Kit for Version 3.1

This section provides an overview of the topics covered in the *Windows for Workgroups Resource Kit for Version 3.1* to serve as an aid in identifying other information that may be relevant to topics covered in this addendum. To further facilitate finding information in both Resource Kit manuals, the index of this addendum is cross-referenced with the *Windows for Workgroups Resource Kit for Version 3.1*.

Part 1: Technical Overview

- **Chapter 1, “Networking—A Technical Discussion,”** contains information targeted toward the support professional that may not have a local area network (LAN) background. This chapter provides a technical discussion of networking concepts and discusses the components that make up a LAN.
- **Chapter 2, “Windows for Workgroups Architecture,”** describes the architecture used by Windows for Workgroups and discusses the components of Windows for Workgroups that differentiate it from Windows version 3.1.

Part 2: Installation and Setup

- **Chapter 3, “Windows for Workgroups Installation,”** contains a technical discussion of the Windows for Workgroups Setup program, details about setting up Windows for Workgroups on a network, and instructions for creating a custom installation routine for automated setup.
- **Chapter 4, “Windows for Workgroups Files,”** describes the purpose for each file installed by Windows for Workgroups in the WINDOWS directory and the Windows SYSTEM subdirectory.
- **Chapter 5, “Windows for Workgroups Setup Information Files,”** contains the details you need to understand to create custom Windows for Workgroups setup information files (SETUP.INF, NETWORK.INF, CONTROL.INF, APPS.INF, and OEMSETUP.INF) for multiple installations.
- **Chapter 6, “Windows for Workgroups Initialization Files,”** describes the contents of Windows for Workgroups initialization files, including WIN.INI, SYSTEM.INI, PROTOCOL.INI, MSMAIL.INI, and SCHDPLUS.INI, and explains how you can change entries in these files.

Part 3: Special Topics

- **Chapter 7, “Additional Windows for Workgroups Information,”** contains tips about using Microsoft Windows for Workgroups. This chapter also discusses special topics related to the components of Windows for Workgroups.
- **Chapter 8, “Network Integration with Microsoft LAN Manager and Novell NetWare,”** contains information about integrating a Windows for Workgroups workstation into an existing LAN environment. Topics covered include integrating Windows for Workgroups with Microsoft LAN Manager and Novell® NetWare® networks.

Part 4: Configuring Windows for Workgroups

- **Chapter 9, “Tips for Configuring Windows for Workgroups,”** presents tips about configuring your system, both for gaining optimal performance and for creating custom Windows for Workgroups configurations.

Part 5: Using Windows for Workgroups

- **Chapter 10, “New and Updated Accessories,”** discusses accessories new for Windows for Workgroups and provides new information about Windows 3.1 accessories that have been updated for Windows for Workgroups.

- **Chapter 11, “Network Dynamic Data Exchange,”** discusses how Dynamic Data Exchange (DDE) functionality has been extended to the network environment to enable information to be exchanged dynamically with other workstations in your Windows for Workgroups workgroup.
- **Chapter 12, “Mail,”** includes information about the Mail application provided with Windows for Workgroups. The architecture of Mail, tips for customizing Mail, and information about integrating Mail with other Windows-based applications are discussed in this chapter.
- **Chapter 13, “Schedule+,”** includes information about the Schedule+ application provided with Windows for Workgroups. Schedule+ architecture and key features of interest to system administrators are discussed in this chapter.

Part 6: Troubleshooting Windows for Workgroups

- **Chapter 14, “Troubleshooting Windows for Workgroups 3.1,”** provides specific information for troubleshooting problems with Windows for Workgroups, showing the key steps for isolating and solving common problems.

Part 7: References, Resources, and Appendixes

This part of the *Windows for Workgroups Resource Kit* contains a glossary, a directory of information resources, a configuration guide for Mail, and an index.

Conventions in This Manual

This document assumes that you have read the Windows for Workgroups 3.1 documentation set and that you are familiar with using menus, dialog boxes, and other Windows features. It also assumes that you have installed Windows for Workgroups on your system and that you are using a mouse with Windows. For keyboard equivalents to the actions described here, see the Microsoft Windows for Workgroups online Help.

This document uses several conventions to help you identify information.

Document Conventions

The following table describes the typographical conventions used in the *Windows for Workgroups Resource Kit*.

Type style	Used for
bold	MS-DOS® command names such as copy or dir , switches such as /? or /a , section and entry names in .INI and .INF files such as [386Enh] or emmexclude= , and text that you type to carry out actions at the command prompt.
<i>italic</i>	Parameter values for which you can supply specific values. For example, to supply a value for a parameter that calls for a <i>filename</i> , you must type a specific filename such as MYFILE.EXE.
ALL CAPITALS	Directory names, filenames, and acronyms. For example, “WINDOWS” is used to represent the Windows main directory, and “SYSTEM” represents the Windows System subdirectory. When you type directory names and filenames at the command prompt or in a dialog box, lowercase letters may be used.

Other conventions in this document include:

- “Windows” refers to Microsoft Windows version 3.1 or later (including Windows for Workgroups).
- “MS-DOS” refers to Microsoft MS-DOS version 3.1 or later.
- Windows NT refers to both the Windows NT base product and Windows NT Advanced Server, unless otherwise specified.
- The Microsoft Windows logo appears in the margin to highlight specific features that are new to Windows for Workgroups 3.11 or updated from Windows for Workgroups 3.1.
- An asterisk (*) preceding a component name (for example, *VNETBIOS) shows that this is an internal function rather than a physical file. You will not find a file with this name on your Windows for Workgroups 3.11 disks.



- “Windows-based application” is used as a shorthand term to refer to an application that is designed to run with Windows and does not run without Windows. All Windows applications follow similar conventions for the arrangement of menus, style of dialog boxes, and keyboard and mouse use.
- “MS-DOS-based application” is used in this document as a shorthand term to refer to an application that is designed to run with MS-DOS but not specifically with Windows and is not able to take full advantage of Windows features (such as graphics or memory management).
- “Command prompt” refers to the command line where you type MS-DOS commands. Typically, you see characters such as “C:\>” to show the location of the command prompt on your screen. When Windows is running, 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 for Workgroups User’s Guide* and the Windows online tutorial.

Syntax Conventions

“Syntax” refers to the order in which you must type an item such as an MS-DOS command with its switches or an entry in a Windows initialization (.INI) file. Elements that appear in bold must be typed exactly as they appear in the syntax example. Elements that appear in italic are placeholders for parameter values for which you must supply specific information.

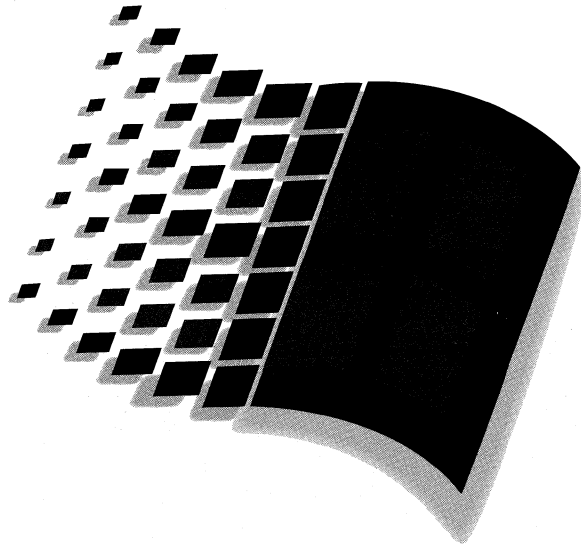
Unless specified otherwise, you can type commands, keynames, parameters, and switches in either uppercase or lowercase letters.

This example shows the syntax for a SYSTEM.INI entry, with each item in the sample explained in the following table.

[*section*]
keyname=*value*, *string*, *source*, *destination*

Entry item	Definition
[<i>section</i>]	The name of a section in an initialization file or setup information file. The enclosing brackets ([]) are required, and the left bracket must be in the leftmost column on the screen—f example, [standard].
<i>keyname</i>	The name of an entry, which usually can consist of any combination of letters and digits. For many entries described in this document, the <i>keyname</i> must be followed immediately by an equal sign (=)—f example, run= .
<i>value</i>	An integer, a string, or a quoted string, depending on the entry.
<i>string</i>	A group of characters to be treated as a unit. A string can include letters, numbers, spaces, or any other characters. Sometimes the syntax definition will indicate that the string must be enclosed in double quotation marks (" ").
<i>source</i>	The location of data to be transferred to a specific destination or to be used as input to a command. <i>Source</i> can consist of a drive letter and colon, a directory name, a filename, or a combination of these elements.
<i>destination</i>	A location to which the data specified by <i>source</i> is to be transferred. <i>Destination</i> can consist of a drive letter and colon, a directory name, a filename, or a combination of these elements.

Note If you have MS-DOS version 5.0 or later on your system, you can get help for any MS-DOS commands, such as **mem**, and for many of the drivers, such as SMARTDRV.EXE, by typing the command name and **/?** at the command prompt (for example, **mem /?**). You can also type **help** plus the command name. Type **help** at the command prompt to see a list of all MS-DOS commands with a brief description of command syntax, parameters, and switches.



Technical Overview

Chapter 1 Windows for Workgroups Architecture

Differences from Windows for Workgroups 3.1	1-3
Networking Component Enhancements	1-5
32-Bit Disk Access	1-12
32-Bit File Access	1-20
Windows for Workgroups 3.11 Boot Sequence	1-33
Driver Configuration Changes from Windows for Workgroups 3.10	1-36
Network Browsing	1-41
Enhanced MS-DOS Drivers and Utilities	1-46

Windows for Workgroups 3.11 Architecture

This chapter describes the architecture implemented in Windows for Workgroups 3.11. Emphasis is placed on the differences between Windows for Workgroups version 3.1 and the enhancements made in version 3.11. This chapter covers changes to the 32-bit networking components and the addition of 32-bit File Access, all delivering improved performance over the previous release. This chapter also includes a description of the boot sequence for Windows for Workgroups version 3.11.

Related information

- *Windows for Workgroups 3.11 Resource Kit Addendum for version 3.11:* Chapter 4, “Windows for Workgroups 3.11 Initialization Files;” Chapter 8, “Integrating with Novell® Netware®;” Chapter 11, “Tips for Optimizing Windows for Workgroups 3.11.”
- *Windows for Workgroups Resource Kit, version 3.1:* Chapter 2, “Windows for Workgroups Architecture.”

Contents of This Chapter

Differences from Windows for Workgroups 3.1.....	1-3
Networking Component Enhancements	1-5
Support for 16-Bit Network Adapter Card Drivers.....	1-5
Support for 32-Bit Network Adapter Card Drivers.....	1-7
Support for ODI Drivers	1-10
Network Protocols.....	1-10
Alerts and Notifications Through the Messenger Service.....	1-11
32-Bit Disk Access.....	1-12
What is 32-Bit Disk Access?.....	1-12
Improved System Performance	1-14
Enabling 32-Bit Disk Access	1-15
Hard Disk Access Scenarios.....	1-16
Components of the 32-Bit Disk Access System.....	1-18
32-Bit File Access	1-20
Enabling 32-Bit File Access.....	1-20
Requirements for 32-Bit File Access	1-22
Real-Mode Mapper.....	1-22
IFS Manager.....	1-24
32-Bit Disk Cache	1-25

Configuration Scenarios	1-29
Windows for Workgroups 3.11 Boot Sequence	1-33
Driver Configuration Changes from Windows for Workgroups 3.10.....	1-36
Review of Windows for Workgroups 3.10 Configuration	1-36
Windows for Workgroups 3.11 Configuration.....	1-37
Network Browsing.....	1-41
Browse List.....	1-42
Role of a Browse Server.....	1-42
Master and Backup Browse Servers	1-43
Browsing Network Resources	1-45
Browsing and Slow Network Connections.....	1-45
How Browsing is Handled When a “Net View” Command is Issued.....	1-45
LAN Manager 2.x Domains	1-46
Enhanced MS-DOS Drivers and Utilities	1-46
SmartDrive 5.0	1-47

Differences from Windows for Workgroups 3.1

Windows for Workgroups 3.11 extends the 32-bit architecture first delivered in Windows for Workgroups 3.10 to support 32-bit network adapter card drivers and 32-bit File Access. In addition to new 32-bit support, a number of changes and enhancements have been made in the Windows for Workgroups 3.11 networking components based on feedback Microsoft received from customers, value-added resellers (VARs), system integrators, and original equipment manufacturers (OEMs).

This chapter covers differences between the architecture used in version 3.11 and that originally provided in version 3.10. The overall architecture of Windows for Workgroups 3.10 is described in Chapter 2 of the *Windows for Workgroups Resource Kit for version 3.1*.

Windows for Workgroups 3.11 features several benefits over Windows for Workgroups 3.10:

- **Improved performance and new 32-bit components**

Windows for Workgroups 3.11 incorporates 32-bit network adapter card drivers that comply with Network Device Interface Standard (NDIS) 3.0 and 32-bit File Access. This provides a full 32-bit code path from the network adapter card, through the network protocol and network client and server software, to the hard disk in the local computer. This provides improved performance for network I/O and disk and file I/O access.

- **Tight integration with the Windows 3.1 environment**

The networking components found in Windows for Workgroups are tightly integrated with the Windows 3.1 environment. Each of the network components is implemented as a Windows virtual device driver (VxD) and provide better integration than MS-DOS-based solutions.

- **Improved configurability and administration for MIS organizations**

Through the use of the administrator configuration utility, ADMINCFG.EXE, system administrators can control Windows for Workgroups 3.11 functionality by disabling file and/or printer sharing if wanted, along with defining password settings that can be enforced on computers running Windows for Workgroups or Workgroup Add-on for MS-DOS.

- **Minimal use of conventional memory**

Windows for Workgroups 3.11 has only a 4-kilobyte conventional memory footprint when using 32-bit network drivers. This allows large MS-DOS-based applications to run under Microsoft Windows in a networking environment.

- **Full support for Windows NT and Windows NT Advanced Server**

Windows for Workgroups 3.11 provides the best level of client support for Windows NT and Windows NT Advanced server. This is because Windows for Workgroups 3.11 offers a client that fully supports the improvements made to the 32-bit networking components. It also takes advantage of enhanced security available with a Windows NT domain. In addition, Windows for Workgroups 3.11 includes the Remote Access Services (RAS) client for remotely accessing other Windows for Workgroups or Windows NT computers by dialing into the RAS server provided with Windows NT and Windows NT Advanced Server.

- **Improved support for Novell NetWare environments**

Windows for Workgroups 3.11 features the ability to run on top of Open Datalink Interface (ODI) network adapter card drivers, support peer sharing services over the IPX protocol, and includes a routable 32-bit IPX/SPX compatible transport with NetBIOS services allowing Windows for Workgroups computers to participate on an IPX backbone including through an IPX router.

- **Better support for standalone computers**

Windows for Workgroups 3.11 features an option to not install the networking components, thus providing the many benefits of improved performance and new functionality to standalone computer users as well as users on a network.

- **Full superset of Windows 3.1 network compatibility**

Windows for Workgroups 3.11 can be configured to run on top of a Windows 3.1 compatible network instead of installing the Microsoft Windows Network components. This provides the benefits of new functionality to users of networks compatible with Windows 3.1 that do not want to use the 32-bit networking components featured in Windows for Workgroups.

- **Incorporation of new and future technology including Microsoft At Work components**

Windows for Workgroups 3.11 features the first PC-based implementation of Microsoft At Work technology in the form of Microsoft At Work fax messaging.

- **Configuration has been simplified by removing network drivers from CONFIG.SYS**

NDIS network adapter card drivers and Windows for Workgroups 3.11 support drivers are loaded from the SYSTEM.INI file rather than the CONFIG.SYS and AUTOEXEC.BAT files. This results in only one real-mode support driver being loaded in the CONFIG.SYS file and one command line present in the AUTOEXEC.BAT file, simplifying the system configuration. More information about this configuration change from Windows for Workgroups 3.1 is discussed in the next section.

- **Networking Components Enhanced**

32-bit networking components (for example, VREDIR, VSERVER) have been enhanced in Windows for Workgroups 3.11. Information on the enhancements to the 32-bit networking components is discussed later in this chapter. Windows for Workgroups 3.11 provides support for the messenger service, allowing Windows for Workgroups 3.11 workstations to send and receive messages and alerts to other computers running the messenger service. Print Manager is also enhanced to allow print servers to send notification of completed print jobs to workstations.

Networking Component Enhancements

Windows for Workgroups 3.11 includes enhancements of the 32-bit networking components first delivered to the Windows environment with Windows for Workgroups 3.1. In addition to the enhancements made to the previously existing components, Windows for Workgroups 3.11 features network adapter card drivers based on the NDIS 3.0 specification that provide a complete 32-bit code path from the network adapter card to the network redirector and server, providing improved performance.

Support for 16-Bit Network Adapter Card Drivers

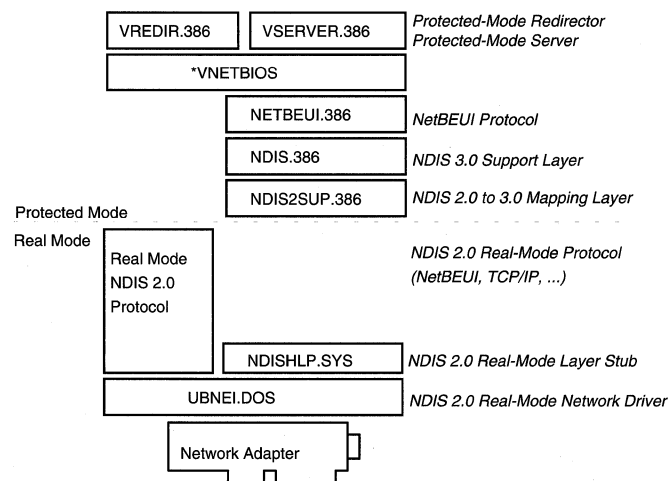
As with Windows for Workgroups 3.10, Windows for Workgroups 3.11 provides support for 16-bit NDIS 2.0 network adapter card drivers.

The characteristics of NDIS 2.0 drivers include:

- NDIS 2.0 drivers are written in assembly language, are 16-bit real-mode code, and reside in conventional memory.
- The filenames for NDIS 2.0 drivers usually end with a .DOS extension.
- Each NDIS 2.0 network adapter card driver loaded in memory supports only one adapter. For example, if you have two 3COM Etherlink adapters, two instances of the same driver must load into memory.
- NDIS 2.0 protocols require the use of NDIS 2.0 network adapter card drivers
- NDIS 3.0 protocols can be used with NDIS 2.0 network adapter card drivers

Figure 1.1 depicts the configuration of Windows for Workgroups 3.11 network components when NDIS 2.0 network adapter card drivers are used.

Figure 1.1
Windows for
Workgroups
configuration using
NDIS 2.0 drivers



If the network adapter card driver is NDIS 2.0-compliant, an NDIS 3.0 protocol (for example, NETBEUI.386 or NWLINK.386) requires the NDIS 2.0 mapping layer (NDIS2SUP.386) and the real-mode stub (NDISHLP.SYS) to bind to the NDIS 2.0 network adapter card driver. Additionally, the NDIS 3.0 protocol requires the NDIS 3.0 support layer (NDIS.386).

In the NDIS 2.0 network adapter card driver configuration, NDIS 3.0 protocols may still be used. The NDIS 3.0 protocol (NETBEUI.386) uses the NDIS 2.0 mapping layer (NDIS2SUP.386) to access the real-mode network adapter card driver. There is a slight performance penalty in this configuration as memory is buffered into the first megabyte of physical memory in order to allow transmission and reception by the real-mode NDIS 2.0 network adapter card driver.

NDIS2SUP.386

This NDIS 2.0/3 support layer is also referred to as a *mapper*. A mapper has the ability to translate real-mode addressing into protected-mode addressing and vice-versa. The NDIS2SUP.386 driver also has the functionality of translating (or mapping) NDIS 2.0 instructions to NDIS 3.0 instructions.

NDIS2SUP.386 sets up a buffer in real mode (below the 1-megabyte address line) for NDIS 2.0 network adapter card drivers to use. NDIS2SUP appears as an NDIS 3.0 network adapter card driver to the NDIS 3.0 protocol driver and an NDIS 2.0 protocol driver to an NDIS 2.0 network adapter card driver.

NDISHLP.SYS

The NDISHLP.SYS driver is the real-mode stub for the NDIS2SUP.386 VxD and assists in the binding process between real-mode NDIS 2.0 network adapter card drivers and NDIS 2.0 protocols.

Stopping the Real-Mode Network

If the real-mode network is loaded (that is, the real-mode redirector has been started), the **net stop** command should be run to stop and remove the real-mode network redirector from memory before starting Windows for Workgroups 3.11 for two reasons:

- It will unload the real-mode NetBEUI protocol and the real-mode redirector. The protected-mode redirector should be used because it provides improved performance when working with the other 32-bit networking components that are provided with Windows for Workgroups 3.11.
- Using the real-mode redirector will not allow Windows for Workgroups 3.11 to load the protected-mode server to share its resources in protected mode.

Support for 32-Bit Network Adapter Card Drivers

New to Windows for Workgroups 3.11 is support for the use of 32-bit protected-mode network adapter card drivers based on NDIS version 3.0. Windows NT also uses NDIS 3.0 for its network adapter card driver implementations.

NDIS 3.0 differs from NDIS 2.0 in several ways:

- NDIS 3.0 uses 32-bit C language APIs to access the network adapter card driver whereas NDIS 2.0 uses a 16-bit assembly language APIs.
- NDIS 3.0 provides code portability allowing OEMs to take NDIS 3.0 drivers written for Windows NT, modify them slightly, and recompile and use them for Windows for Workgroups 3.11 and future versions of Windows.
- NDIS 3.0 drivers on Windows for Workgroups 3.11 run in protected mode and reside in extended memory, whereas NDIS 2.0 drivers run in real mode and reside in conventional memory.
- NDIS 3.0 network adapter card drivers can not be used with NDIS 2.0 protocols. NDIS 2.0 protocols require the use of NDIS 2.0 network adapter card drivers.

The addition of 32-bit NDIS 3.0 drivers to Windows for Workgroups 3.11 provides a 32-bit code path for data from the network wire to the network redirector and server components.

In a pure NDIS 3.0 system, only three layers are necessary to compose the protocol stack:

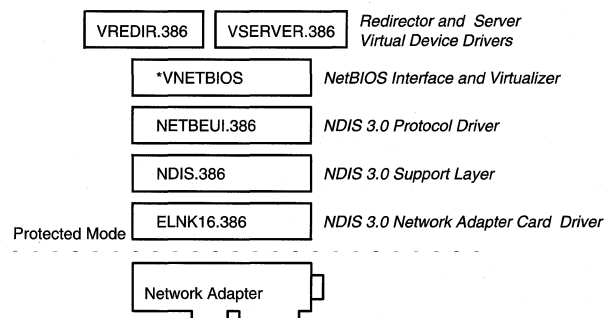
- The NDIS 3.0 compliant network adapter card driver
- The NDIS 3.0 support layer (NDIS.386)
- The NDIS 3.0 protocol

Important An NDIS 3.0 (protected-mode) network adapter card driver *cannot* bind to an NDIS 2.0 (real-mode) protocol. However, the converse is true, as shown in the next section.

Figure 1.2 depicts the configuration of Windows for Workgroups network components when NDIS 3.0 network adapter card drivers are used.

Figure 1.2

Windows for Workgroups configuration using NDIS 3.0 drivers



The configuration shown in Figure 1.2 requires no real-mode memory. All components are 32-bit code running in protected mode for maximum performance.

NDIS.386

All operating system requests for hardware services are passed from NDIS.386 to the network adapter card driver without regard to the hardware configuration. Conversely, any hardware requests for operating system services are passed from the network adapter card driver to NDIS.386 without regard to the operating system specifics. NDIS.386 is responsible for:

- Memory allocation
- Hardware specific requests
- Start-up and shut-down of the operating system
- Parsing instructions from the PROTOCOL.INI file

NETBEUI.386

NetBEUI.386, a virtual device (VxD), is the NDIS 3.0 driver for the NetBEUI protocol. It replaces the NDIS 2.0 VNB.386 driver originally provided with Windows for Workgroups 3.10. (VNB.386 included the protected mode to real mode mapping functionality that is now part of the new NDIS2SUP.386 driver discussed in the previous section.) As with Windows for Workgroups 3.10, this NetBEUI protocol is a NetBIOS provider. (A *provider* is the software component that allows a Windows for Workgroups computer to communicate with the network.)

The Remote Access Services (RAS) AsyBEUI protocol is now built into the NETBEUI.386 protocol driver. AsyBEUI is similar to that of NetBEUI, but is designed to support slow network links such as an asynchronous connection over a phone line. More information on RAS is provided in Chapter 7, "Integrating with Windows NT and Windows NT Advanced Server."

***VNETBIOS**

*VNETBIOS is a virtual device that provides virtualization of the NetBIOS interface for applications running in a virtual machine.

Note The asterisk (*) preceding VNETBIOS shows that this is an internal function. You will not find a file with this name on your Windows for Workgroups 3.11 disks.

It is also necessary for any virtual device that requires the NetBIOS interface, for example VREDIR.386. In Windows for Workgroups 3.10, it loads as a separate file, VNETBIOS.386. In Windows for Workgroups 3.11, it loads as an internal virtual device within WIN386.EXE.

VREDIR.386

VREDIR.386 is the protected-mode redirector virtual device. The redirector provides the mapping from local device names to remote network resources. The VREDIR.386 also contains the browsing service functionality for enumerating the list of available servers across the network.

VSERVER.386

VSERVER.386 is the protected-mode server virtual device. The server provides the ability to share resources on the local computer running Windows for Workgroups 3.11.

Support for ODI Drivers

In addition to supporting NDIS 2.0 and NDIS 3.0 network adapter card drivers, Windows for Workgroups 3.11 also features the ability to run on top of Open Datalink Interface (ODI) drivers and Novell's monolithic IPX protocol stack.

For information about running Windows for Workgroups using ODI and monolithic IPX drivers, see Chapter 8, "Integrating with Novell NetWare."

Network Protocols

In addition to the 32-bit NetBEUI protocol, Windows for Workgroups 3.11 includes a new 32-bit NDIS 3.0 protocol that is IPX/SPX compatible, NWLink. This new 32-bit IPX/SPX compatible protocol is routable and does not natively provide NetBIOS services. NetBEUI is not a routable protocol, and thus cannot be used in a wide-area network (WAN) environment.

Windows for Workgroups 3.11 supports the real-mode Microsoft TCP/IP for Windows for Workgroups protocol. This allows Windows for Workgroups 3.11 to offer network redirector and server functionality over a WAN using TCP/IP. Microsoft TCP/IP for Windows for Workgroups also supports NetBIOS services to host functionality such as Network DDE.

NetBIOS services are available for use with the IPX/SPX compatible transport as a 32-bit protected-mode virtual device, NWNBLink, to provide improved performance and memory savings over Novell's real-mode NETBIOS.EXE terminate-and-stay-resident (TSR) program. The NWNBLink driver also provides connectivity to Windows NT when the IPX/SPX compatible transport is used.

For further information on network protocols for use with Windows for Workgroups 3.11, see Chapter 6, "Integrating with Other Protocols."

Direct Hosting and IPX

The concept of *hosting* refers to the ability for the Windows for Workgroups network functionality to run on top of a given protocol configuration directly. For example, Windows for Workgroups version 3.10 required a NetBIOS provider to support NetBIOS services over which the network redirector and network server could run.

Windows for Workgroups 3.11 extends the hosting capability beyond just NetBIOS providers to allow the Windows for Workgroups network redirector and network server to be directly hosted on top of an IPX transport without a NetBIOS provider. This capability allows Windows for Workgroups 3.11 to run natively over IPX, providing support for a routable protocol in a WAN environment.

Alerts and Notifications Through the Messenger Service

The Windows for Workgroups 3.11 network redirector now supports the LAN Manager Messenger service, allowing Windows for Workgroups users to receive messages and alerts from Microsoft LAN Manager and Windows NT servers and clients. The messenger support is handled by the WINPOPUP.EXE utility and allows a Windows for Workgroups 3.11 user to send messages to and receive messages from the network.

The Windows for Workgroups 3.11 Print Manager uses the Messenger service to send notification of completed print jobs from the print server to the Windows for Workgroups 3.11 user who sent the job to print.

32-Bit Disk Access

The 32-Bit Disk Access feature of Windows, also known as FastDisk, was first introduced with Windows 3.1. It brought new technology to users of the Windows operating system and delivered improved performance over Windows 3.0. Microsoft is continuing to leverage the 32-bit architecture of the Windows environment as delivered in Windows for Workgroups 3.10 by adding 32-bit File Access support to Windows for Workgroups 3.11.

Note The 32-bit Disk Access functionality in Windows for Workgroups 3.11 is the same functionality as that included in Windows 3.1 and Windows for Workgroups 3.10. Information on 32-bit Disk Access is provided in this chapter to give some background in order to discuss the new 32-bit File Access functionality present in Windows for Workgroups 3.11.

What is 32-Bit Disk Access?

One system BIOS is not necessarily identical to the next—some are less efficient in the way they handle hard disk access than others, and some were written before newer, more efficient disk access technology was developed. Microsoft built 32-bit Disk Access into Windows operating system version 3.1 to offset BIOS inefficiency and to allow users to take advantage of new disk-access technology.

The Windows 3.1 32-bit Disk Access is a set of protected-mode device drivers that work together to enhance your system's BIOS. It filters interrupt (Int) 13H calls to the hard disk controller and directs them in the most efficient way for the system—either through the 32-bit interface with the hard disk controller or through the system BIOS.

Supports Most Existing Hardware

The 32-bit Disk Access works directly with the hard disk controller—not with the hard disk itself. It can support any disk controller provided that there is an appropriate virtual device to support that controller.

Windows 3.1 ships with one such device—WDCTRL—which supports all disk controllers that are compatible with the Western Digital™ 1003 controller interface standard. This was the original standard developed for the IBM™ AT™ and is adhered to by 90 percent of installed hard disks on the market. WDCTRL does not support SCSI or ESDI drives; however, these drives may be supported by OEM-supplied virtual devices.

Several hard disk controller manufacturers including Future Domain, UltraStor, Quantum, and Compaq® Computer Corporation, provide 32-bit Disk Access drivers for use with hard disk controller adapters. Contact the appropriate hardware vendor for further information on the availability of 32-bit drivers.

Disabled By Default

Windows operating system version 3.1 features 32-bit Disk Access as an option that is disabled by default when Windows 3.1 is installed on your system. To enable it, simply turn it on in the Enhanced dialog box in the Windows Control Panel. If 32-bit Disk Access remains disabled, you will not benefit from the hard disk access performance improvements it provides, but your system will remain otherwise unaffected.

If a system's hard-disk controller is compatible with the 32-bit Disk Access virtual device driver (WDCTRL) included with Windows 3.1, then Setup will automatically install the proper virtual devices. As a result, if you double-click the Enhanced icon in the Control Panel, choose the Virtual Memory button, and then the Change button, you can select the Use 32-Bit Disk Access check box. If, after Setup, you are not able to select this check box (that is, it is grayed), do not try installing any virtual devices manually. Instead, contact your hardware manufacturer directly to find out when a virtual controller device for Windows 3.1 will be available to support 32-bit Disk Access for the hardware.

Some portable computers, such as laptops and notebooks, power down the hard disk to conserve battery life without notifying the currently-running system software. In addition, portable computers that use Int 13H to detect disk access to power up or power down the hard disk to conserve power, will not properly identify when the 32-bit Disk Access driver is accessing the hard disk. If the hard disk powers down in the middle of a write or read action, data loss may result.

Due to these situations, 32-bit Disk Access is disabled by default. When the user installs the Windows operating system, 32-bit Disk Access is disabled until the user makes the decision to enable it (through the Control Panel). Only OEMs who preinstall Windows 3.1 on a 100-percent-compatible system can turn 32-bit Disk Access on before the user receives the system without jeopardizing the users hard disk. A Windows Ready to Run logo on the PC is your guarantee that the OEM has tested the hardware configuration with Windows 3.1 and configured Windows correctly, including the turning 32-bit Disk Access on or off.

WDCTRL has, however, been put through rigorous testing to make sure it is as safe as possible. WDCTRL is designed with a built-in safety measure—every time it starts, it performs elaborate tests to make sure that it can communicate in the same language as the hard disk controller before it attempts to read and write data. WDCTRL begins testing by looking peripherally at some data on the hard disk for any traces of a Western Digital 1003-compatible controller. If it passes that test, WDCTRL then begins calling up larger pieces of data in an attempt to elicit the correct response.

Finally, after much redundant checking, WDCTRL actually tries reading data from the disk. If it is able to read data, WDCTRL then tries to write data and read it back. Only after the read-write test is passed does WDCTRL continue and start the Windows operating system.

If something does go wrong, WDCTRL may do different things, depending on where it is in the verification process. The controllers with which WDCTRL fails are considered incompatible with 32-bit Disk Access, so WDCTRL simply doesn't load when it detects these unsupported controllers. If WDCTRL fails a test later, after it is installed, the Windows operating system displays an error message that warns the user that something is wrong, and advises the user to reboot. This keeps WDCTRL from loading and 32-bit Disk Access will be disabled.

Improved System Performance

The use of 32-bit Disk Access provides improved system performance for running MS-DOS-based applications. Using 32-bit Disk Access allows for more pageable memory in Windows to page MS-DOS-based applications to disk to free enough RAM for applications when they need to use it. The 32-bit Disk Access feature also improves the performance of Windows all around, making the system run much more quickly. For example, switching between MS-DOS-based applications is faster with 32-bit Disk Access.

This feature also allows for faster paging. When Windows operating system version 3.1 is paging using 32-bit Disk Access, it can load in just the small amount that the application is actually using, so task switching becomes almost instantaneous. And, since only a small part of the application needs to be in RAM at one time, Windows may not have to access the hard disk at all. This becomes very important when RAM is close to being *overcommitted*, meaning that the RAM is nearing its capacity limit, thus causing a dramatic increase in the amount of paging to disk that occurs and slowing system response.

Overlapped I/O

Another advantage of using the 32-bit Disk Access in Windows is that it supports overlapped I/O allowing disk I/O requests to be handled asynchronously. Overlapped I/O helps disk access in two ways:

- Paging can take place in the background while applications are running.
- Applications can make calls simultaneously to the hard disk controller even while other applications are running.

With overlapped I/O, the system can send multiple requests to the hard disk controller at the same time so that they are queued and no idle time passes between requests. This method lets the hard disk controller run more efficiently.

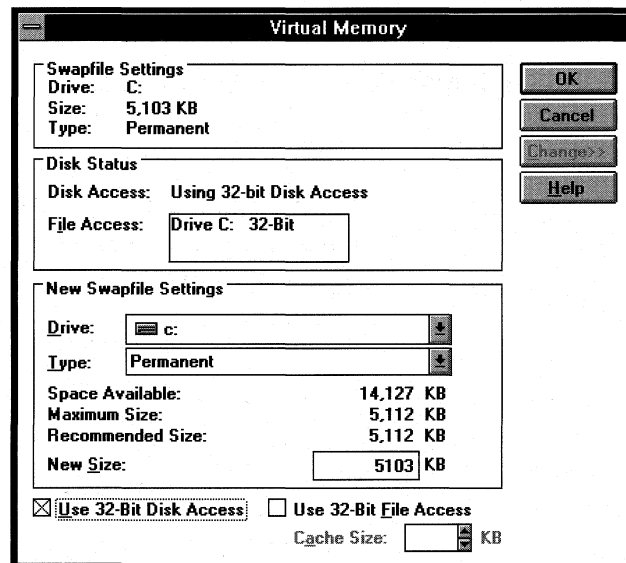
Enabling 32-Bit Disk Access

The 32-bit Disk Access feature is enabled from the Enhanced section of Control Panel. Double-click the Enhanced icon to display the Windows Enhanced dialog box. Choose the Virtual Memory button to display the Virtual Memory dialog box which shows the status of the 32-bit Disk Access feature of Windows (that is, whether 32-bit Disk Access is being used, or whether communication with the hard disk controller is being handled by the BIOS).

Choose the Change>> button to display the virtual memory configuration section of the dialog box which allows 32-bit Disk Access to be enabled. To enable 32-bit Disk Access, select the Use 32-Bit Disk Access check box as shown in Figure 1.3.

Figure 1.3

32-Bit Disk Access is enabled from the Virtual Memory dialog box accessible from the Enhanced section of Control Panel



Hard Disk Access Scenarios

32-Bit Disk Access helps to simplify the process by which information is read from and written to the hard disk controller when running in the Windows environment. To provide an overview of how the use of 32-bit Disk Access helps to improve the system performance, this section examines three scenarios:

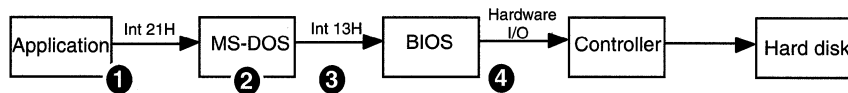
- Hard disk access under MS-DOS
- Hard disk access under Windows without 32-bit Disk Access
- Hard disk access under Windows with 32-bit Disk Access

Hard Disk Access Under MS-DOS

In MS-DOS-based PCs, when an application wants to access a disk, it uses the following path. (The numbers in the diagram correspond to the steps described below.)

Figure 1.4

Hard disk access path under MS-DOS



1. The application makes an Int 21H call to MS-DOS.
2. MS-DOS decodes the hard disk location of the requested part of the file by examining the File Allocation Table (FAT).
3. MS-DOS issues an Int 13H call to the hard disk BIOS. (The BIOS contains programs to control the basic devices in the system, such as the hard disk, keyboard, display, communications ports, etc.)
4. The hard disk BIOS program talks directly to the hard disk controller. Each hard disk controller requires its own BIOS. These BIOS are not independent of the hard disk itself, rather, they are specific to the controller board (or adapter) that connects the hard disk to the rest of the system.

This design works well in the case where the real-mode BIOS is in ROM and covers the hard disk because both were installed and tested at the same time by the computer manufacturer. However, hard disks are often added or upgraded at a later time, and the MS-DOS BIOS installed in the computer may not be able to communicate with the new hard disk.

In this case, the disk manufacturer must provide a specifically designed driver newly installed hard disk. This additional device driver is normally added to the CONFIG.SYS file after installing the software that accompanies the hard disk. (With some devices, such as a CD-ROM drive, a device driver that provides the BIOS interface and Int 13H interface to the device appears in the AUTOEXEC.BAT file.)

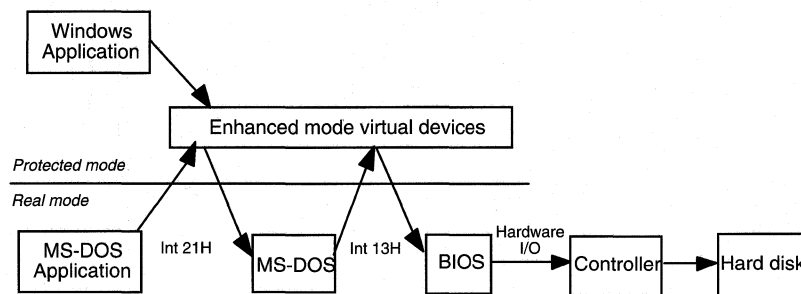
These device drivers intercept Int 13H calls to the hard disk and verify that the calls are understood by the hard disk. Usually, the device drivers will handle any attempts to access the hard disk, so the calls never get passed on to the real ROM BIOS. However, if the call is for a device other than the hard disk, the Int 13H call is passed on to the BIOS, where it is handled in the usual way.

Hard Disk Access Under Windows Without 32-Bit Disk Access

Under the Windows operating system in 386 enhanced mode, the flow of calls to handle file I/O is more complicated than that of MS-DOS due to the necessary transitions between real mode and protected mode.

Figure 1.5

Hard disk access path under Windows without 32-bit Disk Access



Windows, Windows-based applications, and the 386 enhanced mode system all run in protected mode, but must switch back into real mode (or virtual 8086 mode) to run older code (for MS-DOS and the BIOS, for example). Switching modes is time-consuming, and therefore expensive, in terms of performance.

For example, when an MS-DOS-based application running under 386 enhanced mode tries to read from a file, the following occurs: Windows starts running the application in real mode. It makes an Int 21H call to read from the file. The 386 enhanced mode traps this interrupt and switches to protected mode, where a number of virtual device drivers look at the call and try to qualify it. If none of the device drivers intercept the call, then the call is approved, and is subsequently handed off to MS-DOS. Windows then switches back to real mode to let MS-DOS handle the call. MS-DOS takes a considerable amount of time to read a particular location on the disk. Once it is finished, MS-DOS generates an Int 13H call to talk to the BIOS.

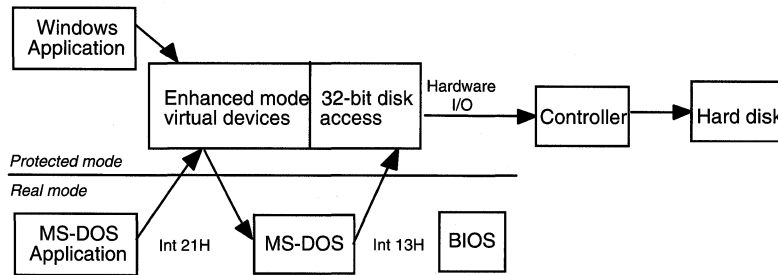
Hard Disk Access Under Windows with 32-Bit Disk Access

32-bit Disk Access helps to reduce the number of mode switches between real mode and protected mode by processing the Int 13H request in protected mode.

Windows 3.1 32-bit Disk Access filters all application calls to the hard disk controller, passing the requests directly to the controller bypassing the system BIOS. This takes the BIOS out of the loop for hard disk access, allowing BIOS calls for that drive to be handled entirely in protected mode.

With 32-bit Disk Access enabled, Windows can start trapping Int 13H calls and handle them entirely in protected mode. With 32-bit Disk Access, the call diagram looks like this:

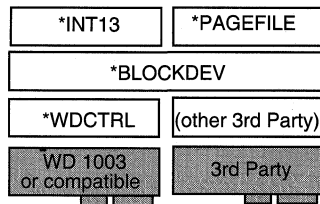
Figure 1.6
Hard disk access path under Windows with 32-bit Disk Access



Components of the 32-Bit Disk Access System

The following diagram shows the 32-bit Disk Access architecture originally designed for Windows 3.1, which is also used by Windows for Workgroups 3.11.

Figure 1.7
32-bit Disk Access Components included with Windows for Workgroups



The 32-Bit Disk Access model is based on Western Digital 1003 controller compatibility and is composed of the following 386 enhanced mode virtual device drivers:

Driver	Function
*Int13	Traps and emulates Int 13H BIOS calls made by the application to the hard disk controller. It passes these calls to BlockDev for filtering and queuing. Int 13 and PageFile (below) act as the input system for 32-bit Disk Access.
*PageFile	Handles virtual memory paging files. It makes calls through BlockDev to the hard disk controller when appropriate.
*BlockDev	This is the core of the 32-bit hard disk access system. It creates and manages the queue of Int 13H calls to the hard disk controller. It filters Read, Write, and Cancel calls and passes them on to the controller, and sends other calls to the BIOS for processing.
*WDCTRL	This is the 32-bit Disk Access device that talks to standard Western Digital 1003 or ST506 hard disk controllers (about 90 percent of the installed base). This device is installed only if the Setup program detects a compatible hard disk controller.

Note The asterisk (*) preceding a component name indicates that this is an internal component of Windows for Workgroups rather than a physical file. You will not find a file with this name on your Windows for Workgroups 3.11 disks.

Sample SYSTEM.INI sections showing 32-bit Disk Access components

```
[386Enh]
32bitdiskaccess=on
device=*blockdev
device=*pagefile
device=*int13
device=*wdctrl
```

This sample shows the entries included in SYSTEM.INI when 32-bit Disk Access is enabled with the WDCTRL FastDisk device driver. If you are using a different FastDisk device driver, an entry reflecting the name of the device driver you are using appears in place of the **device=*wdctrl** entry shown here.

32-Bit File Access

Windows for Workgroups 3.11 extends the 32-bit Disk Access system architecture of Windows 3.1 and Windows for Workgroups 3.1 to provide 32-bit File Access as well. 32-bit File Access provides a 32-bit code path for Windows to access and manipulate information on disk by intercepting the MS-DOS Int 21H services in protected mode, rather than handling the Int 21H services in real mode by MS-DOS. This results in greatly improved disk I/O performance when reading information from or writing information to a supported disk device configuration over a similarly configured computer running Windows 3.1 or Windows for Workgroups 3.10.

The Int 21H services manipulate the MS-DOS File Allocation Table (FAT), which governs the way information is written to and read from a FAT-based disk volume. In addition to protected-mode Int 21H services, 32-bit File Access also provides a 32-bit protected-mode replacement for the MS-DOS-based SmartDrive disk cache program which features more intelligent disk cache management and results in improved disk I/O performance for the Windows environment. The 32-bit File Access functionality in Windows for Workgroups 3.11 is implemented as two Windows virtual device drivers, VFAT.386 and VCACHE.386 (discussed in more detail later in this section).

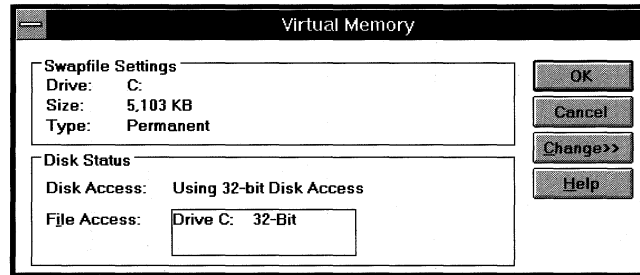
As with 32-bit Disk Access, the 32-bit File Access feature is disabled by default when Windows for Workgroups 3.11 is installed. 32-bit File Access can be enabled through the 386 Enhanced dialog box in the Windows Control Panel. If you don't enable 32-bit File Access, be sure continue using SmartDrive, shipped with Windows for Workgroups 3.11, to provide disk caching functionality.

Enabling 32-Bit File Access

To view the disk status for 32-bit Disk Access and 32-bit File Access to determine whether 32-bit File Access is presently being used to manipulate information on a given disk device, double-click the Enhanced icon in Control Panel and choose the Virtual Memory button. The Disk Status section of the Virtual Memory dialog box shows the state of the different drives detected in the system. For the disk volumes on which 32-bit File Access is supported, "32-Bit" will be displayed next to the drive letter. For disk volumes on which 32-bit File Access is not supported, "16-Bit" will be displayed next to the drive letter. For example, the following dialog box shows that 32-bit File Access is supported on drive C.

Figure 1.8

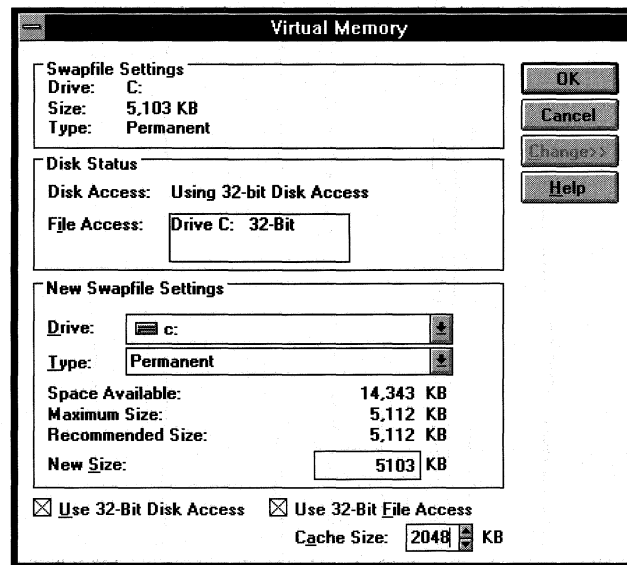
Virtual Memory dialog box is used to configure 32-bit Disk Access and 32-bit File Access



Choose the Change>> button to display the virtual memory configuration section of the dialog box, which allows 32-bit File Access to be enabled and configured. To enable 32-bit File Access, select the Use 32-Bit File Access check box as shown in Figure 1.9. When 32-bit File Access is enabled, you need to set the size of the cache to be used by the 32-bit File Access components. The default size is dependent upon the amount of memory installed in your computer. Most likely, you will want to increase the size of the cache to provide the best level of disk I/O performance when using 32-bit File Access. For recommendations on the cache size configuration, see Chapter 11, "Optimizing Windows for Workgroups 3.11."

Figure 1.9

32-Bit File Access is enabled from the Virtual Memory dialog box accessible from the Enhanced section of Control Panel



Requirements for 32-Bit File Access

As discussed in the previous section, 32-bit Disk Access implemented in Windows intercepts Int 13H calls destined for the BIOS routines which communicate with the hard disk controller. 32-bit File Access intercepts MS-DOS Int 21H calls which manipulate information stored on a disk device. The VFAT virtual device (VFAT.386) provides support for the protected-mode Int 21H services. When VFAT loads, it identifies the different physical hard disk drives in your system and mounts on hard disk volumes that are supported by 32-bit Disk Access components. As related to 32-bit File Access, *mounting* refers to the process that VFAT goes through to tell the system to pass file I/O calls through VFAT rather than through the MS-DOS device driver chain.

Just as MS-DOS uses the real-mode BIOS routines to communicate with the hard disk controller to read and write information to and from a hard disk, VFAT uses the protected-mode 32-bit Disk Access components to read and write information from/to a hard disk. In order for VFAT to mount on a given disk volume, one of the following two conditions is necessary:

- A 32-bit Disk Access driver is used with a compatible disk controller (for example, the WDCTRL driver is used with a controller compatible with the Western Digital 1003 controller).
- The real-mode mapper (described in the next section) is installed to provide a 32-bit Disk Access interface to the MS-DOS device driver chain.

Note If the MS-DOS SUBST utility is invoked before Windows for Workgroups 3.11 is loaded, the 32-bit File Access functionality will not be enabled. If the SUBST utility is used, an error message will be displayed when Windows for Workgroups is started.

Real-Mode Mapper

As mentioned in the previous section, VFAT will only mount on hard disk volumes that have the 32-bit Disk Access components installed. However, some drives may not have a 32-bit Disk Access driver. Even if they do, additional processing may be required after the information is passed off by VFAT towards the disk volume, or before information reaches VFAT from the disk volume.

There are many hard disk controllers that do not have a compatible 32-bit Disk Access driver to provide 32-bit Disk Access. Typical examples include SCSI and ESDI controllers. To mount VFAT on disk volumes attached to these disk controllers, VFAT must see a 32-bit Disk Access interface for a given disk volume. If no 32-bit Disk Access device driver is available to talk to the controller when 32-bit Disk Access is enabled, the disk access interrupt service routine (that is, for Int 13H) must be handled in real mode.

A special virtual device driver called the *real-mode mapper* (RMM.D32) provides a mapping service to take protected-mode file I/O calls from VFAT and send them through the MS-DOS device driver chain. The real-mode mapper is installed by the Virtual Memory dialog box automatically when 32-bit File Access is enabled and when either of the following conditions is true:

- 32-bit Disk Access is disabled
- A compressed disk volume is detected

The real-mode mapper driver file, RMM.D32, is not explicitly listed in the **[386enh]** section of the SYSTEM.INI file, but is loaded by the VXDldr.386 virtual device and supported by the IOS.386 virtual device (there will be a **device=vxdldr.386** and a **device=ios.386** line in the **[386Enh]** section of SYSTEM.INI). You can verify that the real-mode mapper is being used when a drive volume for which 32-bit Disk Access is not supported (for example, 32-bit Disk Access is disabled, or the disk volume is a compressed volume) shows “32-Bit” in the Disk Status section of the Virtual Memory dialog box as shown in Figures 1.8 and 1.9.

When the real-mode mapper is installed, the following lines will be present in the **[386Enh]** section of SYSTEM.INI (if 32-bit Disk Access is enabled, other entries may also be present):

```
[386Enh]
device=ifsmgr.386
device=ios.386
device=vxdldr.386
device=vfat.386
device=vcache.386
```

Disk Compression Software

Another example of when the real-mode mapper driver is used is when you need VFAT support for a disk volume using a software-based disk compression technique, such as DoubleSpace provided with MS-DOS 6.2 or Stacker from Stac Electronics. Because additional processing of the data is necessary before writing information to the disk controller or after reading information from the disk controller, the 32-bit Disk Access components cannot be used on the compressed volume. In this scenario, it is necessary for VFAT to go through the MS-DOS device driver chain to properly handle Int 21H requests.

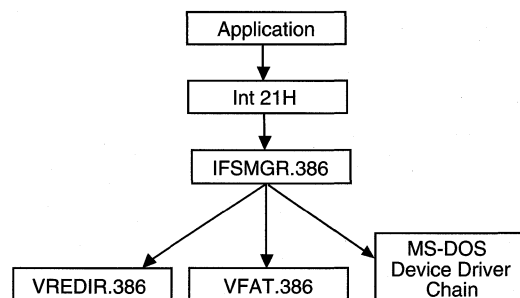
Note VFAT will not mount on a DoubleSpace drive using MS-DOS 6.0. VFAT requires MS-DOS 6.2 to be used. If you are using MS-DOS 6.0, contact Microsoft for information on getting an upgrade to MS-DOS 6.2.

IFS Manager

The heart of the file system components provided in Windows for Workgroups 3.11 is the Installable File System (IFS) Manager virtual device driver (IFSMGR.386). IFS Manager maintains a table identifying the type of file system device associated with each connected disk volume and passes the file I/O request to the appropriate device. When an application makes an Int 21H call, IFSMGR intercepts it and checks its table of installed devices. If the Int 21H call is destined for a network drive, it passes the request to the network redirector (VREDIR.386). If the Int 21H call is for a drive mounted by VFAT, it passes the request to VFAT. If the Int 21H call is not passed to one of the other IFS Manager drivers, it is passed to the real-mode MS-DOS device driver chain and handled by MS-DOS.

Figure 1.10

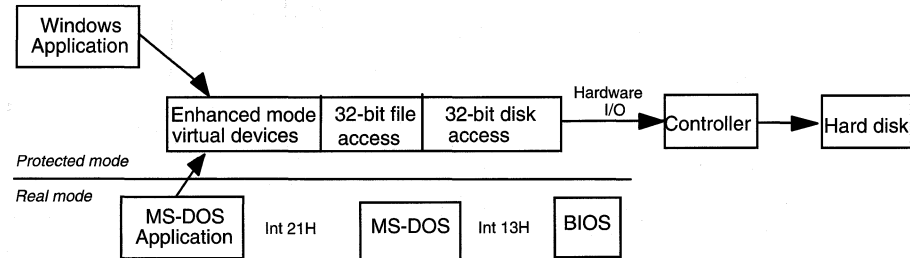
Role of IFS Manager (IFSMGR.386) for passing data to network redirector, 32-bit file access, and MS-DOS



Any Int 21H calls that are processed by VFAT are handled entirely in protected mode. This results in improved disk I/O performance over previous versions of Windows. With 32-bit File Access installed in addition to 32-Bit Disk Access, the sequence of events to process a file I/O request is shown in Figure 1.11:

Figure 1.11

Hard disk access under Windows with 32-bit Disk Access and 32-bit File Access



With VFAT there is only one mode transition to process an Int 21H request from an MS-DOS-based application, and no mode transitions to process an Int 21H request from a Windows-based application. The remaining calls are processed in protected mode. The performance increase obtained by 32-bit Disk Access by avoiding a processor mode transition is now increased further with 32-bit File Access.

A companion driver to VFAT.386 is VCACHE.386. VCACHE is responsible for providing management routines to handle the cache for both VFAT.386 and VREDIR.386. VCACHE is responsible for the cache operations, including allocating cache memory, freeing cache memory, and managing the algorithm that oversees how data is aged in the cache in case existing data in the cache needs to be replaced with newer incoming data.

32-Bit Disk Cache

In addition to providing Int 21H FAT services in protected mode, VFAT, working in conjunction with VCACHE.386, provides a 32-bit protected-mode replacement for the MS-DOS-based SmartDrive disk cache program. VFAT is responsible for reading and writing information from or to the disk device, while VCACHE is responsible for managing the information VFAT writes to or is present in the cache. The caching routines provided as part of 32-bit File Access differ from that offered by SmartDrive in the following ways:

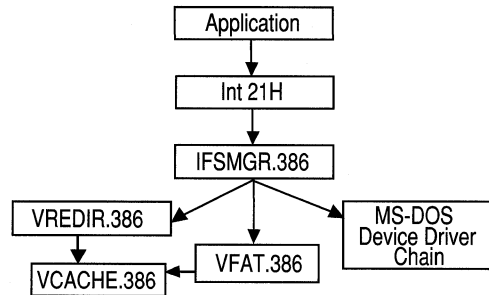
- 32-bit File Access caching routines are implemented as 32-bit protected-mode code, thus reducing the need to transition to real mode to cache disk information.
- 32-bit File Access read-ahead routines work on a per-file basis rather than on a per-sector basis, thus helping to ensure that information read into the disk cache will be used with a higher probability.

- 32-bit File Access caching routines share cache memory with the protected-mode network redirector (VREDIR.386), thus reducing the extra memory overhead for maintaining multiple cache buffers.
- 32-bit File Access caching routines cache information on a per-file basis providing improved performance over SmartDrive, which caches on a contiguous-sector basis.

Figure 1.12 illustrates where VCACHE fits into the Int 21H flow of data and its interaction with VREDIR.386.

Figure 1.12

Relationship of VCACHE.386 virtual device for sharing cache between VREDIR and VFAT



What is a Disk Cache?

One primary function of a disk cache is to intercept system calls to the device drivers for the hard disk controller to try to reduce the need for read-write access to the disk. The disk cache routines interpret any calls to the hard disk and load the needed data into a cache in the extended memory portion of RAM.

Subsequent read-write requests to the hard disk are intercepted by the disk cache routines, which search the cache for the requested data. If the data is already present in the cache, the application will access it directly from RAM - which is faster than reading the information from the hard disk. If the data is not in the cache, the disk cache routine accesses the hard disk and loads the necessary data into the cache. The least-recently used data residing in RAM is discarded, unless a change has been made to it that necessitates writing it back to the hard disk, making room for the new data. By loading blocks of data from the hard disk into RAM, the disk cache software helps decrease the number of accesses to the hard disk, which can slow down applications because accessing the hard disk is considerably slower than accessing RAM. Essentially, the disk cache is responsible for maintaining information in RAM that an application may need from the hard disk in the near future.

A technique called *read-ahead caching*, is used by some disk cache software to try to anticipate the information that the system may need next from the disk device and read this information into the cache before the actual request comes from the system to access this information. If the read-ahead cache contains the information that the system next needs, this will result in a performance improvement as the system does not need to read the information from disk. However, if the read-ahead cache does not contain the information requested by the system, the information will need to be read from the disk. There are several approaches for basing algorithms for performing read-ahead caching activities. Two such approaches are caching on a contiguous-sector basis and caching on a per-file basis.

Caching on a *contiguous-sector basis* means that a given request results in the cache routines also reading ahead additional contiguous sectors from the disk volume with the assumption that the next request is in the next contiguous group of sectors from the previous sector just read. This type of read-ahead feature works well for some database applications or other types of sequential file access. However, this scenario assumes that a given file is contiguous. For a fragmented file, a read-ahead operation on a contiguous sector basis may read parts of other files into the cache that may never be accessed, resulting in filling the cache with unnecessary information that will be eventually be discarded. A cache does not improve performance if information read into the cache is not subsequently accessed from the cache.

Caching on a *per-file basis* means that a given request reads the requested portion (in sectors) of the file and also reads ahead additional sectors of the file with the assumption that the next request is for the next part of the file just read. This type of read-ahead is more efficient since information is only read ahead from within the requested file and unneeded information from other files is not loaded into the cache due to fragmentation as with a contiguous sector-based algorithm.

A technique called *write-behind caching*, or *lazy writing*, is also used by some disk cache systems to cache data destined to be written to the disk device, but delays the actual writing of information to the disk device until a time when the computer system is less busy. The time delay can vary, but is usually no more than a matter of milliseconds or several seconds. When a cache system supports write-behind functionality, control is returned to the application that is writing the data much more quickly because instead of writing the information out to a disk device, the information is stored temporarily in RAM. While the use of a write-behind cache can improve the perceived disk I/O performance, it can pose some problems. With the write-behind cache, the information is not written to the disk device until the information from the cache is flushed. Because of this, it is important to not turn off a computer immediately after performing an operation where an application may have written information into the cache, but before it has had a chance to be written to the hard disk.

Caching and Disk Compression Software

In order for write-behind caching to be safe, it is necessary for the cache routines to be able to reliably know the amount of free disk space left on a given disk volume. Knowing the amount of free disk space on non-compressed disk volumes is pretty straight-forward; however, knowing the amount of free disk space on a compressed volume is difficult. The difficulty lies in not knowing exactly how much space the compressed information will use on the disk given the fact that different types of data compress to different sizes.

By default, write-behind caching is disabled on all compressed disk volumes that VFAT mounts, with the exception of DoubleSpace drives under MS-DOS 6.2. (As mentioned earlier, VFAT will not mount on a DoubleSpace drive under MS-DOS 6.0.) MS-DOS 6.2 features an API mechanism that VFAT can use to query the minimum amount of disk space remaining so that lazy writing can be enabled and used safely. VFAT is unable to reliably determine the minimum amount of free disk space when other disk compression software is installed due to the lack of an API call to obtain this information.

For other disk compression software, lazy writing can be forced on using the **ForceLazyOn=** switch in the **[vcache]** section of the SYSTEM.INI file. For more information, see Chapter 4, "Windows for Workgroups 3.11 Initialization Files."

Warning If lazy writing is forced on for a compressed disk volume other than DoubleSpace under MS-DOS 6.2, check to make sure you have sufficient disk space to complete all data writes to the disk. If the disk becomes full and a lazy write occurs, VFAT will report that the disk is full, but the application program that made the original write will assume that the write was completed successfully. Data loss may result in this case.

Removing or Reconfiguring SmartDrive

With Windows 3.1 and Windows for Workgroups 3.1, it was necessary to use SmartDrive to support disk cache functionality. When 32-bit File Access is enabled, the combination of VFAT and VCACHE replaces the functionality offered by SmartDrive by providing 32-bit protected-mode cache functionality. SmartDrive caching is automatically disabled for drives mounted by VFAT.

(You can identify the drives that SmartDrive is caching when running in Windows for Workgroups 3.11 by starting an MS-DOS command prompt and typing **smartdrv**.) However, 32-bit File Access will not reclaim the memory used by SmartDrive for its cache.

If you are presently using SmartDrive, when 32-bit File Access is enabled the setup code will reconfigure the size of the SmartDrive disk cache to reduce the size of the cache while running in Windows for Workgroups to 128K free up additional memory.

SmartDrive 5.0 offers the ability to cache information on CD-ROM drives and floppy disk drives, while 32-bit File Access does not. If you do not need to cache information on CD-ROM drives or floppy disk drives, you should reduce the size of the cache used by SmartDrive for Windows, or remove the SMARTDRV.EXE line from your AUTOEXEC.BAT file. Also, if you are using MS-DOS 6.0 and DoubleSpace, it is necessary to continue to use SmartDrive to provide support for disk caching.

Chapter 11, "Optimizing Windows for Workgroups 3.11," provides more information on configuring Windows for Workgroups 3.11 to operate optimally. The information covered includes the recommended size of the cache to use with 32-bit File Access based on the amount of memory in your computer and the type of operations you expect to be performing.

Configuration Scenarios

To help further illustrate the interaction of the 32-bit Disk Access and 32-bit File Access drivers and summarize the preceding sections, this section describes some common disk-access scenarios:

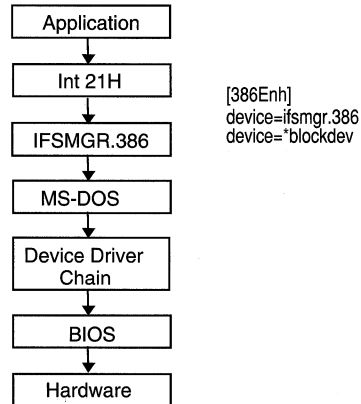
- Non-32-bit Disk Access or non-VFAT mounted volume
- WDCTRL 32-bit Disk Access volume
- VFAT mounted on WDCTRL 32-bit Disk Access volume
- VFAT mounted on non-32-bit Disk Access volume
- VFAT mounted on a compressed non-32-bit Disk Access volume
- VFAT mounted on a compressed WDCTRL 32-bit Disk Access volume

Non-32-Bit Disk Access or Non-VFAT Mounted Volume

By default, Windows for Workgroups does not enable 32-bit Disk Access or 32-bit File Access. After the initial setup of Windows for Workgroups, the flow of file I/O through the Windows device drivers looks like Figure 1.13.

Figure 1.13

Default flow of file I/O



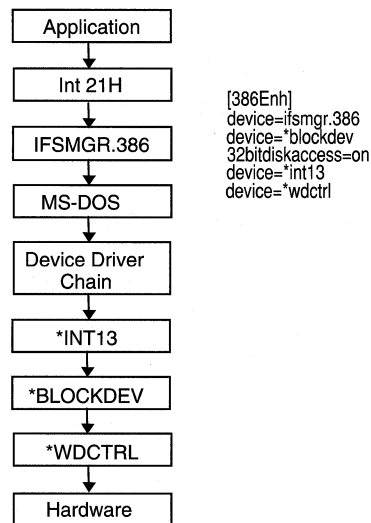
In this scenario, Int 21H calls are processed by MS-DOS and the real-mode MS-DOS device drivers. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also indicated.

WDCTRL 32-Bit Disk Access Volume

If the user enables 32-bit Disk Access, all Int 13H calls are handled by the 32-bit Disk Access driver. Figure 1.14 illustrates the path of information that is passed to the WDCTRL 32-bit Disk Access driver.

Figure 1.14

Flow of file I/O when 32-bit Disk Access is enabled



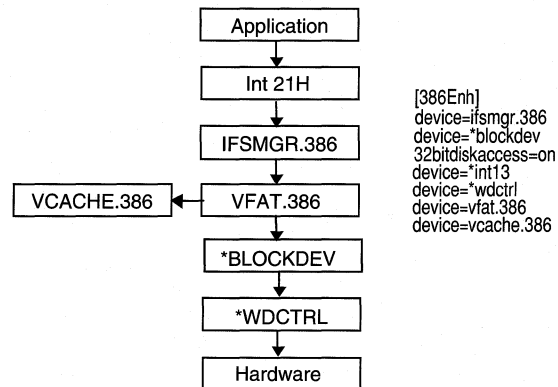
In this case, Int 21H calls are processed by MS-DOS and the real-mode MS-DOS device drivers. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also indicated.

VFAT Mounted on WDCTRL 32-Bit Disk Access Volume

If the user enables 32-bit Disk Access and 32-bit File Access, all Int 13H calls are handled by the 32-bit Disk Access driver WDCTRL, and Int 21H calls are handled by the 32-bit File Access driver VFAT, respectively. Figure 1.15 illustrates the path of information that is passed to the WDCTRL 32-bit Disk access driver after the Int 21H call is processed by VFAT. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also indicated.

Figure 1.15

Flow of file I/O when both 32-bit Disk Access and 32-bit File Access are enabled

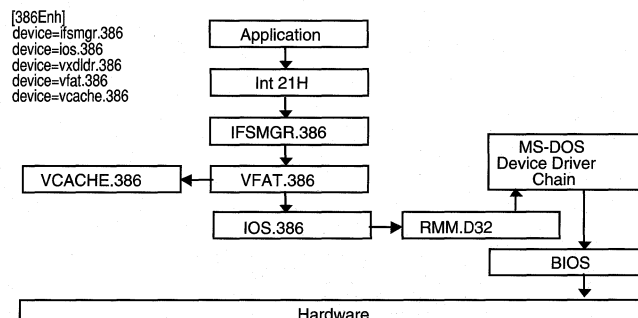


VFAT Mounted on Non-32-Bit Disk Access Volume

Figure 1.16 shows what happens if the user enables 32-bit File Access and VFAT mounts on a non-32-bit Disk Access volume (for example, a disk drive on a SCSI controller).

Figure 1.16

Flow of file I/O when 32-bit File Access is enabled and VFAT is mounted on a non-32-bit volume



In this case, the real-mode mapper (RMM.D32) driver is installed. Int 21H calls are handled by the 32-bit File Access driver VFAT, and then are passed through the real-mode mapper to the MS-DOS device driver chain to be written to or read from the disk device. As shown in Figure 1.16, information is passed through the real-mode mapper after the Int 21H call is processed by VFAT. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also indicated (note that VXDLDR.386 is responsible for loading RMM.D32).

VFAT Mounted on a Compressed Non-32-Bit Disk Access Volume

This time, the user enables 32-bit File Access and VFAT mounts on a non-32-bit Disk Access volume for which disk compression software is used.

Again, the real-mode mapper (RMM.D32) driver is installed and Int 21H calls are handled by VFAT, before being passed through the real-mode mapper to the MS-DOS device driver chain. In turn, the MS-DOS device driver chain passes the information through the compression software drivers.

Figure 1.17

Flow of file I/O when 32-bit File Access is enabled and VFAT is mounted on a non-32-bit volume with disk compression

```
[386Enh]
device=ifsmgr.386
device=ios.386
device=vxldr.386
device=vfat.386
device=vcache.386
```

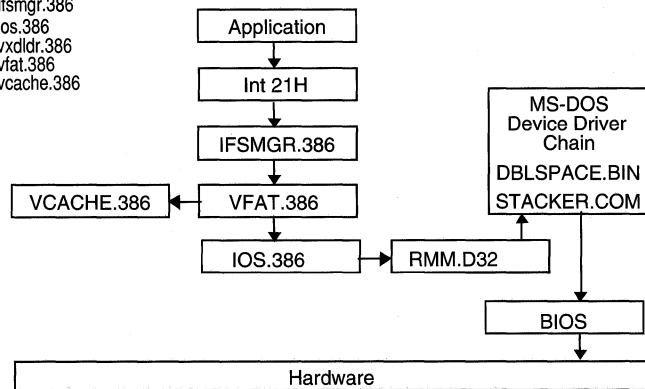


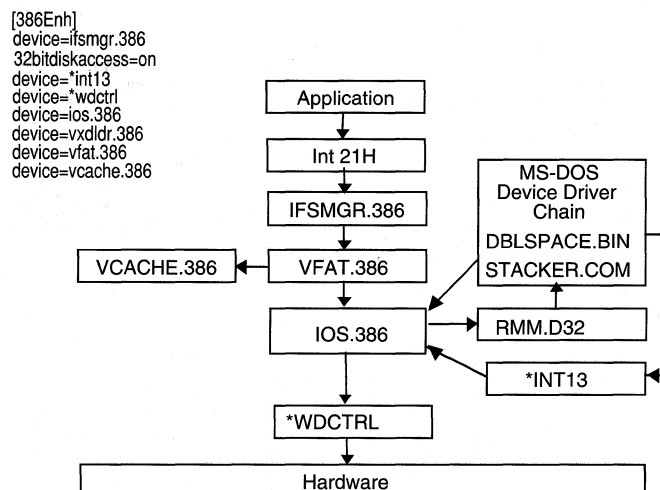
Figure 1.17 shows the path of information that is passed through the real-mode mapper to the compression utility after the Int 21H call is processed by VFAT. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also shown. (Note that VXDLDR.386 is responsible for loading RMM.D32.)

VFAT Mounted on a Compressed WDCTRL 32-Bit Disk Access Volume

Figure 1.18 illustrates what happens when the user enables 32-bit Disk Access and 32-bit File Access, and VFAT mounts on a 32-bit Disk Access volume for which disk compression software is used.

Figure 1.18

Flow of file I/O using
32-bit File Access,
32-bit Disk Access, and
VFAT on a 32-bit
volume with disk
compression



In this scenario, the real-mode mapper (RMM.D32) driver is installed. Int 21H calls are handled by the 32-bit File Access driver VFAT. If the disk volume that is accessed is a compressed volume, the information is passed through the real-mode mapper to the compression software driver. The Figure 1.18 illustrates the path of information flow. On a 32-bit Disk Access volume, after the information is handled by the MS-DOS device driver chain, it is passed back to the 32-bit Disk Access driver for I/O to the disk controller. Information on the relevant entries in the [386Enh] section of SYSTEM.INI is also indicated (note that VXDLDR.386 is responsible for loading RMM.D32).

Windows for Workgroups 3.11 Boot Sequence

So far, this chapter has discussed the new and enhanced components that make up Windows for Workgroups 3.11. This section describes how Windows for Workgroups components are loaded when you boot your computer.

Information covered in this section is helpful to identify the operations that Windows for Workgroups performs between the time the user types **win** at the MS-DOS command prompt and the time Program Manager displays the configured icons for the user to begin invoking applications.

When a user starts Windows for Workgroups 3.11, the following startup process is performed:

1. The user types **win** at the MS-DOS command prompt to invoke WIN.COM.
Windows displays the startup logo image contained in the WIN.COM file.
2. WIN.COM invokes the MS-DOS Exec function to load the Windows 386 enhanced mode system kernel, WIN386.EXE.
Windows clears the logo screen and the video display adapter switches to text mode.
3. WIN386.EXE loads the following:
 - The Virtual Machine Manager (VMM)
 - All virtual device drivers (VxDs) specified in the SYSTEM.INI file.
4. If VXDLDR.386 and IOS.386 are listed in the **[386Enh]** section of SYSTEM.INI, they are initialized next. VXDLDR loads RMM.D32.
5. VFAT begins mounting drives during IFSMGR.386 initialization and begins caching after IFSMGR initialization is completed.
6. VNETSUP.386 initializes and parses the SYSTEM.INI examining the network information.
The NDISLOG.TXT file begins documenting NDIS driver load failures. A new NDISLOG.TXT file is created each time you start Windows for Workgroups.
7. All other network drivers defined in the **[386Enh]** section of SYSTEM.INI initialize and bind. (Each of these drivers refers to VNETSUP.386 for relevant parameters in the SYSTEM.INI file.)
8. The network redirector, VREDIR.386, starts the workstation services.
9. WIN386.EXE loads the 386 enhanced mode kernel, KRNL386.EXE.

10. KRNL386.EXE loads the following files:

- The Windows drivers (identified as *.DRV in the SYSTEM.INI file)
- GDI.EXE
- USER.EXE
- Supporting files (for example, fonts)
- The Windows for Workgroups 3.11 network driver, WFVNET.DRV

The BOOTLOG.TXT file begins documenting driver events. If a BOOTLOG.TXT file already exists, new entries will be appended to the existing file. Then the Windows desktop appears on the screen.

11. If sharing is enabled, the network server, VSERVER.386, starts the server service. If security settings are being updated remotely from a specified network server and share, the updated security settings are downloaded at this time. The persistent network shares as configured by the Windows for Workgroups workstation are shared on the network.

12. If Network DDE is enabled, WFVNET.DRV loads the Network DDE background application, NETDDE.EXE, and the ClipBook Server background application, CLIPSRV.EXE.

The Windows for Workgroups network logon dialog box is displayed.

13. WFVNET.DRV prompts the user to log on to the network if the user has not done so already. If the user initially logged on with no password (that is, the user pressed ENTER at the password prompts), the logon will be done automatically without displaying the logon dialog box.

14. If the user is logged on to the network successfully, WFVNET.DRV then restores the persistent network connections made during the last Windows for Workgroups session according by reading from the CONNECT.DAT file.

15. KRNL386.EXE launches the Windows shell as identified by the **Shell=** entry in the [boot] section of the SYSTEM.INI file. By default, this is the Windows Program Manager, PROGMAN.EXE.

Program Manager displays on the Windows desktop.

16. The **Load=** and **Run=** lines of the WIN.INI are processed.

Items specified by the **Load=** and **Run=** lines in WIN.INI are started.

17. The program items in the StartUp group are processed.

Items specified in the StartUp group are started.

Driver Configuration Changes from Windows for Workgroups 3.10

Windows for Workgroups 3.11 defines and loads network and supporting device drivers in the system differently than Windows for Workgroups 3.10. This section describes the differences and discusses how these changes may affect the use of third-party network protocols or network redirectors.

Review of Windows for Workgroups 3.10 Configuration

Windows for Workgroups 3.10 loads network drivers in the CONFIG.SYS file and any network module commands in the AUTOEXEC.BAT file.

CONFIG.SYS

The system drivers that were used by Windows for Workgroups 3.10 and specified in the CONFIG.SYS file include:

- PROTMAN.DOS, the Protocol Manager driver
- WORKGRP.SYS, the real-mode stub for networking components
- *.DOS files, any installed NDIS network adapter card drivers

In addition to these standard real-mode drivers, real-mode network protocols such as Microsoft TCP/IP for Windows for Workgroups and Microsoft Data Link Control (DLC) protocol for Windows for Workgroups are loaded in the CONFIG.SYS and AUTOEXEC.BAT files in Windows for Workgroups 3.10.

Sample CONFIG.SYS file entries for Windows for Workgroups 3.10

```
C:\WINDOWS\PROTMAN.DOS /I:C:\WINDOWS
C:\WINDOWS\<NDIS MAC driver>.DOS { for example, EXP16.DOS }
C:\WINDOWS\WORKGRP.SYS
{ real-mode protocols as installed }
```

The Protocol Manager, PROTMAN.DOS, needs to load first. It configures network adapter card drivers and protocols, and allow these components to bind together. To work properly, many third-party network protocols and network redirectors require PROTMAN.DOS to load before their components. That is, PROTMAN.DOS must be listed before any of these third-party components are listed in CONFIG.SYS or AUTOEXEC.BAT.

The WORKGRP.SYS driver is a support driver for Windows for Workgroups 3.10 networking components and is usually listed as the last driver file Windows for Workgroups 3.10 loads.

AUTOEXEC.BAT

Windows for Workgroups 3.1 requires a relatively simple AUTOEXEC.BAT file. The **net start** command is used to start the Windows for Workgroups 3.10 networking components. The **net start** command line usually must be listed before any third-party network protocols or networking components are referenced in the AUTOEXEC.BAT file.

Sample AUTOEXEC.BAT file entry for Windows for Workgroups 3.10

```
C:\WINDOWS\net start
```

Third-Party Network Drivers

When a third-party network adapter card driver or network protocol is loaded through the use of an OEMSETUP.INF file provided by the third-party vendor, the Windows for Workgroups 3.10 setup program is responsible for configuring the components by placing the specified lines in either the CONFIG.SYS or AUTOEXEC.BAT file.

Windows for Workgroups 3.11 Configuration

Windows for Workgroups 3.11 further simplifies the configuration for networking components. A major change from Windows for Workgroups 3.10 is that the network adapter card drivers and network support files are specified in the SYSTEM.INI file rather than the CONFIG.SYS file in Windows for Workgroups 3.11.

CONFIG.SYS

Windows for Workgroups 3.11 only puts one line in the CONFIG.SYS file independent of the configuration of drivers that are used on a Windows for Workgroups 3.11 computer.

Sample CONFIG.SYS file entry for Windows for Workgroups 3.11

```
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

The IFSHLP.SYS file is used to provide real-mode support for the IFS manager that is responsible for passing data to the appropriate device, whether the device is installed locally or elsewhere on the network. This is the only line that Windows for Workgroups 3.11 adds to the CONFIG.SYS file. The lines used by Windows for Workgroups 3.10 (described in the previous section) are removed from the CONFIG.SYS file or are moved to the appropriate section of the SYSTEM.INI file as described below.

AUTOEXEC.BAT

Windows for Workgroups 3.11 still uses the **net start** command in the AUTOEXEC.BAT file. Windows for Workgroups Setup usually places this line as the first line in your AUTOEXEC.BAT file.

Sample AUTOEXEC.BAT file entry for Windows for Workgroups 3.11

C:\WINDOWS\net start

SYSTEM.INI

Windows for Workgroups 3.11 places entries defining the network adapter card drivers and network protocols in the SYSTEM.INI file. In the SYSTEM.INI file, NDIS 3.0 32-bit network adapter card drivers are listed in the **[386Enh]** section, and NDIS 2.0 drivers are listed in the **[network drivers]** section.

For further information on these SYSTEM.INI entries, see Chapter 4, "Windows for Workgroups 3.11 Initialization Files."

NDIS 3.0 Configuration

The NDIS 3.0 32-bit entries that are used in the **[386enh]** section include the following:

SYSTEM.INI entry	Description of entry
Netcard=	Identifies NDIS 3.0 network adapter card drivers to conditionally use if an NDIS 2.0 network adapter card driver is not loaded.
Netcard3=	Identifies NDIS 3.0 network adapter card drivers to use whether an NDIS 2.0 network adapter card driver is loaded or not. For example, this is used by the RASMAC driver.
NetMisc=	Identifies miscellaneous network virtual device drivers that are loaded.
Transport=	Identifies NDIS 3.0 network protocols that are to be loaded.

Sample SYSTEM.INI entries for the [386Enh] section

```
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
transport=nwlink.386,nwnblink.386,netbeui.386
netcard=ee16.386
netmisc=ndis.386,ndis2sup.386
netcard3=
```

Note The asterisk (*) preceding a component name indicates that this is an internal component of Windows for Workgroups rather than a physical file. You will not find a file with this name on your Windows for Workgroups 3.11 disks.

This sample NDIS 3.0 configuration uses an Intel EtherExpress 16 network adapter card driver, the NetBEUI protocol, and the IPX/SPX-compatible protocol with NetBIOS.

NDIS 2.0 Configuration

The NDIS 2.0 entries that are used in the [network drivers] section include the following:

SYSTEM.INI entry	Description of entry
DevDir=	Identifies the path name pointing to the location of the network device driver files and the PROTOCOL.INI file
LoadRMDrivers=	Identifies whether NDIS 2.0 real-mode drivers are loaded automatically when NET START is issued
Netcard=	Identifies the NDIS 2.0 network adapter card drivers to use
Transport=	Identifies NDIS 2.0 network protocols that are to be loaded

Sample SYSTEM.INI entries for the [network drivers] section

```
[network drivers]
netcard=exp16.dos
transport=*netbeui,ndishlp.sys
devdir=c:\windows
LoadRMDrivers=yes
```

This sample illustrates a configuration using an Intel EtherExpress 16 network adapter card and the real-mode NetBEUI protocol.

Using Net Initialize with Third-Party Network Drivers

When a third-party network adapter card driver or network protocol loads through the use of an OEMSETUP.INF file provided by a third-party vendor, Windows for Workgroups 3.10 setup program is responsible for configuring the components by placing the necessary lines referencing the appropriate drivers in either the CONFIG.SYS or AUTOEXEC.BAT file. Windows for Workgroups 3.11 should interpret the contents of the OEMSETUP.INF file properly and place the appropriate entries in the SYSTEM.INI file rather than the CONFIG.SYS file. As described in the previous section, real-mode networking components in Windows for Workgroups 3.11 are specified in the **[network drivers]** section of the SYSTEM.INI file.

Some third-party network drivers that load as TSRs require that the NDIS protocol manager load before allowing the TSRs to load. By default, Windows for Workgroups 3.11 loads the protocol manager, in addition to the real-mode network drivers (depending on the state of the **LoadRMDrivers=** entry in the **[network drivers]** section of SYSTEM.INI), and binds them when the **net start** command is issued. To load the Protocol Manager and network adapter card drivers without binding them to support the use of some third-party network components, it may be necessary to issue the **net initialize** (or **net init**) command before the **net start** command in the AUTOEXEC.BAT file.

The **net init** command loads protocol and network adapter card drivers without binding them to Protocol Manager. This command may be required when using a third-party network-adapter driver. You can then bind the drivers to Protocol Manager by typing **net start netbind**—by default, the **net start** command binds the drivers to Protocol Manager when it is issued.

Sample AUTOEXEC.BAT file entries

```
C:\WINDOWS\net init
{ third-party network driver TSRs }
C:\WINDOWS\net start
```

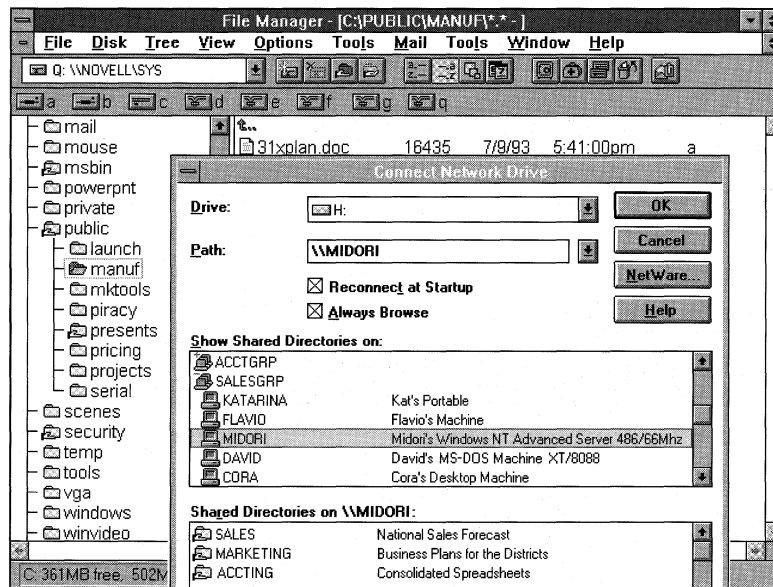
This sample shows the entries needed to support using a third-party TSR network driver.

Network Browsing

The Windows for Workgroups user interface allows users to *browse* network resources to access information or connect to resources available on the network. Users can scroll through a list of available workgroups, a list of available computers in a given workgroup, and a list of available resources on a given computer, to facilitate locating a network resource. For example, the Connect Network Drive dialog box used by File manager and the Connect Network Printer dialog box used by Print Manager will display a list of known workgroups and known computers that are presently running on the network. Figure 1.19 shows the Connect Network Dialog box with a list of workgroups and computers in the highlighted workgroup.

Figure 1.19

Connect Network Dialog box showing different types of Microsoft Windows Network servers.



Many network operating systems provide a mechanism to search for available resources on the network. However, depending on the implementation, browsing for network resources and maintaining a list of available resources on the network can cause an increase in network traffic. The other issue that a browsing implementation needs to contend with is scalability—browsing for resources on a small network can generally be pretty quick, however as the network grows, the issue of scalability becomes much more important in order for the users to experience a reasonable response rate when searching for

network resources. Windows for Workgroups 3.11 implements a browse service in such a way as to minimize the network traffic related to the browsing activity, while also providing an implementation that scales well to support both small and large networks.

Note The browse service used by Windows for Workgroups 3.11 is similar to, but not exactly the same as, the browse service used by Windows NT.

Browse List

In Windows for Workgroups 3.11, the browse service maintains an up-to-date list of domains, workgroups, and computers and provides the list to applications when requested. It provides the lists that are displayed in the Connect Network Drive and Connect Network Printer dialog boxes, for example; anywhere else Windows for Workgroups presents lists of domains, workgroups, or computers (for example, in the Select Computer dialog box in Chat); and also through the real mode networking components such as by the **net view** command.

The list can contain the names of domains, workgroups, and computers that are running the server service, including the following:

- Windows for Workgroups computers
- Workgroup Add-on for MS-DOS servers
- Windows NT workstations
- Windows for Workgroups workgroups
- Windows NT workgroups
- Windows NT Advanced Server domains and servers
- LAN Manager 2.x domains and servers

The browse list is maintained by a *browse server* for a given workgroup.

Role of a Browse Server

A browse server is a Windows for Workgroups 3.11 workstation that has been delegated by the network to support the browsing service requests for the workgroup to which it belongs. The role of a browse server is to provide a Windows for Workgroups 3.11 computer with a list of available network workgroups and computers in a given workgroup (referred to as a browse list)

in response to a request by an application or network component. When a user requests to connect to a network drive or network printer, for example, the Windows for Workgroups network components query one of the browse servers present in the workgroup to which the user's computer belongs, and requests the list of workgroups on the network and the list of computers in the default workgroup.

For each workgroup, the master copy of this list is maintained by a computer that is designated as a master browse server, and a copy of the list may also be maintained by one or more computers designated as backup browser servers.

Master and Backup Browse Servers

The Windows for Workgroups 3.11 browse service uses the concept of a *master* browse server and a *backup* browse server when maintaining the browse list. There is only one master browse server for a given Windows for Workgroups 3.11 workgroup for each network transport used in the workgroup, however there may be one or more backup browse servers for a given workgroup for each network transport.

The master browse server is responsible for maintaining the master list of workgroups, domains, and computers in a given workgroup. In order to minimize the amount of traffic that the master browse server may be subjected to when handling browsing services, backup browse servers may be designated in a workgroup to help offload some query requests. In general, there is approximately one browse server for every 15 Windows for Workgroups computers assigned to a given workgroup.

How a Browse Server is Designated

When Windows for Workgroups 3.11 is started on a computer, the computer first checks to see if a master browse server is already present for the given workgroup. If a master browse server doesn't exist, the computer starts an election to serve as the master browse server for the workgroup.

If a master browse server already exists, Windows for Workgroups 3.11 will detect the number of computers in the workgroup, and the number of browse servers present. If the number of computers in the workgroup exceeds the defined ratio of browse servers to computers in a workgroup, an additional computer in the workgroup may become a backup browse server.

The **MaintainServerList=** entry in the **[network]** section of SYSTEM.INI provides a mechanism to control the designation of computers in a workgroup that can become browse servers. If **MaintainServerList=Yes** is set, the computer will automatically try to be a backup browse server (the default is **auto** which means it is up to the master browse to designate a backup browse server when needed). Otherwise, a computer will only become a backup browse server if requested by a master browse server. For additional information, see Chapter 4, "Windows for Workgroups 3.11 Initialization Files."

How New Computers Are Added to the Browse List

When a Windows for Workgroups 3.11 computer is started on the network, it announces itself to the master browse server for the workgroup it is defined in, and the master browse server adds the new computer to the list of available computers in the workgroup. The master browse server will then send an update notification to the backup browse servers notifying them that a change to the browse list is available. The backup browse servers then request the new or changed information to update their local browse lists. Note that it may take as long as 15 minutes before a backup browse server receives an updated browse list, thus a new computer on the network may not show up in a user's request for a browse list until this time has elapsed.

How Computers Are Removed From the Browse List

When a Windows for Workgroups 3.11 computer shuts down gracefully (i.e., when a user selects to exit Windows for Workgroups rather than powering off the computer or rebooting the computer without exiting), the Windows for Workgroups computer will send an announcement to the master browse server to inform it that the computer is shutting down. The master browse server will then send an update notification to the backup browse servers notifying them that a change to the browse list is available. The backup browse servers will request the changes to the browse list.

If a user turns off his/her computer or reboots the computer without gracefully exiting Windows for Workgroups, the computer will not get a chance to send a message to the master browse server informing it that Windows for Workgroups is shutting down. If the master browse server does not receive notification that the Windows for Workgroups has shut down, the computer name may continue to appear in the browse list until the name entry times out, which can take up to 45 minutes.

Identifying Browse Servers In Your Workgroup

The Windows for Workgroups Resource Kit Addendum for version 3.11 includes a Browse Watcher application which will allow you to identify the master browse server for a given workgroup as well as any backup browse servers that may be designated.

Browsing Network Resources

The Windows for Workgroups 3.11 computer maintains a random list of browse servers that are defined in the workgroup to which it belongs. When the Windows for Workgroups user requests a list of computers in a workgroup, the Windows for Workgroups browse service on the local computer randomly chooses one of the browse servers it is aware of and requests the list of workgroups and computers. The selected browse server sends a list of other workgroups it knows about that are defined on the network, along with a list of computers in the workgroup to which the user belongs.

If the user selects a workgroup to which his/her computer does not belong, the Windows for Workgroups computer will request a list of computers defined in the selected workgroup from a browse server in the selected workgroup.

Browsing and Slow Network Connections

When a known slow network connection is installed on a Windows for Workgroups computer, for example the Remote Access Service MAC driver, Windows for Workgroups will be configured to not designate the computer to be a browse server for the given network connection. The **SlowLanas=** switch in the **[network]** section of SYSTEM.INI identifies the network LANA numbers that the local computer will not serve as a browse server for. However, the user will still be able to request a list of available workgroups and computers on the network across the slow network connection.

How Browsing is Handled When a "Net View" Command is Issued

Browsing network resources in MS-DOS is handled by the real-mode networking components. The **net view** command is used to request a list of computers present in a given workgroup. Unlike a browsing request from one of the Windows for Workgroups user interface components (e.g., File Manager), the **net view** command requests a list of computers directly from the master browse server—the request is not handled by a backup browse server.

The **net view** command is a valuable troubleshooting tool if you suspect the browse list maintained by a backup browse server is incomplete or inaccurate. You can use the **net view** command to get the list of known computers directly from the master browse server. If the list of computers returned from the request by a master browse server is inaccurate, you could reset this computer by exiting Windows for Workgroups to request that a new master browse server be designated for the workgroup.

The syntax for the **net view** command is as follows.

```
NET VIEW [\\computer] [/YES]
NET VIEW [WORKGROUP:wgname] [/YES]
```

computer	Specifies the name of the computer whose shared resources you want to see listed.
/WORKGROUP	Specifies that you want to view the names of the computers in another workgroup that share resources.
wgname	Specifies the name of the workgroup whose computer names you want to view.
/YES	Carries out the NET VIEW command without first prompting you to provide information or confirm actions.

To display a list of computers in your workgroup that share resources, type NET VIEW without options.

LAN Manager 2.x Domains

A LAN Manager 2.x domain is known to the browse servers in a workgroup only if at least one Windows for Workgroups computer, or at least one Windows NT workstation, is a member of that LAN Manager 2.x domain. To configure a Windows for Workgroups or Windows NT workstation to be a member of a domain, set the workgroup name for the computer to be the same as a valid LAN Manager 2.x domain name.

For Windows for Workgroups servers to be visible to LAN Manager 2.x clients, edit or add the **LMAnnounce=** switch in the **[network]** section of the SYSTEM.INI file to set the value to **Yes**. See Chapter 4, "Windows for Workgroups 3.11 Initialization Files," for more information.

Enhanced MS-DOS Drivers and Utilities

Windows for Workgroups 3.11 includes updated system drivers and utilities that are also included with MS-DOS 6.2. These drivers include HIMEM.SYS, RAMDRIVE.SYS, SMARTDRV.EXE, and EMM386.EXE.

A summary of changes in the support provided by SMARTDRV.EXE are described in this section.

SmartDrive 5.0

A number of changes and enhancements have been made to SmartDrive and are included in SmartDrive version 5.0. The differences from SmartDrive 4.2 can be summarized as follows:

- **Write Caching Disabled by Default**

By default, when Windows for Workgroups is installed, SmartDrive is configured with write-behind caching disabled for all drives. Windows for Workgroups Setup adds the `/x` command-line switch to SMARTDRV.EXE by default when Windows for Workgroups is installed, initially placing SmartDrive in a read-cache mode only.

- **Cache Flushing When Returning to Command Prompt**

By default, SmartDrive will flush its cache when it returns to an MS-DOS command prompt. This will help prevent data loss when users turn off their computers with information still residing in the cache. This capability is controlled by the `/f` and `/n` command-line switches when invoking SmartDrive.

The `/f` command-line switch tells SmartDrive to write cached data to disk before returning to the command prompt. This is the default behavior. The `/n` command-line switch tells SmartDrive to not write cached data before returning to the command prompt, but handle writing cached data as it normally does.

- **CD-ROM Caching Support**

SmartDrive version 5.0 includes added support to cache data transferred from CD-ROM drives support through the Microsoft CD-ROM Extensions driver, MSCDEX.EXE. Any CD-ROM drive which is supported by MSCDEX may be cached under this system. Any number of CD-ROMs may be cached up to and including the maximum number of drives supported by MSCDEX.

To cache CD-ROM drives, MSCDEX must be loaded before starting SMARTDRV.EXE, as SmartDrive hooks into existing MSCDEX code. In the event that MSCDEX is not present at the time SmartDrive is started, the extra code normally used for CD-ROM support is unloaded from memory, and thus resident code size for SmartDrive users without CD-ROMs is not increased. If the user has CD-ROM drives, but does not want CD-ROM caching under SmartDrive, a new option (`/u`) has been added to the command-line switches that will unload the extra CD-ROM code regardless of the presence of MSCDEX.

SmartDrive 5.0 supports writable CD-ROMs to the extent that a write automatically flushes the cache before the write is passed to the device. Although this may impede performance on authoring systems equipped with CD-ROMs, data integrity is assured.

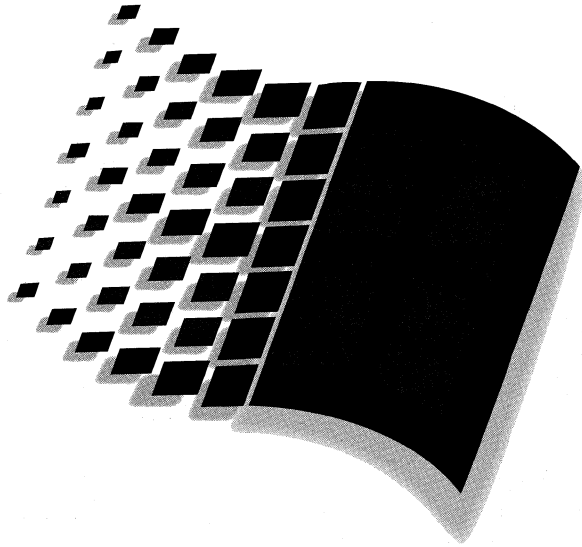
SmartDrive 5.0 supports the inherent disk change logic of the CD-ROM device driver used to detect when a CD-ROM disk has been changed. In the event that the driver returns the “unsure” state for a device change, the cache is flushed.

SmartDrive User Interface Change Summary

The command line switches supported by SmartDrive 5.0 are listed below. New command line switches are highlighted in bold.

smartdrv [/x] [[drive[+|-]]...] [/n] [/f] [/c] [/r] [/l] [/v] [/s]
 [InitCacheSize [WinCacheSize]] [/e:ElementSize] [/b:BufferSize]

Option	Description
/x	Disables write-behind caching for all drives.
<i>drive</i>	Sets caching options on specific drive(s). The specified drive(s) will have write-caching disabled unless you add +.
+	Enables write-behind caching for the specified drive.
-	Disables all caching for the specified drive.
/f	Writes cached data before command prompt returns (default).
/n	Doesn't write cached data before command prompt returns.
/c	Writes all information currently in write-cache to hard disk.
/r	Clears the cache and restarts SmartDrive.
/l	Prevents SmartDrive from loading itself into upper memory.
/v	Displays SmartDrive status messages when loading.
/q	Does not display status information.
/s	Displays additional information about SmartDrive's status.
/u	Do not cache CD-ROM drives.
<i>InitCacheSize</i>	Specifies XMS memory (K) for the cache.
<i>WinCacheSize</i>	Specifies XMS memory (K) for the cache with Windows.
<i>/e:ElementSize</i>	Specifies how many bytes of information to move at one time.
<i>/b:BufferSize</i>	Specifies the size of the read-ahead buffer.



Installation and Setup

Chapter 2 Windows for Workgroups 3.11 Installation and Setup **2-1**

About Windows for Workgroups 3.11 Setup.....2-3
Windows for Workgroups Network Support.....2-3
Windows for Workgroups 3.11 Setup Options.....2-6
Last Known Clean Configuration Files.....2-8
Defining Default Workgroups for Users with WRKGRP.INI.....2-9
Support for MS-DOS 6 Multi-Config Installation.....2-11
Removing Mail, Schedule+, and Microsoft At Work Fax from Windows for Workgroups Setup.....2-15
Quick Windows for Workgroups Installations.....2-16

Chapter 3 Windows for Workgroups 3.11 Files **3-1**

About the Windows for Workgroups 3.11 Files.....3-2
WIN.COM.....3-2
The Core Files.....3-3
Setup-related Files, Driver Files, Fonts, and International Support Files.....3-3
MS-DOS Support Components of Windows for Workgroups 3.11.....3-13
Windows for Workgroups 3.11 Applications, Setup, and Other Files.....3-15
Network Files Used for Microsoft Windows Network.....3-20
Minimizing Files Necessary for Windows for Workgroups 3.11.....3-24

Chapter 4 Windows for Workgroups 3.11 Initialization Files **4-1**

About the Initialization Files.....4-2
SYSTEM.INI: System Initialization File.....4-6
MSMAIL.INI: Microsoft Mail Initialization File.....4-21
EFAXPUMP.INI: Microsoft At Work Fax Settings Initialization File.....4-22

Chapter 5 Windows for Workgroups 3.11 Security Control Enhancements **5-1**

Overview of Security Control Enhancements.....5-2
Configurable Peer Networking.....5-2
Administrator-Defined Password Settings.....5-5
Support for Windows NT Security Features.....5-7
Implementing Windows for Workgroups 3.11 Security Controls.....5-10
Auditing of Network Events.....5-19

**Chapter
2**

Windows for Workgroups 3.11 Setup and Installation

This chapter discusses the enhancements and changes made to Setup for Windows for Workgroups 3.11. It also includes information on tips for configuring and installing Windows for Workgroups in different installation scenarios.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 8, “Integrating Novell NetWare;” Chapter 3, “Windows for Workgroups 3.11 Files.”
- Windows for Workgroups readme files: SETUP.TXT, README.WRI, PRINTERS.WRI, NETWORKS.WRI, and MAIL.WRI
- *Windows for Workgroups Resource Kit for version 3.1:* Chapter 3, “Windows for Workgroups Installation;” Chapter 5, “Windows for Workgroups Initialization Files.”

Contents of This Chapter

About Windows for Workgroups 3.11 Setup	2-3
Separation of MS-DOS–Mode Setup and Windows-Mode Setup	2-3
Windows for Workgroups Network Support	2-3
Standalone Configuration.....	2-4
Microsoft Windows Network.....	2-4
Windows 3.1-Compatible Network Support.....	2-5
Windows for Workgroups 3.11 Setup Options	2-6
Administrative Setup (setup /a).....	2-6
Shared Copy Setup (setup /n).....	2-7
Last Known Clean Configuration Files	2-8
Defining Default Workgroups for Users with WRKGRP.INI	2-9
Sample WRKGRP.INI file.....	2-10
Implementing the WRKGRP.INI file.....	2-11
Support for MS-DOS 6 Multi-Config Installation	2-11
Sample CONFIG.SYS and AUTOEXEC.BAT Files.....	2-14

Removing Mail, Schedule+, and Microsoft At Work Fax from Windows for Workgroups Setup	2-15
Quick Windows for Workgroups Installations	2-16
Quick Network Installation	2-17
Quick Installation Using MS-DOS InterLink Utility	2-19

About Windows for Workgroups 3.11 Setup

Windows for Workgroups 3.11 is available in two different product configurations: *Windows for Workgroups 3.11* full packaged product, and the *Workgroup Add-on for Windows*. The Windows for Workgroups 3.11 product includes Microsoft Windows 3.1 and is used to upgrade a computer running MS-DOS to both Windows and network functionality with a single installation procedure. Workgroup Add-on for Windows upgrades an existing Windows 3.1 or Windows for Workgroups 3.10 installation to add the networking functionality and new capabilities, such as improved performance, that are offered by Windows for Workgroups 3.11.

This chapter discusses changes made to the Setup program of Windows for Workgroups 3.11 as compared with Windows for Workgroups 3.1. Information about special installation scenarios and configurations is also provided.

Separation of MS-DOS–Mode Setup and Windows-Mode Setup

Setup for both Windows 3.1 and Windows for Workgroups 3.1 is handled by the SETUP.EXE executable file, which contains the software code for both the MS-DOS portion of Setup and the Windows portion of Setup.

Setup for Windows for Workgroups 3.11 is separated into two different executable files for the MS-DOS portion of Setup and the Windows portion of Setup, SETUP.EXE and WINSETUP.EXE, respectively.

Windows for Workgroups 3.11 also includes a new icon in the Network Program Group to gain quick access to the Network portion of Setup. This icon invokes a special parameter, /z, which is recognized by WINSETUP.EXE to launch the network portion of Setup.

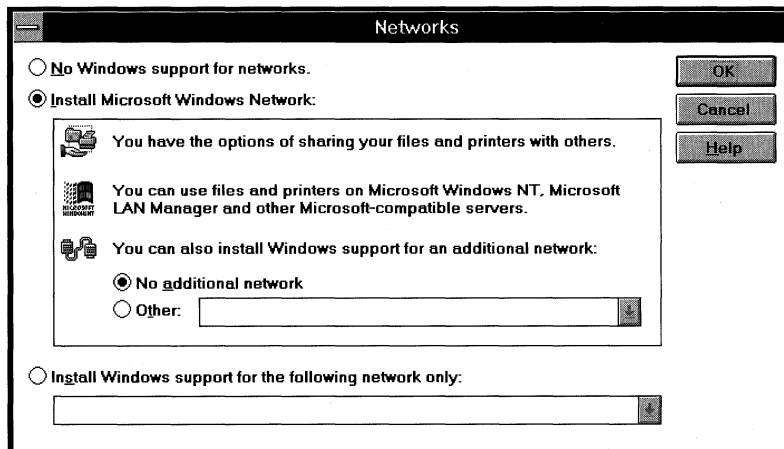
Windows for Workgroups Network Support

Windows for Workgroups 3.11 supports three configurations of network support—no windows support for networks (standalone), Microsoft Windows Network, and Windows 3.1-compatible network support.

In each of these cases, the configuration of network support is chosen from the Networks dialog box as shown in Figure 2.1, accessible through the Network Setup icon in the Network program group.

Figure 2.1

The Networks dialog box for configuring network support in Windows for Workgroups 3.11



Each of the three supported configuration options is discussed in the following sections.

Standalone Configuration

When “No Windows support for networks” is chosen from the Networks dialog box, network functionality is not installed by Windows for Workgroups 3.11 Setup. This configuration option is for stand-alone users who want the extra functionality offered by Windows for Workgroups 3.11 such as Microsoft At Work fax messaging, in addition to the 32-bit file access performance enhancements.

When this configuration option is selected, installation information is read from the SETUP.INF file. Network functionality including network accessories and Network DDE is not installed for this configuration.

Microsoft Windows Network

When “Install Microsoft Windows Network” is chosen from the Networks dialog box, the Windows for Workgroups 3.11 network functionality is installed by Windows for Workgroups 3.11 Setup. This configuration option provides

the network functionality to allow computers running Windows for Workgroups to exchange information with other computers running Windows for Workgroups, Workgroup Add-on for MS-DOS, Windows NT, Windows NT Advanced Server, Microsoft LAN Manager, and other 100-percent Microsoft-compatible network products, including DEC Pathworks. This configuration option also allows Windows for Workgroups 3.11 network functionality to coexist with an additional network configuration including the following network operating systems:

- Novell NetWare workstation shell 3.x, and 4.0 and above
- Banyan VINES 4.11, 5.0, and 5.5
- BW-NFS Network File System version 3.0
- SunSelect PC-NFS version 5.0

Third-party network operating system vendors not supported directly by Windows for Workgroups 3.11 can add additional network support by supplying the appropriate supplemental configuration files. Check with your networking vendor for information on their compatibility with Windows for Workgroups 3.11.

When this configuration option is selected, installation information is read from the SETUP.INF, NETWORK.INF, and the WINNET.INF file. All Windows for Workgroups 3.11 components are installed and configured when this configuration option is specified.

Windows 3.1-Compatible Network Support

Windows for Workgroups 3.11 features a superset of Windows 3.1 network functionality support. As an alternative to using the 32-bit networking functionality offered in Windows for Workgroups 3.11, Windows for Workgroups can be configured to be used on top of Windows 3.1-compatible network software configurations. Windows for Workgroups 3.10 did not provide direct support for Windows 3.1-compatible networks.

When Windows 3.1 compatible network support is configured, the Windows for Workgroups 3.11 networking components are not installed. However, network applications such as Mail and Schedule+ are installed and can be used in conjunction with these other networking products. The benefit of this additional network support in Windows for Workgroups 3.11 is the additional functionality and the 32-bit file access performance enhancements without requiring a change in your desktop networking software.

Windows for Workgroups 3.11 supports the following Windows 3.1-compatible networks:

- 100% MS-Net compatibles
- Artisoft® LANtastic® 3.x, 4.x, 5.x
- Banyan® VINES® 4.11 (5), 5.00 (5), 5.50 (5)
- BW-NFS Network File System (version 3.0)
- DEC® PATHWORKS™ version 4.0, version 4.1 or higher
- IBM OS/2® LAN Server version 1.2 or 1.3, version 1.3 (CSD 5015/5050), version 2.0, without /API option
- Microsoft Windows Network version 3.11 Basic redirector,
- Novell NetWare Workstation shell 3.x, 4.0 and above
- TCS® 10Net version 4.1x with DCA 1M card, version 4.1x, version 4.2 and above, version 5.0
- SunSelect PC-NFS version 5.0

For Microsoft network compatible products, such as Microsoft LAN Manager, Microsoft Workgroup Connection, Microsoft Windows Network, and 100% MS-Net-compatible networks, you will be able to take full advantage of the 32-bit network functionality offered in Windows for Workgroups 3.11 by changing your network client software and selecting the Microsoft Windows Network configuration for your desktop.

Windows for Workgroups 3.11 Setup Options

Windows for Workgroups 3.11 supports installation either from the installation disks, or from a network file server. The administrative setup, **setup /a**, is used to prepare the Windows for Workgroups 3.11 files for a workstation, or shared copy, setup of Windows for Workgroups 3.11.

Administrative Setup (setup /a)

The Windows for Workgroups 3.11 Administrative Setup is identical to that included with Windows for Workgroups 3.1. Administrative Setup is performed by typing **setup /a** at the command prompt. This command expands the compressed contents of each install disk onto a given path name. Setup prompts the user for the location to place the expanded Windows for Workgroups 3.11 files, and then expands each install disk in sequence. As each file is expanded, Setup also enables the read-only file attribute to allow multiple users to access the Windows for Workgroups 3.11 files at the same time.

To perform an Administrative Setup of Windows for Workgroups 3.11, you will need approximately 22 MB of free disk space on which the expanded files may be installed.

Removing the Administrator Configuration Utility

The Administrator Configuration Utility (ADMINCFG.EXE) is one of the files that is expanded from the Windows for Workgroups 3.11 installation disks. A password may be assigned to the security settings file to prevent the user from running the Administrator Configuration Utility unless authorized. However, you may want to simply remove the ADMINCFG.EXE file from the Windows for Workgroups 3.11 network installation point once the administrative setup procedure is complete.

To remove the ADMINCFG.EXE file, you will need to change the read-only file attribute to allow the file to be deleted. To do this, type the following command at the MS-DOS command prompt from the network install directory:

```
ATTRIB -R ADMINCFG.EXE
```

Once the file attribute is changed, you can delete the ADMINCFG.EXE file.

For a detailed discussion of ADMINCFG, see Chapter 5, "Windows for Workgroups 3.11 Security Control Enhancements."

Shared Copy Setup (setup /n)

Windows Setup allows a shared copy of Windows for Workgroups 3.11 created by the administrative setup (see the preceding section) to be run from a network server by specifying the */n* parameter when running Setup to perform a shared

copy setup. The **setup /n** command sequence will create a minimal installation of Windows for Workgroups 3.11 on a given path and will modify .INI files to point to the network install point to reference drivers, accessories, and other application files.

The files installed on the local workstation by performing a shared copy setup of Windows for Workgroups 3.11 use approximately 1 megabyte of disk space. The following files are placed in the local Windows directory by the shared copy setup procedure

HIMEM SYS	NETH MSG	PROTOCOL INI
IFSHLP SYS	PROTMAN EXE	MAIN0 GRP
RAMDRIVE SYS	SPART PAR	ACCESS00 GRP
NDISHLP SYS	SHARES PWL	NETWORK0 GRP
WIN COM	REG DAT	GAMES0 GRP
I82593 DOS	WFWSYS CFG	STARTUP0 GRP
PROTMAN DOS	SYSTEM INI	_DEFAULT PIF
EMM386 EXE	WIN INI	DOSPRMPT PIF
WININIT EXE	PROGMAN INI	SYSTEM CLN
SMARTDRV EXE	NCDINFO INI	WIN CLN
WINVER EXE	SERIALNO INI	PROTOCOL CLN
NET EXE	CONTROL INI	BOOTLOG TXT
NET MSG	WINFILE INI	

Note The files placed in your Windows directory may vary slightly from the files listed here, depending on the configuration you are running.

Last Known Clean Configuration Files

When you change the configuration of Windows for Workgroups 3.11, Setup copies your most recent SYSTEM.INI, PROTOCOL.INI, and WIN.INI, to files with an extension of .CLN. That is, your old SYSTEM.INI file is copied to SYSTEM.CLN, PROTOCOL.INI to PROTOCOL.CLN, and WIN.INI is copied to WIN.CLN. These .CLN files are known as the “last known clean” configuration files for your system.

If after you modify the configuration of Windows for Workgroups with Setup, Windows for Workgroups fails to start or you encounter other not easily solved difficulties, the .CLN files allow you to restore your Windows for Workgroups 3.11 configuration to the last known working state.

You can recover to the last known clean configuration by replacing the .INI files with the .CLN files. At the MS-DOS prompt in the Windows directory, type:

```
copy *.CLN *.INI
```

Defining Default Workgroups for Users with WRKGRP.INI

Windows for Workgroup 3.11 Setup will recognize an initialization file called WRKGRP.INI that can be used by system administrators to specify default workgroups from which users can choose at the time Windows for Workgroups 3.11 is installed. This functionality is new to Windows for Workgroups 3.11. The use of WRKGRP.INI can help system administrators reduce the proliferation of workgroup names, where needed.

The WRKGRP.INI file is used when each user first installs Windows for Workgroups 3.11, and when the user changes the Workgroup name, via the Microsoft Windows Network dialog box, accessible from the Network icon in Control Panel.

The WRKGRP.INI file can contain the following sections:

Section	Purpose
[Options]	Specifies the options that are recognized for using the WRKGRP.INI file.
[Workgroups]	Contains a list of workgroups from which the user may choose.

The details of the contents of each section supported in the WRKGRP.INI file are described below.

[Options]

The **[Options]** section contains information used to interpret the contents of the **[Workgroups]** section and can contain the following entries:

ANSI= *Boolean*

Specifies whether the names in the **[Workgroups]** section need to be converted from the OEM character set to ANSI. If **true**, then the characters used for the names of the workgroups are from the ANSI character set and do not need to be converted from the OEM character set to ANSI. If **false**, the characters must be converted from OEM to ANSI. The default is **false**.

Required= Boolean

Specifies whether the user must choose the name of a workgroup from the names in the **[Workgroups]** section list. If **true**, the user will be restricted to specifying a workgroup that is present in the **[Workgroups]** list. If **false**, then the Workgroup list box is filled with both the names of the workgroups in the **[Workgroups]** section, and with any other workgroups that can be enumerated on the network. The default is **false**.

[Workgroups]

The **[Workgroups]** section contains a list of workgroups from which the user can choose. Each entry in the **[Workgroups]** section must be followed with an equal symbol (“=”). The syntax for the entries that appear in this section is as follows:

```
workgroup_name=
```

where *workgroup_name* is the name of a workgroup from which the user can choose.

Note Each name of a workgroup must be followed by an equal symbol, “=”, in order for the workgroup name to be interpreted correctly and displayed in the Workgroups list box.

Sample WRKGRP.INI file

To restrict users to a defined set of workgroup names, a system administrator should create a WRKGRP.INI file similar to the example below. The following sample WRKGRP.INI file restricts users to be members only of the Finance, Marketing, Support, Sales, or Executive groups:

```
[Options]
ANSI=False
Required=True
```

```
[Workgroups]
Finance=
Marketing=
Support=
Sales=
Executive=
```

As described in the previous section, the **Required=** entry is used in this sample file to require users to select a workgroup from one of the provided workgroup names.

Implementing the WRKGRP.INI file

The WRKGRP.INI file must be present in the user's SYSTEM directory for the Windows for Workgroups 3.11 components to recognize the file. A system administrator can create a WRKGRP.INI file and have this file copied into the user's SYSTEM directory by the Setup program as detailed in the following steps:

1. Create the WRKGRP.INI file with the appropriate workgroup names and restrictions for your organization.
2. If installing Windows for Workgroups 3.11 from a network, place the WRKGRP.INI file on the network install point where you placed the other Windows for Workgroups files by performing an administrative setup (that is, **setup /a**). Or, if installing Windows for Workgroups 3.11 from disk, place the WRKGRP.INI file on one of the Windows for Workgroups 3.11 Setup disks—this discussion assumes that the WRKGRP.INI file was placed on Disk 1.
3. To have the WRKGRP.INI file placed in the user's SYSTEM directory at time of setup, the SETUP.INF file needs to be modified to instruct the setup program to copy the WRKGRP.INI file at the time of installation.
4. Make the necessary modifications to the SETUP.INF file by using a text editor (MS-DOS Editor or some other) to search for the text **[win.other]**. Below the **[win.other]** line, add the following line:

```
#:WRKGRP.INI
```

(Where # is the number of the disk where you placed the WRKGRP.INI file.)

Save the file as unformatted ASCII text.

5. Place the WRKGRP.INI file either on the network install point, or on the disk you identified in step 4.

Support for MS-DOS 6 Multi-Config Installation

MS-DOS version 6.0 or higher lets you define multiple system configurations in a single CONFIG.SYS file. When you install Windows for Workgroups 3.11, if you are running MS-DOS version 6.0 or higher, Setup checks the CONFIG.SYS file for the **[menu]** keyword section to determine whether the CONFIG.SYS file contains multiple configurations. If so, Windows for Workgroups 3.11 Setup will not update your CONFIG.SYS file, but instead creates a file called CONFIG.WIN in the Windows directory which contains the entries that need to be present in the CONFIG.SYS file.

Setup will not automatically change the CONFIG.SYS file in order to preserve your configuration in case it has difficulty interpreting your environment. Once Setup has finished, you can open the CONFIG.SYS file and the new CONFIG.WIN file that Setup created, and merge the two together.

When using the multiple-configuration capability in MS-DOS 6 (or any other third-party product that provides similar capabilities), it is important to note the following information:

Note [Windows for Workgroups] is used to refer to the configuration block in your CONFIG.SYS file that you use for your Windows for Workgroups configuration. The exact name of this block may be different than that used here depending on the name you used for your configuration.

- The following lines should be in either the [Common] configuration block or the [Windows for Workgroups] configuration block of the CONFIG.SYS file so that the Windows for Workgroups 3.11 networking components will load properly:

```
DEVICE=C:\WINDOWS\HIMEM.SYS  
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

Note If you also have a configuration block in your CONFIG.SYS file for running Microsoft LAN Manager or Windows for Workgroups 3.1 that you wish to continue to use after installing Windows for Workgroups 3.11, place the IFSHLP.SYS device driver line in your Windows for Workgroups 3.11 configuration block instead of in the [common] configuration block. If you place IFSHLP.SYS in your [common] configuration block, it will prevent the network drivers for LAN Manager or Windows for Workgroups 3.1 from loading properly.

Other device driver lines that can be in either the **[Common]** configuration block or the **[Windows for Workgroups]** configuration block include:

```
DEVICE=C:\WINDOWS\EMM386.EXE
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
```

- If you were previously using Windows for Workgroups 3.1, you can remove the following device driver lines from the **[Windows for Workgroups]** block in your CONFIG.SYS file if they are still present once Windows for Workgroups 3.11 has been installed.

```
C:\WINDOWS\PROTMAN.DOS /I:C:\WINDOWS
C:\WINDOWS\<NDIS MAC driver>.DOS { for example, EXP16.DOS }
C:\WINDOWS\WORKGRP.SYS
```

If these device driver lines appear in your CONFIG.SYS file more than once, Windows for Workgroups Setup only removes their first occurrence. If your **[Windows for Workgroups]** block is not the first one in your CONFIG.SYS file, you may need to move them by hand from the **[Windows for Workgroups]** block by hand.

- Third-party network transports should be moved to the **transports=** line in the **[network drivers]** section of the SYSTEM.INI file.

Also, note that the CONFIG.SYS and AUTOEXEC.BAT files are no longer used to load the NDIS network adapter card drivers and network protocol drivers. Windows for Workgroups 3.11 specifies the network configuration in the SYSTEM.INI and PROTOCOL.INI files.

If you are using different network adapter card drivers or network protocols and want to switch between these different configurations, the SYSTEM.INI and PROTOCOL.INI files must be changed to reflect the configuration settings. The simplest way to enable a quick change of configurations is to maintain separate copies of SYSTEM.INI and PROTOCOL.INI files that reflect the adapters or protocols you need to support.

Sample CONFIG.SYS and AUTOEXEC.BAT Files

A sample CONFIG.SYS file and AUTOEXEC.BAT file for an MS-DOS 6 Multi-Config scenario is provided below. Your actual CONFIG.SYS and AUTOEXEC.BAT files will vary depending on your system configuration.

Sample Multi-Config CONFIG.SYS File

```
[Menu]
menuitem = WFW, Windows for Workgroups 3.11
menuitem = Clean, Clean Boot Configuration
menudefault=WFW,5
```

```
[Common]
BUFFERS = 20,0
FILES = 40
FCBS = 16,8
STACKS = 9,256
SHELL = C:\DOS\COMMAND.COM C:\DOS\ /p
DEVICE = C:\DOS\DBLSPACE.SYS /MOVE
DEVICE = C:\WINDOWS\IFSHLP.SYS
```

```
[WFW]
DEVICE = C:\DOS\HIMEM.SYS
DEVICE = C:\DOS\EMM386.EXE NOEMS
```

```
[CLEAN]
```

Sample Multi-Config AUTOEXEC.BAT File

```
PROMPT $p$g
C:\DOS\SMARTDRV.EXE 1024 128
```

```
goto %config%
```

```
:WFW
PATH C:\WINDOWS;C:\DOS;C:\NU
SET TEMP=C:\WINDOWS\TEMP
C:\WINDOWS\NET START
goto end
```

```
:clean
```

```
:end
```

Removing Mail, Schedule+, and Microsoft At Work Fax from Windows for Workgroups Setup

In some scenarios, a system administrator may want to configure Windows for Workgroups 3.11 so that Mail, Schedule+, and Microsoft At Work fax will not install when Windows for Workgroups 3.11 is installed for the first time on a workstation. A system administrator may want to do this, for example, if a mail or calendar/scheduling package other than Microsoft Mail and Microsoft Schedule+ are being used.

The Windows for Workgroups 3.11 Setup program reads the SETUP.INF file to determine which files to copy and configure on a workstation at the time of install. To change the default installation environment, you can modify the SETUP.INF file, by adding or removing any components you want.

Once you have modified the SETUP.INF file, place it on the network install point where the other Windows for Workgroups 3.11 files are located, if you are installing from a network drive (that is, the location where you have expanded the Windows for Workgroups 3.11 files with the **setup /a** install), or on the Windows for Workgroups 3.11 Setup and Installation Disk 1.

The relevant sections of the SETUP.INF file where Mail, Schedule+, and Microsoft At Work fax are installed are:

```
[win.copy.win386]
[win.apps]
[win.dependents]
[group8]
```

To remove Mail, Schedule+, and Microsoft At Work fax, identify the sections in the SETUP.INF file, and place a semicolon (“;”) immediately preceding the lines listed below—the semicolon tells Setup to treat the line as a remark rather than a command it must act upon. The contents of any line to the right of a semicolon will be ignored.

Note Do not place a semi-colon preceding the line with the section heading (i.e., the heading that is enclosed within square brackets “[” and “]”).

```
[win.copy.win386]
#mapi, 0:system
```

```
[win.apps]
2:MSMAIL.EXE, "Mail" , 614256, msmail
4:MSMAIL.HLP, "Mail Help" , 72051
2:SCHDPLUS.EXE, "Schedule+" , 746704, schdplus
3:SCHDPLUS.HLP, "Schedule+ Help" , 104115
6:FAXMGR.EXE, "Microsoft At Work Fax" , 1002496, msfax
5:MSFAX.HLP, "Microsoft At Work Fax Help", 45997
```

```
[win.dependents]
msmail = #msmail
schdplus = #sched
msfax = #faxsys, 0:system, #msfax
```

```
[group8]
"Mail", MSMTP.EXE,,, msmail
"Schedule+", SCHDPLUS.EXE,,, schdplus
```

Quick Windows for Workgroups Installations

This section discusses various ways in which the process of installing Windows for Workgroups can be streamlined. This information is designed for support organizations, value-added retailers, and system integrators to help facilitate installing Windows for Workgroups 3.11 on multiple computers.

Several different methods can be used to install Windows for Workgroups 3.11 in the least time possible without installing directly from floppy disk. For example, Windows for Workgroups 3.11 can be installed over a network or by using file transferring software such as InterLink provided with MS-DOS 6.

Tip You can increase the rate at which Windows for Workgroups 3.11 installs on a computer by using the SmartDrive disk cache utility provided with MS-DOS. If SmartDrive is not loaded in your AUTOEXEC.BAT file, type **smartdrv** at the MS-DOS command prompt before running Setup from the local computer to load SmartDrive into memory.

Quick Network Installation

The fastest method of installation for Windows for Workgroups is over a network file server. This holds true either in an environment where a preexisting network is in place (for example, Novell NetWare is being used), or when creating a new network with Windows for Workgroups 3.11.

New Windows for Workgroups Network

This section describes the steps to perform a network installation of Windows for Workgroups 3.11. This process includes two parts—preparing the server and preparing the clients.

To complete this process, you will need a copy of Windows for Workgroups 3.11 for each computer (or a license for each computer) on which Windows for Workgroups 3.11 will be installed. You will also need a single copy of the Workgroup Add-on for MS-DOS product. These steps also assume that a network adapter card has been installed in each computer and that the proper network cable media is being used.

Preparing the server

1. Install Windows for Workgroups 3.11 on the first computer for the network.
2. Create a directory on this first computer, where the expanded Windows for Workgroups 3.11 files will reside.
3. Perform an administrative setup using the **setup /a** command using the Windows for Workgroups 3.11 disks to expand the compressed files to the directory you created in step 2. Note that you will need to perform this from MS-DOS, you can not run Setup from within Windows for Workgroups 3.11.
4. After the Windows for Workgroups files have been expanded, start Windows for Workgroups 3.11 on this computer and share the directory you created in step 2 that contains the expanded Windows for Workgroups 3.11 files. Use the name WFWFILES as the name of the share where the Windows for Workgroups 3.11 files reside—this is an arbitrary name; however, this name is used again in a later step.

Preparing the clients

1. To prepare a client workstation on which you will install Windows for Workgroups 3.11 across the network, install the Microsoft *Workgroup Add-on for MS-DOS* on this computer. This will provide the network client software to allow you to connect to the Windows for Workgroups 3.11 server from which you will perform the installation. When prompted for a network path in which to install the files, specify the name of the directory as NET. (This is an arbitrary name, however it is referenced in a later step.)
2. Setup will reboot computer after the installation is complete.
3. After the computer reboots, the network redirector will load and you will be prompted to enter your user name to log onto the network. Type your user name and related password.
4. Once the Workgroup Add-on for MS-DOS network client software has been started on the workstation, type the following command from the MS-DOS command prompt to connect to the shared Windows for Workgroups 3.11 directory, substituting the name of the computer where the Windows for Workgroups 3.11 files are shared in place of *server*:

```
NET USE G: \\server\WFVFILES
```
5. Once connected to the Windows for Workgroups 3.11 server, default to drive G (or the drive letter used when connecting to the WFVFILES share) and type **setup**. This will run the Windows for Workgroups 3.11 Setup program.
6. Complete the Windows for Workgroups 3.11 Setup procedure by performing either an express or custom setup as wanted.
7. After Windows for Workgroups 3.11 installs, if you only have a single license for the Workgroup Add-on for MS-DOS software, delete the NET directory you created in step 5 above. This will delete the Workgroup Add-on for MS-DOS files. Now that Windows for Workgroups 3.11 has installed successfully, you will not need them.

Windows for Workgroups 3.11 Installation from a Novell NetWare Network

The steps to perform a network install from a Novell NetWare server are similar to the steps described above, however the following components are different:

- The Windows for Workgroups 3.11 administrative setup procedure is performed on the NetWare server.
- Steps for sharing the directory are different. Consult your NetWare documentation for information on sharing the directory where you perform the Windows for Workgroups 3.11 administrative setup.

- The NetWare client software (that is, redirector and IPX protocol) is used for the client workstation instead of the Workgroup Add-on for MS-DOS product.
- Steps for connecting to the server are different. Consult your NetWare documentation for information on connecting to the NetWare server using the NetWare client software.

Note that this information is also relevant if you are installing from another network operating system such as Banyan VINES.

Quick Installation Using MS-DOS InterLink Utility

Installing Windows for Workgroups 3.11 from a network provides the fastest rate of installation. However, there may be scenarios where you either want to install Windows for Workgroups on a stand-alone computer, or on a computer that is not presently networked. Another way to speed up the installation process is to perform an administrative setup to a directory on a laptop computer and then take the laptop computer around to perform an installation on different local workstations.

The InterLink utility which is provided with MS-DOS 6 can be used to facilitate installing Windows for Workgroups 3.11 on stand-alone computers by connecting two computers together with a parallel or serial cable.

Note Consult your MS-DOS 6 documentation for information on using the InterLink utility, or type **help interlnk** from the MS-DOS command prompt to view online information.

These procedures will refer to the laptop computer where the administrative setup of Windows for Workgroups 3.11 has been performed as the *server*, and the computer on which Windows for Workgroups 3.11 will be installed as the *client*. The basic procedures for installing Windows for Workgroups 3.11 using InterLink are as follows:

Setting up the server computer

1. Install the InterLink driver on the server computer by placing the following line in the CONFIG.SYS file on the laptop and then rebooting the computer:

```
device=c:\DOS\INTERLNK.EXE
```

2. Create a directory on the server computer and perform an administrative setup of Windows for Workgroups 3.11 by typing **setup /a** using the Windows for Workgroups 3.11 disks. Use "WFVFILES" as the name of the directory that you create. (This name is arbitrary, however it will be referenced in a later step.)
3. After the administrative setup is complete, start the InterLink server program, INTERSVR, by typing **intersvr** at the MS-DOS command prompt.

Setting up the client computer

1. Connect the server computer and client computer together using either a parallel cable or a serial cable. Consult either your MS-DOS 6 documentation or the online help for InterLink for information on the cable types to use. The use of a parallel cable will provide faster throughput.
2. Install the InterLink driver on the client computer by placing the following line in the CONFIG.SYS file on the laptop and then rebooting the computer:

```
device=c:\DOS\INTERLNK.EXE
```
3. On the client computer, connect to drive C on the server computer by typing (if you performed the administrative setup to a drive other than C, substitute the reference from drive C to the appropriate drive letter):

```
INTERLNK G=C
```
4. On the client computer, default to drive G and change to the WFVFILES directory where the expanded Windows for Workgroups files reside.
5. On the client computer, install Windows for Workgroups from drive G by typing **setup** at the MS-DOS command prompt. Perform an Express or Custom setup as wanted.
6. Once Windows for Workgroups has been installed on the client computer, remove the line referencing the INTERLNK driver from your CONFIG.SYS file that you added in step 5, and reboot the client computer.

Repeat steps 1 through 6 for each additional computer on which you wish to install Windows for Workgroups 3.11.

Chapter
3

Windows for Workgroups 3.11 Files

This chapter describes the purpose for each file installed by Windows for Workgroups 3.11 into the WINDOWS directory and the SYSTEM subdirectory.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 4, "Windows for Workgroups 3.11 Initialization Files;" Chapter 2, "Windows for Workgroups 3.11 Installation and Setup."
- *Windows for Workgroups Resource Kit for version 3.1:* Chapter 4, "Windows for Workgroups Setup Information Files."

Contents of This Chapter

About the Windows for Workgroups 3.11 Files	3-2
WIN.COM	3-2
The Core Files	3-3
Setup-related Files, Driver Files, Fonts, and International Support Files.....	3-3
Setup-related Files	3-3
Driver Files.....	3-4
Font Files.....	3-10
International Support Files	3-13
MS-DOS Support Components of Windows for Workgroups 3.11	3-13
MS-DOS Driver Files.....	3-13
WinOldAp and the Grabber Files.....	3-14
Files for 386 Enhanced Mode	3-15
Windows for Workgroups 3.11 Applications, Setup, and Other Files	3-15
Files for Windows for Workgroups 3.11 Applications	3-15
Files Used for Windows for Workgroups 3.11 Mail, Schedule+, and Microsoft At Work Fax	3-17
Other Files	3-19
Network Files Used for Microsoft Windows Network	3-20
Real Mode Network Support Files	3-21
NDIS 2 Network Adapter Card Driver Files.....	3-21
386 Enhanced Mode Network Drivers.....	3-22
NDIS 3 Network Transport Protocol Drivers.....	3-22
NDIS 3 Network Card Drivers.....	3-23
Files used for Remote Access Services Client	3-23
Minimizing Files Necessary for Windows for Workgroups 3.11.....	3-24
Files You Can Safely Delete	3-24

About the Windows for Workgroups 3.11 Files

When Microsoft Windows for Workgroups 3.11 runs, it performs all operating system duties excluding management of the file system, which is controlled by MS-DOS. Windows for Workgroups calls functions that are stored in a variety of executable files, driver files, and dynamic-link libraries to manage the display, keyboard, and other devices, to manipulate the network, to manage memory, and to execute programs.

The following types of files comprise the Windows for Workgroups 3.11 operating system:

- The WIN.COM file.
- The core dynamic-link libraries (kernel files, USER, and GDI) that contain the code and data for the Windows functions.
- The font files and the drivers for keyboard, display adapter, system, mouse, printers, networks, multimedia, and other devices.
- The files that provide MS-DOS support components for Windows.
- The files that provide the network support functionality—including the ability to share files and printers with other workstations.
- The Windows applications files and other files such as shells, utilities, and accessories, including the files that provide security, Mail, Microsoft At Work fax, and Remote Access Services.

For instructions on how to expand any files from the Windows installation disks, see Flowchart 1.7 in Appendix C of the *Windows for Workgroups Resource Kit for version 3.1*, “Flowcharts for Troubleshooting Windows for Workgroups.” For additional information about the Windows files, see the manuals for the Microsoft Windows *Software Developer’s Kit* and Microsoft *Windows Device Driver Kit*.

WIN.COM

WIN.COM loads Windows for Workgroups. It checks the computer type, memory configuration, and device drivers to determine which mode is appropriate to start Windows for Workgroups. To start Windows for Workgroups, there needs to be sufficient memory, an XMS driver present (such as HIMEM.SYS), and processor support for 386 enhanced mode (80386 or higher).

After WIN.COM determines the appropriate operating mode, it uses the MS-DOS **exec** command to execute WIN386.EXE, which in turn loads Windows for Workgroups 3.11.

To build Windows for Workgroups 3.11, WIN.COM brings together a number of files:

- Core files
- Drivers
- Fonts and language support files
- Support files for MS-DOS-based applications
- MS-DOS support and various mode-specific files
- Windows for Workgroups network support files

The Core Files

Three files make up the Windows core components: Kernel, User, and GDI.

- The kernel (KRNL386.EXE) controls and allocates all the computer resources to manage memory, load applications, and schedule program execution and other tasks.
- USER.EXE creates and maintains windows on the screen, carrying out all requests to create, move, size, or remove a window. USER.EXE also handles requests regarding the icons and other components of the user interface. USER.EXE directs input to the appropriate application from the keyboard, mouse, and other input sources.
- GDI.EXE controls the Graphics Device Interface, which executes graphics operations that create images on the system display and other devices.

Setup-related Files, Driver Files, Fonts, and International Support Files

Setup-related Files

The Windows for Workgroups 3.11 setup program has a number of files for its exclusive use. For example, the *.LGO files contain the code for displaying the opening screen logo, and the *.RLE files contain the actual logo bitmap (in Run Length Encoded format). Setup combines the .LGO and .RLE files with the WIN.CNF file to create WIN.COM. Setup also uses the files listed in the following table.

Filename	Purpose
SETUP.EXE	Windows for Workgroups Setup application file
SETUP.HLP	Setup Help
SETUP.INF	Setup information file
SETUP.INI	Setup initialization file
SETUP.REG	Registration Database template
SETUP.SHH	Automated Setup template
SETUP.TXT	Windows for Workgroups Readme file
VER.DLL	Version Resource and File Installation library
WINVER.EXE	Windows-version utility
WINSETUP.EXE	Windows-based setup program
XMSMMGR.EXE	Setup XMS Manager
EXPAND.EXE	MS-DOS-based file expansion utility
Startup logo files:	
VGALOGO.LGO	VGA startup logo code
VGALOGO.RLE	VGA logo screen
Initialization and information source files:	
APPS.INF	Information file for MS-DOS-based applications
CONTROL.INF	Information file for Control Panel and printer installation
CONTROL.SRC	CONTROL.INI template
NETWORK.INF	Information file for network installation
PRTUPD.INF	Information file for printer driver updates
SYSTEM.SRC	SYSTEM.INI template
WIN.CNF	Windows for Workgroups startup code
WIN.SRC	WIN.INI template
WINNET.INF	Windows for Workgroups network integration settings

Driver Files

Drivers make device independence possible for Windows-based applications, providing the hardware-specific interface between physical devices and Windows. Setup can install several kinds of drivers for Windows, such as:

Comm drivers	Mouse drivers	Printer drivers
Display drivers	Multimedia drivers	Sound drivers
Keyboard drivers	Network drivers	System drivers

The multimedia and printer drivers are optional.

Also, Setup will install drivers to support virtual machines in 386 enhanced mode, as described in "Files for 386 Enhanced Mode" later in this chapter.

System Driver File

The system driver provides support for the system timer, information about system disks, and access to OEM-defined system hooks. SYSTEM.DRV is the driver used by the hardware systems.

Keyboard Driver Files

The keyboard drivers shipped with Windows for Workgroups support keyboard input:

- KEYBOARD.DRV for standard keyboards, installed by default
- KBDHP.DRV for all Hewlett-Packard® machines

The keyboard driver is a standard driver for all systems worldwide. Windows for Workgroups 3.11 is also compatible with international keyboards, including foreign symbols, by using keyboard tables to refer to a language library.

Keyboard table	Language library
KDBBE.DLL	Belgian keyboard
KBDBR.DLL	Brazilian keyboard
KBDCA.DLL	French-Canadian keyboard
KBDDA.DLL	Danish keyboard
KBDDV.DLL	U.S.-Dvorak keyboard
KBDFC.DLL	Canadian multilingual keyboard
KBDFI.DLL	Finnish keyboard
KBDFR.DLL	French keyboard
KBDGR.DLL	German keyboard
KBDIC.DLL	Icelandic keyboard
KBDIT.DLL	Italian keyboard
KBDLA.DLL	Latin American keyboard
KBDNE.DLL	Dutch keyboard
KBDNO.DLL	Norwegian keyboard
KBDPO.DLL	Portuguese keyboard
KBDSF.DLL	Swiss-French keyboard
KBDSG.DLL	Swiss-German keyboard
KBDSP.DLL	Spanish keyboard
KBDSW.DLL	Swedish keyboard
KBDUK.DLL	British keyboard
KBDUS.DLL	U.S. keyboard
KBDUSX.DLL	U.S.-International keyboard

The .DLL filename extension indicates that the file is a dynamic-link library.

Mouse Driver Files

The mouse drivers shipped with Windows for Workgroups 3.11 support pointing devices for use with Windows for Workgroups 3.11 and Windows-based applications.

Driver	Supported mouse or pointing device
LMOUSE.DRV	Logitech™ Serial mouse
MSC3BC2.DRV	Genius/Mouse Systems Serial Mouse on COM2
MSCMOUSE.DRV	Genius/Mouse Systems Serial mouse on COM1
MOUSE.DRV	Logitech Bus or PS/2 style, Microsoft, or IBM PS/2 mouse
NOMOUSE.DRV	No mouse or other pointing device

For information about the related MS-DOS mouse drivers, see “MS-DOS Support Components of Windows for Workgroups” later in this chapter.

Display Driver Files

The display drivers shipped with Windows for Workgroups support the system display adapter and the cursor for the pointing device. The display driver, however, does not support MS-DOS-based applications running in a full screen, because these applications write directly to video.

Driver	Supported display adapter
8514.DRV	8514/a
SVGA256.DRV	Super VGA (800x600 - 256 colors)
SUPERVGA.DRV	Super VGA (800x600 - 16 colors)
VGA.DRV	VGA
V7VGA.DRV	Video Seven™ VGA with 512K (FastWrite, VRAM, 1024i, and compatibles)
XGA.DRV	XGA

Other Driver Files

The communications driver, COMM.DRV, supports serial and parallel device communications.

The Advanced Power Management device driver, POWER.DRV (and POWER.HLP), supports the power management features of laptop and notebook personal computers.

Printer Driver Files

Printer drivers support output to the printer. Some of the printer drivers shipped with Windows for Workgroups have a soft-font installation utility. Related files also include help files for the printer drivers and soft-font installers. In Windows for Workgroups, many dot-matrix drivers have been replaced by a universal printer driver. Other drivers have been updated for performance and to support TrueType fonts.

<i>Printer driver</i>	<i>Representative printer</i>
CANON10E.DRV	Canon® Bubble-Jet BJ-10e
CANON130.DRV	Canon Bubble-Jet BJ-130e
CANON330.DRV	Canon Bubble-Jet BJ-300/330
CIT24US.DRV	Citizen 24-pin
CIT9US.DRV	Citizen 9-pin
DICONIX.DRV	Kodak® Diconix
DMCOLOR.DLL	Universal color printing support library
EPSON24.DRV	Epson® 24-pin
EPSON9.DRV	Epson 9-pin
ESCP2.DRV	Epson ESCP2 dot matrix
EXECJET.DRV	IBM ExecJet®
GENDRV.DLL	Generic library
HPDSKJET.DRV	Hewlett-Packard DeskJet® Series
HPPCL.DRV	HP LaserJet II Series
HPPCL5E.DRV	HP LaserJet 4/4M
HPPCL5E.HLP	HP LaserJet 4/4M printer driver help file
HPPCL5E1.DLL	HP LaserJet 4/4M printer driver support file
HPPCL5E2.DLL	HP LaserJet 4/4M printer driver support file
HPPCL5E3.DLL	HP LaserJet 4/4M printer driver support file
HPPCL5E4.DLL	HP LaserJet 4/4M printer driver support file
HPPCL5MS.DRV	HP LaserJet III Series
HPLOT.DRV	HP Plotter
IBM4019.DRV	IBM Laser Printer 4019
IBM5204.DRV	IBM Quickwriter® 5204
LBPII.DRV	Canon LBP-8 II
LBPIII.DRV	Canon LBPIII
NEC24PIN.DRV	NEC® 24-pin
OKI24.DRV	Okidata® 24-pin
OKI9.DRV	Okidata 9-pin
OKI9IBM.DRV	Okidata 9-Pin IBM Model
PAINTJET.DRV	HP PaintJet®
PANSON24.DRV	Panasonic® 24-pin
PANSON9.DRV	Panasonic 9-pin
PROPRINT.DRV	IBM Pro series
PROPRN24.DRV	IBM Pro 24 pin series

Printer driver	Representative printer	<i>(continued)</i>
PS1.DRV	IBM PS/1	
PSCRIPT.DRV	Postscript (PSCRIPT.HLP is the Help file)	
QWIII.DRV	IBM QuietWriter® III	
THINKJET.DRV	HP ThinkJet® (2225 C-D)	
TTY.DRV	Generic / Text only (TTY.HLP is the Help file)	
UNIDRV.DLL	Microsoft universal library (UNIDRV.HLP is the Help file)	

The following files are soft-font installers for specific printers.

Soft-font installer	Related printer
CAN_ADF.EXE	Canon LBP-8 II or LBPIII
FINSTALL.DLL	HPPCL5/MS (FINSTALL.HLP is the Help file)
SF4019.EXE	IBM Laser Printer 4019

The following files provide additional PostScript® description information for specific printers.

PostScript description	Related printer
40291730.WPD	IBM LaserPrinter 4029 (17 fonts)
40293930.WPD	IBM LaserPrinter 4029 (39 fonts)
DEC1150.WPD	Digital DEClaser 1150
DEC2150.WPD	Digital DEClaser 2150
DEC2250.WPD	Digital DEClaser 2250
DEC3250.WPD	Digital DEClaser 3250
DECCOLOR.WPD	Digital ColorMate PS
DECLPS20.WPD	Digital LPS Print Server
EPL75523.WPD	Epson EPL-7500
HPELI523.WPD	HP LaserJet III Si PostScript
HPIID522.WPD	HP LaserJet IID PostScript
HPIII522.WPD	HP LaserJet III PostScript
HPIIP522.WPD	HP LaserJet IIP PostScript
HP_3D522.WPD	HP LaserJet IIID PostScript
HP_3P522.WPD	HP LaserJet IIIP PostScript
IBM17521.WPD	IBM 4019 (17 fonts)
IBM39521.WPD	IBM 4019 (39 fonts)
L100_425.WPD	Linotronic™ 100 v42.5
L200230&.WPD	Linotronic 200/230
L300_471.WPD	Linotronic 300 v47.1
L300_493.WPD	Linotronic 300 v49.3
L330_52&.WPD	Linotronic 330
L500_493.WPD	Linotronic 500 v49.3
L530_52&.WPD	Linotronic 530
L630_52&.WPD	Linotronic 630
MT_TII01.WPD	Microtek TrueLaser
N2090522.WPD	NEC Silentwriter2 90
N2290520.WPD	NEC Silentwriter2 290

<i>PostScript description</i>	<i>Related printer</i>	<i>(continued)</i>
N2990523.WPD	NEC Silentwriter2 990	
N890X505.WPD	NEC Silentwriter LC890XL	
N890_470.WPD	NEC Silentwriter LC890	
NCM40519.WPD	NEC Colormate PS/40	
NCM80519.WPD	NEC Colormate PS/80	
O5241503.WPD	OceColor G5241 PS	
O5242503.WPD	OceColor G5242 PS	
OL840518.WPD	Oki OL840/PS	
P4455514.WPD	Panasonic KX-P4455	
PHIIPX.WPD	Phaser II PX	
Q2200510.WPD	QMS-PS 2200	
Q820_517.WPD	QMS-PS 820	
SEIKO_04.WPD	Seiko ColorPoint PS Model 04	
SEIKO_14.WPD	Seiko ColorPoint PS Model 14	
TIM17521.WPD	TI MicroLaser PS17	
TIM35521.WPD	TI MicroLaser PS35	
TKPHZR21.WPD	Phaser II PX I	
TKPHZR31.WPD	Phaser III PX I	

Multimedia Driver Files

The following drivers support the multimedia capabilities of Windows for Workgroups.

<i>Filename</i>	<i>Purpose</i>
MCICDA.DRV	MCI CD-audio driver
MCISEQ.DRV	MCI driver for MIDI driver
MCIWAVE.DRV	MCI driver for waveform audio
MIDIMAP.DRV	Driver for MIDI Mapper Control Panel extension
MMSOUND.DRV	Multimedia sound driver
MPU401.DRV	MIDI driver for MPU401 compatibles
MSADLIB.DRV	MIDI driver for Adlib compatibles
SNDBLST.DRV	SoundBlaster™ 1.5 DSP driver
SNDBLST2.DRV	SoundBlaster 2.0 DSP driver
TIMER.DRV	Multimedia timer driver

Font Files

Windows for Workgroups 3.11 has several fonts for use with Windows for Workgroups 3.11, Windows– and MS-DOS–based applications, as well as any data copied to the Clipboard from those applications. For detailed information on about Windows fonts, see Chapter 9, “Fonts,” in the *Windows Resource Kit*.

Font files usually have a .TTF, .FON, or .FOT filename extension.

System Font Files

Three types of fonts are installed to support display and output devices:

- **System** is a proportional font used by default to draw menus, dialog box controls, and other text in Windows 3.x.
- **Fixed** is a fixed-width font used in Windows 2.x and earlier versions as the system font (for menus and dialog boxes).
- **OEM font**, or Terminal, is a fixed-width font used to display the OEM text in the Windows for Workgroups 3.11 ClipBook Viewer. The OEM font also provides an OEM character set used by some Windows-based applications.

The system, fixed, and OEM fonts that ship with Windows for Workgroups 3.11 are listed in the following tables.

System font file	Supported display resolution
8514SYS.FON	8514/a (1024x768) resolution system font
VGASYS.FON	VGA (640x480) resolution system font

Fixed font file	Supported display resolution
8514FIX.FON	8514/a (1024x768) resolution fixed system font
VGAFIX.FON	VGA (640x480) resolution fixed system font

OEM font file	Supported display resolution
8514OEM.FON	8514/a (1024x768) resolution Terminal font (U.S./Europe)
VGAOEM.FON	VGA (640x480) resolution Terminal font (U.S./Europe)

Raster Font Files

Six resolutions of raster screen fonts are shipped with Windows for Workgroups. If used for printing, raster fonts print text and graphics as bitmaps or raster lines. The resolutions are identified by a letter appended to the filename of the font as described in the following table.

Letter	Output device	Resolution	x size*	y size*
A**	CGA display	2:1	96	48
B**	EGA display	1.33:1	96	72
C**	Printer	1:1.2	60	72
D**	Printer	1.66:1	120	72
E	VGA display	1:1	96	96
F	8514 display	1:1	120	120

* x,y indicates the height/width aspect ratio, in pixels per inch.

** These fonts are not included on the Windows for Workgroups installation disks.

By appending the letter that identifies the resolution to the raster font filenames in the following table, you can see the files that Windows for Workgroups installs for a given display or printer. For example, the files for the 8514 raster fonts are COURF.FON, SSERIFF.FON, SERIFF.FON, SMALLF.FON, and SYMBOLF.FON.

Font	Filename	Character set	Font description
Courier	COURx.FON	ANSI	Fixed-width with serifs
MS Sans Serif	SSERIFx.FON	ANSI	Proportional-width sans serif
MS Serif	SERIFx.FON	ANSI	Proportional-width serif
Small	SMALLx.FON	ANSI	Proportional small size
Symbol	SYMBOLx.FON	Symbol	Math symbols

Vector Font Files

Windows for Workgroups 3.11 provides three vector font files: ROMAN.FON, SCRIPT.FON, and MODERN.FON. Vector fonts are fully scalable fonts, whose characters are stored as sets of relative coordinate pair points with connecting lines. Vector fonts can be created in any size desired, although applications or printing devices may have limited support for font sizes.

TrueType Font Files

The TrueType downloadable fonts that ship with Windows for Workgroups 3.11 support the Arial, Courier, Symbol, and Times New Roman font families. Each family requires two files, a .TTF file and an .FOT file.

TrueType filenames	Font name
ARIAL.FOT, ARIAL.TTF	Arial
ARIALBD.FOT, ARIALBD.TTF	Arial Bold
ARIALBI.FOT, ARIALBI.TTF	Arial Bold Italic
ARIALI.FOT, ARIALI.TTF	Arial Italic
COUR.FOT, COUR.TTF	Courier
COURBD.FOT, COURBD.TTF	Courier Bold
COURBI.FOT, COURBI.TTF	Courier Bold Italic
COURI.FOT, COURI.TTF	Courier Italic
TIMES.FOT, TIMES.TTF	Times New Roman
TIMESBD.FOT, TIMESBD.TTF	Times New Roman Bold
TIMESBI.FOT, TIMESBI.TTF	Times New Roman Bold Italic
TIMESI.FOT, TIMESI.TTF	Times New Roman Italic
SYMBOL.FOT, SYMBOL.TTF	Symbol
WINGDING.FOT, WINGDING.TTF	Wingding

Font Files for MS-DOS-based Applications

Windows for Workgroups 3.11 provides a set of fonts for displaying MS-DOS-based applications running in a window. By default, code page 437 (U.S.) fonts are installed. Other font files are included for international language support and are identified by the code page number appended to the filename.

The following font files are provided with the associated code page translation table files.

Font file	Translation table	Code page	Configuration
APP850.FON		850	U.S., 386 enhanced mode
DOSAPP.FON		437	U.S., 386 enhanced mode
CGA40850.FON	XLAT850.BIN	850	Multilingual
CGA40WOA.FON	-	437	U.S.
CGA80850.FON	XLAT850.BIN	850	Multilingual
CGA80WOA.FON	-	437	U.S.
EGA40850.FON	XLAT850.BIN	850	Multilingual
EGA40WOA.FON	-	437	U.S.
EGA80850.FON	XLAT850.BIN	850	Multilingual
EGA80WOA.FON	-	437	U.S.
VGA850.FON	XLAT850.BIN	850	Multilingual
VGA860.FON	XLAT860.BIN	860	Portuguese
VGA861.FON	XLAT861.BIN	861	Icelandic
VGA863.FON	XLAT863.BIN	863	French Canadian
VGA865.FON	XLAT865.BIN	865	Norwegian/Danish

International Support Files

Windows for Workgroups 3.11 provides language libraries to support a number of languages.

<i>Filename</i>	<i>Supported languages</i>
LANGDUT.DLL	Dutch language driver
LANGENG.DLL	General International language driver
LANGFRN.DLL	French language driver
LANGGER.DLL	German language driver
LANGSCA.DLL	Finnish/Danish/Icelandic/Norwegian/Swedish language driver
LANGSPA.DLL	Spanish language driver

MS-DOS Support Components of Windows for Workgroups 3.11

Two kinds of files provide MS-DOS support for Windows for Workgroups 3.11: MS-DOS drivers and grabber files that support data exchange between Windows and MS-DOS-based applications.

MS-DOS Driver Files

Several MS-DOS driver files are included with Windows for Workgroups 3.11. The drivers provided with Windows for Workgroups are the recommended versions to use.

<i>Driver</i>	<i>Purpose</i>
EMM386.EXE	Microsoft MS-DOS 386 EMS manager
HIMEM.SYS	Microsoft MS-DOS XMS manager
IFSHLP.SYS	IFS Manager (IFSMGR.386) real mode stub
RAMDRIVE.SYS	Microsoft MS-DOS RAMDrive utility
SMARTDRV.EXE	Microsoft MS-DOS SMARTDrive 5.0 disk-caching utility
LMOUSE.COM	MS-DOS Level Logitech mouse driver
MOUSE.COM	MS-DOS mouse driver
MOUSE.SYS	MS-DOS mouse driver (installed at MS-DOS boot time)
MSCDEX.EXE	Microsoft CD-ROM Extensions driver

WinOldAp and the Grabber Files

Two primary parts of Windows support MS-DOS-based applications when Windows for Workgroups is running in standard mode: WinOldAp and the grabber. When Windows for Workgroups 3.11 runs in 386 enhanced mode, the limited resources on the computer are virtualized to provide virtual memory, virtual displays, virtual communications, and a number of other services. The related files are discussed in “Files for 386 Enhanced Mode” later in this chapter.

WinOldAp and grabber files support data exchange between MS-DOS-based applications and Windows. Support for MS-DOS-based applications varies, depending on the capabilities of the system CPU.

WINOA386.MOD is used for Windows for Workgroups 3.11 in 386 enhanced mode.

The grabber for your system is specific to the display driver.

386 grabbers that support Windows 386 enhanced mode provide the following capabilities:

- Copying text from MS-DOS-based applications
- Displaying data in a windowed virtual machine
- Selecting data in a windowed virtual machine
- Copying graphics to the Windows Clipboard
- PrintScreen

Files that provide font support for the grabbers are listed below, with descriptions of the kinds of display drivers that the grabbers support.

386 grabber support file

Display device supported

V7VGA.3GR	Video 7
VGA.3GR	VGA
VGA30.3GR	VGA (version 3.0)
VGADIB.3GR	DIB (8514/a monochrome)

Files for 386 Enhanced Mode

Virtual memory support in Windows for Workgroups 3.11 is provided by WIN386.EXE, which is executed by WIN.COM. When WIN386.EXE begins to load, it searches for the files identified in the [386enh] section of SYSTEM.INI. Some standard files are built into WIN386.EXE (designated with the "*" symbol preceding the name of the driver in SYSTEM.INI entries). The other files WIN386.EXE loads to support virtual devices are listed in the following table.

<i>Filename</i>	<i>Virtual device supported</i>
IOS.386	Windows I/O supervisor device
IFSMGR.386	Installable File System Manager
LPT.386	Virtual LPT driver
LVMD.386	Logitech virtual mouse device
HPEBIOS.386	EBIOS virtual device for Hewlett-Packard machines
MSCVMD.386	Mouse Systems virtual mouse device
RMM.D32	Real mode disk driver (used to support VFAT.386)
SERIAL.386	Serial communications driver
V7VDD.386	Video Seven virtual display device
VADLIBD.386	Virtual DMA device for Adlib
VCACHE.386	32-bit cache manager
VCOMM.386	Virtual communications driver
VFAT.386	Virtual 32-bit FAT device driver
VDD8514.386	8514/a virtual display device
VDDSVGA.386	Super VGA virtual display device
VDDVGA30.386	VGA virtual display device (version 3.0)
VDDXGA.386	XGA® virtual display device
VPOWERD.386	Advanced Power Management virtual device
VSBD.386	SoundBlaster virtual device
VTDAPI.386	Multimedia virtual timer device
VXDLDR.386	Dynamic VxD loader
WIN386.PS2	Support for PS/2 architecture

Windows for Workgroups 3.11 Applications, Setup, and Other Files

Files for Windows for Workgroups 3.11 Applications

Windows for Workgroups files also include applications, shells, utilities, accessories, and games. The following table lists the applications and associated files, with a brief description of each application.

Filename	Associated files	Application name and description
CALC.EXE	CALC.HLP	Calculator (general/scientific)
CARDFILE.EXE	CARDFILE.HLP	Cardfile (desktop Rolodex)
CHARMAP.EXE	CHARMAP.HLP	Character Map
CLIPBRD.EXE	CLIPBRD.HLP CLIPSRV.EXE	ClipBook Viewer ClipBook DDE server application
CLOCK.EXE		Clock (analog/digital)
CONTROL.EXE	CONTROL.HLP CONTROL.INI CPWIN386.CPL DRIVERS.CPL LZEXPAND.DLL MAIN.CPL MIDIMAP.CFG SND.CPL WFWSETUP.DLL	Control Panel Initialization file 386 enhanced mode extension for Control Panel Installable drivers extension for Control Panel File expansion utility for Control Panel Main Control Panel extension MIDI Mapper extension file for Control Panel Sound extension for Control Panel WFW network setup extension for Control Panel
MPLAYER.EXE	MPLAYER.HLP MMSYSTEM.DLL MMTASK.TSK	Media Player Multimedia system library Multimedia background task
MSD.EXE	MSD.INI	Microsoft Diagnostics utility and initialization file
MSHEARTS.EXE	MSHEARTS.HLP CARDS.DLL	Hearts card game
NETDDE.EXE		Network DDE background application
	NDDEAPI.DLL NDDENB.DLL	Network DDE—DDE shares API support Network DDE driver for NetBIOS
NETWATCH.EXE	NETWATCH.HLP	Net Watcher
NOTEPAD.EXE	NOTEPAD.HLP	Notepad (desktop text editor)
PACKAGER.EXE	PACKAGER.HLP	Object Packager
PBRUSH.EXE	PBRUSH.DLL PBRUSH.HLP	Paintbrush
PIFEDIT.EXE	PIFEDIT.HLP	PIF Editor
PRINTMAN.EXE	PRINTMAN.HLP	Print Manager (Windows print spooler)
PROGMAN.EXE	PROGMAN.INI PROGMAN.HLP	Program Manager (shell)
RECORDER.EXE	RECORDER.HLP RECORDER.DLL	Recorder (desktop macro recorder)
REGEDIT.EXE	REGEDIT.HLP REGEDITV.HLP DDEML.DLL OLECLI.DLL OLESVR.DLL	Registration Editor and supporting files DDE management library Client library and server for object linking and embedding
SHELL.DLL		Shell library
SOL.EXE	SOL.HLP	Solitaire game
SMARTDRV.EXE		Disk-caching utility

Filename	Associated files	Application name and description	<i>(continued)</i>
SOUNDREC.EXE	SOUNDREC.HLP	Sound Recorder	
SYSEDIT.EXE		Windows System Editor	
TASKMAN.EXE		Task Manager (application switcher)	
TERMINAL.EXE	TERMINAL.HLP	Terminal (desktop communications)	
TOOLHELP.DLL		Windows Tool Helper library	
WINCHAT.EXE	WINCHAT.HLP	Chat	
WINFILE.EXE	WINFILE.HLP	File Manager	
WINHELP.EXE	WINHELP.HLP	Help (Windows help engine)	
	GLOSSARY.HLP	Windows Help glossary	
WINMETER.EXE		System performance meter	
WINMINE.EXE	WINMINE.HLP	MineSweeper game	
WINTUTOR.EXE	WINTUTOR.DAT	Windows Tutorial	
WRITE.EXE	WRITE.HLP	Write (desktop word processor)	

Control Panel uses LZEXPAND.DLL to expand files from the Windows for Workgroups installation disks. Because most of the files on the Windows for Workgroups installation disks are compressed (except SETUP.INF, SETUP.EXE, and EXPAND.EXE), Control Panel must expand the files to install a new printer or to add fonts. LZEXPAND is a Windows library counterpart to EXPAND.EXE.

Files Used for Windows for Workgroups 3.11 Mail, Schedule+, and Microsoft At Work Fax

The files Windows for Workgroups 3.11 uses for Mail, Schedule+, and Microsoft At Work fax are all related. The files used for each of these components is identified in this section.

Files used for Mail

The following files are used for Mail.

Filename	Associated files	Application name and description
MSMAIL.EXE	MSMAIL.HLP	Mail Application
	SENDFILE.DLL	File Manager extension to send file as attachment
	AB.DLL	Address Book user interface support functions
	DEMILAYR.DLL	MS WGA System Services layer
	FRAMEWRK.DLL	Microsoft WGA Application Framework layer
	IMPEXP.DLL	Mail message file import utility
	MAILMGR.DLL	Mail Manager API support functions
	MAILSPL.EXE	MS Mail for Windows—Mail spooler

Filename	Associated files	Application name and description	(continued)
	MAPI.DLL	MS Messaging Applications Programming Interface	
	MSSFS.DLL	Microsoft shared file system transport	
	STORE.DLL	Message store support functions	
	VFORMS.DLL	Mail viewed forms DLL	
	WGPOMGR.DLL	Windows for Workgroups Post Office Manager	

functions

Files used for Schedule+

The following files are used for Schedule+.

Filename	Associated files	Application name and description
SCHDPLUS.EXE	SCHDPLUS.HLP SCHDPLUS.INI	Schedule+ Application
	MSREMIND.EXE	Schedule+ background reminder notification
	SCHEDMSG.DLL	Schedule+ message forms for MS Mail
	TRNSCHED.DLL	Schedule+ shared file system transport

Files used for Microsoft At Work Fax

The following files are used for Microsoft At Work fax.

Filename	Application name and description
AWCAS.DLL	Fax CAS modem driver
AWCLASS1.DLL	Fax Class 1 modem driver
AWCLASS2.DLL	Fax Class 2 modem driver
AWFAXIO.DLL	Fax protocol to pump interface
AWFXPROT.DLL	Fax enhanced protocol DLL
AWT30.DLL	Fax T30 protocol DLL
DLLSCHED.DLL	Fax scheduler
EFAXDRV.DRV	Fax printer driver
EFAXPUMP.DLL	Fax pump
EFAXRUN.DLL	Fax file-based transport interface
FAX.CPL	Fax control panel driver
FAXCODEC.DLL	WFW T.4 Codec
FAXCOVER.DLL	Fax cover page DLL
FAXMGR.EXE	Fax manager
FAXNSP.DLL	Fax name service provider
FAXOPT.DLL	Fax options DLL
FAXSTUB.DLL	Mail shared file system transport
FAXVIEW.EXE	Fax viewer application
FAXVIEW.HLP	Fax viewer application help file

Filename	Application name and description	<i>(continued)</i>
IFKERNEL.DLL	Fax OS kernel extensions	
KEYVIEW.EXE	Fax security keyfile importer	
LINEARIZ.DLL	Fax BFT linearizer	
MSFAX.HLP	Fax help file	
NETFAX.DLL	Fax network implementation	
SIGVIEW.EXE	Fax Security Signature viewer	
VPMTD.386	Fax scheduler VxD device	

Other Files

The following files serve a wide range of functions, including support for PS/2 architectures and README files for general information.

Filename	Purpose
MORICONS.DLL	Icons for MS-DOS-based applications
Bitmaps files for wallpaper:	
ARCADE.BMP	Arcade wallpaper
ARGYLE.BMP	Argyle wallpaper
CASTLE.BMP	Castle wallpaper
EGYPT.BMP	Egypt wallpaper
HONEY.BMP	Honey wallpaper
REDBRICK.BMP	Red brick wallpaper
RIVETS.BMP	Rivets wallpaper
SQUARES.BMP	Squares wallpaper
THATCH.BMP	Thatch wallpaper
WINLOGO.BMP	Logo wallpaper
ZIGZAG.BMP	Zigzag wallpaper
Screensaver files:	
SSFLYWIN.SCR	Flying Windows
SSMARQUE.SCR	Marquee screen saver
SSSTARS.SCR	Stars screen saver
MIDI sound file:	
CANYON.MID	Canyon MIDI sound
Wave-form sound files:	
CHIMES.WAV	Exit sound
DING.WAV	Default beep
RINGIN.WAV	Chat incoming ring sound
RINGOUT.WAV	Chat outgoing ring sound

Filename	Purpose	(continued)
README files:		
MAIL.WRI	README file for mail client	
NETWORKS.WRI	README file for networks	
PRINTERS.WRI	README file for printers	
README.WRI	README file	
SYSINI.WRI	README file for SYSTEM.INI	
WININI.WRI	README file for WIN.INI	
Miscellaneous hardware support and other supporting files:		
386MAX.VXD	Qualitas® 386MAX virtual device for standard mode	
BLUEMAX.VXD	Qualitas BlueMAX™ virtual device	
COMMCTRL.DLL	WFW internal custom-control user interface functions	
COMMMDLG.DLL	Windows Common Dialogs library	
WIN87EM.DLL	80x87 math coprocessor emulation library	
WINDOWS.LOD	Qualitas 386MAX/BlueMAX loadable module	

Network Files Used for Microsoft Windows Network

Network Driver Files

Network drivers provide a network interface to the Windows for Workgroups File Manager, Control Panel, Print Manager, and system utilities.

Driver	Support file	Supported network
WFWNET.DRV	WFWNET.HLP	Microsoft Windows for Workgroups network driver
	NETAPI.DLL	Windows for Workgroups network API library
	PMSPL.DLL	Windows for Workgroups printer API library
	LMScript.EXE LMScript.PIF	LAN Manager script support utility
MSNET.DRV		Generic network driver*

* MSNET.DRV supports 3Com 3+Share®, 3Com 3+Open LAN Manager (XMS only), Banyan® VINES® 4.0, Microsoft LAN Manager 1.x (and compatibles), Microsoft LAN Manager 2.0 Basic (and compatibles), Microsoft Network (and compatibles), and IBM PC LAN Program.

For a list of supporting virtual device files for network drivers, see “Files for 386 Enhanced Mode” later in this chapter.

Real Mode Network Support Files

The network support files included with Windows for Workgroups 3.11 are listed in the following table.

<i>Driver</i>	<i>Purpose</i>
NET.EXE	WFW MS-DOS network redirector
NET.MSG	WFW network redirector message file
NETH.MSG	WFW network redirector help message file
PROTMAN.EXE	WFW protocol manager TSR
PROTMAN.DOS	WFW protocol manager driver

NDIS 2 Network Adapter Card Driver Files

The following NDIS 2 drivers are provided with Windows for Workgroups 3.11 to support network adapter cards.

<i>Driver</i>	<i>Related Network Adapter Card</i>
AM2100.DOS	Advanced Micro Devices AM2100/PCnet
DEPCA.DOS	DEC EtherWorks
E20ND.DOS	Cabletron E2000 Series
E21ND.DOS	Cabletron E2100 Series
ELNK16.DOS	3Com EtherLink® 16
ELNK3.DOS	3Com EtherLink III
ELNKII.DOS	3Com EtherLink II
ELNKMC.DOS	3Com EtherLink/MC
ELNKPL.DOS	3Com EtherLink Plus
EVX16.DOS	Everex™ SpeedLink /PC16 (EV2027)
EXP16.DOS	Intel EtherExpress 16
HPLANB.DOS	HP PC LAN Adapter
HPLANP.DOS	HP PC LAN Adapter Plus
I82593.DOS	Intel Motherboard Module
IBMTOK.DOS	IBM Token Ring
MAC586.SYS	DCA® 10 Mb
NCC16.DOS	Tulip NCC-16
NDIS39XR.DOS	Proteon Token Ring
NE1000.DOS	Novell/Anthem NE1000 (or compatible)
NE2000.DOS	Novell/Anthem NE2000 (or compatible)
NI6510.DOS	Racal-Interlan NI6510

Driver	Related Network Adapter Card (continued)
OLITOK.DOS	Intel TokenExpress™ 16/4
PCMNIC.DOS	IBM PCMCIA-NIC
PENDIS.DOS	Xircom Pocket Ethernet I
PE2NDIS.DOS	Xircom Pocket Ethernet II
PRO4.DOS	Proteon ISA Token Ring
PRO4AT.DOS	Proteon ISA Token Ring
SMC3000.DOS	SMC 3000 Series
SMCMAC.DOS	SMC (WD) EtherCard PLUS
SMC_ARC.DOS	SMC ARCNET
STRN.DOS	NCR Token Ring
TCCARC.DOS	Thomas Conrad TC6x4x (Enhanced Mode)
TLNK.DOS	3Com TokenLink

Note Other NDIS drivers are available as part of the Windows Driver Library (WDL). See Appendix A for more information on how to obtain the WDL.

386 Enhanced Mode Network Drivers

Filename	Virtual device supported
VNETSUP.386	WFW virtual network support device
NDIS.386	NDIS 3 wrapper
NDIS2SUP.386	NDIS 2 real mode mapper
NWSUP.386	ODI/NDIS 3 support driver
VREDIR.386	WFW virtual network redirector device
VSERVER.386	WFW virtual network server device
VSHARE.386	WFW virtual file sharing device

NDIS 3 Network Transport Protocol Drivers

Filename	Virtual device supported
NETBEUI.386	Windows for Workgroups 3.11 NetBEUI NDIS 3 transport
NWLINK.386	Windows for Workgroups 3.11 32-bit IPX/SPX compatible transport
NWNBLINK.386	Windows for Workgroups 3.11 32-bit NetBIOS driver for IPX/SPX

NDIS 3 Network Card Drivers

<i>Filename</i>	<i>Virtual device supported</i>
DECLAN.386	DEC DEPCA Ethernet card
EE16.386	Intel EtherExpress 16
ELNK16.386	3Com EtherLink 16
ELNK3.386	3Com EtherLink III
ELNKII.386	3Com EtherLink II
ELNKMC.386	3Com EtherLink MCA
HPISA.386	HP PC LAN Adapter - ISA
HPMCA.386	HP PC LAN Adapter - MCA
IBMTOK.386	IBM Token Ring
NE1000.386	Novell/Anthem NE1000 (or compatible)
NE2000.386	Novell/Anthem NE2000 (or compatible)
NE3200.386	Novell/Anthem NE3200 (or compatible)
NI6510.386	Racal NI6510
PROTEON.386	Proteon Token Ring (P1390)
SMC8000W.386	SMC EtherCard (all types except 8013/A)

Files used for Remote Access Services Client

The files used for the Remote Access Services (RAS) client are listed in the following table.

<i>Filename</i>	<i>Associated files</i>	<i>Application name and description</i>
RASMAC.386		RAS MAC driver - for Remote Access Services client
RASPHONE.EXE	RASPHONE.HLP	RAS connection application
	RASSTART.EXE	RAS startup application
	RASMAN.DLL	RAS manager
	RASSAUTH.DLL	RAS server side authentication
	RASSER.DLL	RAS serial DLL
	RASSVR.DLL	Remote Access Server
	PAD.INF	X.25 pad information file
	SWITCH.INF	RAS switch information file
	RASMON.EXE	RAS monitor
	RASAPI16.DLL	RAS API DLL
	RASCAUTH.DLL	RAS client authentication DLL
	RASCONF.DLL	RAS configuration DLL
	RASMXS.DLL	RAS modem DLL
	RASFILE.DLL	RAS file I/O DLL

Minimizing Files Necessary for Windows for Workgroups 3.11

To reduce the disk footprint of Windows for Workgroups 3.11, you can load only the files required to run the operating system. Before deleting any files from your Windows for Workgroups 3.11 WINDOWS or SYSTEM directory, turn on the File Delete confirmation option in File Manager, or make a backup copy of the files in the specified directories.

Note Some applications may place files in your Windows for Workgroups 3.11 WINDOWS or SYSTEM directory. The recommendations provided in this section are based on the knowledge of only the files provided with Windows for Workgroups 3.11 that may be removed without affecting system usage. If you have any applications that have installed files in the WINDOWS or SYSTEM directory, carefully review the contents of these directories before deleting any files.

Files You Can Safely Delete

Because of the large number of files that the Windows for Workgroups 3.11 setup program installs, you may want to delete some of the files to free disk space.

Note Do not delete any of the files listed below, while Windows for Workgroups 3.11 is running. Instead, quit Windows for Workgroups 3.11, and then delete the files at the MS-DOS command prompt.

You can safely delete the following files when Windows for Workgroups 3.11 is *not* running without degrading Windows for Workgroups 3.11 performance:

- Any files in the TEMP directory (temporary files have a .TMP filename extension).
- Any files that start with the characters ~WOA or ~GRB.
- Any files named WIN386.SWP (a temporary Windows swap file). DO NOT delete files named 386SPART.PAR or SPART.PAR — these files are used for a permanent swap file and should not be removed manually. (Use Control Panel to change the size or remove the permanent swapfile.)

From Windows Setup, choose Add/Remove Windows Components from the Options menu to remove any of these files from your system:

- Any accessories you do not use (such as Paintbrush, Write, and Cardfile) with their related .HLP and .DLL files (if any)

- Games
- Screen savers
- Wallpapers (.BMP files) and sound files (.WAV files)

Help Files

If you don't need any help files for Windows for Workgroups applications or accessories, you can delete all files with the extension .HLP.

ReadMe files

If you don't need any of the readme files provided with Windows for Workgroups, you can delete all files with the extension .WRI.

Screen Savers

If you don't need any of the screen saver files provided with Windows for Workgroups, you can delete all of the files with the extension .SCR.

Bitmap Images/Wallpapers

If you don't need any of the bitmap image files provided with Windows for Workgroups, you can delete all of the files with the extension .BMP.

Wave (Sound) Files

If you don't need any of the wave (sound) files provided with Windows for Workgroups, you can delete all of the files with the extension .WAV.

Games

If you don't need any of the game files provided with Windows for Workgroups, you can delete:

- SOL.EXE - Solitaire
SOL.HLP
- HEARTS.EXE - Hearts
HEARTS.HLP
- WINMINE.EXE - Minesweeper
WINMINE.HLP

**Chapter
4**

Windows for Workgroups 3.11 Initialization Files

This chapter contains information about the new or updated settings that are present in the Windows for Workgroups 3.11 initialization files. For entries not listed in this chapter, refer to Chapter 6 of the *Windows for Workgroups Resource Kit for version 3.1*.

The information in this chapter is provided for reference and describes the entries that may be present in some of the initialization files used by components of Windows for Workgroups 3.11, including the SYSTEM.INI, MSMAIL.INI, and EFAXPUMP.INI. This chapter describes the sections of each initialization file and each of the related entries. The chapter also specifies the default value used for an entry (the default value is used if the entry is not present in the initialization file), and the means for changing an entry present in an initialization file.

Related Information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 1, “Windows for Workgroups 3.11 Architecture;” Chapter 2, “Windows for Workgroups 3.11 Setup and Installation;” Chapter 11, “Tips for Optimizing Windows for Workgroups 3.11.”
- *Windows for Workgroups Resource Kit for version 3.1:* Chapter 5, “Windows for Workgroups Setup Information Files;” Chapter 6, “Windows for Workgroups Initialization Files;” Chapter 13, “Troubleshooting Windows for Workgroups.”

Contents of This Chapter

About the Initialization Files	4-2
Format of the .INI Files	4-3
Changing Entries in .INI Files	4-4
Editing .INI Source Files	4-6
SYSTEM.INI: System Initialization File	4-6
MSMAIL.INI: Microsoft Mail Initialization File	4-21
EFAXPUMP.INI: Microsoft At Work Fax Settings Initialization File	4-22

About the Initialization Files

The Windows for Workgroups 3.11 initialization files contain information that defines the Windows for Workgroups 3.11 environment. Microsoft Windows for Workgroups 3.11 and Windows-based applications use the information in these files to configure themselves according to each user's needs and preferences.

The Windows for Workgroups 3.11 initialization files that are either new or contain new or updated settings are SYSTEM.INI, MSMAIL.INI, and EFAXPUMP.INI files. For information on other settings in initialization (.INI) files provided with Windows for Workgroups 3.11, see Chapter 6, "The Windows for Workgroups Initialization Files," in the *Windows for Workgroups Resource Kit, version 3.1*.



.INI file	File contents
SYSTEM.INI	Contains entries for configuring Windows for Workgroups 3.11 to meet system specific hardware needs.
MSMAIL.INI	Contains entries that define the appearance and behavior of Mail.
EFAXPUMP.INI	Contains entries that enable sharing of custom Mail commands and custom messages with other members of a workgroup.

Important Errors made by editing initialization files can lead to undesirable results when you run Windows for Workgroups 3.11. Before changing any entry, make a backup copy of the file. Read "Changing Entries in .INI Files" later in this chapter for guidelines.

Format of the .INI Files

The Windows for Workgroups 3.11 setup initialization files are text files that contain one or more sections. The format for each section is:

```
[section]
keyname= value           ; comment
```

Value	Definition
[<i>section</i>]	The name (header) of a section. The enclosing brackets ([]) are required, and the left bracket must be in the leftmost column of the file.
<i>keyname</i>	The name of an entry, which can consist of any combination of letters and digits. For many entries, the <i>keyname</i> must be followed immediately by an equal sign.
<i>value</i>	The value of each entry, which can be an integer, a string, or a quoted string, depending on the entry.
; <i>comment</i>	Some entries include brief comments below the header or on the same line as an entry. You can include comments anywhere in an .INI file by prefacing the comment with a semicolon (;).

In this chapter, the sections that appear in bold contain the actual words that are used in the INI file. For example: [**windows**] section. When a section is referenced generically, the section name is shown in italics, in bold brackets. For example, PROTOCOL.INI contains the [*netcard_protocol*] section that actually includes separate sections for each network adapter card name, such as [**MS\$EE16**] for the Intel EtherExpress 16 or 16TP adapter card.

Some variable entries must be substituted for specific values in the entry. These entries are shown in italics in this format:

```
keyname= profile, description, filesize
```

Case (capital or lowercase letters) does not matter for values, unless specified for a particular item. Some items must be enclosed in double quotation marks (“ ”). For example: **caption**= “Windows Setup”.

The actual words of an entry are shown in bold, such as “**Beep= Yes | No**”. The values that can be substituted in the entry are shown in italics. When the value can be one of several choices, the choices are separated with a pipe character (|). For example:

```
Beep= Yes | No
```

For many entries, the *value* is shown as *Boolean*. To enable an entry that requires a Boolean value, you can enter **True, Yes, On, or 1**. To disable such an entry, you can enter **False, No, Off, or 0**. These entries are not case sensitive.

Any entry listed here but which does not appear in your .INI file is automatically assigned the default value shown in this chapter.

Changing Entries in .INI Files

Windows for Workgroups creates the initialization files during installation and assigns default values. Some entries are added or changed when you install or configure a Windows application. You can edit these entries to change the appearance or performance of Windows for Workgroups.

You can use the following options to change the entries in an .INI file:

- Use Control Panel, Program Manager, File Manager, Mail or Schedule+ to change entries with the menu commands and dialog box options.
- Run Windows Setup again to change system settings, the keyboard or mouse configuration, or network options, and to add or remove printers and fonts.
- Choose a command such as Printer Setup from the File menu in Print Manager and specify new options.
- Use a text editor such as Notepad to edit the file directly.

Many of the entries in this section list the most appropriate method for changing the entry.

Important Always create a backup copy of the .INI file before you open it, and use care when making changes. Incorrect changes can lead to unexpected results when you run Windows for Workgroups 3.11. Edit the entries for .INI files only when necessary. Do not use a formatting editor, such as a word processor in document mode. Some editors can damage characters with ANSI values of greater than 127. We recommend that you use the Control Panel or Setup interface when possible to make changes. If you must hand-edit the file, use a text editor such as Notepad, System Editor, or Edit (provided with versions 5.0 and higher of MS-DOS).

To change .INI file entries with a text editor

1. **Important** Create and save a backup copy of the .INI file.
2. Open the .INI file with a text editor such as Notepad.
3. Edit the specific entries and save the file in ASCII (text only) format.
4. Restart Windows for Workgroups 3.11 and the changes made to the .INI file will take effect.

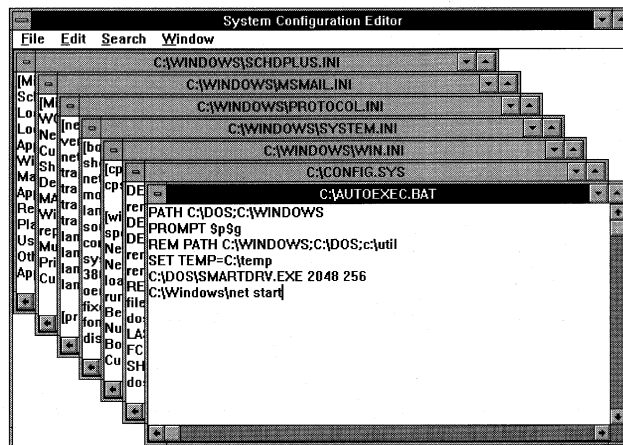
To edit system files with System Editor:

You can use the System Editor utility in Windows for Workgroups 3.11 to edit AUTOEXEC.BAT, CONFIG.SYS, WIN.INI, SYSTEM.INI, PROTOCOL.INI, MSMAIL.INI, and SCHDPLUS.INI at the same time if needed. The System Editor is installed in your WINDOWS directory by Windows Setup.

1. **Important** Create a backup copy of the .INI file you want to edit.
2. Choose Run from the File Menu in Program Manager. Type `sysedit` on the command line and press ENTER.
3. Click on the window in System Editor that contains the file you want to edit.

Figure 4.1

The System Editor in
Windows for
Workgroups 3.11



4. Edit the file, using the same text editing techniques as in Notepad.
5. Save the file, and choose Exit from the File menu to close System Editor.
6. Restart Windows for Workgroups 3.11 to enable the changes you made to take effect. If you edit CONFIG.SYS or AUTOEXEC.BAT, you must reboot your system for the changes to take effect.

Editing .INI Source Files

If you copy the Windows for Workgroups 3.11 files to a network server using the **setup /a** option (to install a shared copy of Windows for Workgroups 3.11), Setup uses WIN.SRC, SYSTEM.SRC, and CONTROL.SRC to build WIN.INI, SYSTEM.INI, and CONTROL.INI. To create custom initialization files for multiple installations, you can modify the .SRC files.

To edit the .SRC files, first save a backup copy of the original file, then make editing changes in the file, following the guidelines in this chapter. Save the file with an .SRC filename extension in the WINDOWS directory on the network server. Test the new .SRC file on a single system before installing Windows for Workgroups 3.11 on multiple systems by verifying the appropriate operations with the created INI file.

SYSTEM.INI: System Initialization File

When you install Windows for Workgroups 3.11, Setup creates the SYSTEM.INI file. SYSTEM.INI contains global system information that Windows for Workgroups 3.11 uses when it starts, and contains settings that you can customize to meet your system's hardware needs.

The SYSTEM.INI sections discussed in this chapter appear here in alphabetical order for easy reference, the sections may not appear in this sequence in the initialization file. The SYSTEM.INI file can contain the following sections:



Section	Purpose
[386Enh]	Contains information used by Windows for Workgroups 3.11 in 386 enhanced mode.
[network]	Contains information for defining the Windows for Workgroups 3.11 network configuration.
[network drivers]	Contains information for defining the Windows for Workgroups 3.11 real-mode network configuration.
[NWNBLink]	Contains information used by the 32-bit NetBIOS driver for IPX.
[vcache]	Contains information for defining the Windows for Workgroups 3.11 cache management settings.

Many of the other entries described in this chapter are rarely needed and do not appear in the SYSTEM.INI file unless they are added manually. Most of these entries have a default value that is present whether or not the entry appears in SYSTEM.INI. You might need to change one or more of these values to improve the performance of Windows for Workgroups 3.11 or a specific application.

The possible methods for changing values are noted for each entry in this chapter. Most of the SYSTEM.INI entries cannot be changed through the Control Panel interface. You can change many of the settings by running the Setup program from the Main program group. Other values in SYSTEM.INI can be changed only by opening the file and editing it manually with a text editor such as Notepad.

The changes you make to the SYSTEM.INI file do not take effect until you restart Windows for Workgroups 3.11. Refer to “Editing .INI Source Files” earlier in this chapter.

[386Enh]

The [386Enh] section contains information specific to running Windows for Workgroups 3.11 in 386 enhanced mode, including information used for virtual memory page swapping.

For entries in this section that specify virtual devices, the value can appear in two ways—either as the filename of a specific virtual device driver (with path if necessary), or as an asterisk (*) followed immediately by the device name to refer to a virtual device built into the WIN386.EXE file.

This section can contain the following entries:



DisableVFATWarning= on | off

Specifies whether the 32-bit File System warning screens are to be displayed or not. For example, one of the warning screens provides instructions to the user on how to tell Windows for Workgroups to install the 32-bit File System support drivers to allow 32-bit disk caching on a compressed disk volume. Set **DisableVFATWarning= to on** to prevent the warning screen from being displayed. The default is **off** (the warning screen is displayed).

EnableSharingPopUps= Boolean

Specifies whether a SHARE.EXE sharing violation message is to appear when a sharing violation occurs while using the VSHARE.386 device. If the value for this setting is **True**, the SHARE.EXE messages appear. Set this value to **True** if you are using an MS-DOS-based application that relies on the sharing-violation message. If the value for this setting is **False**, the SHARE.EXE message does not appear and will not be notified if a sharing violation occurs. The default is **False**.

**Netcard= drivervname [, ...]**

Specifies a comma separated list of NDIS 3.0 network adapter card drivers that Windows for Workgroups 3.11 conditionally loads on startup. If NDIS 2.0 network protocols are loaded on startup, the entries on the **Netcard=** line are ignored.

**Netcard3= drivervname [, ...]**

Specifies a comma separated list of NDIS 3.0 network adapter card drivers that Windows for Workgroups 3.11 loads on startup. These NDIS 3.0 network adapter card drivers are always loaded.

**NetMisc= drivervname [, ...]**

Specifies a comma separated list of miscellaneous network Virtual device drivers that Windows for Workgroups 3.11 will load. Typically, the drivers include the mappers and other network support layers, such as NDIS.386, NDIS2SUP.386, MSODISUP.386, and NWSUP.386.

Network= filename | device name

Specifies the core virtual network drivers that are used when Windows for Workgroups is in 386 enhanced mode. The default is ***vnetbios, *vwc, vnetsup.386, vredir.386, vservers.386**. This entry is a synonym for **Device=**. Setup assigns an appropriate value based on your system configuration.

SecondNet= filename

Specifies the virtual network drivers for the additional network you have configured on your workstation. The **secondnet=** entry is synonymous with **device=**. The default is none (blank). Setup sets this value to match your configuration. (For example, if NetWare is selected as the additional network, the **secondnet=** entry will be defined as **secondnet=vnetware.386**.)

Transport= *filename* [, ...]

Specifies a comma separated list of NDIS 3.0 protected-mode network protocol drivers that Windows for Workgroups 3.11 uses. The **transport=** entry is synonymous with **device=**. Setup sets this value to match your configuration when NDIS 3.0 network protocols are installed.

V86ModeLANAs= *LANA number, LANA number*

Limits the real-mode NetBIOS LANA numbers that will be supported while Windows for Workgroups 3.11 is running to only those LANA numbers listed. This setting is for real-mode NetBIOS drivers only. This setting should not include any LANA numbers for protected-mode protocols or NetBIOS drivers. This setting is useful with NetBIOS protocols which incorrectly identify themselves as being active on LANA numbers others than those assigned to them, for example, the NetWare NETBIOS.EXE TSR. Make sure that the values for this setting do not include LANA numbers assigned to protected-mode protocols such as VNB.386. The default is none (blank). The LANAs for protocols are specified in PROTOCOL.INI. To change this entry, you must edit SYSTEM.INI.

OverlappedIO= *Boolean*

This entry is added if Novell NetWare support installed with Windows for Workgroups 3.11. If **On**, several virtual machines can make read and write requests to a disk before the first request has been completed. If this entry is **Off**, virtual machines cannot issue a request to read or write to a disk until any previous read and write requests have been completed. The default is **Off** if **InDOSPolling= on**. Otherwise, the default is **On**. To change this entry, you must edit SYSTEM.INI. (You should not need to change this entry—Setup adds this entry if NetWare is configured as an additional network.)



[*net.cfg*]

This section contains entries used by the Windows Setup program when configuring Windows for Workgroups 3.11 to use Novell NetWare support.

The [**net.cfg**] section can contain the following entry:



path= *path name*

Specifies the path to the NetWare NET.CFG file containing the ODI driver configuration information. When Novell NetWare support is configured for use with Windows for Workgroups, the user is prompted by the Windows Setup program to identify the location of the Novell NET.CFG file. The value the user specifies during Setup is stored in this entry.

[network]

This section contains settings that affect how your computer interacts with the network. To change the values of the settings described in the [network] section, use the Network tool in Control Panel, except where specified.

The [network] section can contain the following entries:



AuditEnabled= *Boolean*

Specifies whether the event log has been enabled, providing auditing of network access events that occur when other users access your computer. The default for this setting is **No**. To change this setting, select the Event Log button in the Network section of Control Panel.



AuditEvents= *hexadecimal number*

Identifies the events that are being audited in the event log. The value shown for the **AuditEvents=** field is set to reflect the events that the user chooses to monitor. To change this setting, select the Event Log button in the Network section of Control Panel.



AuditLogSize= *number*

Specifies the maximum size to which the audit log grows. The number represents the size of the file in kilobytes. Once the event log exceeds the given size, no further events are added to the log. To change this setting, select the Event Log button in the Network section of Control Panel.

AutoLogon= *Boolean*

Specifies whether you are automatically logged on when you start Windows for Workgroups 3.11. If you are using a logon password, the Windows for Workgroups Logon dialog box appears and asks you to enter your logon password. To log on, you must supply your password. If you have a blank logon password, you will be logged on and no prompt appears. If set to **No**, you are not automatically logged on at startup. The default is **Yes**. To make changes to this entry, run the Network tool in Control Panel and select the Log On at Startup check box in the Startup Settings dialog box.

AutoStart= Full | Basic | Popup | Netbind | Netbeui | Workstation [, ...]

Specifies the additional real-mode components that are loaded when the **net start** command is issued from the command prompt or in AUTOEXEC.BAT. The **Full** value is used to load full redirector support (unless otherwise specified, **Full** is the default value for the redirector support). The **Basic** value is used to load basic redirector support. The **Popup** value is used to load the popup interface. The **Netbind** value is used to bind protocols and network adapter drivers. The **Netbeui** value is used to load the NetBEUI protocol. The **Workstation** value is used to load the default redirector. If you want to specify more than one real-mode component, separate each value by a comma. By default, the **net start** command will perform only the **net bind** functionality. To change this entry, you must edit SYSTEM.INI.

CacheThisPassword= Boolean

Determines whether the Save This Password In Your Password List check box in the Enter Password or LAN Manager Log On dialog box is selected by default the next time the dialog box is displayed. If this entry is **Yes**, the check box is selected. If this entry is **No**, the check box is not selected. When you select or clear the check box, this value is changed in the SYSTEM.INI file. The default is **No**, or the last value specified by the user.

comment= string

Provides a description of your computer (maximum of 48 characters) that appears to other users when they are browsing the workgroup—the string value specified for this entry cannot contain commas. This description appears next to your computer name in the Connect Network Drive, Connect Network Printer, and Select Computer dialog boxes. The default is none (blank).

ComputerName= name

Specifies the name of your computer on the network. Your computer name must be unique, can be a maximum of 15 characters long, and can contain letters, numbers, and any of the following characters (the computer name should not contain a space character, an underscore character should be used instead):

! # \$ % & () - . @ ^ _ ' { } ~

Your computer name appears in the Connect Network Drive, Connect Network Printers, and Select Computer dialog boxes when browsing through workgroups for computers, directories or printers. The default is the name you specified for your computer during setup.

**DeferBrowsing= Boolean**

Specifies whether browsing of network resources occurs automatically when the Connect Network Drive or Connect Network Printer dialog box is displayed. If the value of this field is set to **Yes**, then browsing is deferred and will not automatically occur when the dialog box is displayed. If the value of this field is **No**, then when the dialog box is displayed, the network is browsed for the names of other workgroups that exist and the names of computers defined in your workgroup. The value for this setting is set based on the state of the Always Browse check box in the Connect Network Drive or Connect Network Printer dialog box.

**DirectHosting= on | off**

Specifies whether direct hosting on top of IPX is to be supported. By default, the value for this field is set to **on**, which means that the Windows for Workgroups networking components will first try to talk to other computers using direct hosting, and then will try hosting over NetBIOS if unsuccessful. Configurations that use the NWSUP.386 driver (for example, monolithic IPX, or ARCNet configurations over IPX) require the value for this setting to be set to **off**.

EnableSharing= Boolean

Defines the state of resource sharing depending on the values for **FileSharing=** and **PrinterSharing=** entries. If one or more of the sharing entries is enabled, the value for this entry is **Yes**. If both file sharing and printer sharing are disabled, the value for this entry is **No**. This entry is set by the Network Settings dialog box in Windows Setup.

Exclude= LANA number [, ...]

Indicates that Windows for Workgroups 3.11 should not use the protocols represented by the LANA numbers assigned to this setting. This setting takes precedence over the **LANAs=** or **V86ModeLANAs=** entries, so that a LANA number listed on this line will never be used even if it is also listed in those entries. This setting should be used when a NetBIOS protocol is present but cannot be used by the Windows for Workgroups 3.11 network components; for example, the NetWare NETBIOS.EXE TSR. The default is none (blank). To change this entry, you must edit SYSTEM.INI.

**FileSharing= Boolean**

Specifies whether file sharing is enabled on your computer as selected from the Windows Network Setup dialog box. If the value of this setting is set to **Yes**, then file sharing is enabled. If the value of this setting is set to **No**, then file sharing is disabled. If both **FileSharing=** and **PrinterSharing=** are set to **No**, the Windows for Workgroups Server Virtual device driver (VSERVER.386) will not be loaded into memory. To change this setting, select the Sharing... button from the Windows Network Setup dialog box.

KeepConn= seconds

Specifies the number of seconds Windows for Workgroups 3.11 is to wait before disconnecting an implicit connection that is no longer being used. This is useful if you are performing several directory searches or lists using an implicit connection, or several tasks that involve pipes. If the applications that you are using to perform these tasks run slowly, then increase this value. The default is **600**. (You should not need to change this setting.)

LANAs= LANA number [, ...]

Limits the automatic detection of protocols to the specified list of LANA numbers if you start the network before starting Windows for Workgroups 3.11, and specifies that Windows for Workgroups 3.11 is to use only those protocols present that are assigned LANA numbers included in this setting. This setting is useful with NetBIOS protocols which incorrectly identify themselves as being active on LANA numbers others than those assigned to them, for example, the NetWare NETBIOS.EXE TSR. The default is none (blank). To change this entry, you must edit SYSTEM.INI.

LMAnnounce= Boolean

If this entry is **Yes**, your computer announces its presence to LAN Manager computers in your workgroup. If computers in your workgroup that are running LAN Manager need to see your computer when they browse the network, set this value to **Yes**. The default is **No**, which tells the Windows for Workgroups 3.11 server not to broadcast its presence to LAN Manager clients, and minimizes the level of network traffic. To change this entry, you must edit SYSTEM.INI.

LMLogon= 0 | 1

Specifies whether the LAN Manager Logon dialog box is shown to permit you to log on to a LAN Manager domain when you start Windows for Workgroups 3.11. If this entry is **1**, and you have stored the domain password in your password list, Windows for Workgroups 3.11 logs you on to a LAN Manager domain and runs your logon script, if you have one. If the domain password is not in your password-list, the LAN Manager Logon dialog box appears so that you can pick the domain you want to log on to and specify the password for that domain. The default value is **0**, indicating that you will not log onto a domain. To change this entry, change the state of the Log On to LAN Manager Domain check box in the LAN Manager Settings dialog box.

**LoadHigh= Boolean**

Specifies whether real-mode network drivers load into the upper memory area (UMA) or into conventional memory. Some network drivers contain code to load themselves into the UMA area automatically, this setting overrides the default load method of each real-mode driver. If this entry is **Yes**, real-mode drivers will be loaded into the UMA if space is available. If this entry is **No**, the real-mode drivers will be loaded into conventional memory. The default is **Yes**. To change this setting, you must edit SYSTEM.INI.

**LoadNetDDE= Boolean**

Specifies whether the Network DDE application (NETDDE.EXE) is to be loaded on startup. The Network DDE application is necessary to support Network DDE conversations as used by applications like Chat, Hearts, and ClipBook. Network DDE requires that a protocol be loaded that provides NetBIOS services. If this entry is **No**, the NETDDE.EXE application will not be loaded. The default is **Yes**. To change this setting, select the Startup icon from the Network section of Control Panel and select the Enable Network DDE check box.

**LogonDisconnected= Boolean**

Specifies whether the network redirect just initializes the data structures for persistent network connections such as network drive and printers (ghosted connections) or physically attaches to the network resource. If this entry is **Yes**, connections are “ghosted” and the network connection data structures are initialized, but the physical connection to the network resource is not made until the resource is actually accessed — this results in a lower startup time. If this entry is **No**, the default, then when persistent network connections are restored, the network connection is made to the network resource. To change this setting, enable the Ghosted Connections check box from the Startup icon in the Network section of Control Panel.

LogonDomain= *domain name*

Specifies the name of the default LAN Manager domain (workgroup) that validates your password, if you choose to logon to a LAN Manager domain when you start Windows for Workgroups 3.11 (as specified by the **LMLogon=** entry). The default is the designated workgroup for your computer.

LogonValidated= *Boolean*

Indicates whether your logon was validated by a LAN Manager server when you last logged on. If you decide to change the **LMLogon=** value while you are still logged on by selecting or clearing the Log On To LAN Manager Domain check box in Control Panel, the **LogonValidated=** entry ensures that you are logged off properly when you end your Windows for Workgroups 3.11 session, or if you choose to log off using Control Panel. The default is **No**. (You should not need to change this setting.)

MaintainServerList= *Yes | No | Auto*

Specifies whether your computer will maintain the list of computers in your workgroup and the names of workgroups defined on your network. If this entry is **Yes**, your computer will be used to maintain the list of computers in your workgroup and workgroups on your network, and increases the likelihood that your computer will become the “master” computer in your workgroup which maintains these lists. If this entry is **No**, your computer is never used to maintain these lists—use this setting if your computer has very little free memory, is connected to the rest of your workgroup only by a slow link (such as a telephone-line connection), or other special conditions apply which would cause performance problems. If this entry is **Auto**, your computer will maintain these lists when Windows for Workgroups 3.11 determines that it is necessary. The default is **Auto**. (You should not need to change this value.) To change this entry, you must edit SYSTEM.INI. At least one computer in your workgroup must have a value of either **Auto** (the default) or **Yes** for this entry in order to ensure that the list of workgroups and computers on your network is available.

Multinet= *network name [, ...]*

Specifies the name of one or more active secondary networks that you have added support for in Windows for Workgroups 3.11. The default is none (blank). You can change this entry in the Network Settings dialog box from Windows Setup.

NumBigBuf= *number*

Specifies the number of buffers used by the protected-mode redirector VREDIR.386 to cache data read from the network. Increasing this entry can improve the performance of network operations, but reduces the amount of memory available for applications. This entry is only used if the network is not started from MS-DOS before starting Windows for Workgroups. By default, the redirector uses one eighth of the available physical memory free at the time when it is loaded, so the number of cache buffers is that amount of memory divided by the size of each buffer (which is 4096 bytes in size), rounded down. This entry has a minimum of **2** and a maximum of **4096**.

PrintBufTime= *seconds*

Specifies the number of seconds of idle printing time that Windows for Workgroups 3.11 is to wait before indicating that the end of a print job has been reached when printing from an MS-DOS-based application. When printing to a network printer from an MS-DOS-based application, your documents do not start printing until the application finishes processing the print job. If you are using an MS-DOS-based application that processes print jobs quickly and you want your documents to print sooner, decrease this value. If you are using an MS-DOS-based application that takes longer to process print jobs or if your print job is broken into multiple documents, increase this value. The time an MS-DOS-based application is suspended is not counted. The default value is **45**. To change this entry, you must edit SYSTEM.INI.

**PrinterSharing=** *Boolean*

Specifies whether printer sharing is enabled on your computer as selected from the Windows Network Setup dialog box. If the value of this setting is set to **Yes**, then printer sharing is enabled. If the value of this setting is set to **No**, then printer sharing is disabled. If both **PrinterSharing=** and **FileSharing=** are set to **No**, the Windows for Workgroups Server virtual device driver (VSERVER.386) will not be loaded into memory. To change this setting, select the Sharing... button from the Windows Network Setup dialog box.

priority= *number*

Specifies the relative priority value for sharing resources (VSERVER.386). The lower the number, the less time is given to sharing resources. The higher the number, the more time is given to sharing resources. The default priority is **80**. To make changes to this entry, choose the Network icon in Control Panel and change the position of the Performance Priority slider bar.

reconnect= Boolean

Defines the default state for the Reconnect At Startup check box in the Connect Network Drive or Connect Network Printer dialog box. The Reconnect At Startup check box is used to determine whether the given network connection is re-established when Windows for Workgroups 3.11 is re-started. If this entry is **Yes**, the Reconnect At Startup check box in the Connect Network Drive or Connect Network Printer dialog box is selected the next time the dialog box is displayed. If this entry is **No**, the check box is not selected. When you select or clear the check box, the value for this setting changes in the SYSTEM.INI file to reflect its current state. The default is **Yes**.

reshare= Boolean

Defines the default state for the Reshare At Startup check box in the Share Directory or Share Printer dialog box. The Reshare At Startup check box determines whether the given share is automatically re-shared at startup. If this entry is **Yes**, the Reshare At Startup check box in the Share Directory or Share Printer dialog box is selected the next time the dialog box is displayed. If this entry is **No**, the check box is not selected. When you select or clear the check box, this value is changed in the SYSTEM.INI file to reflect its current state. The default is **Yes**.

**SlowLanas= LANA [, LANA ...]**

Identifies the LANA numbers which are used for slow network connections, for example the Remote Access Service (RAS). For slow LANAs, raw I/O from the redirector is disabled to enable packet sizes to be reduced to support sending across a low speed network link - this prevents the network from timing out when sending NetBIOS data across the slow link. The **SlowLanas=** switch also prevents the local Windows for Workgroups 3.11 computer from becoming a browse server for the given LANA values across slow network connections.

**StartMessaging= Boolean**

Specifies whether the messaging service is started when Windows for Workgroups 3.11 is started and the WinPopup application is loaded to send and receive messages and alerts. When messaging is enabled (**Yes**), Print Manager will send notifications of completed print jobs and WinPopup will receive the sent messages. The default is **No**. To change this setting, select the Startup icon from the Network section of Control Panel and select the Enable WinPopup check box.

username= *name*

Specifies the default logon name (maximum of 20 characters) that is used to log on to Windows for Workgroups 3.11. The value for this setting changes to the logon name you specify when you log on to Windows for Workgroups 3.11 for the first time. The default is your computer name until you log on for the first time. Then the default value becomes the logon name you specify in the Welcome To Windows For Workgroups dialog box.

**WinNet=** *name*

Specifies the name of the primary Windows network (WinNet) driver. When Microsoft networking is enabled, the value for this entry is **wfwnet**. The value for this setting is defined by the networking option selected in the Windows Network Setup dialog box.

WorkGroup= *name*

Specifies the workgroup (maximum of 15 characters) that your computer belongs to. You can change this entry using the Network icon in the Control Panel.

**[network drivers]**

This section contains entries that specify the real-mode NDIS 2.0 network drivers that load when Windows for Workgroups 3.11 is started. The entries in this section are created or modified when you configure your network drivers from the Network Settings dialog box in Windows Setup.

The **[network drivers]** section can contain the following entries:

**devdir=** *path name*

Specifies the path name pointing to the location of the network device driver files and the PROTOCOL.INI file. These drivers include PROTMAN.DOS, PROTMAN.EXE and all drivers listed on the **transport=** and **netcard=** lines. For a new installation, the **devdir=** entry is set to point to the WINDOWS directory.

**LoadRMDrivers= Boolean**

Specifies whether the real-mode NDIS 2.0 drivers are loaded automatically when the NET START command is issued at the MS-DOS command prompt. If the value for this entry is **Yes**, then the real-mode network drivers will load automatically and bind at the time **net start** is run. These drivers are the NDIS 2.0 MAC drivers, NDISHLP.SYS, other NDIS 2.0 protocols, and PROTMAN.DOS. If the value for this entry is **No**, the real-mode drivers will not load unless the real-mode network services are started manually with one of the NET commands (for example; **net start workstation**, **net use**, **net initialize**, **net start net bind**, **net start full**, **net start basic**, **net view**). If NDIS 2.0 drivers are installed, the default value for this entry is **Yes**.

**netcard= path name, ...**

Specifies a comma separated list of the names of the NDIS 2.0 network adapter card drivers that are configured for your system. The driver names listed for this setting will most likely end in .DOS or .SYS and must be real-mode NDIS 2.0 drivers. The value for this entry is set when you add or remove network adapter cards using the Network Settings dialog box in Windows Setup.

**transport= path name**

Specifies a comma separated list of the names of the NDIS 2.0 protocol drivers that are configured for your system. The driver names listed for this setting will most likely end in .DOS or .SYS and must be real-mode NDIS 2.0 drivers. The value for this entry is set when you add or remove network protocols using the Network Settings dialog box in Windows Setup.

**<NetworkCardDriver>.DOS= low | high**

Specifies whether given real-mode NDIS 2.0 driver is loaded into conventional memory (low), or into the upper memory area (high). <NetworkCardDriver> represents the name of the NDIS 2.0 driver (for example, EXP16.DOS). By default, unless the network adapter card driver contains code to load itself into the UMA, the network adapter card driver will be loaded into conventional memory.



[NWNBLink]

This section contains entries used by the NetBIOS services driver for IPX/SPX, NWNBLINK.386. NetBIOS requires a lanabase entry to map the NetBIOS services to a specific network adapter card.

The [NWNBLink] section may contain the following entry:



lanabase= *LANA number*

Specifies the LANA number on which to assign to the NWNBLink NetBIOS services driver. This entry is created or modified when the IPX/SPX Compatible Transport with NetBIOS is installed or when the IPX Support Driver (Monolithic) with NetBIOS transport is installed. This entry has identical functionality to the LANABASE= entry in the PROTOCOL.INI for the NetBEUI protocol.



[vcache]

This section contains entries that specify parameters for the 32-bit file access cache. Only the **MinFileCache** parameter is written to the SYSTEM.INI by default. The entries for the other settings are not modified by the Windows for Workgroups 3.11 user interface and need to be edited manually. Take special care when editing any of these settings.

The [vcache] section can contain the following entries:



MinFileCache= *number*

Specifies the size of the cache for the 32-bit file access driver, VFAT.386. The size of the cache is represented in kilobytes. Setup installs a 512K cache size when Windows for Workgroups 3.11 is installed. If this entry is not present, the size of the cache is defaulted to 64K. For information on recommended cache sizes based on computer configuration, see Chapter 11, "Tips for Optimizing Windows for Workgroups 3.11."



ForceLazyOn= *drive letters*

Specifies that VCACHE should enable lazy writing for the given drive letters. This entry allows a user to override the default lazy write condition of 32-bit file access (VFAT). The drive letters should be concatenated together as parameters for this entry (for example, "DEF" identifies drive letters D, E, and F). The default state of lazy writing is dependent upon the computer configuration. Use of this switch should be done with caution, as a disk full

condition may result in data loss if you do not have sufficient disk space to complete disk write operations. To change the state of lazy writing, you need to edit SYSTEM.INI to add this option. You should not need to change the values for this option.



ForceLazyOff= *drive letters*

Specifies that vcache should disable lazy writing for the given drive letters. This entry allows a user to override the default lazy write condition of 32-bit file access (VFAT). The default state of lazy writing is dependent upon the computer configuration. The drive letters should be concatenated together as parameters for this entry (for example, "DEF" identifies drive letters D, E, and F). The default state of lazy writing is dependent upon the computer configuration. Using this option provides additional security for assuring data is written to disk from the cache immediately, rather than delaying the write operation, however the use of this option may result in lower performance. To change the state of lazy writing, you need to edit SYSTEM.INI to add this switch. You should not need to change the values for this option.

MSMAIL.INI: Microsoft Mail Initialization File

The MSMAIL.INI file is the Microsoft Mail initialization file that is used by the Mail application provided with Windows for Workgroups 3.11. MSMAIL.INI can contain the following sections:

Section	Purpose
----------------	----------------

[EFAX Transport]	Contains information about the state of the EFAX transport when Microsoft At Work fax messaging is installed.
-------------------------	---

The information below is written to your MSMAIL.INI file when the Microsoft At Work fax messaging components are installed.

[EFAX Transport]

This section is used to define setting information needed by Mail for using the fax transport.

LocalFax= 0 | 1

Specifies whether the fax transport drivers are installed. The fax setup adds this entry when the fax components are installed from Control Panel, and sets the value to **1** (Yes). The default is **0** (No).



EFAXPUMP.INI: Microsoft At Work Fax Settings Initialization File



The EFAXPUMP.INI file is the initialization file that is used by the Microsoft At Work fax components provided with Windows for Workgroups. EFAXPUMP.INI can contain the following sections:

<i>Section</i>	<i>Purpose</i>
[COMn]	Specifies the configuration for a fax modem on a given communications port.
[EFAX Pump]	Specifies the configuration of the fax message mail pump to send outgoing fax messages.
[Message]	Specifies the default values for the options used when sending a fax message.
[Modem]	Specifies information for the fax modem to use when sending a fax message.
[Network]	Specifies entries used for maintaining information about shared fax modems
[Received]	Contains temporary information about received faxes before they are turned into message attachments and placed in you mail Inbox.
[Security]	Specifies information about securing fax messages.

Many of the entries in this section are defined by default when the Microsoft At Work fax messaging components are installed. Other entries can be changed using the Fax options dialog from Mail or configured from the Fax section of Control Panel.

[COMn]

This section identifies the configuration for a fax modem on a given communications port. Communication sections that may be present in your EFAXPUMP.INI include **[COM1]**, **[COM2]**, **[COM3]**, and **[COM4]** depending on the number of communication ports configured on your system.



AnswerMode= 0 | 1 | 2

Defines the mode for the fax modem for answering an incoming call. The values for this setting are: **2** = never answer, **1** = manual answer, **0** = auto answer.



AreaCode= area code

Specifies the area code where the local fax modem resides.

**BlindDial= 0 | 1**

Specifies whether blind dial is allowed. The values for this entry are: **0** = don't allow blind dial, **1** = allow blind dial. Blind dialing is useful when sending faxes in countries where your fax modem doesn't properly recognize the dial tone.

**Class = *n***

Specifies the type of fax modem that is installed in the computer. Identifies the communication standard that the At Work fax software uses to communicate with the fax modem. A value of **2** indicates Class 1, a value of **4** indicates Class 2, and a value of **6** indicates your modem supports both.

**Class0ModemID= [string]; [string]; [string]; [string]; [string]; [string]; [string]; [string];**

Provides an identification of the modem being used on the COM port. Each string is the first non-blank line response from your modem of an ATIO-7 command.

**Class2ModemID= [string]; [string]; [string];**

Provides an identification of the modem being used on the COM port for a Class 2 modem. Each string is the first non-blank line response from your modem to the +FMFR?, +FMDL?, and +FREV? commands.

**CommaDelay= *seconds***

Specifies the number of seconds delay for a comma in a phone number sequence.

**CopyQualityCheckLevel= 0 | 1 | 2 | 3 | 4**

Determines how thoroughly received Group 3 faxes are checked for errors. A value of **0** causes very little error checking. A value of **4** causes a high level of error checking. If received faxes are visually accurate, but the computers that sent the fax to you report errors, you may consider reducing this value. The default value is **3**.

**CountryCode= *string***

Specifies the country dialing code for the local fax modem.

**DisableECM= 0 | 1**

Specifies whether Email format is available for fax messages. A value of **1** disables sending Email format. A value of **0** enables sending Email format. The default is **0**.

**EnableV17Recv= 0 | 1**

A value of **1** enables receiving faxes using V.17 at 14400 bits per second (bps) and 12000 bps. A value of **0** disables this feature with a maximum of 9600 bps using V.29. Your modem must have the capability to support V.17 in order for this to work properly. The default is **0**.

**EnableV17Send= 0 | 1**

A value of **1** enables sending faxes using V.17 at 14400 bps and 12000 bps. A value of **0** disables this feature with a maximum of 9600 bps using V.29. Your modem must have the capability to support V.17 in order for this to work properly. The default is **0**.

**ExitCommand= *string***

Specifies the user command sent to the fax modem last before shutdown of fax services.

**FixModemClass= *n***

Forces the modem to use a particular class. A value of **1** forces the modem to use Class 1. A value of **2** forces the modem to use Class 2. Your modem must have the capability to support the specified class in order to work properly.

**FixSerialSpeed= *baud rate***

Sets the DTE-DCE communicate rate. The default is **19200**. A value of 9600 sets the rate to 9600 instead of the default. Setting the value to 9600 restricts the fax transmission rate over the phone line to 4800 baud. This feature may not work with all modems.

**HangupDelay= *n***

Specifies the number of seconds to wait before hanging up an unanswered outgoing call. The default is **60** seconds.

**HighestSendSpeed** = *baud rate*

Specifies the highest baud rate to try to synchronize with the remote modem. The default is **9600**.

**InternationalPrefix** = *string*

Specifies the international dialing prefix.

**LongDistancePrefix** = *string*

Specifies the local distance outside area code dialing prefix.

**LocalNumber** = *string*

Specifies the local phone number for the phone line to which the fax modem is connected.

**LocalPrefix** = *string*

Specifies the local dialing prefix for the phone line to which the fax modem is connected.

**Log** = **0** | **1**

Specifies whether fax transmission information is recorded in the file FAXWATCH.LOG in the Windows directory. If you are having difficulties with your fax transmission then this file can be sent to Microsoft Product Support Services so that we can get a better understanding of where the problems are occurring. A value of **0** means that the transmission information is not recorded in FAXWATCH.LOG. A value of **1** means that the transmission information is recorded.

**LowestSendSpeed** = *baud rate*

Specifies the lowest baud rate to try to synchronize to the remote modem before giving up the connection attempt. The default is **2400**.

**ModemFaxClasses** = *n*

Specifies the type of fax modem that is installed on the COM port. Identifies the communication standard that the At Work fax software uses to communicate with the fax modem. A value of **2** indicates Class 1, a value of **4** indicates Class 2, and a value of **6** indicates your modem supports both.

**ModemID = string**

Identifies the modem used on the COM port. This allows the At Work software to recognize if the modem has been replaced with a different modem.

**ModemIDCmd = string**

Identifies the modem used on the COM port along with ModemID. This allows the At Work software to recognize if the modem has been replaced with a different modem.

**ModemRecvSpeeds = n**

Specifies the speeds and communication protocols available in this modem for receiving faxes. A 4-bit map is used to represent the available receiving capabilities of the modem. The low-order bit represents V.29 at 9600 and 7200 bps. The second-lowest bit represents V.27 at 4800 bps. The third bit represents V.33 at 12000-14400 bps. The high-order bit represents V.17 at 7200-14400 bps.

**ModemSendSpeeds = n**

Specifies the speeds and communication protocols available in this modem for sending faxes. A 4-bit map is used to represent the available receiving capabilities of the modem. The low-order bit represents V.29 at 9600 and 7200 bps. The second-lowest bit represents V.27 at 4800 bps. The third bit represents V.33 at 12000-14400 bps. The high-order bit represents V.17 at 7200-14400 bps.

**NumRings = n**

Specifies the number of rings after which the fax modem answers an incoming call. The default is 3.

**PreAnswerCommand= string**

Specifies the user command to be sent to the fax modem just before an incoming call is answered.

**PreDialCommand=** *string*

Specifies the user command to be sent to the fax modem just dialing an outgoing call.

**PulseDial=** *n*

Specifies whether pulse dialing or touch-tone dialing is to be used when making an outgoing call. A value of **0** indicates touch-tone, and a value of **1** indicates pulse dial. The default is **0**.

**SetupCommand=** *string*

Specifies the user command that is sent to the modem after the **at&f** command is sent. This command string is used to initialize the fax modem.

**SmallFrameECM=** *0 | 1*

Specifies whether 64 byte or 256 byte frames are used for ECM. A value of **0** forces 256 byte frames. A value of **1** forces 64 byte frames. This should be set to **1** if you are sending faxes over a phone line with a lot of static or interference. The default is **0**.

**SpeakerMode=** *n*

Specifies the state of the speaker on the fax modem. A value of **0** indicates that the speaker is always off, a value of **1** indicates that the speaker is on during an outgoing dial, and a value of **2** indicates that the speaker is always on.

**Volume=** *n*

Specifies the volume level to use for the fax modem speaker when **SpeakerMode=** switch is not set to **0**. The speaker volume values can range from **1** to **9**, with **1** being the lowest volume level and **9** being the highest.

[EFAXPump]

The entries in this section are used to configure the fax message mail pump to send outgoing fax messages.

**MaxRetries= *n***

Specifies the maximum number of attempts that are made to send an outgoing fax message before failing.

**SpoolDirectory= *path name***

Specifies a path name for where fax messages are spooled while residing in the outgoing queue. By default, fax messages are spooled to the directory identified by the TEMP environment variable.

[Message]

The entries in this section identify the default values for the options used when sending a fax message.

**CheapTimeEnds= *n***

Specifies the time when cheap phone times end, using a 24-hour clock. The default value for this entry is **600** (6 a.m.).

**CheapTimeStarts= *n***

Specifies the time when cheap phone times start, using a 24-hour clock. The default value for this entry is **1800** (6 p.m.).

**DeliveryFormat= *n***

Specifies the default delivery format for sending an outgoing fax message. A value of **0** indicates that the fax message should be sent as a binary message. A value of **1** indicates that the fax message should be sent as a rendered Group 3 facsimile transmission. A value of **2** indicates that the fax message should be sent as email if the destination machine supports that type of message, otherwise, a group 3 facsimile will be transmitted. The default is **2**.

**ImageQuality= *n***

Specifies the default image quality for an outgoing fax message that is rendered. A value of **0** indicates standard resolution. A value of **1** indicates fine resolution. A value of **2** indicates 300 dots per inch (dpi). A value of **3** indicates that the best image quality supported by the destination machine will be used. The default is **3**.

**IncludeCover= *n***

Specifies whether a cover page should be included with the fax message. A value of **0** indicates that the cover page should not be included, while any other value indicates that a cover page should be used. The default is **0**.

**LastLogoFile1= *path name***

Specifies the path name to a previously used bitmap for the logo on a cover page. The path name must be a fully qualified path name referencing the given bitmap image.

**LastLogoFile2= *path name***

Specifies the path name to a previously used bitmap for the logo on a cover page. The path name must be a fully qualified path name referencing the given bitmap image.

**LastLogoFile3= *path name***

Specifies the path name to a previously used bitmap for the logo on a cover page. The path name must be a fully qualified path name referencing the given bitmap image.

**LastLogoFile4= *path name***

Specifies the path name to a previously used bitmap for the logo on a cover page. The path name must be a fully qualified path name referencing the given bitmap image.

**LastLogoFile5=** *path name*

Specifies the path name to a previously used bitmap for the logo on a cover page. The path name must be a fully qualified path name referencing the given bitmap image.

**LogoFile=** *path name*

Specifies the default bitmap for the logo for the cover page. The path name must be a fully qualified path name referencing the bitmap image.

**MinutesBetweenRetries=** *n*

Specifies the number of minutes to wait before retrying the attempt to send the fax message after a send fails. The default is **10** minutes.

**PaperSize=** *n*

Specifies the default paper size to use when rendering the fax message image. Valid setting values include: **0** = letter, **1** = legal, **2** = A4, **3** = B4, **4** = A3. The default is **0**.

**ScheduledTransmitTime=** *n*

Specifies the default transmit time for an outgoing fax message when a specific time is wanted, using 24-hour clock. The default is **1200** (12 p.m.).

**TransmitPriority=** *n*

Specifies the default priority to use when sending a fax message. A value of **0** indicates ASAP, a value of **1** indicates cheap, and a value of **2** indicates at specified transmit time. The default is **0**.

[Modem]

The switches in this section identify information for the fax modem to use when sending a fax message.



DefaultFax= *n*

Specifies the default fax device to use. A value of **0** is undefined or no default, values in the range of **1-4** indicate COM ports 1-4, values in the range of **6-21** are the allowable 16 network connections, and a value of 38 indicates a Communications Application Specification (CAS) modem. The value of **5** is not used. There is no default.



ValidPorts= *n*

Specifies the valid communication ports (1 through 4) that are available in the system using a four bit map. The low order bit means COM1 is valid, second lowest bit means COM2 is valid, and so on. This setting is determined at the time the fax components are installed.



CasModem= *n*

A value of **0** specifies that no CAS modem is installed. A value of **1** indicates that a modem is installed. The default value is **0**.

[Network]

Entries in this section are used for maintaining information about shared fax modems.



NetworkNamenn= *string*

Specifies the share name and type of fax modem configured on the given share. The valid range for *nn* is 00 through 15 and identifies the 16 possible network shares. The *string* identifies the name of a share that is serving as the fax modem queue.

**ValidNetConns= *n***

Specifies which of the **Net*nn*** entries that are actually installed. A 16-bit map is used to represent the existence of the **Net*nn*** present, with the low-order bit representing 00, and the high-order bit representing 15.

[security]

Entries in this section are used for maintaining information about fax message security.

**AlwaysEncrypt= 0 | 1**

Specifies whether fax messages sent in email format should be key-encrypted by default. A value of **0** disables this feature by default. A value of **1** enables encrypting each of these messages by default.

**AlwaysLogin= 0 | 1**

Specifies whether fax advanced security is enabled. A value of **0** means advanced security features are disabled. A value of **1** means they will be enabled then next time the user starts the At Work fax transport. The user will be required to enter their fax security password at that time.

**AlwaysSign= 0 | 1**

Specifies whether attachments of fax messages sent in Email format should be digitally signed by default. A value of **0** disables this feature by default. A value of **1** enables digitally signing each of these attachments by default.

Chapter
5

Windows for Workgroups 3.11 Security Control Enhancements

This chapter describes the security control enhancements implemented in Windows for Workgroups 3.11. These enhancements include the ability to disable file and printer sharing, configure password settings, and leverage the security mechanisms of Windows NT Advanced Server. A discussion of the functionality offered by the administrator configuration utility (ADMINCFG.EXE) that is included with Windows for Workgroups 3.11 is provided along with tips on how to implement the administrator security settings in a network environment.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:*
Chapter 2, "Windows for Workgroups 3.11 Setup and Installation;"
Chapter 7, "Integrating with Windows NT and Windows NT Advanced Server."

Contents of This Chapter

Overview of Security Control Enhancements	5-2
Configurable Peer Networking	5-2
Administration of Security Settings	5-4
Administrator-Defined Password Settings	5-5
Password Settings	5-5
Banner Options	5-6
Support for Windows NT Security Features	5-7
Implementing Windows for Workgroups 3.11 Security Controls	5-10
Expanding the ADMINCFG.EXE Utility	5-10
Creating the Security Settings File (WFWSYS.CFG)	5-11
Password-Protecting the Security Settings File	5-11
Installing the Security Settings File	5-12
Updating Security Settings Remotely	5-13
Scenario Examples for Remote Update of Security Settings	5-15
Auditing of Network Events	5-19
Net Watcher	5-19
Event Log	5-20

Overview of Security Control Enhancements

Windows for Workgroups 3.11 has many enhanced security features to prevent unauthorized access to shared information on the network as well as unauthorized access to the network. The system administrator may define and control some or all of the security settings for users of Windows for Workgroups 3.11 and Workgroup Add-on for MS-DOS.

The security model in Windows for Workgroups 3.1 was designed to protect data in a networking environment, without requiring a network administrator to perform complicated procedures to enable the security system. Windows for Workgroups 3.11 contains enhancements to the security system provided with Windows for Workgroups 3.1, but maintains the ease of use and flexibility for the system administrator.

Windows for Workgroups 3.11 provides the following improved security controls:

- **Configurable peer networking**

The system administrator can disable peer file and/or printer sharing, and users cannot restore this capability.
- **Administrator-defined password settings**

An administrator can define and control password settings that Windows for Workgroups uses.
- **Support for Windows NT Advanced Server security features**

Through a validated logon to Windows NT Advanced Server domain, access to the network is restricted if the user isn't granted permission by the network administrator.
- **Auditing of network events**

Users can monitor network access to their local computers by other network users.

Configurable Peer Networking

Many corporate MIS organizations that are responsible for administering dedicated server operating systems, such as Microsoft Windows NT Advanced Server and Novell NetWare, require the ability to disable file sharing or printer sharing on some workstations on the network.

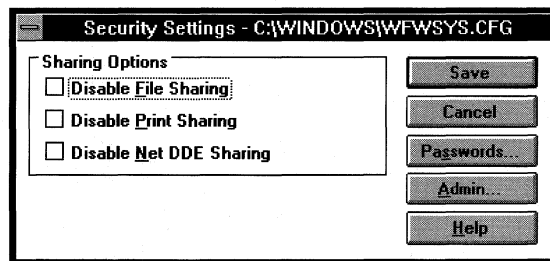
Windows for Workgroups 3.11 brings configurable peer networking to the corporate environment, enabling system administrators to control the networking privileges for each user. The administrator can selectively disable file sharing, printer sharing and Network DDE conversations using the Security Settings configuration application. These settings are stored in an encrypted file (WFWSYS.CFG) on each workstation. There are several mechanisms in place to prevent a user from circumventing the security settings configured for a specific workstation. If a user deletes the WFWSYS.CFG file on a workstation, the user will not have access to the network. It is also impossible for a user to use a copy of a WFWSYS.CFG file from another workstation because each WFWSYS.CFG file is uniquely identified with the computer on which it is originally installed.

The system administrator can maintain a central set of security-settings files that can be used by workstations on the network. The administrator can modify the security-settings file in the central location and then the Windows for Workgroups-based workstations will synchronize their security settings with the new settings.

The Security Settings application, ADMINCFG.EXE, is used to configure the security settings for a workstation running Windows for Workgroups 3.11 or Workgroup Add-on for MS-DOS.

Figure 5.1

The Security Settings dialog box allows the system administrator to configure the peer networking features of Windows for Workgroups.



The peer networking features of Windows for Workgroups that can be controlled by the system administrator are:

- **Disable File Sharing**

This setting prevents the workstation from sharing directories with other users on the network. Selecting this option will disable only the ability to share files — the workstation will still be able to access shared files on the network.

- **Disable Print Sharing**

This setting prevents the workstation from sharing any printers that may be connected to it. Selecting this option will disable only the ability for that workstation to share its printers with others—the workstation will still be able to access shared printers on the network.

- **Disable Network DDE Sharing**

If Network DDE Sharing is disabled, the workstation will not be able to act as a Network DDE server. It can act as a client to other Network DDE servers. This setting is used to prevent access to information on the local computer by other computers using the Network DDE inter-application communication mechanism.

Administration of Security Settings

A useful feature of the security system in Windows for Workgroups 3.11 is that it enables a system administrator to configure the security settings and then distribute them remotely. Due to the security settings synchronization architecture in Windows for Workgroups 3.11, if the administrator finds it necessary to change any of the security settings, the changes can be updated automatically when Windows for Workgroups 3.11 starts up on each workstation.

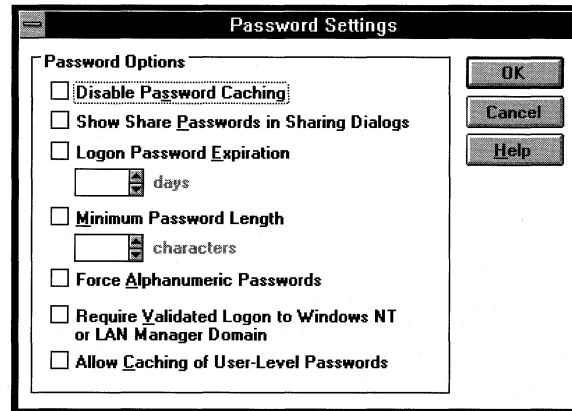
The system administrator can specify a network location where common security-settings files reside, allowing the security-settings files on multiple workstations to be updated from a single location. Workstations can be managed individually or in groups. This eases the burden on the system administrator when it comes time to a change to the security setting. Configuring different security-settings files for different users allows an administrator to vary the levels of users' security. More information on remote updating of security settings is presented later in this chapter.

Administrator-Defined Password Settings

In addition to controlling file sharing, printer sharing, and Network DDE conversations on the network, Windows for Workgroups 3.11 features enhanced password security. Using the Security Settings configuration application, a network administrator can define settings for the various password controls.

Figure 5.2.

The Password Setting dialog box, displayed by choosing the Passwords button in the main Security Settings dialog box



Password Settings

The password settings that an administrator can configure for a computer running Windows for Workgroups 3.11 or Workgroup Add-on for MS-DOS are:

- **Disable Password Caching**

When password caching is enabled, Windows for Workgroups creates a password file containing the names of the shared network resources and the passwords required to connect to them. If password caching is disabled, the user must type in the correct password each time he or she connects to a password protected share.

- **Show Share Passwords in Sharing Dialogs**

When enabled, this setting forces the actual characters of a password, rather than asterisks, to display when typed into a password field in a dialog box used to share resources.

- **Logon Password Expiration**

When enabled, this setting specifies the maximum number of days a user can use a password. After this period expires, the user must change the password.

- **Minimum Password Length**

When enabled, this setting controls the minimum number of characters accepted for a user's logon password.

- **Force Alphanumeric Passwords**

When enabled, this setting forces a user's logon password to be a combination of numbers and letters.

- **Require Validated Logon to Windows NT or LAN Manager Domain**

When enabled, this setting requires the user to be validated by either a Windows NT or LAN Manager domain controller before the user will be allowed any access to the network. See the next section for more details.

- **Allow Caching of User-level Passwords**

When enabled, this setting allows password caching. *Password caching* allows a user to reconnect to password-protected shares after a validated logon without re-entering the required password each time. However, to maintain a secure Windows NT domain, Windows for Workgroups 3.11 will not cache passwords to servers with user-level security. When a connection is made to a user-level server, Windows for Workgroups 3.11 will first try the user's logon password. If that fails, a password dialog will appear, and the user must type in the appropriate password.

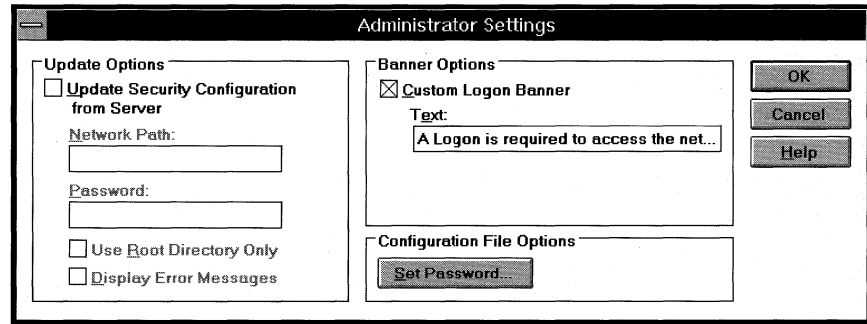
Banner Options

In addition to password settings, the administrator can change the logon banner that is displayed at the top of the Windows for Workgroups 3.11 logon dialog box.

To change the text displayed in the logon banner from the default, which is “Welcome to Windows for Workgroups,” to text defined by the administrator, choose the Admin... button in the Security Settings dialog box. To enable the custom banner, select the Custom Logon Banner check box, and type the appropriate text into the Text field as shown in Figure 5.3.

Figure 5.3

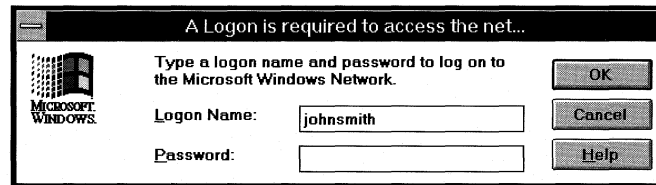
The Administrator Settings dialog with customized logon banner



When the custom logon banner is enabled, the text will appear in the title bar of the dialog box used to logon to Windows for Workgroups 3.11 as displayed in the following figure.

Figure 5.4

The customized Windows for Workgroups 3.11 logon dialog box



Support for Windows NT Security Features

While Windows for Workgroups 3.11 provides a secure environment for a workgroup, there may be additional security needs in your organization. In a networked environment where Windows NT Advanced Server or Microsoft LAN Manager security mechanisms are in use, Windows for Workgroups 3.11 can be configured to adhere to the logon validation specified by the domain controller. This allows tighter control of access to the network. This restricted access is user-specific rather than workstation-specific.

Including a computer that runs Windows NT Advanced Server in a Windows for Workgroups-based network enhances the security implemented in Windows for Workgroups 3.11 to include:

- **Validated logon**

The validated logon to Windows NT allows a network administrator tighter security controls to prevent unauthorized network access. If a user isn't validated by the Windows NT domain, the user is not granted permission to access the network and will not be able to connect to network resources (for example, files or printers).

- **User-level security**

Information stored on a Windows NT Advanced Server can be made available to network users on a per-user basis. User-level security can be used to specify which users have access to the shared information, and what access rights each user has.

Figure 5.5

The Windows NT New User dialog box provides access to user logon restrictions including time of day and logon location.

The screenshot shows the 'New User' dialog box in Windows NT. The title bar reads 'New User'. The dialog contains the following elements:

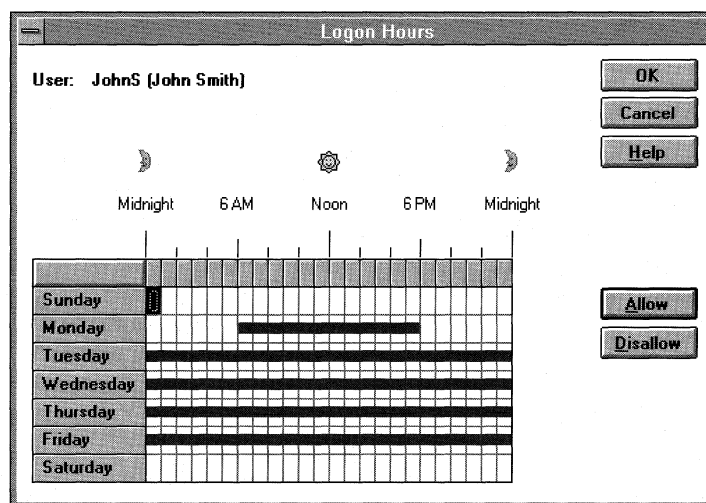
- Username:** JohnS
- Full Name:** John Smith
- Description:** (empty field)
- Password:** (empty field)
- Confirm Password:** (empty field)
- Buttons:** Add, Cancel, Help
- Checkboxes:**
 - User Must Change Password at Next Logon
 - User Cannot Change Password
 - Password Never Expires
 - Account Disabled
- Bottom Row Buttons:** Groups, Profile, Hours, Logon From, Account

- **Time-of-day logon restrictions**

The time-of-day logon restriction setting supported by Windows NT Advanced Server allows a network administrator to restrict users of Windows for Workgroups to log onto the network during certain days of the week and certain hours of the day.

Figure 5.6

The Windows NT Logon Hours dialog box. Access this dialog box by choosing the Hours button in the New User Dialog box.

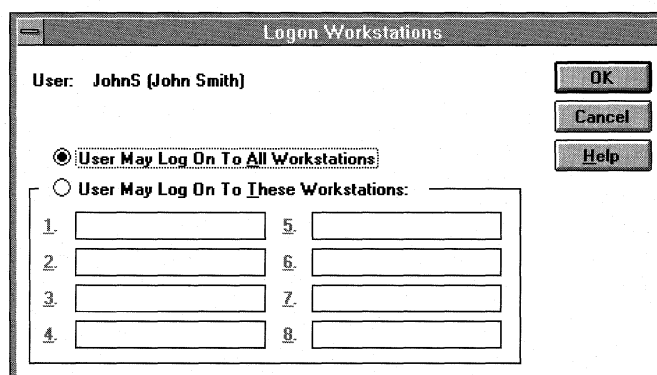


- **Physical logon location restrictions**

The physical logon location restriction setting allows a network administrator to prevent a user of a Windows for Workgroups from logging onto the network from specified computers.

Figure 5.7

The Windows NT Logon Workstations dialog box restricts the physical locations from which a user may log onto the system.



The support for the Windows NT security model accommodates the changing needs of businesses that want to start with a Windows for Workgroups network, and then enhance it as their computing needs grow and mature.

Implementing Windows for Workgroups 3.11 Security Controls

So far, this chapter has highlighted the security enhancements present in Windows for Workgroups 3.11. This section discusses how to implement the new security controls in a network environment.

Expanding the ADMINCFG.EXE Utility

The ADMINCFG utility is used to configure the security controls for a computer running Windows for Workgroups 3.11 or the Workgroup Add-on for MS-DOS as previously discussed in this chapter. Because the ADMINCFG utility is designed for use by system administrators or other users that want to take advantage of the additional security controls present in Windows for Workgroups 3.11, the ADMINCFG utility is not installed by the Windows for Workgroups 3.11 setup program. ADMINCFG is left in compressed form on the last disk of the Windows for Workgroups 3.11 disk set.

To use the ADMINCFG utility, it is necessary to expand the compressed file into the Windows directory, as explained in the following procedure:

To expand the ADMINCFG utility off the installation disks into the Windows directory

1. With Windows for Workgroups running, place the last disk of your Windows for Workgroups 3.11 disk set into either drive A or drive B.

(The following installation steps will assume the disk is in drive A, if you are using drive B, substitute that drive letter as appropriate.)

2. From Program Manager in Windows, choose Run from the File menu.
3. On the command line, type:

```
Expand a:admincfg.ex_ c:\windows\admincfg.exe
```

(Substitute the name of your Windows directory, as appropriate.)

Tip To make it convenient to access the ADMINCFG utility, you may want to create a Program Item in Program Manager for the ADMINCFG.EXE file.

Creating the Security Settings File (WFWSYS.CFG)

This section describes how to customize, install, and activate the security settings file (WFWSYS.CFG) on a computer running Windows for Workgroups or the Workgroup Add-on for MS-DOS.

A default WFWSYS.CFG file is created on a user's workstation when Windows for Workgroups 3.11 or the Workgroup Add-on for MS-DOS is installed. An administrator can update a user's WFWSYS.CFG file with additional security controls enabled.

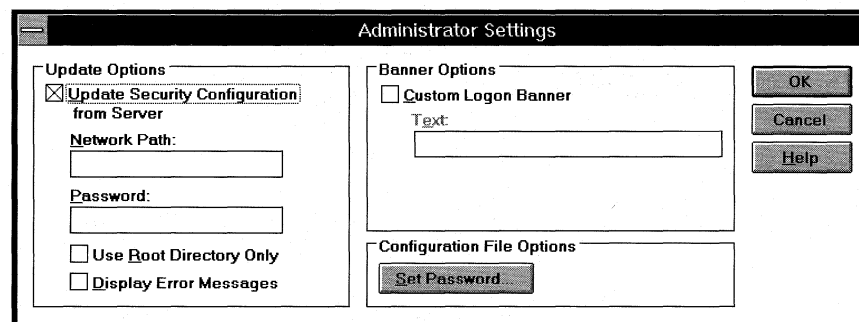
After installing the ADMINCFG utility on a workstation, the system administrator can run it to specify the security settings necessary to control network access to suit the organization. Using the ADMINCFG utility, the administrator can configure peer networking and disable file sharing, printer sharing, or Network DDE. Administrators can also configure password options and administrator settings with ADMINCFG.

Password-Protecting the Security Settings File

To prevent users from modifying the security settings file (WFWSYS.CFG) residing on the computer, the system administrator must assign an administrator password to the file. When a security settings file is first created, the administrator will be prompted to specify a password to protect the file. To assign a password to an existing security settings configuration file, select the Admin... button from the Security Settings dialog box, and then select the Set Password... button in the Administrator Settings dialog box.

Figure 5.8

The Administrator Settings dialog box provides the ability to assign a password to protect unauthorized modification of security settings.



When a password is assigned to a security settings file, a user will need to know the password to make changes to the security settings file. If a user does not know the password, that user will not be able to run the ADMINCFG file at all, therefore making it impossible to change the security settings that have been enabled on his or her workstation.

Installing the Security Settings File

Administrators can install the WFWSYS.CFG on their users' computers in two ways, network installation or individual installation.

- **Network Installation**

If Windows is installed over a network, the administrator can place a preset configuration file in the directory from which the users are installing. The Windows for Workgroups 3.11 setup program will copy this WFWSYS.CFG file to the local Windows directory at the time of installation.

- **Individual Installation**

If Windows is purchased preinstalled on computers or installed from disk, the administrator-defined security settings file can be copied into the users' Windows directory for each computer where the customized security controls are wanted.

In either of these cases, the first time Windows for Workgroups 3.11 is run the security settings configuration file is associated with that individual computer, preventing a user from being able to copy a security settings file from another computer in an attempt to override the settings enabled by the administrator.

Note Once a security settings configuration file (WFWSYS.CFG) has been associated with an individual computer, the settings file can NOT be copied to another workstation and used. Windows for Workgroups will detect this as a security violation and will require the administrator to either create a new configuration file or for the user to reinstall Windows for Workgroups.

Network Installation

A network installation of Windows for Workgroups is created on a network installation point by performing an Administrative Setup by typing **setup /a** as described in Chapter 2, "Windows for Workgroups 3.11 Setup and Installation." Once the expanded files are placed on the network install point, you can specify a default security settings file that should be used by copying the configured WFWSYS.CFG file to the network install point.

When a user installs Windows for Workgroups from the network install point either by performing a standard Setup or by setting up a shared copy of Windows for Workgroups by using the **/n** option when running Setup, the WFWSYS.CFG file will be copied from the network install point and placed in the users Windows directory.

Individual Installation

If you are not installing Windows for Workgroups from a network, you can run the ADMINCFG utility against a local workstation. To do this, you can place an expanded copy of the ADMINCFG.EXE file on a disk, and then run the administrator configuration utility from the disk. You will then be able to open the WFWSYS.CFG file residing on the hard disk of the local workstation, modify the security control settings, and then save the changed security settings file back to the local workstation.

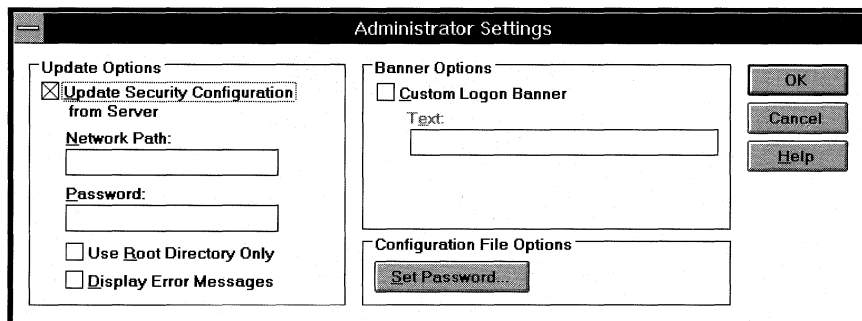
Updating Security Settings Remotely

In an environment where the security controls offered in Windows for Workgroups 3.11 are enabled and you expect to change the settings, you can configure the security controls file to remote update security settings from a specified server on the network. However, if you do not expect to change the security settings for a workstation once configured, you do not need to configure the security settings file to remotely update the settings.

The administrator can specify a network location (a UNC path name or drive letter and path) from which Windows for Workgroups or the Workgroup Add-on for MS-DOS should update its security settings at startup. This is useful for providing centralized administration and makes it easy for administrators to perform operations such as changing the administrator password for the WFWSYS.CFG file, changing administrator-defined password settings, or enabling/disabling file or printer sharing after Windows for Workgroups is installed. The administrator may maintain the file on a read-only, password-protected share to help ensure that the configuration file is secure. The administrator can then make changes to the security configuration and computers that update from that file will inherit the new settings the next time Windows for Workgroups is restarted.

Figure 5.9

The Administrator Settings dialog box allows an administrator to define a network location from which security settings are updated.



During an update, Windows for Workgroups will open the remote configuration file and copy the values of its settings to the local configuration file. If an update is specified, it will occur every time Windows for Workgroups is started. By default, Windows for Workgroups will not display error messages if it fails to update the local security settings file from the network location. Reasons for failed updates include the unavailability of the server where the global security settings files are stored. For troubleshooting, administrators can select the Display Error Messages check box to display error messages on the local workstation if the update fails. In the case of failed updates, the most recent security settings that are in effect will be used.

To specify that the security settings file should update its values from a defined network location, select the Update Security Configuration from Server check box as shown in Figure 5.9, above. The Update Options include:

- **Network Path**

The network path can take the form of a Universal Naming Convention (UNC) path name, or can explicitly reference a network drive and path. For practical purposes, the UNC name is more desirable as it doesn't require a drive letter to be mapped to a network drive before it can be accessed. The UNC name uses the following syntax:

```
\\server_name\share_name
```

where *server_name* identifies the name of the server where the security settings file reside, and *share_name* identifies the name of the shared directory on the given server.

- **Password**

If a password is assigned to the shared directory where the security settings files reside, the password should be specified here.

- **Use Root Directory Only**

When Windows for Workgroups attempts to update the security settings from a configuration file residing on a server, it will first look to see if a subdirectory exists matching the local computer name, and if that subdirectory contains a valid configuration file. If the subdirectory contains a valid configuration file, the configuration file assigned to the local computer will be used. If this option is enabled, Windows for Workgroups will not check for a subdirectory matching the local computer name.

Note If the subdirectory feature for remotely updating security settings is to be used, the computer names must be no more than eight characters in length.

Scenario Examples for Remote Update of Security Settings

This section will illustrate the configuration scenarios available in Windows for Workgroups 3.11 to provide flexibility when administering security settings and configuring the peer networking functionality of Windows for Workgroups.

The following scenarios are outlined in this section:

- Disabling file sharing for all users
- Handling exceptions for security settings
- Configuring security settings by department

Disabling File Sharing for all Users

In some cases, administrators may find that it is necessary to disable file sharing for all Windows for Workgroups 3.11 users on the network. This is easily done by using the ADMINCFG utility.

To disable file sharing for all users

Note This procedure assumes the network server's name is ADMIN and the shared directory's name is CONFIG.

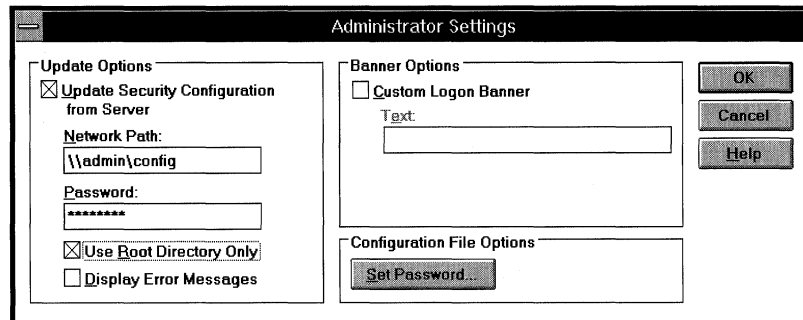
1. Create a directory on the network server to store the WFWSYS.CFG security settings file, named CONFIG. Share the directory with the access rights set to Read Only. Optionally, assign a password.
2. Run the ADMINCFG utility to create a WFWSYS.CFG security settings file in the shared CONFIG directory.
3. Set the security settings as appropriate. In this scenario, select the Disable File Sharing check box to disable file sharing.
4. Select the Update Security Configuration from Server check box and type **\\admin\\config** as the Network Path. Also type the appropriate password, if the share is password protected.

Alternately, select the Use Root Directory Only check box if you do not want to support exceptions to the security settings controls. (Exceptions are discussed in the following section.)

The Administrator Settings dialog box should now look similar to this:

Figure 5.10

Administrator Settings dialog box



5. Choose the Set Password... button to assign a password to the security settings file. This will prevent users from being able to change their security settings.
6. Choose the OK button on the Administrator Settings dialog box.
7. Choose the Save button in the Security Settings dialog box to save the changes made to the WFWSYS.CFG.

To put the custom configured security settings into effect on all workstations

Do one of the following:

- Place the WFWSYS.CFG file on the network installation point which will then be automatically copied to each user's workstation when Windows for Workgroups 3.11 is installed from the network installation point.

-Or-

- Copy the WFWSYS.CFG file to each workstation.

Handling Exceptions for Security Settings

In many cases the administrator may find it necessary to disable peer networking services on many workstations, but still allow file and/or printer sharing capabilities for specific users.

Allowing exceptions to the default WFWSYS.CFG

Note As done previously, this procedure assumes that the default WFWSYS.CFG file is placed in the root directory of the network server, referred to as \\ADMIN\\CONFIG.

This example assumes that file sharing is to be enabled on the computers named COMPUTR1, COMPUTR2, COMPUTR3, and disabled on all other computers.

1. Create a subdirectory on the \\ADMIN\\CONFIG share to match the name of each workstation on which you want to enable file sharing. The name of each subdirectory must match the Computer Name of each workstation as defined in the Network icon in Control Panel for each of the computers.

Create subdirectories of the root directory called COMPUTR1, COMPUTR2, and COMPUTR3.

2. Copy the default WFWSYS.CFG file from the root directory to the COMPUTR1 directory.
3. Run the ADMINCFG utility and open the WFWSYS.CFG file in the COMPUTR1 directory. Provide the appropriate password to open the WFWSYS.CFG file.
4. Deselect the Disable File Sharing check box to enable file sharing.
5. Select the Admin... button and deselect the Use Root Directory Only check box so that Windows for Workgroups will use the WFWSYS.CFG in the COMPUTR1 subdirectory, rather than the default security settings file from in the root directory.
6. Save the security settings file.
7. Copy the WFWSYS.CFG file from the COMPUTR1 directory and place a copy in the COMPUTR2 and COMPUTR3 directories.
8. Copy the WFWSYS.CFG file from the COMPUTR1 directory to the Windows directory located on COMPUTR1, COMPUTR2, and COMPUTR3.

Configuring Security Settings for a Group of Workstations

Another possible configuration scenario is when the system administrator wants to administer security settings to a collection of computers rather than handling individual exceptions. In this case, it is necessary to create different share points on a the network server to address each collection of computers. If wanted, the administrator can then choose to use the remote subdirectory update feature to handle exception cases on an individual basis.

Let's assume there are three different collections of computers called USER, MANAGER, and SERVER. For the USER group, you want to disable file and printer sharing. For the MANAGER group, you want to enable file sharing and printer sharing, but you want to assign administer-defined password settings. For the SERVER group, you want to enable file sharing and printer sharing, but you want to disable Network DDE Sharing.

In this scenario, you could set up a common Network Path for all collections of computers, say \\ADMIN\\CONFIG, and then create subdirectories for each individual computer with the appropriately customized WFWSYS.CFG file, but this would be tedious and time-consuming. Instead, the best way to address this configuration scenario is to create a different share point for each collection of computers on a given server; in this case USER, MANAGER, and SERVER on the network server called, ADMIN.

To configure security settings for a group of workstations

1. Create a directory on the ADMIN server for each collection of users and share the directories, with passwords as appropriate. In this scenario, create a directory called USER, MANAGER, and SERVER, and share each of these directories.
2. Create a WFWSYS.CFG file with file sharing and printer sharing disabled and place it in the USER directory. Update the Network Path field to point to \\ADMIN\\USER. Assign a password to the security settings file.
3. Create a WFWSYS.CFG file with the administrator-defined password settings configured in the MANAGER directory. Update the Network Path field to point to \\ADMIN\\MANAGER. Assign a password to the security settings file.

4. Create a WFWSYS.CFG file with Network DDE Sharing disabled in the SERVER directory. Update the Network Path field to point to \\ADMIN\SERVER. Assign a password to the security settings file.

If a given computer is already configured with Windows for Workgroups, place the appropriate WFWSYS.CFG file in the Windows directory on that computer

For computers where Windows for Workgroups is not installed, you may either create three separate network installation points configured with the appropriate WFWSYS.CFG file in the network install directory, or after Windows for Workgroups is installed, copy the appropriate WFWSYS.CFG file to a given computer.

For each collection of computers, you can then handle individual exceptions as described in the previous procedure.

Auditing of Network Events

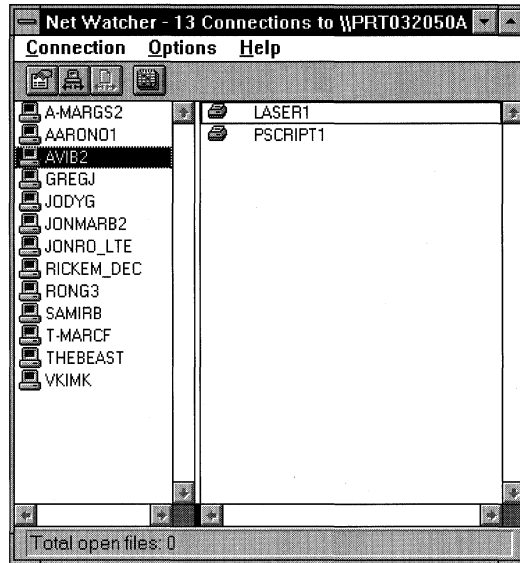
In addition to improved security enhancements for peer networking within MIS organizations and improved mechanisms for restricted network access, Windows for Workgroups 3.11 includes networking auditing functionality. This functionality allows a user to identify the users who are connected to the local computer at any time. The Windows for Workgroups 3.11 auditing mechanism also maintains a log of network events to facilitate tracking of access to shared resources.

Net Watcher

With the Windows for Workgroups 3.11 Net Watcher tool, users can identify who is connected to shared directories and who has which files opened. For more information on Net Watcher, see Chapter 10, "New and Updated Accessories," in the *Windows for Workgroups Resource Kit for version 3.1*.

Figure 5.11

This Net Watcher dialog box shows fifteen users connected to a Windows for Workgroups computer.



Event Log

Another way to monitor access of resources on a computer sharing files and printers is to audit specific network events that occur on the computer. With Windows for Workgroups 3.11, a user can enable system monitoring of networking events and a log file will be created. This is useful both as a security mechanism to help trace unauthorized access, and as a diagnostic aid to observe when different network events happen on a given computer. You can enable the Event Log can be from the Network section of Control Panel by selecting the Event Log icon.

The Event Log is stored in a file called AUDIT.LOG, which you can open and view from the Net Watcher tool by choosing View Event Log from the Connection menu.

Figure 5.12

The Event Log records the occurrence of selected network events.

Date/Time	Computer	User	Share	Type	Access	Document	Event
7/29 1:03:39 PM		AVIB	PSCRIPT1	Printer	Full	Mail Messa	Print job completed
7/29 1:07:52 PM	T-JOHNMA	T-JOHNMA	PSCRIPT1	Printer	Full		User disconnected
7/29 1:07:52 PM	T-JOHNMA	T-JOHNMA	LASER1	Printer	Full		User disconnected
7/29 1:13:38 PM	LENS33C	LENS	LASER1	Printer	Full		User disconnected
7/29 1:14:32 PM	AVIB-LAPTOF	AVIB	PSCRIPT1	Printer	Full		User disconnected
7/29 1:14:53 PM	JING	JING CHEN	LASER1	Printer	Full		User disconnected
7/29 1:15:03 PM	GASTON	TOMA	LASER1	Printer	Full		User disconnected
7/29 1:15:03 PM	GASTON	TOMA	LASER1	Printer	Full	C:\TEMP\	Print job spooled
7/29 1:15:07 PM		TOMA	LASER1	Printer	Full	C:\TEMP\	Print job completed
7/29 1:15:12 PM		JIMH2	JIMH	LASER1	Printer	Full	User disconnected
7/29 1:15:24 PM	JONMARB2	JONMARB	LASER1	Printer	Full		User disconnected
7/29 1:15:26 PM	SAMMCK	SAMMCK	LASER1	Printer	Full		User disconnected
7/29 1:15:26 PM	THEBEAST	TOMA	LASER1	Printer	Full		User disconnected
7/29 1:15:26 PM	THEBEAST	TOMA	LASER1	Printer	Full		User connected

The Event Log can record the following events related to Windows for Workgroups 3.11-based servers:

- **Server Startup**

The Event Log creates an entry each time the server starts.

- **Server Shutdown**

The Event Log creates an entry each time the server shuts down.

- **Connect to Server**

Each time a user connects to the server, the Event Log creates an entry recording the computer name, user name, the share that was accessed, the type of access made by the user, and the time of the connection.

- **Disconnect from Server**

Each time a user disconnects from the server, the Event Log creates an entry recording the computer name, user name, the shared resource that was accessed, the type of access, and the time of the disconnection.

- **Unsuccessful Connect Attempt**

Each time a user tries to connect to the server and fails, the Event Log creates an entry recording the computer name, user name, and time of the connection attempt.

- **Spool Print Job**

Each time a print job is spooled to the server, the Event Log creates an entry recording the computer name, user name, the time the print job was spooled, and the name of the document.

- **Pause Print Job**

If a user pauses a print job as it is spooling to the server, the Event Log creates an entry recording the time the print job was paused and all of the user's information.

- **Resume Print Job**

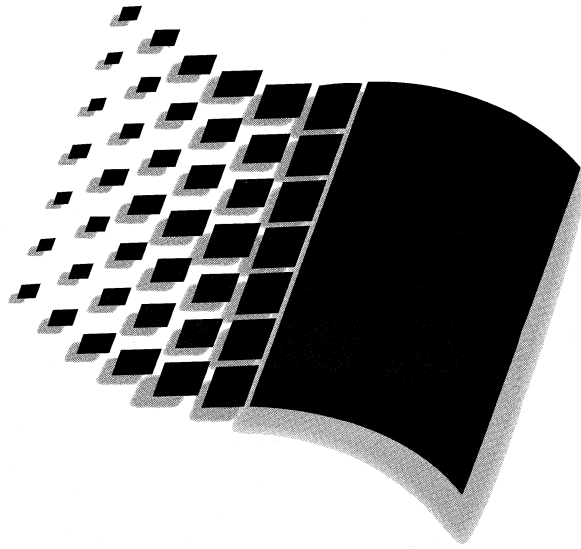
If a user resumes a paused print job in the server's queue, the Event Log creates an entry recording the time the print resumed and all of the user's information.

- **Delete Print Job**

If a user deletes a print job as it is spooling to the server, the Event Log creates an entry recording the time the print job was deleted as well as all of the user's information.

- **Complete Print Job**

When a print job is done printing and is no longer in the queue, the Event Log creates an entry recording the time the print job finished and all of the user's information.



Network Integration

Chapter 6 Windows for Workgroups 3.11 Network Protocols **6-1**

Windows for Workgroups 3.11 Protocol Support.....	6-2
NetBEUI.....	6-2
NWLink: 32-bit IPX/SPX-Compatible Transport.....	6-3
Microsoft TCP/IP for Windows for Workgroups.....	6-7
Microsoft Data Link Control Protocol for Windows for Workgroups.....	6-26

Chapter 7 Integrating with Windows NT and Windows NT Advanced Server **7-1**

Overview of Support for Integrating Workgroups 3.11 with Windows NT	7-2
Enhanced Security Features in a Windows NT Environment	7-4
Remote Access Services Client	7-6

Chapter 8 Integrating with Novell NetWare **8-1**

Overview of Enhancements to Novell NetWare Support.....	8-3
Installing Support for Novell NetWare	8-4
Workstation Configuration Files	8-21
32-Bit IPX/SPX-Compatible Transport with NetBIOS.....	8-25
NetBIOS Services over IPX	8-28
Specific Novell NetWare Issues.....	8-29
Sample Files for Configuration Scenarios.....	8-31
NDIS 2.0 Protocols on ODI Drivers.....	8-39

Chapter 9 Integrating with Other Networks **9-1**

Summary of Network Support.....	9-2
Microsoft LAN Manager	9-4
Banyan VINES	9-4
DEC PATHWORKS	9-6
Windows 3.1-compatible Networks	9-7

Chapter
6

Windows for Workgroups 3.11 Network Protocols

This chapter contains information about the various protocols or transports with which Windows for Workgroups 3.11 is commonly integrated. This chapter discusses NetBEUI—the native protocol to Microsoft networks, NWLink—the IPX/SPX-compatible transport, Microsoft TCP/IP for Windows for Workgroups, and Microsoft Data Link Control (DLC).

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 7, “Integrating with Windows NT and Windows NT Advanced Server;” Chapter 8, “Integrating with Novell NetWare;” Chapter 9, “Integrating with Other Networks;” Chapter 13, “Troubleshooting Windows for Workgroups 3.11.”

Contents of This Chapter

Windows for Workgroups 3.11 Protocol Support.....	6-2
NetBEUI.....	6-2
NWLink: 32-bit IPX/SPX-Compatible Transport.....	6-3
NWNBLink: 32-bit NetBIOS Provider for IPX.....	6-4
Novell NetWare Connectivity.....	6-4
Installation of IPX/SPX Compatible Transport.....	6-5
Components of the Default NWLink Stack.....	6-5
Supported Frame Types.....	6-5
PROTOCOL.INI Parameters.....	6-6
Microsoft TCP/IP for Windows for Workgroups.....	6-7
How TCP Works.....	6-8
How IP Works.....	6-8
Overview of Windows Sockets.....	6-10
Installing Microsoft TCP/IP for Windows for Workgroups.....	6-11
Configuring TCP/IP.....	6-14
Troubleshooting TCP/IP Connections.....	6-18
PROTOCOL.INI Parameters.....	6-19
TCPUTILS.INI Parameters.....	6-23
Microsoft Data Link Control Protocol for Windows for Workgroups.....	6-26
Installing and Configuring Microsoft DLC.....	6-27
Configuring Microsoft DLC.....	6-30
Microsoft DLC Protocol Parameters.....	6-32
PROTOCOL.INI Parameters for Microsoft DLC.....	6-34

Windows for Workgroups 3.11 Protocol Support

Windows for Workgroups 3.11 supports a broad array of networking standards, providing connectivity suitable for small workgroups as well as enterprise-wide networks. Windows for Workgroups 3.11 has support for multiple-protocol networking, including NetBEUI, TCP/IP, IPX/SPX and the Microsoft DLC protocol. It works with network operating systems including Windows NT Advanced Server, Microsoft LAN Manager, Novell NetWare, Sun PC-NFS, Banyan VINES, DEC Pathworks and IBM LAN Server.

Windows for Workgroups 3.11 provides the ability to support peer services— including the ability to share files and printers and support for Network DDE— using popular network protocols. In addition to the offerings from Microsoft, several third party companies have released implementations of network transport protocols that can be used with Windows for Workgroups 3.11.

The following sections outline how to install configure and use the following protocols—NetBEUI, IPX, TCP/IP and Data Link Control (DLC).

NetBEUI

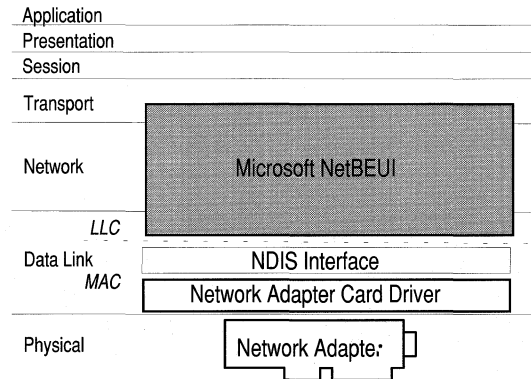
Windows for Workgroups ships with the NetBEUI (NetBIOS Extended User Interface) protocol to interconnect computers running Windows for Workgroups, MS-DOS, Windows NT, and Microsoft LAN Manager-compatible networks, in a local area network environment. NetBEUI is a small, efficient protocol designed for use on a departmental LAN of 20 to 200 workstations. For enterprise-wide networks where a routable protocol is required, TCP/IP or IPX should be used.

NetBEUI was first introduced by IBM in 1985. It has powerful flow control, tuning parameters, and robust error detection. It conforms to IBM's NetBEUI specifications and thus can communicate with IBM's NetBEUI protocol. It includes performance enhancements related to NetBIOS 3.0 and supports high data throughput rates. NetBEUI's small and efficient design is ideal for workgroup networking. NetBEUI is ideal for large I/O requests such as copying files from network servers or launching applications from network servers.

NetBEUI is implemented as both a real-mode protocol and a protected-mode protocol.

Figure 6.1

NetBEUI protocol shown in reference to the seven-layer OSI model



NWLink: 32-bit IPX/SPX-Compatible Transport

Windows for Workgroups 3.11 provides NWLink, a 32-bit routable network protocol (also called a transport) that is compatible with IPX. Microsoft introduced the NDIS 3.0 IPX/SPX protocol, NWLink, with Windows NT. This protected-mode protocol is best used with an NDIS 3.0 network adapter card driver. This combination uses the pure 32-bit stack without mappers or real-mode stub drivers, providing the best level of performance.

NWLink can be used instead of NetBEUI to establish connections between Windows for Workgroups 3.11 computers and, in conjunction with NWNBLink, Windows NT computers, to share and access resources.

NWLink does not, however, allow a Windows for Workgroups 3.11 computer to connect to a Novell NetWare server directly or to act as a server to a Novell NetWare client. NWLink is useful if you have NetWare client applications which use the IPX/SPX API or if you have applications which use NetBIOS or Novell NetBIOS. NWLink can also serve as the protocol used by the default redirector and server for Windows for Workgroups 3.11.

The 32-bit protected-mode implementation of NWLink in Windows for Workgroups 3.11 provides improved performance for IPX/SPX applications by sending IPX/SPX data directly from protected mode, rather than first passing the data through the real-mode IPX protocol. NWLink allows Windows for Workgroups 3.11-based workstations to communicate with client-server solutions that recognize IPX/SPX as the communication protocol, such as Microsoft SQL Server, Lotus Notes® and Btrieve®.

NWLink is the ideal protocol to use where Windows for Workgroups 3.11-based workstations need to communicate with other computers on an IPX backbone. Note that in order for a Windows for Workgroups 3.11-based workstation to access files and printers residing on a NetWare server, the NetWare redirector (either 3.x or 4.x) and real-mode IPX protocol are required.

NWNBLink: 32-bit NetBIOS Provider for IPX

NWNBLink is a NetBIOS version 3 provider that runs in conjunction with NWLink and uses the Novell NetBIOS frame format to provide full compatibility with Novell's NetBIOS version 1 implementation. It provides support using NetBIOS for interoperating with other Windows for Workgroups and Windows NT-based computers, and with computers running Novell's NetBIOS driver. Using NWNBLink provides application connectivity to NetBIOS-based environments such as Lotus Notes, without loading the Novell NETBIOS.EXE driver, and saves as much as 30K of conventional memory.

The combination of NWLink and NWNBLink allows Windows for Workgroups 3.11-based workstations to support file and printer peer networking over the IPX/SPX-compatible transport to Windows NT and Windows NT Advanced Server.

Novell NetWare Connectivity

Microsoft's IPX/SPX protocol, NWLink, is a routable protocol. It conforms to the IPX specification which dictates for it to provide routable datagram packets.

Microsoft implemented an NDIS 3.0 model of this protocol due to the routability of IPX and its implementation across the majority of network environments.

NWLink can use Novell NetWare servers configured as routers (and other IPX routers) to transfer its packets across LANs to access the resources of other Windows for Workgroups 3.11 computers.

Since NWLink is a protected-mode driver and does not load in real mode, Novell NetWare's shell, NETX.EXE, will not load unless a real-mode IPX protocol driver is also installed. Novell NetWare's shell, NETX.EXE is required to access Novell NetWare's file server resources. Without the implementation of 32-bit NCPs and a protected-mode shell or a mapper to real-mode NETX, access to Novell NetWare servers is not possible with only NWLink.

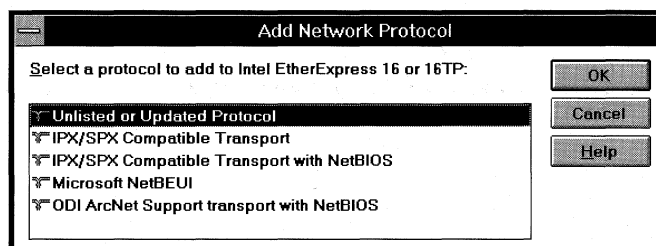
For more information on integrating Windows for Workgroups 3.11 with Novell NetWare, see Chapter 8, "Integrating with Novell NetWare."

Installation of IPX/SPX Compatible Transport

The user interface refers to NWLink as “IPX/SPX Compatible Transport.” IPX/SPX Compatible Transport with NetBIOS adds both the NWLink.386 and the NWNBLINK.386 drivers, along with related SYSTEM.INI entries.

Figure 6.2

Add Network Protocol dialog box showing 32-bit IPX/SPX compatible transport entries

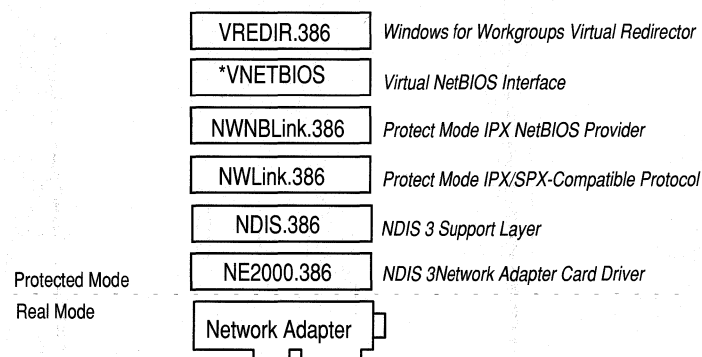


Components of the Default NWLink Stack

The following diagram illustrates the 32-bit protected mode architecture for the NDIS 3.0 IPX/SPX compatible transport with NetBIOS protocol. There are no real-mode components in this configuration. The NWLINK.386 virtual device driver is the 32-bit IPX/SPX compatible transport, and the NWNBLINK.386 virtual device driver is the 32-bit NetBIOS support driver for IPX. Note that Novell NetWare server resources cannot be accessed unless real-mode IPX and the NetWare redirector is installed too.

Figure 6.3

Default components used by Windows for Workgroups when the IPX/SPX Compatible transport with NetBIOS is installed



Supported Frame Types

The IPX/SPX compatible transport, NWLink, can be run on Ethernet, Token Ring, FDDI, and ArcNet topologies. Each topology requires a different frame format. Ethernet supports Ethernet_II, “raw 802.3,” 802.2, or SNAP frame formats. Token Ring and FDDI supports 802.2 and SNAP. ArcNet supports “raw ArcNet” framing only.

It is important to make sure that the NWLink on the Windows for Workgroups computers is using the same framing used by the client computer. On Ethernet networks, standard frame format specified by Novell for NetWare 2.2 and NetWare 3.1 is 802.3. Starting with NetWare 4.0, the default frame format used is 802.2.

PROTOCOL.INI Parameters

Configuration parameters for the NWLINK (32-bit IPX/SPX compatible transport) protocol are listed in the [NWLink] section of PROTOCOL.INI. A summary of these parameters and their meaning is provided in this section. For entries not present in your [NWLink] section, default values are used as indicated for the entry.

EVEN_PACKETS= Yes | No

Some older NetWare Ethernet drivers discard any odd length frames they receive and evenize frames on transmit. To maintain compatibility with these drivers, an Ethernet driver has to evenize frames on transmits (for both raw 802.3 and Ethernet II). To maintain compatibility with these older drivers (and any other drivers that are transmitting compatible packets), an Ethernet driver should also be able to receive both even length and odd length Ethernet frames. This switch specifies whether NWLink will only transmit even length IPX frames, or will support both even length and odd length frames. Even length IPX packets are used by the MSIPX.COM protocol used by Windows for Workgroups 3.1. The default is **No**—NWLink supports both odd and even length frames.

FRAME= *string*

Specifies the frame type to be used for the NWLink protocol. The valid options are **ETHERNET_802.2**, **ETHERNET_802.3**, **ETHERNET_II**, and **TOKEN-RING**. Select the appropriate frame type used on your network to allow the NWLink protocol to be able to communicate with other workstations on your network. The default frame type used depends on the media type used. For Ethernet, the default is **ETHERNET_802.3**, which is the same frame format as used by NetWare 3.x. See the previous “Supported Frame Types” section for information on frame types supported by Novell NetWare.

MAX_CONNECTIONS= *integer*

Specifies the maximum number of simultaneous SPX connections that are supported by the NWLink protocol. The range is **1** to **128**. The default is **16**.

MAX_SOCKETS= *integer*

Specifies the maximum number of simultaneous IPX sockets that are supported by the NWLink protocol. The range is **1** to **128**. The default is **20**.

SOURCE_ROUTING= *integer*

Specifies the number of entries supported in the source routing cache size for token-ring source routing. If the **SOURCE_ROUTING=** entry is present in your PROTOCOL.INI file, token-ring source routing is enabled thus allowing NWLink to communicate over source routing bridges. This entry is the same as if the Novell NetWare ROUTE.COM TSR is used. The range is **16** to **128** entries. The default is **16** entries.

Microsoft TCP/IP for Windows for Workgroups

Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems. TCP/IP can be used with Windows for Workgroups or to connect to Microsoft LAN Manager or non-Microsoft (for example, UNIX®) hosts.

TCP (transmission control protocol) and IP (internet protocol) are only two protocols in the family of Internet protocols. Over time, however, “TCP/IP” has been used in industry to denote the family of common Internet protocols.

The Internet protocols are a result of a Defense Advanced Research Projects Agency (DARPA) research project on network interconnection in the late 1970s. It was mandated on all United States defense long-haul networks in 1983 but was not widely accepted until the integration with 4.2 BSD (Berkeley Software Distribution) UNIX. The popularity of TCP/IP is based on:

- Robust client-server framework. TCP/IP is an excellent client-server application platform, especially in wide-area network (WAN) environments.
- Information sharing. Thousands of academic, defense, scientific, and commercial organizations share data, electronic mail, and services on the connected Internet using TCP/IP.
- General availability. Implementations of TCP/IP are available on nearly every popular computer operating system. Source code is widely available for many implementations. Additionally, bridge, router, and network analyzer vendors all offer support for the TCP/IP protocol family within their products.

TCP/IP is viewed as the most complete and accepted networking protocol available. Virtually all modern operating systems offer TCP/IP support, and most large networks rely on TCP/IP for all their network traffic.

Microsoft TCP/IP provides cross-platform connectivity and a client-server development framework that many software vendors and corporate developers are using to develop distributed and client-server applications in heterogeneous enterprise networks over TCP/IP.

TCP/IP for Windows for Workgroups also offers the Windows Sockets interface, which is ideal for developing client-server applications. A Windows Sockets application developed to be used with Microsoft TCP/IP will be able to run other vendors' Windows Sockets-compliant stacks as well.

How TCP Works

TCP is a reliable, *connection-oriented* protocol. Connection-oriented implies that TCP first establishes a connection between the two systems that intend to exchange data. Since most networks are built on shared media (for example, several systems sharing the same cabling), it is necessary to break chunks of data into manageable pieces so that no two communicating systems monopolize the network. These pieces are called *packets*. When an application sends a message to TCP for transmission, TCP breaks the message into packets, sized appropriately for the network, and sends them over the network.

Sequence Numbers, Checksum, and Port ID

Because a single message is often broken into many packets, TCP marks these packets with sequence numbers before sending them. The sequence numbers allow the receiving system to properly reassemble the packets into the original message. Being able to reassemble the original message is not enough—the accuracy of the data must also be verified. TCP does this by computing a *checksum*. A checksum is a simple mathematical computation applied, by the sender, to the data contained in the TCP packet. The recipient then does the same calculation on the received data and compares the result with the checksum that the sender computed. If the results match, the recipient sends an acknowledgment (ACK). If the results do *not* match, the recipient asks the sender to resend the packet. Finally, TCP uses port IDs to specify which application running on the system is sending or receiving the data.

TCP Headers

The port ID, checksum, and sequence number are inserted into the TCP packet in a special section called the *header*. The header is at the beginning of the packet containing this and other “control” information for TCP.

How IP Works

IP is the messenger protocol of TCP/IP. The IP protocol, much simpler than TCP, basically addresses and sends packets. IP relies on three pieces of

information, which you provide, to receive and deliver packets successfully: IP address, subnet mask, and default gateway.

IP Addresses

The *IP address* identifies your system on the TCP/IP network. IP addresses are 32-bit addresses that are globally unique on a network. They are generally represented in dotted decimal notation, which separates the four bytes of the address with periods. An IP address looks like this:

102.54.94.97

Although an IP address is a single value, it really contains two pieces of information:

- Your system's network ID
- Your system's host (or system) ID

Subnet Mask

The *subnet mask*, also represented in dotted decimal notation, is used to extract these two values from your IP address. The value of the subnet mask is determined by setting the network ID bits of the IP address to 1's and the host ID bits to 0's. The result allows TCP/IP to determine the host and network IDs of the local workstation. For example:

Understanding an IP Address

When the <i>IP address</i> is	102.54.94.97	(specified by the user)
And the <i>subnet mask</i> is	255.255.0.0	(specified by the user)
The <i>network ID</i> is	102.54	(IP address and subnet mask)
And the <i>host ID</i> is	94.97	(IP address and subnet mask)

Network and Host IDs

The network ID identifies a group of systems that are all located on the same physical network. In internetworks (networks formed by a collection of networks), there are as many unique network IDs as there are networks. TCP/IP networks are connected by routers (or gateways), which have knowledge of the networks that are connected in the Internet. The host ID identifies your system within a particular network ID.

Default Gateway

The default gateway is needed only for systems that are part of an Internet. When IP gets ready to send a packet on the wire, it inserts the local (source) IP address and destination address of the packet in the IP header, and verifies that

the network ID of the destination matches the source. If they match, the packet is sent directly to the destination system on the local network. If the network IDs do *not* match, the packet is forwarded to the default gateway for delivery. Since the default gateway has knowledge of the network IDs of the other networks in the Internet, it forwards the packet to other gateways until the packet is eventually delivered to a gateway connected to the specified destination. This process is known as *routing*.

Overview of Windows Sockets

Microsoft TCP/IP for Windows for Workgroups includes support for Windows Sockets. A *socket* provides an end point to a connection; two sockets form a complete path. A socket works as a bi-directional pipe for incoming and outgoing data. The Windows Sockets API is a networking API tailored for use by programmers using the Microsoft Windows operating system. Windows Sockets is a public specification based on Berkeley UNIX sockets and aims to:

- Provide a familiar networking API to programmers using Windows or UNIX.
- Offer binary compatibility between heterogeneous Windows-based TCP/IP stack and utilities vendors.
- Support both connection-oriented and connectionless protocols.

If you are running an application that uses Windows Sockets, be sure to enable Windows Sockets when you configure Microsoft TCP/IP.

To get a copy of the Windows Sockets specification via anonymous FTP

1. Type:

```
ftp microdyne.com
```
2. Log in as *anonymous*.
3. Type your electronic mail address for the *password*.
4. Type:

```
cd /pub/winsoc/winsoc-1.1
```
5. Choose the file with the format you want, ASCII (.TXT), PostScript® (.PS), or Microsoft Word for Windows (.DOC), and then type:

```
get winsoc.ext
```

(Where “*ext*” represents the appropriate extension.)

Alternate method for getting a copy of the Windows Sockets specification via anonymous FTP

1. Type:
`ftp vax.ftp.com`
2. Log in as *anonymous*.
3. Type your email address for the *password*.
4. Type:
`cd /pub/winsocapi/winsoc-1.1`
5. Choose the file with the format you want, ASCII (.TXT), PostScript (.PS), or Microsoft Word for Windows (.DOC), and then type:
`get winsoc.ext`
(Where "ext" represents the appropriate extension.)

To get a copy of the Windows Sockets specification from CompuServe®

1. Type:
`go msl`
2. Browse using the keywords "windows sockets."
3. Choose the file with the format you want, ASCII (.TXT), PostScript (.PS), or Microsoft Word for Windows (.DOC), and then type:
`get winsoc.ext`
(Where "ext" represents the appropriate extension.)

There is also an electronic mailing list designed for discussion of Windows Sockets programming. To subscribe to this mailing list, send email to winsocapi-request@microdyne.com.

Installing Microsoft TCP/IP for Windows for Workgroups

For Support Support for Microsoft TCP/IP for Windows for Workgroups is not available from the standard Windows for Workgroups Product Support Services phone line. If you have questions, please contact your Microsoft Solutions Channel member. Support for this product is also available through Microsoft's fee-based support plans. For information on locating a Solutions Channel member near you or about Microsoft's support options, call Microsoft Inside Sales at (800) 227-4679.

Before Installing Microsoft TCP/IP

Before you install Microsoft TCP/IP on you Windows for Workgroups 3.11 workstation, you need to know the following information:

- Default gateway
- IP address
- Subnet mask
- Whether to enable Windows Sockets
- Whether to enable Domain Name Service (DNS) lookups

Information about installing Microsoft TCP/IP for Windows for Workgroups on top of ODI network adapter card drivers in a Novell NetWare environment is provided in Chapter 8, "Integrating with Novell NetWare."

Installing Microsoft TCP/IP

Before installing the Microsoft TCP/IP protocol, make sure the Network Setup application is not running.

Important You *must* run the Microsoft TCP/IP setup program as described in the following procedure. Do not attempt to simply add TCP/IP as another protocol using Network Setup.

To install Microsoft TCP/IP on a workstation with Windows for Workgroups

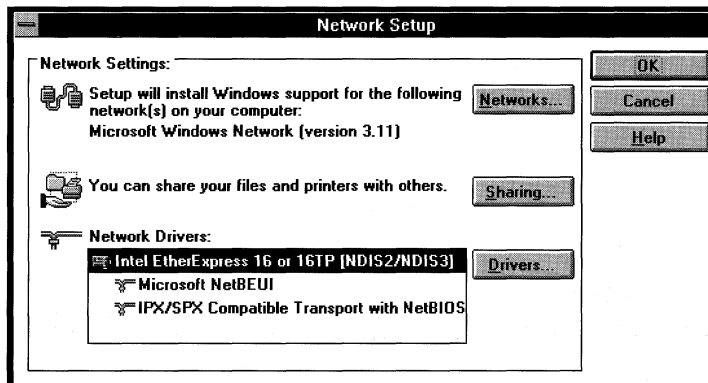
1. Insert the Microsoft TCP/IP for Windows for Workgroups disk in drive A.
2. From File Manager or Program Manager, select the Run command from the File menu.
3. In the command-line box, type:

a:setup.exe

Some of the distribution files are copied to the workstation's hard drive and the Network Setup dialog box appears:

Figure 6.4

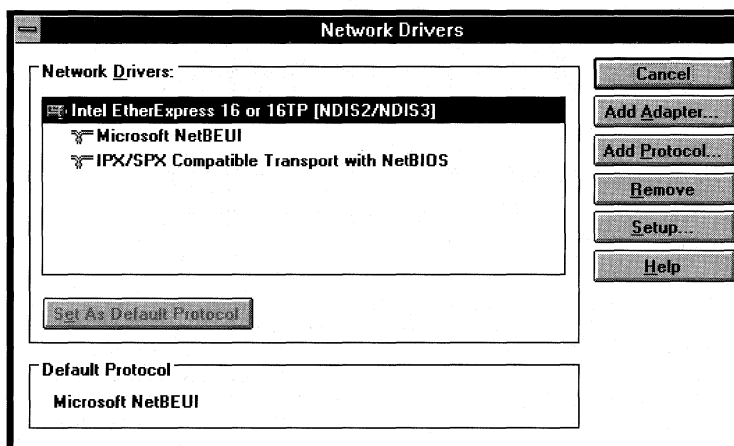
Network Setup dialog box used to install network drivers



4. Choose the Drivers... button. The Network Drivers dialog box appears:

Figure 6.5

Network Drivers dialog box used to add additional protocols

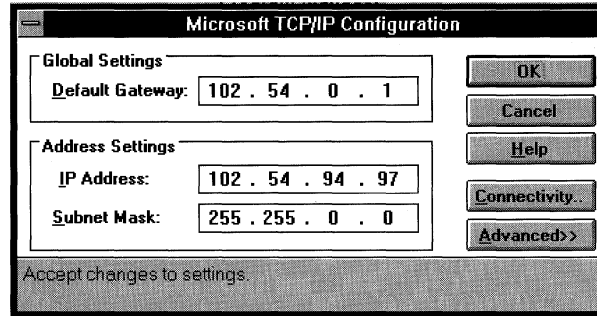


5. In the Network Drivers list box, select the adapter on which you want to run Microsoft TCP/IP. (You can choose only one adapter.)
6. Choose the Add Protocol... button. The Add Network Protocol dialog box appears. Note: You must have your network card set up as NDIS 2/NDIS 3 or you will receive an error message telling you to do so.
7. Select the Unlisted or Updated Protocol option from the list of available protocols and then choose OK. The Install Driver dialog box appears.
8. In the Install Driver dialog box, enter the location of the Microsoft TCP/IP for Windows for Workgroups disk (usually A:), and choose OK.
The Unlisted or Updated Protocol dialog box appears.
9. Select Microsoft TCP/IP.
10. Choose OK.

The Microsoft TCP/IP for Windows for Workgroups software is now on the workstation's hard drive, and the Microsoft TCP/IP Configuration dialog box appears.

Figure 6.6

Microsoft TCP/IP
Configuration dialog box



Continue with the configuration procedure, as described in the next section, “Configuring TCP/IP.”

Configuring TCP/IP

To configure Microsoft TCP/IP on a workstation

1. In the Microsoft TCP/IP Configuration dialog box, type in values for Default Gateway, IP Address, and Subnet Mask, as described in the following table.

Field	Description
Default Gateway	Specifies the IP address of the default gateway used to forward packets to other networks or subnets. This parameter is required only for nodes on internetworks. If this parameter is not provided, IP functionality will be limited to the local subnet. Your network administrator should provide you with the correct value for this parameter.
IP Address	Specifies the IP address associated with your local workstation. Your network administrator should provide you with the correct value for this parameter. Note that IP addresses on the network must be unique. Duplicate IP addresses might cause some systems on the network to “hang” or function unpredictably.
Subnet Mask	Specifies the subnet mask associated with the adapter to which TCP/IP is bound. Each interface used by TCP/IP must have a subnet mask configured. This allows the workstation to separate the IP address into host and network IDs. Your network administrator should provide you with the correct value for this parameter.

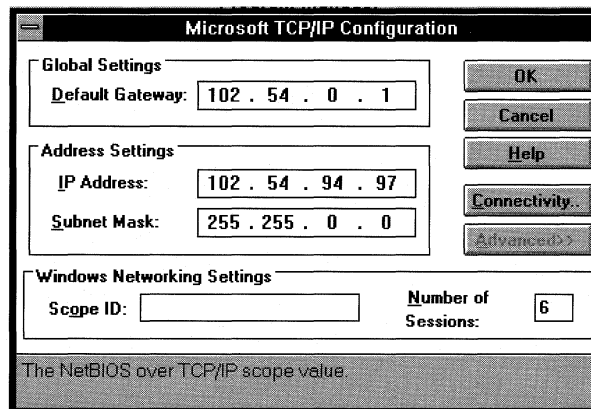
- Tip** When entering IP addresses, you can use the space bar, the period key, the right arrow key, or the mouse to advance to the next field in the address. As in other dialog boxes, use the TAB key to advance to the next field in the dialog box. Notice also, that when your cursor is located in a field box, a “hint” for that field appears at the bottom of the dialog box.

The TCP/IP for Windows for Workgroups configuration program will check the validity of the IP address, default gateway, and subnet mask automatically.

- To set advanced NetBIOS over TCP/IP (NBT) parameters, choose the Advanced>> button. The dialog expands, as shown in Figure 6.7:

Figure 6.7

Microsoft TCP/IP
Advanced Configuration
dialog box



- Type values for the Scope ID and Number of Sessions, as described below.

Field	Description
Scope ID	Specifies the NetBIOS scope parameter for the NBT module. To be able to communicate, all computers on a NetBIOS network must have the same scope ID. Your network administrator can provide you with the correct value for this parameter, but you can generally leave this value blank.
Number of Sessions	Specifies the number of simultaneous NBT sessions that your workstation can have. If a lot of people will connect to your workstation at one time, increase this value.

If Windows Sockets is enabled, the sum of the Number of Socket Sessions and the Number of Sessions values must be less than or equal to 22. The default Number of Sessions is 6.

- Choose the Connectivity button to set options for the Microsoft TCP/IP utilities and other TCP/IP-based applications, such as Windows Sockets-based applications. A dialog box similar to that in Figure 6.8 appears.

Figure 6.8

Microsoft
TCP/IP - Connectivity
Configuration dialog box

Setting these parameters allows you to specify remote TCP/IP nodes by their host name rather than by their IP address. The local HOSTS file also facilitates this.

The following table describes the fields in this dialog box.

Field	Description
Use DNS for Hostname Resolution	Determines whether or not to enable DNS (domain name service) host name resolution. When selected, the DNR (domain name resolver) software is loaded at startup and is used to resolve host names, in conjunction with the local HOSTS file.
Primary DNS Server	Specifies the IP address for the primary DNS server that will be used to resolve host names. If DNS is not to be used when resolving domain names (when the Use DNS for Hostname Resolution box is cleared), this list has no effect and is disabled.
Secondary DNS Server	Specifies the IP address of the secondary DNS server used for host name resolution. If DNS is not to be used when resolving domain names (when the Use DNS for Host name Resolution box is cleared), this list has no effect and is disabled.
Enable Windows Sockets	Specifies whether or not the Windows Sockets interface will load at startup. Select this option only if you are running applications that use the Microsoft MS-DOS® sockets interface or Windows Sockets.
Number of Socket Sessions	Specifies the number of sockets sessions that will be allocated at startup. If Window Sockets is not selected, this entry is disabled. If Window Sockets is selected, this parameter is required. The sum of the Number of Socket Sessions and the Number of Sessions parameters must be less than or equal to 22. The value of the Number of Sockets Sessions parameter can be 1 through 21. The default value is 4.
Host name	Specifies the host name for this computer. The host name is used to identify the local workstation by name for authentication by utilities. Other TCP/IP-based utilities and applications can use this value to learn the name of the local workstation. This value defaults to the Windows for Workgroups computer name and it can be altered without affecting the computer name's value. The Host name parameter is optional.

Field	Description
Domain	Identifies your group in the DNS hierarchical naming convention, with descending levels of detail. The fully qualified domain name (FQDN) for the workstation is the host name followed by a period (.) followed by the domain name, for example, rhino.microsoft.com, where rhino is the host name and microsoft.com is the domain name. During DNS queries, the local domain name is appended to short names. Specifying a Domain parameter is optional.

Note The DNS domain is not the same as a Windows NT or LAN Manager domain.

5. When you are done setting connectivity values, choose OK.
The Microsoft TCP/IP - Connectivity Configuration dialog box closes.
 6. Choose the OK button to accept the configuration values you set and to close the Microsoft TCP/IP Configuration dialog box.
Microsoft TCP/IP is now listed as a protocol under your network adapter card in the Network Drivers dialog box.
 7. Choose the Close button.
The Network Drivers dialog box closes.
 8. In the Network Setup dialog box, choose the OK button.
A message appears, notifying you that your startup files have been updated.
 8. Choose the OK button.
A message box appears, notifying you that you must reboot for Microsoft TCP/IP to take effect.
 9. To make changes to your system files, choose the Continue button before rebooting your workstation, or choose the Restart Computer button to reboot your computer and put Microsoft TCP/IP into effect on your workstation.
-

Note If you change any of the TCP/IP parameters, exposed in the configuration dialogs or in the PROTOCOL.INI file, you *must* reboot your workstation for the changes to take effect.

Troubleshooting TCP/IP Connections

The Ping Utility

The **ping** utility, included with TCP/IP for Windows for Workgroups, can isolate network hardware problems and incompatible configurations by allowing you to verify a physical connection to a remote computer. The syntax of the **ping** utility is:

```
ping remote_computer [-t [timeout_value]] [-n [num_times]]
```

where

remote_computer

Is the host name or IP address of a remote computer.

-t [*timeout_value*]

Is the number of seconds that this node waits for an ICMP echo reply from a remote computer. The range is from 1 through 300 seconds; the default is 20 seconds.

-n [*num_times*]

Is the number of times **ping** sends an echo request to the remote computer. The default is 1 echo request.

Note There is a one second delay between echo requests.

Use the **ping** utility to test both the host name and the IP address of the host. If the IP address is verified but the host name is not, you have a name resolution problem. In this case, be sure that the host name you are querying is in either the local HOSTS file or the in DNS database.

PROTOCOL.INI Parameters

Microsoft TCP/IP for the Windows for Workgroups operating system is optimized for everyday users. The graphical installation and configuration process allows most users to configure their systems easily and effectively. If, however, you want to fine-tune options, you can change values in the Windows for Workgroups PROTOCOL.INI file with a text editor. You must then reboot for the changes to take effect. This section lists the available parameters that can be changed, as needed, in the [**tcpip**] section of the PROTOCOL.INI file.

Important Adjusting any PROTOCOL.INI parameters can severely degrade or impede system performance. Be sure that you fully understand the effect(s) your changes will have. You should back up your PROTOCOL.INI file before making any changes. In the event that a change “breaks” your system, revert to the defaults shown in Table 4 or use your backup settings.

Note that many of the parameters described in this appendix can be specified using the Network option in the Control Panel. In fact, using the Network option is the recommended method for updating values because the values you enter will be validated before they are modified; simply editing the PROTOCOL.INI file provides no validation.

Parameter Definitions

Required entries in the [**tcpip**] section of the PROTOCOL.INI file are:

drivename = TCPIP\$
bindings

The following table summarizes the possible entries and values in the [tcpip] section of the PROTOCOL.INI file:

TCP/IP PROTOCOL.INI Parameter Definitions

Entry	Units	Range	Default
bcastaddr	IP address	—	255 255 255 255
bindings	drivers	—	No default
defaultgateway0	IP address	—	No default
drivername	—	—	TCPIP\$
ipaddress0	IP address	—	No default
lanabase	integer	0–255	0
nbsessions	integer	1–22	6
netfiles	path	—	lanroot\ETC
numnames	integer	4–127	9
scope	string	64 character maximum	No default (Null)
subnetmask0	IP address	—	Default based on ipaddress0
tcpconnections	integer	0–22	No default
tcpconntimeout	seconds	1–32767	30
tcpkeepalive	seconds	1–32767	600
tcpsegmentsize	bytes	—	1450
tcpwindowsize	bytes	—	1450

The entries you are most likely to adjust (to enhance system performance) are **tcpconnections** and **tcpwindowsize**. Keep in mind as you adjust these entries that the more connections you have, the smaller the window size will be.

Note In the PROTOCOL.INI file, IP addresses must be entered with spaces instead of periods as separators.

Entries in the [tcpip] section have the following meanings:

bcastaddr

Determines which IP address NBT uses to broadcast name requests and name queries. This entry is usually not needed since NBT uses the local IP address in conjunction with the subnet mask to determine a valid IP address to broadcast on. This parameter is used in cases where the network requires broadcasts to be issued on IP addresses 0.0.0.0 or 255.255.255.255. Keep in mind that it is possible to configure any IP address for NBT to use as a broadcast IP address, even one that is not a broadcast IP address. When such an address is used, the protocol will treat it as a unique IP address and will send broadcast traffic directly to the IP address.

bindings

Binds information taken from the PROTOCOL.INI file to with the protocol and driver modules. This entry and value are supplied during installation by the Windows for Workgroups installation program.

defaultgateway0

Specifies the gateway used when the IP address is not on the local network.

drivename

Identifies the TCP/IP driver name. This entry must be **TCPIP\$** (in all capital letters) and is set during installation by TCP/IP for Windows for Workgroups installation program.

ipaddress0

Identifies the IP address of the local Windows for Workgroups–based workstation.

lanabase

Determines which network adapter number applies to NBT. This entry is used only when more than one NetBIOS driver is loaded by the computer. This entry is set during installation by the Windows for Workgroups installation program.

nbsessions

Specifies the maximum number of supported NetBIOS sessions. This entry should be set to the maximum number of servers the workstation will connect to plus the number of clients expected to connect to the local workstation.

netfiles

Identifies the path to all ASCII database files, such as HOSTS and LMHOSTS.

numnames

Specifies the maximum number of supported, local NetBIOS names that the workstation can register (for example, user name, domain name, and computer name).

scope

Specifies a character string that determines the NBT scope. The default is a null scope. This entry is used to interoperate with other NBT implementations that make use of the NBT scope. Before NBT transmits any packet that contains an NBT name, the NBT scope is first appended to the name. This includes packets such as name queries, name registrations, and session requests. On the receiving end, the NBT scope in any packet must match the locally configured NBT

scope. If the scopes do not match, the packet will be ignored. Therefore, only computers that have the same scope can communicate with each other. The use of the NBT scope allows two computers on the network to have the same NBT name.

subnetmask0

Identifies the subnet mask, which masks the IP address.

tcpconnections

Specifies the total of NBT sessions, sockets sessions, and Telnet sessions for the computer. Adjusting this value can enhance system performance. Changing the **nbsessions** parameter adjusts this parameter automatically, and is the recommended method.

tcpconntimeout

Specifies the amount of time to wait (in seconds) before dropping an unresponsive connection.

tcpkeepalive

Specifies the interval, in seconds, between TCP level checks to make sure that a connection is still active.

tcpsegmentsize

Specifies the maximum amount of data (in bytes) that can be sent by the computer in a single packet. The value depends on the number of **tcpconnections**. For maximum memory conservation, set **tcpsegmentsize** to 1024. A large segment is 1450.

tcpwindowsize

Specifies the maximum amount of data (in bytes) that can be accepted by a workstation into its buffer. The value depends on the number of **tcpconnections** and on the network–adapter card. The minimum size is 512 bytes. To conserve memory, use a window size less than or equal to 4350. For best performance, set the window size to a multiple of **tcpsegmentsize**. The suggested multiple is 3 or 4, depending on whether **tcpsegmentsize** is 1450 or 1024, respectively. For maximum memory conservation, set **tcpwindowsize** to 1024.

Note If you use a 3Com® EtherLink® card (3C501) (instead of an EtherLink II® card), set the window size equal to the segment size for all applications. Window and segment sizes must both be equal to either 1024 or 1450. Otherwise, performance could be seriously degraded.

TCPUTILS.INI Parameters

The installation program for Microsoft TCP/IP for Windows for Workgroups sets the parameters in the TCPUTILS.INI file, and usually you don't need to change them. This section lists the parameters that can be changed, as needed, in the TCPUTILS.INI file.

Important Adjusting any TCPUTILS.INI parameters can severely degrade or impede system performance. Be sure that you fully understand the effect(s) your changes will have. You should back up your TCPUTILS.INI file before making changes. In the event that a change "breaks" your system, revert to the defaults shown in the "Sections of the TCPUTILS.INI File" table or use your backup settings.

The following table shows the TCPUTILS.INI sections and their functions in TCP/IP.

Sections of the TCPUTILS.INI File

Section	Function
SOCKETS	Sockets protocol driver
DNR	Domain name resolver protocol driver
TCPGLOBAL	Section with common TCP/IP entries shared by TCP/IP drivers

The following sections provide information about each of these sections in TCPUTILS.INI.

[sockets] Section

The following entry in the [sockets] section of the TCPUTILS.INI file is required:

```
drivename = SOCKETS$
```

The following table summarizes the possible entries and values in the **[sockets]** section:

[sockets] Section Parameter Definitions

Entry	Units	Range	Default
drivename	—	—	SOCKETSS\$
maxsendsize	bytes	32–2048	1024
numsockets	integer	1–31	4
poolsize	bytes	3200–28800	3200

Entries in the **[sockets]** section have the following meanings:

drivename

Identifies the sockets driver name. This entry must be **SOCKETSS\$** (in all capital letters).

maxsendsize

Specifies the maximum send size (in bytes) allowed on user datagram protocols (UDPs) or nonblocking TCP sends.

numsockets

Specifies the maximum number of sockets to be supported.

poolsize

Specifies the buffer size (in bytes) used by the sockets driver for nonblocking send calls. This entry is set when the system is initialized.

[dnr] Section

The following entry in the **[dnr]** section of the TCPUTILS.INI file is required:

drivename = DNR\$

The following table summarizes the possible entries and values in the **[dnr]** section:

[dnr] Section Parameter Definitions

Entry	Units	Range	Default
drivename	—	—	DNR\$
domain	string	Up to 116 characters	No default
nameserver0	IP address	—	No default
nameserver1	IP address	—	No default

Entries in the **[dnr]** section have the following meanings:

drivename

Identifies the DNR driver name. This entry must be **DNR\$** (in all capital letters).

domain

Identifies the TCP/IP domain name, which helps identify the workstation to other computers on the network. The domain name can contain as many fields as will fit within 116 characters. Each field must begin with an alphanumeric character and must be followed by letters, digits, or hyphens. Each field can have between 1 and 63 characters. Adjacent fields must be separated by periods.

nameserver0

Specifies the IP address of the primary domain server, which maintains a database of domain names.

nameserver1

Specifies the IP address of the secondary domain server.

[tcpglobal] Section

The following entry in the **[tcpglobal]** section of the TCPUTILS.INI file is required:

username = *user name*

The following table summarizes the possible entries in the **[tcpglobal]** section:

[TCPGLOBAL] Section Parameter Definitions

Entry	Units	Range	Default
host name	string	—	No default
username	string	—	No default

Entries in the **[tcpglobal]** section have the following meanings:

host name

Identifies the TCP/IP name of your workstation on the network.

username

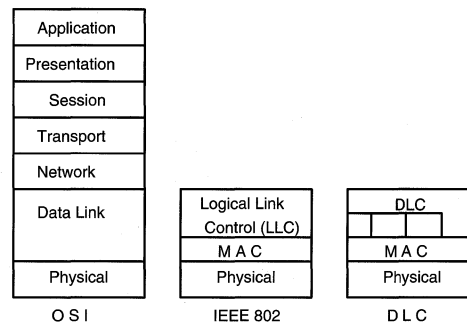
Identifies the local name used to logon.

Microsoft Data Link Control Protocol for Windows for Workgroups

Microsoft Data Link Control (DLC) Protocol for Windows for Workgroups allows Windows for Workgroups-based personal computers to operate in IBM SNA environments and to connect to mainframes and minicomputers, such as the AS/400®. The DLC interface is most commonly used by 3270 terminal emulators to communicate to IBM mainframes. Support of the emulators is the main role of the Microsoft DLC protocol. Products from companies such as DCA, Attachmate, IBM, Microcom, and Wall Data support the Microsoft Data Link Control protocol.

The MS-DLC Protocol Interface provides a direct data link control interface for MS-DOS workstations using Windows for Workgroups. The DLC interface is most commonly used by 3270 terminal emulators to communicate with IBM mainframes, and by 5250 terminal emulators to communicate with IBM AS/400s via Advanced Program-to-Program Communication (APPC). Support of these emulators is the main role of the MS-DLC protocol.

Figure 6.9
Stack Comparisons of
OSI, IEEE 802, and
DLC



In relation to the OSI reference stack, the DLC protocol interface provides a data link layer interface to the network. The data link layer is responsible for point to point transmission of data. In further defining the functionality of the data link layer, the IEEE has divided the layer even further into the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The Network Driver Interface Standard (NDIS) used for developing device drivers for network cards defines the function calls (protocol) that connect the MAC layer at the top end to the LLC layer at the bottom. The MS-DLC driver supports the NDIS protocol on the bottom, and allows programs to interface directly to it.

Terminal emulation applications call the Microsoft DLC protocol with the Int 0x5C (NetBIOS) interrupt vector. The Microsoft DLC protocol communicates only through the terminal emulation applications; it does not use Windows for Workgroups networking components to communicate with the network. It does not have a NetBIOS interface. The Microsoft DLC protocol can co-exist with other protocols. The Microsoft DLC protocol conforms to NDIS 2.0.

Installing and Configuring Microsoft DLC

For Support Support for Microsoft Data Link Control (DLC) protocol for Windows for Workgroups is not available from the standard Windows for Workgroups support line, however support is available from the advanced networking support group in PSS. For assistance with installing or using DLC with Windows for Workgroups, call Microsoft Product Support Services at (206) 635-7022. Service charge of \$150.00 per call. Charges will be billed to your Visa, MasterCard, or American Express.

This section describes the process for installing and using the Microsoft DLC protocol on a workstation running Windows for Workgroups 3.11.

Before installing the Microsoft DLC protocol, make sure the Network Setup application is not running.

Note If SETUP.EXE provided with Microsoft DLC is dated 3/8/93, do NOT run Setup — doing so will replace your FFWSETUP.DLL driver with an older version preventing Setup from running properly. In this case, add Microsoft DLC as an additional protocol from the Network Drivers dialog box in Windows network setup beginning with step number 4.

To install the Microsoft DLC protocol on a Windows for Workgroups workstation

1. Insert the Microsoft DLC for Windows for Workgroups disk in drive A.
2. From File Manager or Program Manager, select the Run command from the File menu.

The Run dialog box appears.

Important You should run the Microsoft DLC setup program as described in the following procedure instead of simply adding DLC as another protocol using Network Setup.

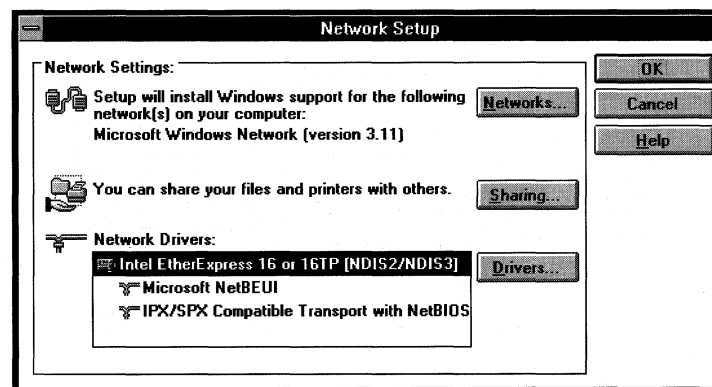
3. In the Command Line box, type:

```
a:setup.exe
```

Some of the distribution files are copied to your workstation and the Network Setup dialog box appears.

Figure 6.10

The Network Setup dialog box

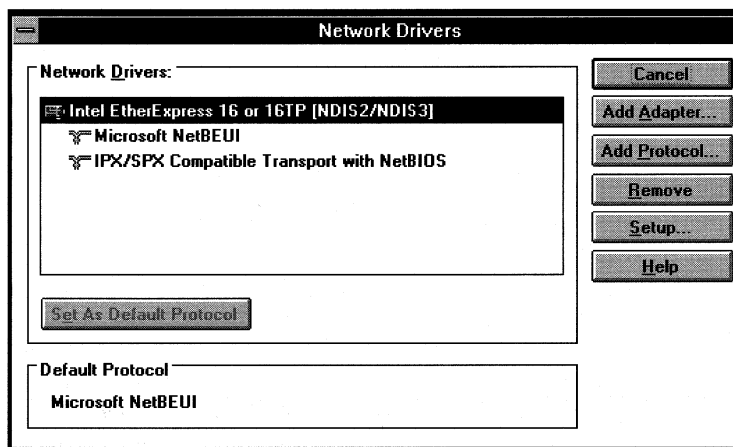


- Choose the Drivers... button.

The Network Drivers dialog box appears.

Figure 6.11

The Network Drivers dialog box, accessible through Network Setup

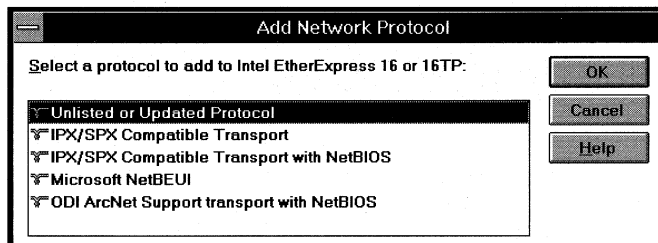


- In the Network Driver list box, select the adapter on which you want to use Microsoft DLC. (You can select only one adapter.)
- Choose the Add Protocol... button. The Add Network Protocol dialog box appears.

The Network Drivers dialog box, accessible through Network Setup.

Figure 6.12

The Add Network Protocol dialog box, accessible through the Network Setup application.



- Select the Unlisted or Updated Protocol option from the list of available protocols and then choose OK. The Install Driver dialog box appears.
- In the Install Driver dialog box, type **A:** for the location of the Microsoft DLC for Windows for Workgroups disk, then choose OK.

The Unlisted or Updated Protocol dialog box appears.

- Select Microsoft DLC.
- Choose OK.

The Microsoft DLC for Windows for Workgroups protocol software is copied to your workstation.

11. If Microsoft DLC is not listed as the default protocol at the bottom of the Network Drivers dialog box, highlight Microsoft DLC and click the Set As Default Protocol button.
12. Choose OK to close any dialog boxes that may be open, and re-boot your system for the changes to take effect.

To customize the configuration of the DLC protocol, continue with the next procedure.

Configuring Microsoft DLC

This section describes the process for configuring the Microsoft DLC protocol (once you have installed it on your workstation). The following section lists all of the available parameters that can be changed via the Microsoft DLC Configuration dialog box. In most cases, you do not need to change any parameter values when the Microsoft DLC protocol is installed. If, however, you want to tune the Microsoft DLC protocol yourself, follow the procedures in this section, and refer to the next section for information on each of the available settings.

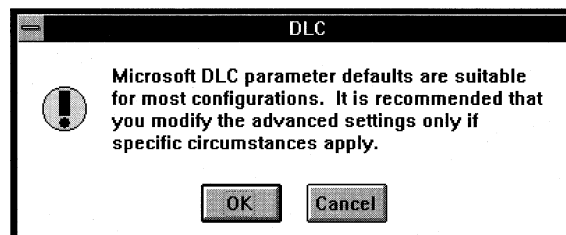
To configure the Microsoft DLC protocol on a workstation

1. Double-click the Network Setup icon in the Network program group.
The Network Setup dialog box appears.
2. In the Network Driver list box, select the adapter on which you previously installed Microsoft DLC.
3. Choose the Drivers... button.
The Network Drivers dialog box appears.
4. Select the Microsoft DLC protocol from the Network Drivers list box.
5. Choose the Setup... button.

A message box like the following displays, letting you know that for most users, the default DLC protocol settings are suitable. Therefore you may not need to change any of the DLC parameters.

Figure 6.13

DLC parameter message box

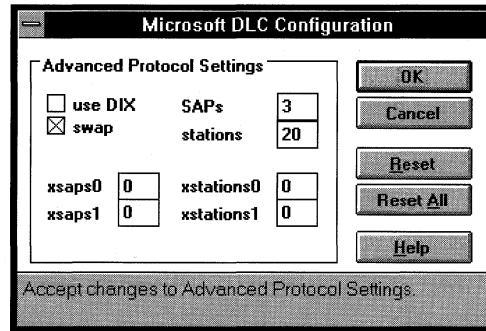


Choose OK to continue configuring the DLC parameters, or choose Cancel to return to the Network Drivers dialog box.

If you choose OK, the Microsoft DLC Configuration Dialog box appears.

Figure 6.14

Microsoft DLC
Configuration dialog box



6. Update the values for the parameters you want to change.

Tip When your cursor is on a particular field, you can use the Reset button to reset that value to its default. You can also use the Reset All button to reset all values to their defaults.

For detailed information on each of the settings in the Microsoft DLC Configuration dialog box, see the following topics in this chapter.

The Microsoft DLC for Windows for Workgroups configuration program will check the validity of the values you enter. or other Microsoft DLC parameters that can be modified, by directly editing the PROTOCOL.INI file, see "PROTOCOL.INI Parameters," later in this chapter.

7. When you are through making changes to the Microsoft DLC Configuration dialog box, choose OK.
8. In the Network Drivers dialog box, choose the Close button.
9. In the Network Setup dialog box, choose OK.

A message box appears notifying you that your startup files have been modified. Choose OK.

10. A message box appears notifying you that you must reboot for changes made to your system to take effect.
 - To first make any additional changes to system files before rebooting your workstation, choose the Continue button.

Alternately, to reboot your workstation and put the Microsoft DLC protocol into effect, choose the Restart Computer button.

Note You *must* reboot your workstation for the Microsoft DLC protocol to take effect.

Microsoft DLC Protocol Parameters

The following Microsoft DLC protocol parameters can be updated from the Microsoft DLC Configuration dialog box.

use DIX

Sets the frame format. By default, this value is disabled.

Disable this value for 802.3 Ethernet format. Enable this value for Ethernet DIX 2.0 (Ethernet 0x80D5) format. (Ethernet DIX frames have an extra type-field.)

swap

Turns on address bit-swapping when it is enabled and Microsoft DLC is bound to an Ethernet driver. By default, this value is enabled.

If you previously used the IBM DXME0MOD.SYS driver successfully, use the following table to map its **xmit_swap** parameter to Microsoft DLC parameters.

DXME0MOD.SYS xmit_swap	Microsoft DLC swap	Microsoft DLC Use DIX
0	enable	disable
1	enable	enable
2	disable	disable
3	disable	enable

saps

Indicates the number of **SAPs** that can be opened simultaneously. The range for **SAPs** is 1 to 255 inclusive. The default is 3.

For a description of **SAPs**, see the *IBM Local Area Network Technical Reference*. For more information about adjusting the **SAPs** value, see the **stations** parameter.

stations

Indicates the number of link stations that can be opened simultaneously. The range for **stations** is 1 to 255 inclusive. The default is 20.

Each application requires a certain number of SAPs and stations. Because each SAP or station takes up memory, you should provide just enough for your application to run. The following table provides some examples of the number of SAPs and stations needed by specific applications.

Application	SAPs	Stations
DCA® IRMA® Workstation for DOS	3	10
Dynacomm® Elite for DOS	2	4
Eicon Access version 3.11	1	1
Attachmate Extra for DOS version 2.23	2	2
Attachmate Extra for Windows version 3.3	2	8
IBM® PC 3270 version 2 for DOS	2	20
IBM PC 3270 version 2 for Windows	2	20
IBM Personal Communication Support (PCS)	1	3
Microcom® Relay Gold 5.00 (for DOS)	2	2
Microcom Relay Gold 5.0b (for Windows)	2	2
Wall Data® Rumba® version 3.1	2	1

xsaps0

Update the value for this parameter if you need to run more than one DLC application. The range for **xsaps0** is 0 to 127 inclusive. The default is 0.

Specifying a value for this parameter causes this value to be compared to the maximum value for SAPs (specified by the application program) during the **dir.open.adapter** call for **adapter #0**, and the larger of the two is used. If the sum **xsaps0 + xsaps1** exceeds the value specified for **SAPs**, **SAPs** will automatically be increased to the value of **xsaps0 + xsaps1**.

For example, if you are running two DLC applications and each requires two SAPs, set **xsaps0** to 4. When the first DLC application issues the **dir.open.adapter** call, it will ask for two SAPs but will get four SAPs because of the **xsaps0** parameter. This way, the second DLC application receives enough SAPs to run.

xsaps1

Similar to **xsaps0**, but for **adapter #1**. The range for **xsaps1** is 0 to 127 inclusive. The default value is 0.

xstations0

Similar to **xsaps0**, but used for changing the number of link stations, rather than the number of SAPs. The range for **xstations0** is 0 to 127 inclusive. The default is 0.

If the sum of **xstations0** + **xstations1** exceeds the value for **stations**, **stations** will automatically be increased to the value of **xstations0** + **xstations1**.

xstations1

Similar to **xstations0**, but for **adapter #1**. The range for **xstations1** is 0 to 127 inclusive. The default is 0.

PROTOCOL.INI Parameters for Microsoft DLC

The default Microsoft DLC for Windows for Workgroups protocol settings are acceptable for most users. The graphical installation and configuration process should allow most users to configure their systems effectively. If, however, you want to fine-tune options, you can change values in the Windows for Workgroups PROTOCOL.INI file with a text editor. You must reboot for the changes to take effect. This appendix documents all of the available parameters that can be changed, as needed, in the [**msdlc_xif**] section of the PROTOCOL.INI file.

Important

Adjusting any PROTOCOL.INI parameters might severely degrade (or impede) system performance. Be sure you fully understand the effect(s) your changes will have. In the event that a change “breaks” your system, revert to the defaults shown in the following tables.

Note that many of the parameters described in this section can be configured using the Network option in the Control Panel. Using the Network option is the recommended method for updating values because of the validation feature this method provides. No validation feature is provided when you directly edit the PROTOCOL.INI file.

Required PROTOCOL.INI Parameters

The following table summarizes the required entries and their default values in the [msdlc_xif] section of the PROTOCOL.INI file.

Required entry	Units	Range	Default
bindings	drivers	—	no default
drivername	—	—	msdlc\$
transport	drivers	—	msdlc
lana#	drivers	—	no default

Entries in the [network.setup] section of the PROTOCOL.INI file have the following meanings:

lana#

Identifies the binding between the network adapter and the network protocol, as configured during installation.

transport

Specifies the name of the network transport driver protocol, in this case **msdlc**. This required value is set during installation.

Optional PROTOCOL.INI Parameters

The following table summarizes the possible entries and values in the [msdlc] section of the PROTOCOL.INI file.

Entry	Units	Range	Default
adaptrate	milliseconds	0-65535	0
bufqelements	buffers	1-2048	64
class1timeout	seconds	0-65535	120
commands	descriptors	1-255	24
denysaps	—	0x02-0xFE	0xF0
ipackets	packets	1-1000	24
looppackets	packets	1-1000	2
maxgroup	packets	1-126	0
maxin	packets	1-127	1
maxmember	packets	1-127	0
maxout	packets	1-127	12
msdlcretries	retries	1-65535	8

Entry	Units	Range	Default
saps	—	1–255	3
stacksize	bytes	512–4096	2048
stations	—	1–255	20
swap (<i>Ethernet only</i>)	—	0–1	1
t1_tick_one	40 milliseconds	1–255	5
t1_tick_two	40 milliseconds	1–255	25
t2_tick_one	40 milliseconds	1–255	1
t2_tick_two	40 milliseconds	1–255	10
timers	timers	1–255	12
ti_tick_one	40 milliseconds	1–255	25
ti_tick_two	40 milliseconds	1–255	125
trxbuffers	buffers	0–32	0
trxbuFSIZE	bytes	0–16000	0
uipackets	packets	2–300	16
usedix (<i>Ethernet only</i>)	—	0–1	0
windowerrors	errors	0–10	0
xsaps0	—	0–127	0
xsaps1	—	0–127	0
xstations0	—	0–127	0

Entries in the **[msdlc]** section of the PROTOCOL.INI file have the following meanings.

adaptrate

Specifies the time in milliseconds between runs of the *adaptive window algorithm*. For each link, the Microsoft DLC driver uses the algorithm to match the **maxin** and **maxout** values with the remote station's values as closely as possible. The algorithm also considers the conditions of the link (such as adapter receiver buffers, load, and so on).

When no dropped packets are detected, the adaptive window algorithm increases the send window (see **maxout**). If dropped packets are detected (more than the value of **windowerrors**), the algorithm decreases the send window. Similarly, the algorithm adjusts the receive window based on the time-out expiration of the **t2** timer.

Adaptrate should be large in relation to **t1** and **t2**—usually above one second—but it can be smaller than **ti**.

A value of 0 turns off the algorithm, meaning that the **maxin** and **maxout** values never change.

bindings

Names the driver(s) to which Microsoft DLC binds. The Microsoft DLC driver can bind to as many as two network adapter drivers. Use commas to separate the driver names.

bufqelements

Specifies the total number of buffers that can be pooled in the driver at one time. This is not a per-pool limit, but a limit across all pools.

class1timeout

Specifies the length of time a network adapter driver should spend trying to send a UI frame before giving up and freeing the resources.

commands

Specifies the number of CCB descriptors to allocate for managing CCBs submitted to the Microsoft DLC driver. Specifies the number of commands pending simultaneously. The equivalent entry in the Microsoft NetBEUI protocol is called **ncbs**.

denysaps

Specifies a list of SAP values that can not be opened on the driver. The NetBIOS SAP (0xF0) is denied by default. To allow the NetBIOS SAP, set no value for **denysaps**.

drivername

Identifies the driver name of the network device driver. The base portion of the driver's filename, plus a dollar sign, is the **drivername**. The Microsoft DLC **drivername** is **msdlc\$**.

ipackets

Specifies the number of I-frame packet descriptors that the Microsoft DLC driver can use to build DLC frames.

load

Specifies whether to load Microsoft DLC into conventional or high memory. This required value is set during installation. You can change where Microsoft DLC is loaded later by editing this entry. The next time Microsoft DLC is loaded, the new value will take effect.

looppackets

Specifies the number of frames to be looped back at one time. Packets are used when the workstation sends a message to itself.

maxgroup

Specifies the maximum number of Group SAPs that can be opened simultaneously.

The default values for **maxgroup** and **maxmember** are zero because most applications do not use Group SAPs. Increase these values if your applications use Group SAPs.

maxin

Specifies the number of packets to be received before sending an acknowledgment. This number is often called the *receive window*.

When the **adaptrate** entry is present and has a value of zero, the **maxin** value is not dynamically adjusted. Otherwise, the Microsoft DLC driver adjusts the **maxin** value as described in the **adaptrate** entry in this section.

maxmember

Specifies the maximum number of SAPs that can belong to each Group SAP.

The default values for **maxgroup** and **maxmember** are zero because most applications do not use Group SAPs. Increase these values if your applications use Group SAPs.

maxout

Specifies the number of packets to send before expecting an acknowledgment. This number is often called the *send window*.

When the **adaptrate** entry is present and has a value of zero, the **maxout** value is not dynamically adjusted. Otherwise, the Microsoft DLC driver adjusts the **maxout** value as described in the **adaptrate** entry in this section.

msdleretries

Specifies the number of transmission retries that Microsoft DLC makes before assuming that the receiver is not responding. You can lower the value of this entry on a highly reliable network, where few packets are dropped. Raise the value if the network is prone to dropping packets.

The types of network adapters on the network affect reliability because some have limited buffering capabilities and might drop packets because of a buffer-resource problem.

saps

Indicates the number of SAPs that can be opened simultaneously. For a description of SAPs see the *IBM Local Area Network Technical Reference*. For more information about adjusting the **saps** entry, see the **stations** entry.

stacksize

Indicates the size, in bytes, of the Microsoft DLC protocol's internal stack.

stations

Indicates the number of link stations that can be opened simultaneously.

Each application requires a certain number of SAPs and stations. Because each SAP or station takes up memory, you should provide just enough for your application to run. Here are some examples of the number of SAPs and stations needed by specific applications.

Application	SAPs	Stations
DCA IRMA Workstation for DOS	3	10
Dynacomm Elite for DOS	2	4
Eicon Access version 3.11	1	1
Attachmate Extra for DOS version 2.23	2	2
Attachmate Extra for Windows version 3.3	2	8
IBM PC 3270 version 2 for DOS	2	20
IBM PC 3270 version 2 for Windows	2	20
IBM Personal Communication Support (PCS)	1	3
Microcom Relay Gold 5.0b (for Windows)	2	2
Microcom Relay Gold version 5.0 (for DOS)	2	2
Wall Data Rumba version 3.1	2	1

If you do not know the number of SAPs and stations your application requires, and you want to minimize the memory usage of your terminal emulation applications, start with large values and gradually reduce them until the application no longer works.

The default is set to **saps=3** and **stations=20**. This is more than enough for most Microsoft DLC applications.

swap

When Microsoft DLC is bound to an Ethernet driver, setting this parameter to 1 (enable) turns on address bit-swapping.

If you previously used the IBM DXME0MOD.SYS driver successfully, this is how to map its **xmit_swap** parameter to the Microsoft DLC driver's **swap** and **usedix** parameters.

DXME0MOD.SYS xmit_swap	Microsoft DLC swap	Microsoft DLC usedix
0	1	0
1	1	1
2	0	0
3	0	1

t1_tick_one

Sets the retransmission-timer “short tick” value in units of 40 milliseconds. This timer determines the delay before retransmitting a link-level frame if no acknowledgment is received.

The Microsoft DLC protocol uses three timers: **t1** (retransmission), **t2** (acknowledgment), and **ti** (inactivity). Each timer has a “short tick” rate and a “long tick” rate that individual commands use in determining timer values. A command such as **dlc.open.sap** specifies a timer value with a number range of 1–10 units of milliseconds.

When the number is in the range of 1–5 units of milliseconds, the actual timer value is:

$$(\text{number selected}) * (\text{short-tick value}) * 40 \text{ milliseconds}$$

When the number is in the range of 6–10 units of milliseconds, the actual timer value is:

$$(\text{number selected} - 5) * (\text{long-tick value}) * 40 \text{ milliseconds}$$

Some network application programs adjust these timer entries automatically. The **dlc.open.adapter** command can override the default value.

t1_tick_two

Sets the retransmission-timer “long tick” value in units of 40 milliseconds. This timer determines the delay before retransmitting a link-level frame if no acknowledgment is received.

For an explanation of the relationship among timer entries, see the **t1_tick_one** entry in this section.

t2_tick_one

Sets the delayed-acknowledgment timer “short tick” value in units of 40 milliseconds. This timer determines the delay before acknowledging a received frame when the receive window has not been reached.

For an explanation of the relationship among timer entries, see the **t1_tick_one** entry in this section.

t2_tick_two

Sets the delayed-acknowledgment timer “long tick” value in units of 40 milliseconds. This timer determines the delay before acknowledging a received frame when the receive window has not been reached.

For an explanation of the relationship among timer entries, see the **t1_tick_one** entry in this section.

timers

Specifies the number of timers running at one time using the Microsoft DLC timer primitives.

ti_tick_one

Sets the inactivity-timer “short tick” value in units of 40 milliseconds. This timer determines how often an inactive link is checked to see whether it is still operational. For an explanation of the relationship among timer entries, see the **t1_tick_one** entry in this section.

ti_tick_two

Sets the inactivity-timer “long tick” value in units of 40 milliseconds. This timer determines how often an inactive link is checked to see whether it is still operational.

For an explanation of the relationship among timer entries, see the **t1_tick_one** entry in this section.

trxbuffers

Specifies the number of internal transmit buffers. Increase this value only if your configuration issues transmits containing more buffers than the network adapter driver can accept in one transfer call.

trxbufsize

Specifies the size of internal transmit and receive buffers. Increasing this value is required only when running applications that use Group SAPs or that issue transmits containing more buffers than the media access control driver can accept in one transfer call.

uipackets

Specifies the number of data descriptors to allocate for sending UI-frames.

unload

Specifies how to unload Microsoft DLC from memory. This value should not be changed.

usedix (Ethernet only)

Sets the frame format. Set the value to 0 (the default, disable) for 802.3 Ethernet format. Set the value to 1 (enable) for Ethernet DIX 2.0 (Ethernet type 0x80D5) format. (Ethernet DIX frames have an extra type-field.)

windowerrors

Specifies the number of dropped packets that the adaptive window algorithm allows before it decreases the send window. (For more information on the adaptive window algorithm, see the **adaptrate** entry in this section.) For example, if **windowerrors** has a value of 1, one packet can drop between runs of the algorithm without having any effect; if 2 packets drop, the algorithm decreases the send window.

Keep the value of **windowerrors** low for a lightly loaded network, and increase it for a heavily loaded network.

xsaps0

Update the value for this parameter if you need to run more than one DLC application. Specifying a value for this parameter causes this value to be compared to the maximum value for SAPs (specified by the application program) during the **dir.open.adapter** call for **adapter #0**, and the larger of the two is used. If the sum **xsaps0** + **xsaps1** exceeds the value specified for **SAPs**, **SAPs** will automatically be increased to the value of **xsaps0** + **xsaps1**.

xsaps1

Similar to **xsaps0**, but for **adapter #1**.

xstations0

Similar to **xsaps0**, but used for changing the number of link stations, rather than the number of SAPs. If the sum of **xstations0** + **xstations1** exceeds the value for **stations**, **stations** will automatically be increased to the value of **xstations0** + **xstations1**.

xstations1

Similar to **xstations0**, but for **adapter #1**.

Integrating with Windows NT and Windows NT Advanced Server

This chapter focuses on the features of the Windows NT and Windows NT Advanced Server operating system that benefit a Windows for Workgroups 3.11 user in an integrated networking environment. The areas emphasized in this chapter are configuration issues—including supported protocols, enhanced security—highlighting the use of domains, as well as the Remote Access Services (RAS) server provided with Windows NT Advanced Server.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 6, “Integrating with Other Protocols;” Chapter 8, “Integrating with Novell NetWare;” Chapter 9, “Integrating with Other Networks;” Chapter 13, “Troubleshooting Windows for Workgroups 3.11.”
- *Microsoft Windows NT Resource Kit*
- Microsoft Windows NT system documentation
- Remote Access Service help file, RASPHONE.HLP

Contents of This Chapter

Overview of Support for Integrating Workgroups 3.11 with Windows NT	7-2
Protocol Support.....	7-3
Enhanced Security Features in a Windows NT Environment	7-4
Share-Level Security and User-Level Security	7-4
Domain Support	7-4
Remote Access Services Client	7-6
Accessing the Remote Access Server Provided with Windows NT and Windows NT Advanced Server.....	7-6
RAS Features.....	7-7
Choosing and Configuring a Modem on a Windows for Workgroups 3.11 computer.....	7-8
Direct Serial Connections via NULL Modem.....	7-11
Remote Access Security Features	7-13
RAS Support for ISDN	7-13

Overview of Support for Integrating Workgroups 3.11 with Windows NT

Windows for Workgroups 3.11 integrates seamlessly with Windows NT and Windows NT Advanced Server in a networking environment.

Windows for Workgroups 3.11 is an excellent peer for Windows NT, a fully 32-bit operating system that supports preemptive multi-tasking. Windows NT, designed for high-end, power-user desktops, provides client services as well as server capabilities, including file and printer sharing. Windows NT, like Windows for Workgroups 3.11, provides peer-to-peer networking, or can participate in domains. Windows NT is similar to Windows for Workgroups 3.11 in its peer-to-peer nature, but differs greatly in feature set and architecture.

Windows for Workgroups 3.11 is also an excellent client for Windows NT Advanced Server, also a 32-bit, multitasking operating system, which offers enhancements over Windows NT. Windows NT Advanced Server provides enhanced security features including domain controller services, increased fault tolerance, and many additional features including a Remote Access Services (RAS) server that remote Windows for Workgroups 3.11 users, Windows NT users, and Windows NT Advanced Server users can dial-in to access data.

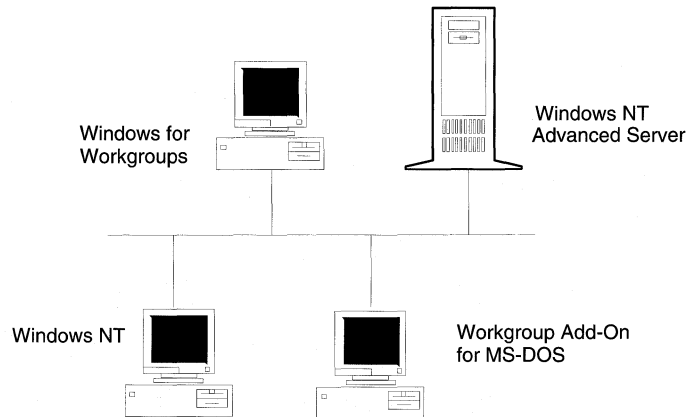
Windows for Workgroups 3.11 and Windows NT and Windows NT Advanced server integrate seamlessly. Besides installing the appropriate protocol on all computers that will need to communicate, there is no additional configuring required to enable a Windows for Workgroups 3.11 computer and a Windows NT or Windows NT Advanced Server computer to “see” each other on the network.

Computers running Windows for Workgroups, Windows NT, Windows NT Advanced Server and the Workgroup Add-on for MS-DOS can share and access resources on each of the platforms without the use of any additional software or any special configuration steps.

Windows for Workgroups 3.11 and Windows NT appear exactly the same when looking at the various shared resources on the network. Sharing files, directories, and printers is done the same way on both platforms. Connectivity to Windows NT Advanced Server from a client running Windows for Workgroups 3.11 or Windows NT is just as straightforward.

Figure 7.1

All components of the Windows family can work together seamlessly on the same network



Protocol Support

For a computer running Windows for Workgroups 3.11 to communicate with a computer running Windows NT or Windows NT Advanced Server, the same protocol must be installed on both. The NetBEUI protocol is installed by default during the setup programs of Windows for Workgroups 3.11, Windows NT and Windows NT Advanced Server. Windows for Workgroups 3.11, Windows NT and Windows NT Advanced Server provide IPX/SPX and NWLINK protocols, in addition to NetBEUI.

An alternative to running the NetBEUI protocol is to run the IPX/SPX protocol with NetBIOS (NWLink and NWNBLink). This configuration allows computers running Windows for Workgroups 3.11, Windows NT or Windows NT Advanced Server to communicate through a router (such as a Novell NetWare server) via the routable IPX protocol.

For more information on Windows for Workgroups 3.11 protocols, see Chapter 6, "Integrating with Other Protocols." For more information on NWLink and NWNBLink, see Chapter 8, "Integrating with Novell NetWare."

Enhanced Security Features in a Windows NT Environment

Windows for Workgroups 3.11 has many enhanced security features to prevent unauthorized access to shared information on the network as well as unauthorized access to the network. The system administrator may define and control some or all of the security settings for users of Windows for Workgroups and the Workgroup Add-on for MS-DOS. Workstations running Windows for Workgroups 3.11 can be configured to adhere to Windows NT domain security to control access to the network. Security settings can be defined using the administrator configuration utility, ADMINCFG.EXE, provided with Windows for Workgroups 3.11 — see Chapter 5, “Windows for Workgroups 3.11 Security Control Enhancements,” for more information.

Share-Level Security and User-Level Security

Share-level security creates a secure computing environment by allowing system administrators or users to protect shared network resources by assigning a password to network share names. For example, after a system administrator assigns a password to a network share, the user who wants to access a file on the protected shared resource must type in the appropriate to access it. If the shared resource is not password-protected, everyone with access to the network has full access to that resource.

User-level security creates a tightly secured computing environment by requiring each user on the network to have a type of identification. Each user has a user name and password which must be validated by the network's security database to determine what privileges the user has on the network. When a user attempts to access a network share in a user-level secured environment, the user name and password are sent to the server for validation against the network's security database. If this validation fails, the user will be refused access to the network share.

Windows for Workgroups 3.11 supports share-level security only. Windows NT and Windows NT Advanced Server support user-level security.

Domain Support

The Windows NT Advanced Server architecture supports the concept of *domains*, which allow multiple servers to be grouped together for unified administration. With domains, both domain administrators and users receive the benefits of using one account across all domains in an enterprise.

In contrast to a domain is a workgroup. A *workgroup* is a logical group of computers and their resources. The computers participating in a workgroup maintain their own security system for validating local user logons and resource access. They do not share security with other computers, and do not rely on other computers to provide security. Examples of workgroup computers are MS-DOS workgroup clients, Windows for Workgroups 3.11 computers and Windows NT workstations participating in a workgroup.

User and Group Accounts

Windows NT and Windows NT Advanced Server support user-level security via two types of accounts, individual user (including guest) accounts, and group accounts.

A *user account* includes information about a user such as a user name, a full name, a password, and rights on the system. Each user needs one or more accounts in order to log on to a server with user-level security. A user account grants a specific user a set of privileges, or rights, defining how they may use the system.

A *guest account* on a Windows NT computer, Windows NT Advanced Server, or Microsoft LAN Manager Server is an account in which a person without a valid individual user account and password may still access resources on the user-level secured server.

By setting up a guest account, it is possible to make some files on a server available to everyone, without setting up a user account for each person who may need access to the files. Instead, everyone can have access to the files via one guest account. This may be considered a “public” account that is available to all users.

On a Windows NT computer the guest account is available by default. On a Windows NT Advanced Server, the guest account is disabled by default.

A *group account* is used to establish privileges for multiple users. Group accounts provide a convenient way to give and control access to multiple users who perform similar tasks and hence require similar privileges on the network. Group accounts make it easy to make changes to multiple users privileges on the network at once.

In addition, there are local and global group accounts. On Windows NT computers there are only local groups where permissions only validate on the local computer. In a Windows NT Advanced Server domain, all Windows NT Advanced Server computers share the same local group. Windows NT Advanced Server computers may also have global groups that can be shared with other computers joining the domain.

For further information on the Windows for Workgroups 3.11 security system and how it interacts with Windows NT and Windows NT Advanced Server, please refer to Chapter 5, "Windows for Workgroups 3.11 Security Control Enhancements."

Remote Access Services Client

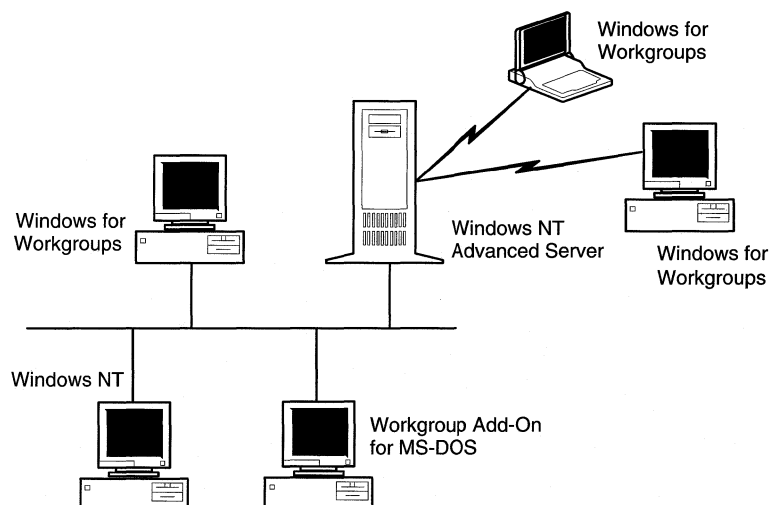
Windows for Workgroups 3.11 provides a Remote Access Services (RAS) client which enables a remote computer running Windows for Workgroups 3.11 to dial-in to a Windows NT or Windows NT Advanced Server RAS server, which then provides full seamless access to network resources as if the user were physically present on the remote network. This functionality is especially useful for Windows for Workgroups 3.11 users on an existing network in a satellite office, or a portable computer user running Windows for Workgroups 3.11 at a remote site or on the road.

Accessing the Remote Access Server Provided with Windows NT and Windows NT Advanced Server

The Remote Access server provided with Windows NT and Windows NT Advanced Server enables remote computer users using Windows for Workgroups 3.11 or Windows NT to dial into the network to access shared network resources and make use of client-server applications remotely. RAS supports dial-in access for as many as 64 computers simultaneously with the Windows NT Advanced Server acting as a NetBIOS bridge to provide the remote workstation with full access to all authorized network resources (a Windows NT workstation only supports one dial in connection at a time). This allows a remote user to access resources available on a Windows NT Advanced Server as well as resources present on other computers on the network running Windows for Workgroups, Windows NT and Workgroup Add-on for MS-DOS, provided that the remote user has security clearance to access the resources.

Figure 7.2

Windows for Workgroups RAS client provides remote access to the network and shared resources



RAS Features

Microsoft Windows NT Advanced Server Remote Access Server offers the following features that benefit Windows for Workgroups 3.11 users:

Transparent access to the network for telecommuters, mobile workers, and remote system administrators, including:

- Support for named pipes, Remote Procedure Call (RPC), and the LAN Manager application programming interface (API).
- Client access to resources on application servers such as SQL Server, SNA Server for Windows NT, and Lotus Notes®.
- Compatibility with workstations and servers running previous versions of the Remote Access Service.
- Support for public telephone, X.25, and Integrated Services Digital Network (ISDN) wide-area networks.
- Support for data compression and error control on modems.
- Software compression.

A secure environment via:

- Integration with Windows NT Advanced Server security
- Domain-based and trusted domain-based security
- Encrypted authentication at connect time
- Support for third-party security hosts that authenticate users
- Central administration of servers and users

Additional features:

- Up to 64 simultaneous connections per Windows NT Advanced Server (or one connection for Windows NT).
- Support for over 100 modems.
- Local network protocol independence, allowing a Remote Access client to log on to any server on any network to which the Remote Access server is connected, regardless of the target server's network protocol, as long as the Remote Access server has the same NetBIOS protocol as the target server.

Choosing and Configuring a Modem on a Windows for Workgroups 3.11 computer

Microsoft has tested with a number of modems on the market and provides direct support for the modems identified in the MODEM.INF file. The MODEM.INF file is used by the RAS client software when the user selects the modem configuration they are using.

To troubleshoot a supported modem

If you are using one of the supported modems listed in the MODEM.INF file, when you set up Remote Access and cannot connect to a RAS server, follow these steps:

1. Make sure your cabling is correct.
2. Check the modem's documentation to verify that the modem has been correctly installed.
3. Try using a terminal emulation program, such as Windows Terminal, to see if you can issue commands to the modem. Be sure to check to make sure Terminal is configured for the proper baud rate and communication settings. More information on using Terminal to troubleshoot your configuration is provided later in this section.

4. If the modem still does not work with the Remote Access Service, call Microsoft Product Support Services (PSS) for assistance.

Unsupported Modems

Modems other than those listed in the MODEM.INF file may also work with the Remote Access Service, even though they are not present in the list and have not yet been tested with the software. If you choose an unsupported modem, for best results, make sure they conform to the following industry standards established by the International Consultative Committee for Telephone and Telegraph (CCITT).

Industry Standards for Modems

Speed in bps	CCITT standard
1200	V.22 or Bell 212A
2400	V.22bis
9600	V.32
14,400	V.32bis

When configuring an unsupported modem for the Remote Access Service, you will have to select from the list of supported modems a modem that matches yours as closely as possible. For best results, make your choice by first comparing entries in the MODEM.INF file with commands for your modem. You can find these commands in your modem's documentation.

To configure an unsupported modem

1. In the Network program group, double-click the Remote Access icon.
2. Install Remote Access Service and from the list of modems, select the modem that is as similar to your unsupported modem as possible.
3. If you configure a new port for the unsupported modem, restart your computer.

If you reconfigure a port already in use, you don't need to restart your computer, but you do need to restart the Remote Access Service.

If you have trouble connecting through an unsupported modem, test the modem's compatibility.

To test a modem's compatibility

1. Check the modem's documentation to make sure you have installed and configured the modem correctly.
2. Make sure that your modem is connected to a serial communication (COM) port on your computer and that your software is set for the same port.
3. Turn on your modem.
4. Check to see if the modem works properly with Windows Terminal. For instructions, see the following procedure, "To Test a Modem with Windows Terminal."

If the test works, you can assume the modem is not malfunctioning.

5. If the modem still does not work after you have verified that it works with Windows Terminal, contact your modem's manufacturer and request a modem command file compatible with the Remote Access Service MODEM.INF file.

To test a modem with Terminal

1. From the Accessories group, double-click the Terminal icon.
2. From the Terminal screen, select Settings.
3. From the Settings menu, choose Communications.
4. In the Communications dialog box, select the bps at which your modem sends and receives data, and select the COM port your modem is connected to. Click OK.
5. On the Terminal screen, type **at** and press ENTER.

Your modem should return "OK," which is echoed on the screen. Some modems return 0, depending on their result code settings.

6. If your modem won't work through Terminal, call the modem's manufacturer.

Modem Compatibility and Speed

Modems from different manufacturers, and even different models from the same manufacturer, may not be completely compatible in all settings and circumstances. Even modems that claim to follow the Hayes AT command set may not be able to communicate with other Hayes-compatible modems in every situation.

High-speed modems may perform their own error-correction and data compression, which you can take advantage of by setting modem features during setup on a server or through the Phone Book on a client.

Compatibility problems increase when you begin to consider high-speed modems of 9600 bps or above because of the way some modems achieve these high speeds of transmission. Even modems that follow the same standards for compression and error correction may be unable to communicate with each other at 9600 bps and may resort to communicating at 2400 bps.

If you plan to connect more than one type of modem to a server, you can assign a different telephone number to each modem. That way, users can choose exactly which modem to connect to. The disadvantage to assigning different telephone numbers to each modem is that users may have to dial several different modems before finding one that is not in use.

Note For rates of 12,000 bps and higher, modem manufacturers often require that computer-to-modem communication occur at 19,200 bps. For this reason, the Remote Access software assumes that modems able to connect at 12,000 or 14,400 bps can function at the computer-to-modem speeds of 19,200 bps or faster. Virtually all high-speed modems are capable of this.

Direct Serial Connections via NULL Modem

You can select a NULL modem to establish a direct serial connection between two computers. Although a direct serial connection eliminates the need for a network adapter card, it is a slow link, and password authentication is still required. A NULL modem configuration works well only for computers physically located near each other.

To configure your system for a direct serial connection

- Select a NULL modem from the list of modems during RAS setup when configuring the COM ports for a serial connection. A null modem must be configured on both the client and the server.

Cable Wiring for NULL Modem Connections

If you are using a NULL modem to make a direct serial connection between two computers, your cable must be wired as shown in the following tables.

Off-the-shelf NULL modem cables might not be wired properly. Be sure to tell your dealer that your NULL modem cables must be wired as shown in the 9-pin or 25-pin NULL modem table.

9-Pin NULL Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
3	2	Transmit Data
2	3	Receive Data
7	8	Request to Send
8	7	Clear to Send
6, 1	4	Data Set Ready and Data Carrier Detect
5	5	Signal Ground
4	6, 1	Data Terminal Ready

25-Pin NULL Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
2	3	Transmit Data
3	2	Receive Data
4	5	Request to Send
5	4	Clear to Send
6, 8	20	Data Set Ready and Data Carrier Detect
7	7	Signal Ground
20	6, 8	Data Terminal Ready

Remote Access Security Features

The Remote Access Service server provided in Windows NT and Windows NT Advanced Server has a wide range of security features. Some of the items included in the RAS security feature set are the following:

- The ability to restrict a user's access to the network once they connect to a RAS server
- The ability to restrict users to the dial-in server only
- The ability to restrict users' access to a part of the network
- Support for dial-back security to restrict users to dialing in from only certain locations.

For more information on the Remote Access security features, please refer to the Windows NT documentation and the *Windows NT Resource Kit*.

RAS Support for ISDN

Integrated services digital network (ISDN) offers a much faster communication speed than the telephone line. The phone line communicates typically at 9600 bits per second (bps), whereas ISDN communicates at speeds of 64 or 128 kilobits per second. Businesses that need this kind of speed usually have a large telecommuting work force or need to do extensive administrative tasks remotely such as installing software on off-site workstations.

To use the RAS client provided with Windows for Workgroups 3.11 to connect to Windows NT or Windows NT Advanced Server via ISDN, it is necessary to have the following:

- ISDN Basic Rate Interface (BRI) service to your remote location. Check with your local telephone company for service availability.
- An ISDN line Network Termination Unit (NT1)
- An ISDN PC board with ISDN drivers (ISDN drivers are available from the manufacturer of your ISDN PC board and may also be available as part of the Windows Driver Library from Microsoft).

See the online RASPHONE.HLP help file provided with Windows for Workgroups 3.11 for more information.

Chapter
8

Integrating with Novell NetWare

Windows for Workgroups 3.11 features improved operability and compatibility with Novell NetWare environments. This chapter discusses of the improved support and describes special information to assist configuring and integrating Windows for Workgroups with Novell NetWare. The information in this chapter supersedes the information contained in Chapter 8, "Network Integration with Microsoft LAN Manager and Novell NetWare," of the *Windows for Workgroups 3.1 Resource Kit*. For more information on configuring Novell components, consult your NetWare documentation.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 1, "Windows for Workgroups 3.11 Architecture;" Chapter 2, "Windows for Workgroups 3.11 Setup and Installation;" Chapter 6, "Integrating with Other Protocols;" Chapter 7, "Integrating with Windows NT and Windows NT Advanced Server;" Chapter 13, "Troubleshooting Windows for Workgroups 3.11."
- Novell NetWare documentation

Contents of This Chapter

Overview of Enhancements to Novell NetWare Support.....	8-3
Installing Support for Novell NetWare	8-4
Required NetWare Support Files for Windows.....	8-4
Obtaining NetWare Client Files and Windows Support Files.....	8-5
Configuring Windows for Workgroups with Novell NetWare	8-9
Installing for Open Datalink Interface Configuration	8-11
Installing for Monolithic IPX Configuration.....	8-16
NetWare Integration Using ARCNet Network Adapter Cards	8-19
Workstation Configuration Files	8-21
NET.CFG and MLID Settings.....	8-23
NET.CFG Link Driver Parameters.....	8-24
32-Bit IPX/SPX-Compatible Transport with NetBIOS.....	8-25
Novell NetWare Connectivity	8-27
NetBIOS Services over IPX	8-28
Specific Novell NetWare Issues	8-29
LastDrive Parameter in CONFIG.SYS.....	8-29
Log On to NetWare Server Before Starting Windows	8-31

Sample Files for Configuration Scenarios	8-31
Open Datalink Interface Configuration	8-31
Monolithic IPX Configuration	8-34
MSIPX Configuration	8-36
NDIS 2.0 Protocols on ODI Drivers.....	8-39
Installing the ODINSUP Driver for Use with Microsoft TCP/IP for NetWare 3.x.....	8-39
Installing the ODINSUP Driver for Use with Microsoft TCP/IP for NetWare 4.x.....	8-46

Overview of Enhancements to Novell NetWare Support

Windows for Workgroups 3.11 greatly enhances the interoperability with Novell NetWare over the support provided by Windows for Workgroups 3.1. The additional support for integrating with NetWare includes:

Improved NetWare network adapter card driver support

- The ability to install Windows for Workgroups networking components on top of Open Datalink Interface (ODI) network adapter card driver
- The ability to install Windows for Workgroups networking components on top of IPX monolithic protocol stack (IPX.COM)
- Support for Windows for Workgroups and NetWare interoperability when using ARCNet network adapter cards

Improved network redirector support

- Support for running Windows for Workgroups in conjunction with the NetWare 3.x or 4.x workstation shell

Improved networking support and functionality

- Support for Windows for Workgroups peer sharing over IPX, allowing Windows for Workgroups computers to interoperate across an IPX router
- 32-bit protected-mode implementation of an IPX/SPX-compatible protocol for IPX/SPX applications, providing network connectivity to other Windows for Workgroups 3.11 computers, as well as network connectivity to Windows NT and Windows NT Advanced Server
- Improved virtualization of the IPX protocol when the 32-bit IPX/SPX compatible protocol provided with Windows for Workgroups is used
- 32-bit protected-mode implementation of NetBIOS services to provide better performance than Novell's real-mode NetBIOS driver while eliminating conventional memory footprint

Installing Support for Novell NetWare

To support Novell NetWare integration with Windows for Workgroups, the workstation on which you are installing Windows for Workgroups should be properly configured to connect to a NetWare server. This requires that the workstation is configured with either the monolithic IPX driver (IPX.COM), or an ODI driver in addition to either a NetWare 3.x or 4.x workstation shell to access file or print services from a NetWare server. Novell recommends that NetWare users use ODI-based drivers rather than the monolithic IPX driver.

If the workstation is preconfigured with the Novell drivers, the Windows for Workgroups 3.11 setup program will detect these drivers and will automatically configure Novell NetWare support in addition to installing the Windows for Workgroups 3.11 networking components.

If the workstation is not correctly configured with the necessary Novell drivers, this must be done as described in the NetWare documentation before installing Windows for Workgroups 3.11.

Note that Windows for Workgroups 3.11 does not support NetWare interoperability using NDIS network adapter card drivers, nor do any NetWare components ship with Windows for Workgroups 3.11. Information on obtaining the necessary Novell files (or updates for the latest versions of the Novell files) is discussed later in this section.

Required NetWare Support Files for Windows

In addition to the base Novell NetWare client software, which consists of the NetWare redirector and IPX protocol, required to communicate with a NetWare server, there are some additional NetWare support files necessary for the Novell components to work properly in the Windows environment. These required NetWare files are written and provided by Novell. They include the following:

File(s)	Description
netware.drv, netware.hlp	Windows network driver and associated help file to provide access to network redirector functionality from Windows File Manager.
nwpopup.exe	NetWare messaging utility. Used to receive messages and alerts from a NetWare server.
vnetware.386	Virtual device driver providing virtualization services for NetWare redirector for Windows environment and across MS-DOS virtual machines.
vipx.386	Virtual device driver providing virtualization services for NetWare IPX protocol for Windows environment and across MS-DOS virtual machines.

When Windows for Workgroups 3.11 is configured to support Novell NetWare in addition to Windows for Workgroups network functionality, Setup will check to see if these files reside in the Windows directory. If the files are not in the Windows directory, Setup will prompt the user for a disk or network drive location for these files.

Obtaining NetWare Client Files and Windows Support Files

If your workstation is not configured with the necessary NetWare client software, or if you don't have the Windows support files that Windows for Workgroups Setup requires to properly configure your workstation, several sources are available from which they may be obtained. The files that make up the NetWare client software for different configuration scenarios will be discussed later in this chapter.

Important It is highly recommended that you use the *latest* version of Novell driver files that are available. If you are using drivers dated or with versions numbered earlier than those listed in this section, you should obtain updated drivers.

To obtain the necessary software files, check the following sources:

- First check with your NetWare system administrator to see if he or she has the latest client files.
- Check the Novell Files forum (or Novell Library forum) on CompuServe by typing **go novfiles** at a system prompt. Novell posts the latest revisions of their NetWare client software and drivers on this forum. Alternatively, check the Novell Library forum by typing **go novlib** at a system prompt.
- Contact Novell or your local Novell representative.

As of October 1, 1993, Novell was offering the following files on the Novell Files forum:

DOSUP7.EXE dated 8/18/93

DOSUP7.EXE contains updated DOS client files. This file includes NetWare shells version 3.32 (NETX.EXE, EMSNETX.EXE, XMSNETX.EXE, BNETX.EXE), compatible with MS-DOS 3.0 and above, and Windows 3.0 and 3.1. This file also includes shells for MS-DOS 6.0. Support for both ODI and dedicated (monolithic) IPX are included as well as Packet Burst, NetBIOS and other DOS client files.

To ensure you are using the latest versions of the Novell drivers, the files contained in the DOSUP7.EXE file include:

Self-Extracting File Name: DOSUP7.EXE

Files Included	Size	Date	Time
DOSUP7.TXT		readme file	
DOSNP.EXE	9971	5-26-92	11:00a
EMSNETX.EXE	89390	2-17-93	1:43p
HISTORY.DOC	20674	4-20-93	2:57p
IPXODI.COM	30051	1-22-93	9:48a
INT2F.COM	640	7-28-88	11:48a
IPX.OBJ	20340	11-21-91	12:50a
LANSUP.COM	21943	2-02-93	11:54a
LSL.COM	8780	11-05-92	2:40p
NETX.EXE	77582	2-17-93	1:41p
NE1000.COM	19791	1-14-93	2:27p
NE1500T.COM	29242	12-21-92	2:25p
NE2.COM	20176	1-14-93	2:00p
NE2000.COM	21049	1-18-93	11:48a
NE2100.COM	29240	12-21-92	2:25p
NE2_32.COM	19887	1-14-93	2:28p
NE3200.COM	26552	2-08-93	1:51p
NETBIOS.EXE	24162	1-21-93	2:45p
ODINSUP.DOC	42015	4-08-93	10:15a
ODIINFO.DOC	24499	12-09-92	2:43p
ODINSUP.COM	33867	2-23-93	8:58a
PCN2L.COM	21058	2-13-93	8:06a
PBURST.NLM	95736	11-12-92	10:34a
ROUTE.COM	4881	7-02-92	1:40p
RPLFIX.COM	1746	9-30-91	9:39a
RPLFIX.DOC	2255	2-21-91	2:47p
RPLODI.COM	1652	3-21-91	2:24p
TBMI2.COM	25018	1-28-93	1:31p
TOKEN.COM	25012	12-21-92	2:39p
TRXNET.COM	18765	12-21-92	2:27p
XMSNETX.EXE	86064	2-17-93	1:45p

The following list shows version of the files included in DOSUP7.EXE. Files changed since last update are marked with an asterisk (*). Note that no further development is being done on IPX.OBJ. Novell recommends you use the ODI client software.

DOSNP.EXE: NetWare DOS NP Extender v1.30 Rev G (920526)
 * EMSNETX.EXE: NetWare EMS Workstation Shell v3.32 (930217)
 INT2F.COM: Novell Network BIOS Interrupt 2Fh Emulator V2.12 (880728)
 IPX.OBJ: Novell IPX/SPX v3.10 (911121)
 * IPXODI.COM: NetWare IPX/SPX Protocol v2.10 (930122)
 * LANSUP.COM: IBM LAN Support MLID v1.27 (930202)
 * LSL.COM: NetWare Link Support Layer v2.01 (921105)

```

* NE1000.COM: Novell NE1000 Ethernet MLID v1.27 (930114)
* NE1500T.COM: Novell NE1500T Ethernet MLID v1.26 (921221)
* NE2.COM: Novell NE2 Ethernet MLID v1.26 (930114)
* NE2_32.COM: Novell NE2-32 Ethernet MLID v1.29 (920114)
* NE2000.COM: Novell NE2000 Ethernet MLID v1.51 (930118)
* NE2100.COM: Novell NE2100 Ethernet MLID v1.26 (921221)
* NE3200.COM: Novell NE3200 Ethernet MLID v1.16 (930208)
* NETBIOS.EXE: Novell NetBIOS Emulation Package V3.13 (930121)
* NETX.EXE: NetWare Workstation Shell v3.32 (930217)
* ODINSUP.COM: ODI Support Interface for NDIS v1.22 (930223)
  PBURST.NLM: NCP Packet Burst, Large Internet Packet & Packet
  Sig. Support
* PCN2L.COM: IBM PC Network II & II/A MLID v1.40 (920213)
* ROUTE.COM: NetWare Source Routing Driver v2.00 (920702)
  RPLFIX.COM: NetWare Boot Disk Image Patch Program v1.02
  RPLODI.COM: Novell RPL ODI v1.02 (910321)
* TBMI2.COM: Task Switched Buffer Manager for IPX/SPX v3.11
* TOKEN.COM: IBM Token-Ring MLID v1.25 (921221)
* TRXNET.COM: Novell Turbo RxNet & RxNet/2 MLID v1.35 (921221)
* XMSNETX.EXE: NetWare XMS Workstation Shell v3.32 (930217)

```

WINUP7.EXE dated 8/18/93

WINUP7.EXE contains updated Windows client files. This file includes the NetWare Driver Set version 2.02 for Windows 3.0 and 3.1 and related files. Support for IPX/SPX under Windows 3.0 and 3.1 is included.

To ensure you are using the latest versions of the Novell drivers, the files contained in the WINUP7.EXE file include:

```

Self-Extracting File Name: WINUP7.EXE
-----
Files Included      Size      Date      Time
-----
WINUP7.TXT          readme file
NETWARE.DRV        126144    10-27-92    7:38a
NETWARE.HLP        34348     2-12-92     3:12p
NWPOPOP.EXE        4208      10-28-92    10:32a
VIPX.386           24362     9-04-92     1:01p
VNETWARE.386       10093     10-19-92    3:55p
NWIPXSPX.DLL       30016     10-31-92    12:53a
TBMI2.COM          17999     12-04-91    2:46p
TBMI.COM           17089     7-10-91     12:27a
VPICDA.386         11063     1-30-91     10:58a
TASKID.COM         2623      12-19-90    3:48p
NETAPI.DLL         7168      6-24-91     11:05a
NWNETAPI.DLL       106047    1-23-92     4:36p
NWPSERV.DLL        11616     8-02-91     1:22a
BINDFIX.EXE        63297     2-12-91     2:10p
-----

```

Version of the files included in WINUP7.EXE:

```

BINDFIX.EXE:    v3.52
NETAPI.DLL:    v1.3D
NETWARE.DRV:   v2.02 (021026)
NWIPXSPX.DLL:  v1.32
NWNETAPI.DLL:  v1.30
NWPOPOP.EXE:   v2.02 (021027)
NWPSEV.DLL:    v1.22
NWSAP.DLL:     v1.22
TASKID.COM:    Task Identification Program - v1.0
TBMI.COM:      Task Switched Buffer Manager for IPX/SPX - v1.1
TBMI2.COM:     Task Switched Buffer Manager for IPX/SPX - v2.1
VIPX.386:     v1.13 (920903)
VNETWARE.386: v1.06 (921015)
VPICDA.386:   v3.02

```

VLMUP1.EXE dated 6/29/93

VLMUP1.EXE contains updated Virtual Loadable Module (VLM) components (v1.02) to work with NetWare 4.0 and above. Those using version 1.01 of the NetWare Client for DOS/Windows can use these files to solve various problems.

The following files are included in this revision:

Self-Extracting File Name: VLMUP1.EXE

Files Included	Size	Date	Time
VLMUP1	TXT	readme file	
AUTO	VLM	4250	05-10-93 12:57p
BIND	VLM	4616	05-10-93 12:57p
CONN	VLM	10289	05-10-93 12:56p
FIO	VLM	18008	05-10-93 12:57p
GENERAL	VLM	3996	05-10-93 12:57p
HISTORY	DOC	3836	06-15-93 2:19p
IPXNCP	VLM	8056	05-10-93 12:56p
NDS	VLM	10360	05-10-93 12:56p
NETX	VLM	14906	05-10-93 12:57p
NWP	VLM	6324	05-10-93 12:57p
PRINT	VLM	7301	05-10-93 12:57p
REDIR	VLM	12367	05-10-93 12:57p
RSA	VLM	19552	05-10-93 12:58p
SECURITY	VLM	7978	05-10-93 12:57p
TRAN	VLM	1545	05-10-93 12:56p
VLM	EXE	35408	05-10-93 12:56p

Version of the files included in WINUP7.EXE:

```

RSA.VLM:        NetWare RSA authentication module v1.02
                 (930510)
IPXNCP.VLM:     NetWare IPX transport module v1.02 (930510)
TRAN.VLM:       NetWare transport multiplexor module v1.02
                 (930510)
NDS.VLM:        NetWare directory services protocol module v1.02
                 (930510)
BIND.VLM:       NetWare bindery protocol module v1.02 (930510)

```

```

NWP.VLM:      NetWare protocol multiplexor module v1.02
              (930510)
SECURITY.VLM: NetWare security enhancement module v1.02
              (930510)
AUTO.VLM:     NetWare auto-reconnect module v1.02 (930510)
PRINT.VLM:    NetWare printer redirection module v1.02
              (930510)
REDIR.VLM:    NetWare DOS redirector module v1.02 (930510)
FIO.VLM:      NetWare file input-output module v1.02 (930510)
NETX.VLM:     NetWare workstation shell module v4.00 (930510)
GENERAL.VLM:  NetWare general purpose function module v1.02
              (930510)
CONN.VLM:     NetWare connection table manager v1.02 (930510)
VLM.EXE:      NetWare virtual loadable module manager v1.02
              (930510)

```

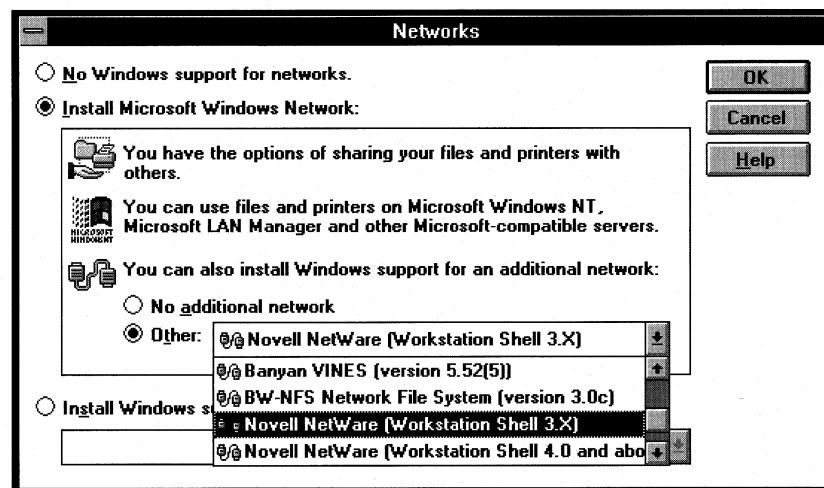
Configuring Windows for Workgroups with Novell NetWare

If the Novell NetWare client software is loaded and running at the time Windows for Workgroups is installed, Setup will detect the NetWare configuration and automatically select Novell NetWare as an additional network.

If the NetWare client software is not running at the time Windows for Workgroups is installed, it is necessary to configure Windows for Workgroups to work in conjunction with the NetWare client software. To configure Windows for Workgroups to work properly with the NetWare workstation shell, choose the appropriate additional network option to match the version of the Novell NetWare Workstation Shell you are using. Windows for Workgroups supports Workstation Shells version 3.x, and version 4.0 and above as shown in Figure 8.1.

Figure 8.1

Configuring Novell NetWare support as an additional network



Once Windows for Workgroups Setup is run and “Novell NetWare (Workstation Shell 3.x)” or “Novell NetWare (Workstation Shell 4.0 and above)” is selected as an additional network (in conjunction with the Microsoft Windows Network), the network detection code will attempt to determine the NetWare driver model you are using.

Important

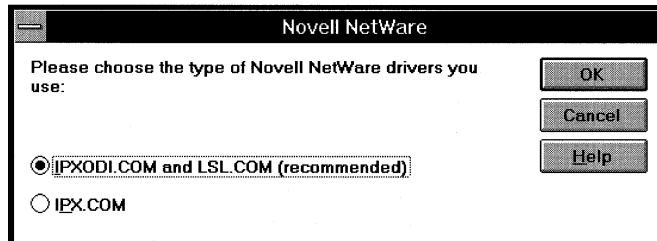
It is important that the Novell NetWare client software including network adapter card drivers be loaded and that you are able to successfully connect and use resources on a NetWare server at the time you install Windows for Workgroups. This will help to ensure Windows for Workgroups can properly detect your configuration to allow your installation of Windows for Workgroups on Novell drivers to be successful.

For example, if you have started the NetWare client software (including loading the network adapter card driver and the network redirector), Windows for Workgroups Setup will detect the ODI Multiple Link Interface Driver (MLID) you have loaded and where query the name of the MLID to add to the PROTOCOL.INI file that Windows for Workgroups uses.

If for some reason Windows for Workgroups is unable to detect the driver model and network adapter card driver (for example, you have not started the NetWare client software), Setup will display the dialog box as shown in Figure 8.2. If Windows for Workgroups Setup is able to detect the driver model you are using, the Novell NetWare dialog box will not be displayed.

Figure 8.2

Novell NetWare network adapter card driver model dialog box

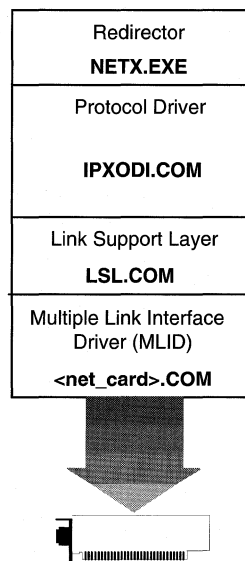


If you are using ODI drivers, choose the “IPXODI.COM and LSL.COM (recommended)” selection. If you are using monolithic/dedicated IPX, select the “IPX.COM” choice. The proper selection is important for Windows for Workgroups to install the necessary support files to be able to run on top of the Novell driver models.

Installing for Open Datalink Interface Configuration

The Open Datalink Interface (ODI) specification was defined by Novell Corporation and Apple Computer Corporation to simplify driver development and to provide support for multiple protocols on a single network adapter. Similar to NDIS in many respects, ODI provides a protocol, a consistent API to communicate with a network adapter card driver, and supports the use of multiple protocols on a network adapter card driver. Novell recommends using ODI-based client software rather than dedicated IPX drivers. To provide the most flexibility in Windows for Workgroups 3.11 for other protocol support along with NetWare integration, ODI drivers should be used.

Figure 8.3
ODI driver model



ODI consists of three main components:

- The Link Support Layer (LSL), LSL.COM, provides a foundation for network adapter card drivers to communicate with multiple protocol drivers, and for protocol drivers to communicate with multiple network adapter card drivers. LSL.COM performs functions similar to the protocol manager in LAN Manager and Windows for Workgroups 3.1x.

- The Multiple Link Interface Driver (MLID) is the ODI-compliant network adapter card driver created by the adapter card manufacturer. This component usually identifies the name of the supported adapter in the filename. Examples of MLIDs include NE2000.COM for the Novell NE-2000 card, 3C509.COM for the 3-COM Etherlink III card, and EXP16ODI.COM for the Intel EtherExpress 16 card.
- The ODI-compliant version of the IPX/SPX protocol, IPXODI.COM, is used in place of the monolithic IPX.COM driver on a workstation configured with ODI drivers. This serves as the network protocol for communicating between a NetWare client and a NetWare server.

A workstation using ODI and the IPX protocol would have the following file entries in its AUTOEXEC.BAT:

Component	Function
LSL.COM	The link support layer
NE2000.COM	The hardware dependent MLID (varies, depending on network adapter card)
IPXODI.COM	The ODI-IPX compatible protocol driver
NETX.EXE	The NetWare redirector

Before Installing Windows for Workgroups on ODI Drivers

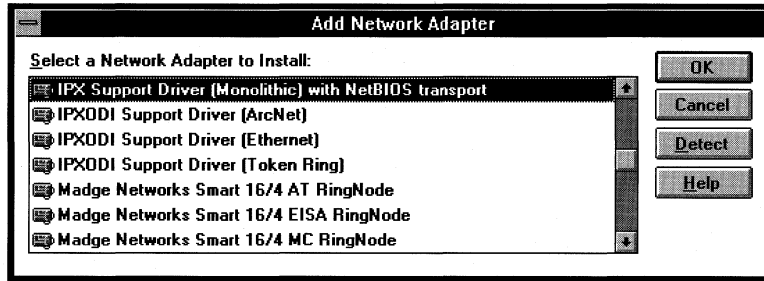
It is important that the real-mode ODI IPX network is configured and working properly *before* installing Windows for Workgroups 3.11. Before installing Windows for Workgroups 3.11, test to confirm that there are no errors when loading LSL.COM, IPXODI.COM, and MLID, and NETX.EXE, or when accessing resources on NetWare servers.

If the NetWare ODI drivers are installed and running on the computer when Windows for Workgroups 3.11 is installed, Setup detects that ODI drivers are being used and will automatically identify the network adapter card and configure Windows for Workgroups to run on top of the ODI drivers.

If Windows for Workgroups is unable to identify the ODI MLID being used, it may be necessary to manually configure the network adapter. In this case, the appropriate IPXODI Support Driver should be chosen to match the type of network adapter card you are using. For example, if you are using an Ethernet adapter, you should choose the "IPXODI Support Driver (Ethernet)" as your network adapter.

Figure 8.4

IPXODI Support Driver listing for manually adding ODI support



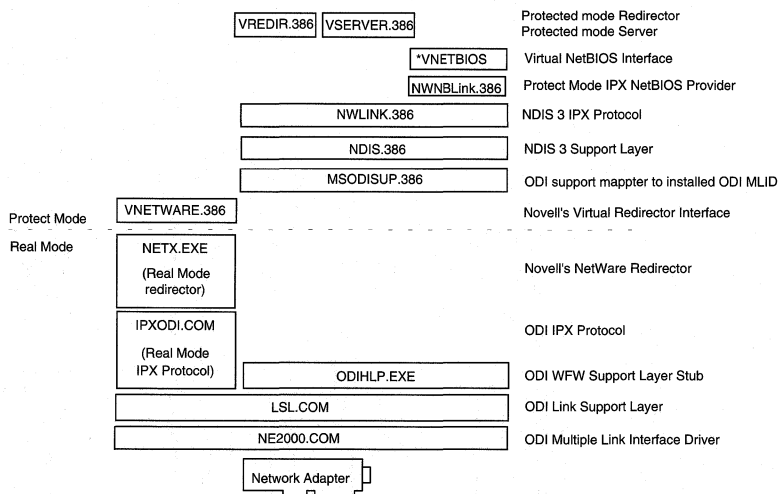
When Windows for Workgroups 3.11 is installed on top of ODI drivers, the IPX/SPX compatible transport with NetBIOS is installed by default from the Protocol Setup dialog box. This provides the 32-bit implementation of the IPX/SPX compatible transport and loads the NetBIOS service provider support.

Components of the Default IPX ODI Stack

Once Windows for Workgroups 3.11 has been installed to run on top of the ODI driver configuration, the final configuration of drivers resembles Figure 8.5:

Figure 8.5

Driver configuration in the default ODI IPX configuration



A description of the Novell drivers involved with this configuration scenario follows:

Novell Drivers	Description
NE2000.COM - MLID driver	ODI MLID network adapter card driver from network adapter card vendor or Novell (varies with network adapter card used)
LSL.COM	Link Support Layer (LSL) driver from Novell
IPXODI.COM	Real-mode IPX protocol for use with NetWare redirector from Novell
NETX.EXE	NetWare redirector from Novell
VNETWARE.386	NetWare redirector virtual device driver from Novell

Note Since the virtualization of the IPX protocol is handled by the NWLINK.386 virtual device driver provided with Windows for Workgroups 3.11, the Novell VIPX.386 virtual device driver is not needed and is removed if previously present. More information on the 32-bit IPX/SPX compatible protocol (NWLink) is provided later in this Chapter).

A description of the Microsoft drivers involved with this configuration scenario follows:

Microsoft Drivers in Windows for Workgroups	Description
ODIHLP.EXE	Real-mode stub for ODI support layer
MSODISUP.386	NDIS to ODI Mapping Support layer
NDIS.386	NDIS Support layer
NWLink.386	32-bit IPX/SPX compatible protocol virtual device driver
NWNBLink.386	NetBIOS services provider virtual device driver for supporting NetBIOS applications with the NWLink protocol
*VNETBIOS	Virtual device driver for virtualizing NetBIOS services in Windows and across MS-DOS virtual machines.

When Windows for Workgroups is installed over an ODI configuration, the IPX/SPX Compatible Transport with NetBIOS and NetBEUI NDIS 3.0 protocols, are installed by default.

Windows for Workgroups ODI Support Files

An NDIS 3.0 protocol driver (such as NWLINK.386 or NETBEUI.386) can bind to an ODI driver with the help of two support files:

- MSODISUP.386 is the ODI support layer which maps NDIS 3.0 protocols to an ODI MLID.
- ODIHLP.EXE is the real-mode stub that allows LSL to complete its binding process in real mode (similar to NDISHLP.SYS). It hooks all the real-mode entry points so that MSODISUP.386 can use this information when working in protected mode.
- ODIHLP.EXE acts as a default stack for all frame types. That is, ODIHLP will accept any packet that is of one of the frame types listed in the NET.CFG file. More information on the NET.CFG file and its entries are provided later in this chapter.

With LSL 2.01 or later, multiple default stacks are supported, called default chained stacks. ODIHLP.EXE will bind as a default chained stack on current LSL versions. If another ODI compliant protocol loads and is registered as a default stack, then ODIHLP.EXE loads after that protocol.

Driver Versions

The base versions of Novell drivers for the ODI IPX configuration should be as listed below. To obtain the latest Novell drivers, see the “Obtaining NetWare Client Files and Windows Support Files” section earlier in this chapter.

MS-DOS Drivers

In addition to the MS-DOS drivers listed below, you should confirm that your ODI MLID driver for your network adapter card is the latest version. The NETX NetWare workstation shell 3.x is listed, if you are using the NetWare 4.x client software, you should be using version 4.0 of the NETX.VLM, and version 1.02 of the other VLM client support files.

Driver name	File Date	Description and version number
LSL.COM	11-05-92	NetWare Link Support Layer v2.01 (921105)
IPXODI.COM	1-22-93	NetWare IPX/SPX Protocol v2.10 (930122)
NETX.EXE	2-17-93	NetWare Workstation Shell v3.32 (930217)

Windows Drivers

Driver name	File date	Version number
NETWARE.DRV	10-27-92	v2.02 (021026)
NETWARE.HLP	2-12-92	
VNETWARE.386	10-19-92	v1.06 (921015)
NWPOPUP.EXE	10-28-92	v2.02 (021027)

Installing for Monolithic IPX Configuration

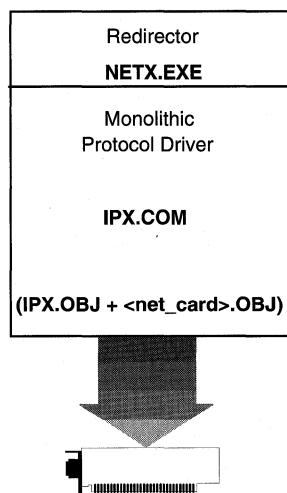
The monolithic/dedicated implementation of the IPX protocol, IPX.COM, is used by many of the installed base of NetWare workstations. IPX.COM is called *monolithic* because it contains the NetWare IPX/SPX protocol stack and the network adapter card driver for communicating with the network adapter in one code module or driver file.

When Windows for Workgroups is configured to run on top of a monolithic/dedicated IPX driver, NetBIOS is used to support Windows for Workgroups peer services over real mode IPX. Support for peer sharing over IPX requires NetBIOS when using monolithic IPX drivers.

Note Novell recommends that the ODI client software be used instead of the dedicated IPX drivers—information on using Windows for Workgroups with an ODI configuration is discussed in the previous section.

Figure 8.6

Monolithic IPX model



IPX.COM is generated from the IPX.OBJ file and a particular network adapter card driver file (*net_card.OBJ*) using the NetWare SHGEN or WSGEN programs. IPX.COM must be configured for each individual workstation based on the individual network adapter card and its hardware configuration (IRQ, I/O address, RAM address in the upper memory area and DMA channel).

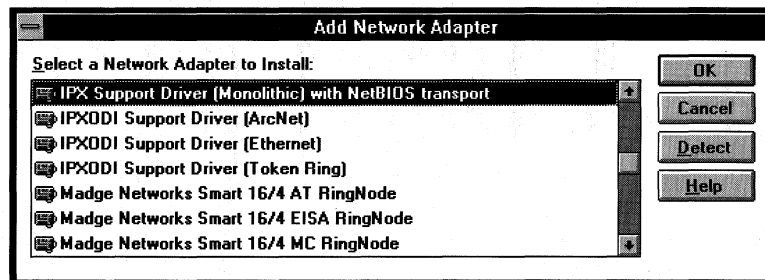
Before Installing Windows for Workgroups on top of Monolithic IPX

It is important that the real-mode monolithic IPX network is configured and working properly *before* installing Windows for Workgroups 3.11. Before installing Windows for Workgroups 3.11, test to confirm that there are no errors when loading IPX.COM and NETX.EXE or when accessing resources on NetWare servers.

If Windows for Workgroups is unable to detect your IPX.COM configuration (for example, the IPX.COM file has not been loaded at the time Windows for Workgroups is installed), choose the "IPX.COM" selection from the Novell NetWare dialog box as shown in Figure 8.1. Selecting "IPX.COM" configures Windows for Workgroups the same as if the user manually selects the "IPX Support Driver (Monolithic) with NetBIOS protocol" item from the Add Network Adapter dialog box as shown in Figure 8.7.

Figure 8.7

Manually adding IPX Support Driver (Monolithic) with NetBIOS protocol for monolithic IPX configuration

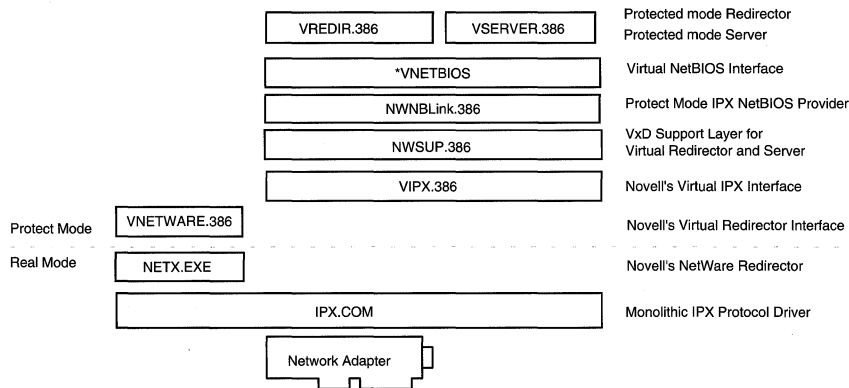


Components of the Default Monolithic IPX Stack

Once Windows for Workgroups has been installed to run on top of the monolithic IPX configuration, the final configuration of drivers resembles that shown in the following Figure 8.8.

Figure 8.8

Driver configuration in the default monolithic IPX configuration



A description of the Novell drivers involved with this configuration scenario follows:

Novell Driver	Description
IPX.COM	Monolithic IPX driver from Novell
NETX.EXE	NetWare redirector from Novell
VNETWARE.386	NetWare redirector virtual device driver from Novell
VIPX.386	NetWare IPX virtual device driver from Novell

A description of the Microsoft drivers involved with this configuration scenario follows:

Driver from Windows for Workgroups	Description
NWSUP.386	NetWare support file from Windows for Workgroups 3.11. This driver is used to support running the Windows for Workgroups network redirector and network server on top of monolithic IPX.
NWNBLink.386	NetBIOS services provider virtual device driver for supporting NetBIOS on top of IPX protocol from Windows for Workgroups 3.11.
*VNETBIOS	Virtual device driver for virtualizing NetBIOS services in Windows and across MS-DOS virtual machines.

Information on sample configurations for Windows for Workgroups running on top of monolithic IPX drivers is provided later in this chapter.

Driver Versions

The base versions of Novell drivers for the dedicated IPX configuration should be as listed below. To obtain the latest Novell drivers, see the “Obtaining NetWare Client Files and Windows Support Files” section earlier in this chapter.

MS-DOS Drivers

Driver name	File date	Description and version number
IPX.OBJ	11-21-91	Novell IPX/SPX v3.10 (911121)
NETX.EXE	2-17-93	NetWare Workstation Shell v3.32 (930217)

Windows Drivers

Driver name	File date	Version number
NETWARE.DRV	10-27-92	v2.02 (021026)
NETWARE.HLP	2-12-92	
VNETWARE.386	10-19-92	v1.06 (921015)
NWPOPUP.EXE	10-28-92	v2.02 (021027)

NetWare Integration Using ARCNet Network Adapter Cards

Windows for Workgroups 3.11 allows users to support connectivity to Novell NetWare servers as well as other Windows for Workgroups computers over an ARCNet network. Windows for Workgroups 3.1 supported connectivity with other Windows for Workgroups computers running over an ARCNet network, but support for concurrent NetWare integration functionality was not provided.

When Windows for Workgroups is configured to support NetWare integration over ARCNet, NetBIOS is used to support Windows for Workgroups peer services over IPX. Direct hosting over IPX without NetBIOS is not supported when using real-mode IPX on ARCNet network adapter cards. This is true whether a monolithic/dedicated IPX driver or an ODI ARCNet MLID is being used.

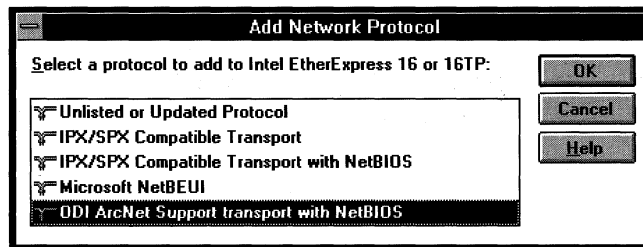
If the ArcNet MLID and NetWare workstation shell are running when Windows for Workgroups 3.11 is installed, Windows for Workgroups Setup will detect your configuration and automatically install the proper components.

However, if you are using a generic ArcNet MLID or Windows for Workgroups is unable to detect that you are using an ArcNet driver, it may be necessary to manually configure Windows for Workgroups to run on top of your ArcNet

configuration. In addition to configuring Windows for Workgroups to run on top of an ODI or monolithic/dedicated IPX driver, you will also need to select and install the “ODI ArcNet Support transport with NetBIOS” from the Add Network Protocol dialog box as shown in Figure 8.9 if you are using an ODI MLID. Selecting this network protocol will install the necessary support files for Windows for Workgroups to support peer services over your ArcNet network card. As noted above, if Windows for Workgroups 3.11 Setup is able to detect your configuration properly, this network protocol will automatically be installed when you are using an ODI ArcNet MLID.

Figure 8.9

Add ODI ArcNet Support protocol with NetBIOS protocol for use with ODI ArcNet drivers

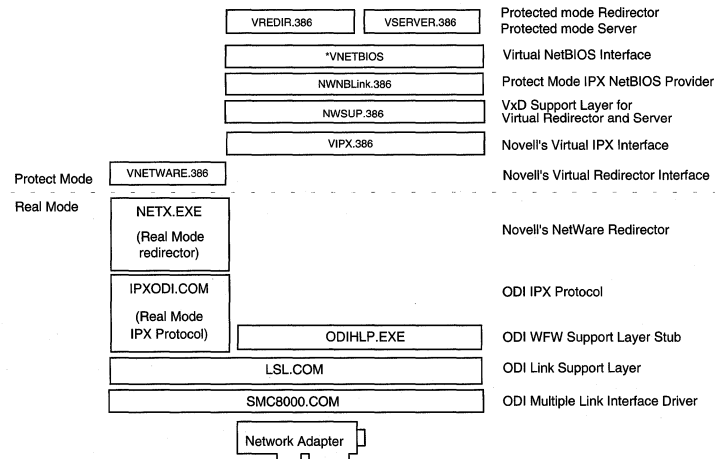


Components of the IPX ODI Stack on ARCNet

Once Windows for Workgroups 3.11 has been installed to run on top of the ARCNet ODI driver configuration, the final configuration of drivers resembles the following Figure 8.10.

Figure 8.10

ARCNet configuration using ODI drivers



Note This configuration is very similar to configuring Windows for Workgroups 3.11 to run on top of monolithic/dedicated IPX drivers, except that ODI drivers are used.

A description of the Novell drivers involved in this configuration scenario follows:

Novell Drivers	Description
SMC8000.COM - MLID driver	ODI MLID network adapter card driver from network adapter card vendor or Novell (varies depending on network adapter card used)
LSL.COM	Link Support Layer (LSL) driver
IPXODI.COM	Real-mode IPX protocol for use with NetWare redirector from Novell
NETX.EXE	NetWare redirector from Novell
VNETWARE.386	NetWare redirector virtual device driver from Novell
VIPX.386	IPX virtual device driver from Novell

A description of the Novell drivers involved in this configuration scenario follows:

Driver from Windows for Workgroups	Description
NWSUP.386	NetWare support file from Windows for Workgroups 3.11. This driver is used to support running the Windows for Workgroups network redirector and network server on top of monolithic IPX.
NWNBLink.386	NetBIOS services provider virtual device driver for supporting NetBIOS on top of IPX protocol from Windows for Workgroups 3.11.
*VNETBIOS	Virtual device driver for virtualizing NetBIOS services in Windows and across MS-DOS virtual machines.

Workstation Configuration Files

Just as CONFIG.SYS and AUTOEXEC.BAT setup the local environment, either of two workstation configuration files—SHELL.CFG or NET.CFG—is responsible for the setup and configuration of the network environment for the workstation. SHELL.CFG and NET.CFG are ASCII files used to configure custom workstation parameters for NETX, IPX, NetBIOS or the general NetWare environment.

NetWare began using SHELL.CFG as the configuration file name with monolithic IPX, and is now using NET.CFG for ODI. NET.CFG is the preferred file name to use and has some very specific uses for the Open Datalink Interface that will be discussed later in this section.

If both SHELL.CFG and NET.CFG exist, both are processed (first SHELL.CFG, then NET.CFG). Any NET.CFG settings duplicated from SHELL.CFG are ignored. Neither SHELL.CFG nor NET.CFG are required for a NetWare workstation. If these files do not exist, default settings are used.

If you are using ODI drivers, LSL.COM uses information from the NET.CFG file to configure the MLID before the NETX shell does. LSL will look for the NET.CFG in the current directory, execution directory, or the directory specified by the “/C=*pathname*” command line parameter when LSL.COM is invoked.

Important It is important that LSL find the proper NET.CFG file. To verify that you do not have more than one NET.CFG file, type “**dir \net.cfg /s**” at the MS-DOS command prompt (or select the Search option from the File menu in File Manager and search for NET.CFG from your root directory) to identify any NET.CFG files that may be present on your system.

SHELL.CFG and/or NET.CFG are processed by the IPX protocol driver and NETX.EXE when they are invoked. By default the system looks for the .CFG file in the same directory as NETX.EXE. To override this default behavior, run NETX.EXE (or the IPX protocol driver) with the “/c=*drive:pathfilename*” command line switch. Example:

```
NETX /c=d:\netstuff\net.cfg
```

Using the “/c=*drive:pathfilename*” will only load the single .CFG file specified.

Below is are sample entries from a SHELL.CFG file containing NetWare environment information. Consult your NetWare documentation for specific information on the various settings supported by the SHELL.CFG and NET.CFG files.

Sample .CFG File

```
FILE HANDLES=60  
SHOW DOTS=ON  
PREFERRED SERVER=NW_311
```

Special Configuration File Settings

A NetWare file server does not include the directory entries dot (.) and double dot (..) as MS-DOS does. However, the NetWare shell (version 3.01 or later) can emulate these entries when applications attempt to list the files in a directory. If you have problems listing files or deleting directories, turn on the Show Dots feature. To do this, add the following line to the beginning of your NET.CFG file:

```
show dots=on
```

Turning on Show Dots will cause problems with earlier versions of some 80286-based NetWare utilities, such as BINDFIX.EXE and MAKEUSER.EXE. Make sure you upgrade these utilities if you upgrade your NetWare shell. For more information, contact your Novell dealer.

By default, NetWare allows you access to only 40 files at a time. When you are running applications with Windows, you can exceed this limit rather quickly. If you do, you might see unexpected error messages. To increase the file access limit, add the following line to the beginning of your NET.CFG file:

```
file handles=60
```

You should also add the following to your CONFIG.SYS file:

```
files=60
```

See the NETWORKS.WRI file provided with Windows for Workgroups 3.11 for additional information on Novell NetWare configuration file settings.

NET.CFG and MLID Settings

Since an ODI workstation can have multiple MLIDs and multiple protocols loaded and bound, ODI uses the NET.CFG configuration file to identify the network adapter card and protocol configuration and binding information. NET.CFG for ODI is similar to the PROTOCOL.INI file used for NDIS.

The monolithic implementation of IPX does not require a settings file because there is only one protocol and one network adapter card driver and they are bound together in a specific way. The IPX.COM file contains the network adapter card configuration information, including the interrupt and base memory address used by the card.

The NET.CFG is not required. The MLID assumes the default configuration of the network adapter card. When loading *only* IPXODI, the default binding is to the first MLID loaded.

Just like the PROTOCOL.INI, NET.CFG for ODI consists of section headings and settings. Section headings are left-justified and the settings within the section are indented with a space (or combination of spaces) or a tab.

Network adapter card configuration information is contained in a Link Driver section. In the Link Driver section for the network adapter card, you can specify the network adapter card's interrupt, I/O address, memory address, frame types and protocols installed.

Note The LSL driver loads and initializes information contained in the NET.CFG file. The NET.CFG file should reside in the same directory as LSL.COM and the Novell NETX.EXE network redirector.

An example of a sample NET.CFG file is shown below:

Sample NET.CFG for an SMC Ethercard Plus Elite 16

```
show dots=on
file handles=60
preferred server=NW_311
Link Driver SMC8000
    int 5
    port 240
    mem D000
    Frame Ethernet_802.3
    Protocol IPX 00 Ethernet_802.3
```

NET.CFG Link Driver Parameters

The following table lists selected information commonly found in the NET.CFG file under the **Link Driver** section. As described in the previous section, not all of this information may be in the NET.CFG file. For information not found in the NET.CFG file, default settings for the network adapter card are assumed. Consult your NetWare documentation for more information on the parameters used in the NET.CFG file.

Parameter	Description
DMA	DMA Channel Number. Can assign up to two DMA channels by designating them "DMA #1 x" and "DMA #2 y".
INT	IRQ Number. Can assign up to two IRQs by designating them "IRQ #1 x" and "IRQ #2 y".

Parameter	Description
MEM	Memory Address in UMA. Can assign up to two UMA Addresses by designating them "MEM #1 x" and "MEM #2 y".
PORT	I/O Port Address. Can assign up to two I/O Port Addresses by designating them "PORT #1 x" and "PORT #2 y".
NODE ADDRESS	Assigns new 12-digit MAC Address to the network adapter card.
SLOT	Network adapter card Slot Number (MCA, EISA)
FRAME	Specifies alternate MAC layer frame encapsulations for the network adapter card. The default is ETHERNET_802.3 if not specified. Frame Types: ETHERNET_802.3 ETHERNET_802.2 ETHERNET_II ETHERNET_SNAP TOKEN_RING TOKEN_RING_SNAP
PROTOCOL	Registers Protocols to be used with ODI drivers. You must specify the protocol, protocol id and the frame type. The default "PROTOCOL" line is "PROTOCOL IPX 0 ETHERNET_802.3"

32-Bit IPX/SPX-Compatible Transport with NetBIOS

As discussed in Chapter 6, "Integrating with Other Protocols," Windows for Workgroups 3.11 includes NWLink, a 32-bit IPX/SPX-compatible protocol (also called a transport). NWLink is an NDIS 3.0-compliant protocol allowing Windows for Workgroups 3.11 workstations to communicate over a routable IPX-compatible protocol.

Although Windows for Workgroups 3.11 can run natively on top of a real-mode IPX protocol, the NWLink protocol provides the following additional benefits:

- **Improved virtualization of the IPX protocol**

When the 32-bit IPX/SPX compatible protocol is installed, all virtualization of the IPX protocol is handled by the NWLink.386 protocol. The NWLink protocol is responsible for ensuring that all IPX/SPX traffic is sent to the appropriate process running on the computer. This provides improved system stability when using IPX in the Windows environment. Because the NWLink.386 driver handles the virtualization of IPX, it is not necessary to load the Novell VIPX.386 driver.

- **32-bit protected-mode NetBIOS support (when 32-bit NetBIOS is installed)**

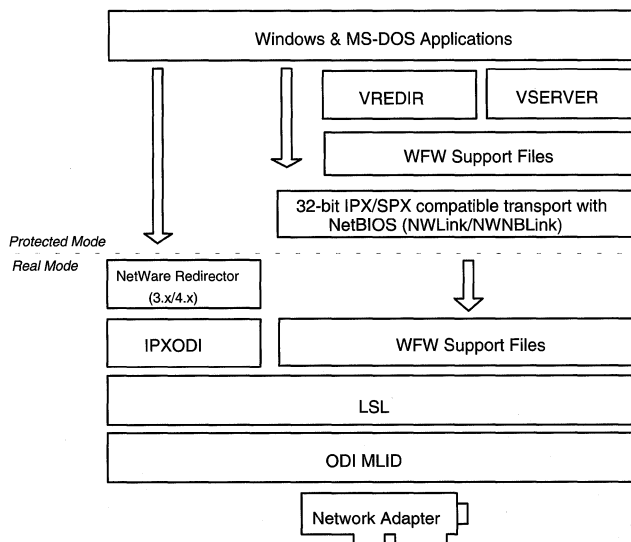
The 32-bit NetBIOS support provider, NWNBLink.386, is compatible with Novell's NetBIOS support driver and includes enhancements to provide improved performance when using NetBIOS. When the 32-bit NetBIOS support driver is installed (for example, the "32-bit IPX/SPX Compatible Transport with NetBIOS" protocol is installed), the Novell NETBIOS.EXE TSR can be removed from the system, saving approximately 40K of conventional memory.

On a computer configured with the NetWare client software, the NWLink protocol processes all non-NetWare Core Protocol (NCP) IPX traffic. The Windows for Workgroups components do not process NCP traffic that is used by the NetWare redirector to communicate with a NetWare server for file and printer services. In order to support file and printer services from NetWare servers, the NetWare redirector and real-mode IPX protocol must be loaded.

Figure 8.11 illustrates the flow of information from Windows and MS-DOS-based applications running under the Windows for Workgroups environment.

Figure 8.11

Flow of IPX information when the NWLink protocol is used along with the NetWare redirector and real-mode IPX protocol



A computer can install both protected-mode and real-mode IPX drivers on the same adapter running ODI or NDIS.

Choosing the Right IPX/SPX Compatible Transport Configuration

Depending on the functionality you want, you should choose the appropriate 32-bit protected-mode implementation of the IPX/SPX Compatible Transport (NWLink) with or without NetBIOS services. The following table provides a matrix showing when the “IPX/SPX Compatible Transport” and when the “IPX/SPX Compatible Transport with NetBIOS” should be installed.

Functionality Wanted	IPX/SPX Compatible Transport (NWLink)	IPX/SPX Compatible Transport with NetBIOS (NWLink/NWNBLink)
NetBIOS support		X
Connectivity to Windows NT		X
Connectivity with Windows for Workgroups	X	X (if Network DDE is wanted)
Network DDE over IPX		X

Novell NetWare Connectivity

Microsoft’s IPX/SPX protocol, NWLink, is a routable protocol. It conforms to the IPX specification which dictates for it to provide routable datagram packets.

The routable feature of IPX and its implementation across the majority of network environments are the reasons Microsoft implemented an NDIS 3.0 model of this protocol.

NWLink can use Novell NetWare servers configured as routers (and other IPX routers) to transfer its packets across LANs to access the resources of other Windows for Workgroups 3.11 computers.

Since NWLink is a protected-mode driver and does not load in real mode, Novell NetWare’s shell, NETX.EXE, will not load unless a real-mode IPX protocol driver is also installed. Novell NetWare’s workstation shell, NETX.EXE, is required to access Novell NetWare’s file server resources.

NetBIOS Services over IPX

NetBIOS is a high-level interface used by applications to communicate with other NetBIOS-compliant protocols. The NetBIOS interface is responsible for establishing logical names on the network, establishing connections (called sessions) between two logical names on the network, and supporting reliable data transfer between computers that have established a session.

Novell provides a terminate-and-stay-resident NetBIOS driver called NETBIOS.EXE which is a Level 1 NetBIOS provider and consumes approximately 40K of conventional memory. Novell's NetBIOS driver acknowledges each frame received, thus increasing the amount of traffic generated when NetBIOS is used.

Windows for Workgroups 3.11 provides a 32-bit protected-mode NetBIOS driver that provides NetBIOS services on top of IPX, called NWNBLink. NWNBLink is compatible with Novell's NetBIOS support driver and provides enhancements to improve performance when using NetBIOS in conjunction with IPX. These performance enhancements include acknowledgment of previous frames in response frames (called PiggyBackAck). They also include a "sliding window" acknowledgment mechanism. These performance enhancements for NetBIOS are used only when communicating with other computers using the NWNBLink NetBIOS driver, including other computers running Windows for Workgroups 3.11 and Windows NT.

Note When the NWNBLink driver is loaded, the Novell real-mode NETBIOS.EXE TSR can be removed from the system, saving 40K of conventional memory.

When Windows for Workgroups supports peer services on top of IPX, NetBIOS is necessary to provide support for Network DDE services. Network DDE uses NetBIOS to communicate between other workstations.

The NetBIOS interface over NWLink, NWNBLink, is required for Windows for Workgroups 3.11 computers to communicate with Windows NT computers that are using the NWLink protocol and NWNBLink support driver. Windows for Workgroups 3.11 users must install for IPX/SPX Compatible Transport with NetBIOS. The IPX/SPX protocol option in Windows NT automatically installs the NetBIOS component.

By default, the NWNBLink driver is installed in a monolithic IPX configuration when the user selects the IPX Support Driver (Monolithic) with NetBIOS transport as the network adapter card to use from the Add Network Adapter dialog box.

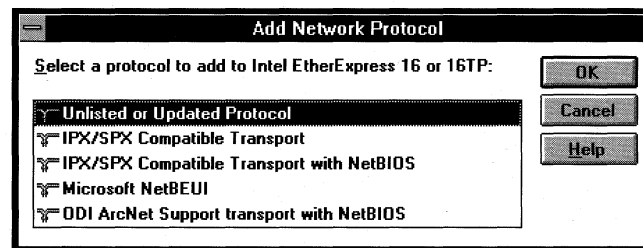
It is important to understand when it will be necessary to add the NetBIOS layer, NWNBLink, when installing IPX/SPX (or NWLink). The two most common scenarios to consider are:

- Connecting to Windows NT servers configured without NetBEUI
- Using any NetBIOS applications on a NetWare (or IPX) server, such as Lotus Notes

NWNBLink is not necessary for Windows for Workgroups 3.11 computers to communicate with other Windows for Workgroups 3.11 computers. The Windows for Workgroups 3.11 redirector and server have additional code that allows them to communicate with the IPX protocol directly without NetBIOS. This is referred to as Direct Hosting over IPX, as discussed in Chapter 6, “Integrating with Other Protocols.”

Figure 8.12

Available network protocols provided with Windows for Workgroups 3.11



To add the NWNBLink driver to your system, choose the IPX/SPX Compatible Transport with NetBIOS protocol from the Add Network Protocol dialog box from Network setup. If you do not need NetBIOS services over IPX, choose the IPX/SPX Compatible Transport as the protocol to use.

Specific Novell NetWare Issues

This section describes specific issues related to using the Novell NetWare client software along with Windows for Workgroups.

LastDrive Parameter in CONFIG.SYS

MS-DOS uses the **LastDrive=** entry in the CONFIG.SYS file to preallocate enough storage space in the internal memory structures of MS-DOS to recognize drive letters for devices through the given value for this entry. For example, a setting of “**LastDrive=Z**” tells MS-DOS to recognize drive letters from A to Z.

Windows for Workgroups allows drive letters to be assigned to redirected network drives through the drive letter identified by the **LastDrive=** entry in your CONFIG.SYS file. For example, if "**LastDrive=E**" is used, you can assign drive letters D and E to network drive resources (assuming drive C is the only physical hard disk drive in the system). However, drive letters defined beyond the value for the **LastDrive=** entry can not be used—that is, in this example drive E can be used, but drive F can not.

The NetWare 3.x redirector, on the other hand, begins mapping NetWare volumes after the value specified for the **LastDrive=** entry. This usually means that the NetWare login drive will be the first drive letter after the value used for the **LastDrive=** entry. For example, if "**LastDrive=E**" is used, the login drive is usually drive F.

If NetWare 3.x support is enabled when Windows for Workgroups is installed, then the line "**LastDrive=P**" is placed in the CONFIG.SYS. This allows Windows for Workgroups to use available drive letters through P, and the NetWare redirector to use drive letters Q through Z. Drive P is used as this is the middle of the alphabet. This may affect your NetWare configuration if you are using login scripts, as the login scripts may be assuming the login drive to be a certain drive—if the "**LastDrive=P**" entry specifies a value for the **LastDrive=** entry that is different from the value used before Windows for Workgroups is installed, your login scripts may be referencing an incorrect drive letter.

Note If the NetWare 3.x redirector is used, the support for Novell NetWare in Windows for Workgroups may change the behavior of your login scripts due to the value for the **LastDrive=** entry. To correct this, change your login script, or change the value for the **LastDrive=** entry.

The Novell NetWare 4.x redirector handles the **LastDrive=** entry as Windows for Workgroups does. That is, both the NetWare 4.x redirector and Windows for Workgroups allow drive letters to be used to connect to redirected network drives up through the drive letter specified by the **LastDrive=** entry. By default, Windows for Workgroups sets the entry to read "**LastDrive=Z**" in your CONFIG.SYS file when the NetWare 4.0 and above Workstation Shell is selected as the additional network.

Note The NetWare 4.x redirector uses the "**First Network Drive=**" entry in the NET.CFG file to identify the first mappable network drive. For more information on this setting, consult your NetWare documentation.

Log On to NetWare Server Before Starting Windows

Do not try to log in, log out, attach, or detach a Novell server from the MS-DOS Prompt within Windows. You should log in before you start Windows for Workgroups, and attach or detach servers by using File Manager or Print Manager.

The Novell NetWare components for using the NetWare client software with Windows 3.1 requires that the user log on to the appropriate NetWare server *before* starting Windows (or in this case, Windows for Workgroups 3.11). Attempting to log on to a NetWare server or perform one of the forementioned operations from within Windows for Workgroups 3.11 can produce undesirable affects.

Sample Files for Configuration Scenarios

In this section, sample configuration files are provided for the different configuration scenarios that were discussed in the "Installing NetWare Support" section presented earlier in this chapter.

These sample files are provided as a guide to help you identify problems if you modify your system files.

Note The CONFIG.SYS and AUTOEXEC.BAT files provided below contain only the minimum commands that will be present in the respective files. The contents of your MS-DOS system files may be different depending on your system configuration.

Open Datalink Interface Configuration

The sample CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI, PROTOCOL.INI, and NET.CFG files for integrating Windows for Workgroups with NetWare using an ODI configuration are provided in this section. See the section called "Installing for Open Datalink Interface Configuration," earlier in this chapter, for more information.

Sample CONFIG.SYS

```

DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
FILES=30
BUFFERS=10
LASTDRIVE=P
STACKS=9,256
DEVICE=C:\WINDOWS\IFSHLP.SYS

```

Sample AUTOEXEC.BAT

```

C:\WINDOWS\net start
C:\WINDOWS\SMARTDRV.EXE /X
C:\NOVELL\LSL.COM
C:\NOVELL\<Novell MLID driver>.COM
C:\NOVELL\IPXODI.COM
C:\WINDOWS\odihlp.exe
C:\NOVELL\NETX.EXE
PROMPT $p$g
PATH C:\WINDOWS;C:\DOS
SET TEMP=C:\WINDOWS\TEMP

```

Sample SYSTEM.INI Sections

```

[386Enh]
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
transport=nwlink.386,nwnblink.386,netbeui.386
secondnet.driv=netware.driv
secondnet=vnetware.386
OverlappedIO=off
netmisc=ndis.386,msodisup.386
netcard=
InDOSPolling=FALSE
netcard3=

```

```

[network]
multinet=netware3
winnet=wfwnet/00025100

```

```

[NetWare]
NWShareHandles=FALSE
RestoreDrives=TRUE

```

```

[network drivers]
netcard=
transport=
devdir=C:\WINDOWS
LoadRMDrivers=No

```

```
[NWNBLINK]
LANABASE=1
```

Sample PROTOCOL.INI (Using DEC Etherworks Turbo/TP - Ethernet Network Adapter)

Bold lines designate lines specific to this network adapter and its configuration.

Note When using Novell's ODI drivers, the "BINDINGS=" should be the same as the Novell MLID name.

```
[network.setup]
version=0x3110
netcard=ms$ewtrbtp,1,MS$EWTRBTP,4
transport=ms$nwlinknb,NWLINK
transport=ms$netbeui,NETBEUI
lana0=ms$ewtrbtp,1,ms$netbeui
lana1=ms$ewtrbtp,1,ms$nwlinknb
```

```
[net.cfg]
PATH=C:\NOVELL\net.cfg
```

```
[MS$EWTRBTP]
```

```
[Link Driver DEPCA]
Frame Ethernet_SNAP
Frame Ethernet_802.2
Frame Ethernet_II
Frame Ethernet_802.3
```

```
[NWLINK]
BINDINGS=DEPCA
```

```
[NETBEUI]
BINDINGS=DEPCA
LANABASE=0
SESSIONS=10
NCBS=12
```

Sample PROTOCOL.INI (Using IBM Token Ring 16/4 Network Adapter)

Bold lines designate lines specific to this network adapter and its configuration.

Note When using Novell's ODI drivers, the "BINDINGS=" should be the same as the Novell MLID name.

```
[network.setup]
version=0x3110
netcard=ms$ibmtr4,1,MS$IBMTR4,4
transport=ms$nwlinknb,NWLINK
transport=ms$netbeui,NETBEUI
lana0=ms$ibmtr4,1,ms$netbeui
lana1=ms$ibmtr4,1,ms$nwlinknb
```

```
[net.cfg]
PATH=C:\NOVELL\net.cfg
```

[MS\$IBMTR4]

```
[Link Driver TOKEN]
Frame Token-Ring
Link Driver TOKEN
```

```
[NWLINK]
BINDINGS=TOKEN
```

```
[NETBEUI]
BINDINGS=TOKEN
LANABASE=0
SESSIONS=10
NCBS=12
```

Sample NET.CFG (typical Ethernet adapter)

Bold lines indicate lines added by Windows for Workgroups 3.11 network setup. User specific Novell network configurations may dictate additional entries.

```
Link Driver DEPCA
Frame Ethernet_802.3
INT 5
PORT 300
MEM D8000
Frame Ethernet_II
Frame Ethernet_802.2
Frame Ethernet_SNAP
```

Sample NET.CFG (using IBM Token Ring 16/4 network adapter)

Bold lines indicate lines added by Windows for Workgroups 3.11 network setup. User specific Novell network configurations may dictate additional entries.

```
Link Driver TOKEN
Frame Token-Ring
```

Monolithic IPX Configuration

The sample CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI, PROTOCOL.INI, and NET.CFG files for integrating Windows for Workgroups with NetWare using a monolithic/dedicated IPX configuration are provided in this section. See the section called "Installing for Monolithic IPX Configuration," earlier in this chapter, for more information.

Sample CONFIG.SYS

```
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
FILES=30
BUFFERS=10
LASTDRIVE=P
STACKS=9,256
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

Sample AUTOEXEC.BAT

```
C:\WINDOWS\net start
C:\WINDOWS\SMARTDRV.EXE /X
PROMPT $p$g
PATH C:\WINDOWS;C:\DOS
SET TEMP=C:\WINDOWS\TEMP
C:\IPX.COM
C:\NETX.EXE
```

Sample SYSTEM.INI Sections

```
[386Enh]
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
transport=
secondnet.driv=netware.driv
secondnet=vnetware.386
OverlappedIO=off
netmisc=
netcard=
InDOSPolling=FALSE
netcard3=nwsup.386,nwnblink.386,vipx.386
```

```
[network]
multinet=netware3
winnet=wfwnet/00025100
directhost=no
```

```
[NetWare]
NWShareHandles=FALSE
RestoreDrives=TRUE
```

```
[network drivers]
netcard=
transport=
devdir=C:\WINDOWS
LoadRMDrivers=No
```

```
[NWNBLINK]
LANABASE=0
```

Sample PROTOCOL.INI (Using NE2000 Network Adapter)

```
[network.setup]
version=0x3110
netcard=ms$nwsupnb,1,MS$NWSUPNB,2
lana0=ms$nwsupnb,1,mono
```

```
[MS$NWSUPNB]
```

```
[NWSUP]
Adapters=MS$NWSUPNB
```

Sample SHELL.CFG

```
SHOW DOTS=ON
FILE HANDLES=60
```

MSIPX Configuration

This section identifies the changes that are made to the system configuration files, CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI, and PROTOCOL.INI, when upgrading from a workstation configured with Windows for Workgroups 3.10 and the MSIPX driver to Windows for Workgroups 3.11.

Note The Windows for Workgroups 3.11 setup utility detects MSIPX when upgrading from Windows for Workgroups 3.1 and install support for it. However, if after install, changes are made in the network setup, MSIPX support may be removed. There is no option to reinstall for it. Standard IPX.COM or IPXODI (preferred) support will need to be installed.

Changes made to CONFIG.SYS

Windows for Workgroups 3.10 configuration:

```
C:\WINDOWS\PROTMAN.DOS /I:C:\WINDOWS
C:\WINDOWS\WORKGRP.SYS
C:\WINDOWS\<NDIS MAC driver>.DOS
C:\WINDOWS\MSIPX.SYS
```

For the Windows for Workgroups 3.11 configuration, the above lines are replaced with:

```
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

Sample AUTOEXEC.BAT

Windows for Workgroups 3.11 Setup adds the /X switch to the SMARTDRV.EXE line.

```
C:\WINDOWS\SMARTDRV.EXE /X
C:\WINDOWS\net start
C:\WINDOWS\msipx
C:\WINDOWS\netx
PROMPT $p$g
PATH C:\WINDOWS;C:\DOS
SET TEMP=C:\WINDOWS\TEMP
```

Sample SYSTEM.INI Sections

```
[386Enh]
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
transport=netbeui.386,nwlink.386,nwnblink.386
secondnet.driv=netware.driv
secondnet=vnetware.386
OverlappedIO=off
netmisc=ndis.386,ndis2sup.386,vipx.386
netcard=declan.386
InDOSPolling=FALSE
```

```
[network]
multinet=netware3
winnet=wfnwnet/00025100
```

```
[NetWare]
NWShareHandles=FALSE
RestoreDrives=TRUE
```

```
[network drivers]
netcard=depca.dos
transport=*netbeui,msipx.sys,ndishlp.sys
devdir=C:\WINDOWS
LoadRMDrivers=Yes
```

```
[NWNBLINK]
LANABASE=1
```

Sample PROTOCOL.INI (using DEC Etherworks Turbo/TP network adapter)

```
[network.setup]
version=0x3110
netcard=ms$ewtrbtp,1,MS$EWTRBTP,3
transport=ms$netbeui,NETBEUI
transport=ms$ipx,MS$IPX
transport=ms$nwlinkb,NWLINK
transport=ms$ndishlp,MS$NDISHLP
lana0=ms$ewtrbtp,1,ms$ipx
lana1=ms$ewtrbtp,1,ms$netbeui
lana2=ms$ewtrbtp,1,ms$nwlinkb
lana3=ms$ewtrbtp,1,ms$ndishlp
```

```
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
```

```
[MS$EWTRBTP]
DriverName=DEPCAS$
RamAddress=0xD800
[MS$IPX]
DriverName=IPX$
MediaType=Novell/Ethernet
BINDINGS=MS$EWTRBTP
```

```
[LANCE]
Adapters=MS$EWTRBTP
```

```
[NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=MS$EWTRBTP
LANABASE=0
```

```
[NWLINK]
BINDINGS=MS$EWTRBTP
Interrupt=5
MaxMulticast=8
MaxTransmits=16
IOAddress=0x300
AdapterName=DE200
```

```
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=MS$EWTRBTP
```

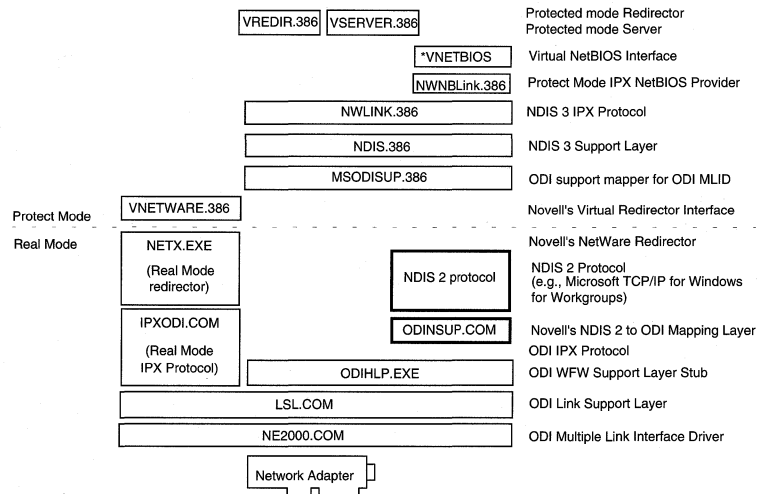
NDIS 2.0 Protocols on ODI Drivers

Windows for Workgroups natively provides support for network adapter card drivers and network protocols based on NDIS. Novell natively provides support for the Open Datalink Interface (ODI). Windows for Workgroups 3.11 provides support for mapping NDIS 3.0 protocols to run on top of ODI, however support for NDIS 2.0 protocols on top of ODI is not directly provided. In a NetWare environment where ODI drivers are being used, you may want to use NDIS 2.0. In this case, Novell offers the ODINSUP driver to map NDIS 2.0 protocols to ODI network adapter card drivers (MLIDs).

The Novell ODINSUP driver allows NDIS 2.0 protocol stacks to run over the ODI LSL and talk to an ODI MLID. For example, the ODINSUP driver can be used to allow the Microsoft TCP/IP for Windows for Workgroups NDIS 2.0 protocol or Microsoft DLC protocol for Windows for Workgroups NDIS 2.0 protocol on top of an ODI configuration as shown in Figure 8.13.

Figure 8.13

ODINSUP configuration supporting NDIS 2.0 protocols on ODI drivers



For more information about ODINSUP, see the ODINSUP.DOC file provided as part of the Novell NetWare DOS client software set.

Note For support assistance concerning Novell's ODINSUP.COM, contact Novell Technical Support.

Installing the ODINSUP Driver for Use with Microsoft TCP/IP for NetWare 3.x

In this section, we'll discuss the installation procedure for using the Microsoft TCP/IP for Windows for Workgroups protocol stack with ODI network adapter card drivers when the NetWare 3.x Workstation Shell is used.

Before You Begin

Since this configuration requires the Novell IPXODI drivers, you must have your computers set up and attached to a Novell server using IPXODI.COM at MS-DOS before proceeding to the "Setup Instructions" below.

Be sure to back up your AUTOEXEC.BAT file so that you can restore this configuration later if necessary.

Setup Instructions

Note that this example uses the 3COM 3C509 network adapter card as an example.

1. Install Windows for Workgroups using the Custom Setup option. When you get to the Network Setup dialog box, choose the "Novell NetWare (Workstation Shell 3.x)" entry as an additional network.

Then click on the "Drivers" button and choose the network adapter card driver for your network adapter card along with both the "NetBEUI" (NetBEUI is not required) and the "IPX/SPX Compatible Transport with NetBIOS" protocols.

Next, in the same "Network Drivers" box, click Setup and choose "Real Mode NDIS Driver". This is important because even though you are really running an ODI driver, with ODINSUP, Windows for Workgroups will think you are running on an NDIS driver. Choose OK and continue on with Setup. Just ignore the error messages about ODI drivers.

After Setup completes, you should restart your computer and start Windows, then install MS TCP/IP with WFW. You will probably get some error messages which you could suppress by using the **win /n** command to start Windows.

2. After completing MS TCP/IP setup, edit the SYSTEM.INI file and remove the NDIS 2.0 driver (<ELNK3.DOS>) from the netcard line of the [Network Drivers] section.

Note If you are using a different network adapter card, the NDIS network adapter card driver (for example, <ELINK3.DOS> in the above example for the 3Com 3C509 card) will be different.

3. Edit the AUTOEXEC.BAT file so that it contains the following lines:

```
C:\WINDOWS\NET INIT          <==This loads protman and ndis protocols
C:\<PATH>\LSL.COM
C:\<PATH>\<your netcard's ODI MAC driver>.COM
C:\<PATH>\ODINSUP.COM
C:\WINDOWS\Net Start Netbind <==This binds the protocols to ODINSUP
C:\<PATH>\IPXODI.COM
C:\<PATH>\NETX.EXE
C:\WINDOWS\umb               <==The rest of these files are for MS TCP/IP
C:\WINDOWS\tcptsr
C:\WINDOWS\tinyrfc
C:\WINDOWS\nmtsr.exe
C:\WINDOWS\emsbfr.exe
```

4. Edit the NET.CFG file and verify that it contains the following lines. If these lines don't exist, add them to the appropriate sections of the NET.CFG file. If you do not have a NET.CFG file, create one using a text editor (such as Microsoft Windows Notepad), and save it in the directory from which LSL.COM is run. Note that some of the lines in the NET.CFG file are indented and must be for them to work.

```
PROTOCOL ODINSUP
  BIND 3c509
  BUFFERED
LINK DRIVER 3c509          <== where 3C509 is the filename of your
                           network adapter card's ODI driver
  INT n                    <== where "n" is the one-digit interrupt number
  MEM nnnnn               <== where "nnnnn" is the five-digit memory address
  PORT ###                <== where "nnn" is the three-digit I/O port address
FRAME ETHERNET_802.2
FRAME ETHERNET_802.3
FRAME ETHERNET_II
FRAME ETHERNET_SNAP
PROTOCOL IPX 0 ETHERNET_802.3
```

Note If you've been using ODI to attach to a Novell server at MS-DOS and you haven't specified the INT, MEM, PORT, DMA, SLOT, and so on, parameters in the NET.CFG file, you probably don't need to add them now. However, depending on the ODI MAC driver (Novell refers to this as the "MLID") you are using, you may need to place the INT, MEM, PORT, and so on, lines after the FRAME lines. Additionally, list your network's frame type FIRST in the list of "FRAME ETHERNET_xxxx" entries. (This probably will be ETHERNET_802.3" or "ETHERNET_II.")

5. Edit the PROTOCOL.INI file as follows:

Replace the “**BINDINGS=**” lines in the [NWLINK], [NETBEUI], [MS\$NDISHLP], and [TCPIP] sections with the Novell ODI MAC driver (MLID) as follows.

Important If the ODI MLID filename begins with a numeral, you must preface the filename with an “x” in the **BINDINGS=** statement. For example, 3COM’s 3C509 network adapter card uses an ODI MLID with a filename of “3C509.COM.” In the PROTOCOL.INI file, the **BINDINGS=** statements would need to be:

```
BINDINGS=x3C509.COM
```

```
[NWLINK]
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the “x” in front.

[NETBEUI]
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the “x” in front.
LANABASE=0
SESSIONS=10
NCBS=12
DriverName=netbeui$

[MS$NDISHLP]
DriverName=ndishlp$
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the “x” in front.

[TCPIP]
DefaultGateway0=130 25 0 1
SubNetMask0=255 255 0 0
IPAddress0=130 25 40 20
NBSSessions=6
NetFiles=C:\WINDOWS
DriverName=TCPIP$
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the “x” in front.
LANABASE=2
```

Warning After you make these modifications, do *not* make any changes in the Network Drivers section of Network Setup. If you do, the CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI files will be overwritten and the ODINSUP driver may not work properly.

Sample Configuration Files

Below are samples of modified CONFIG.SYS, AUTOEXEC.BAT, NET.CFG, and PROTOCOL.INI files as they appear if you are using Novell's ODINSUP with Windows for Workgroups 3.11 configured to use the Microsoft TCP/IP for Windows for Workgroups, NetBEUI and NWLink with NetBIOS protocols, on top of ODI network adapter card drivers.

Sample CONFIG.SYS

```
DEVICE=C:\WINDOWS\HIMEM.SYS
DOS=HIGH
BUFFERS=30
FILES=40
DEVICE=C:\DOS\SETVER.EXE
SHELL=C:\DOS\COMMAND.COM C:\DOS\ /p /e:2048
STACKS=9,256
LASTDRIVE=P
DOS=HIGH
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

Sample AUTOEXEC.BAT

```
C:\WINDOWS\NET INIT
C:\NOVELL\LSL
C:\NOVELL\3C509
C:\NOVELL\ODINSUP
C:\WINDOWS\NET START NETBIND
C:\NOVELL\IPXODI
C:\NOVELL\NETX
C:\WINDOWS\umb
C:\WINDOWS\tcptsr
C:\WINDOWS\tinyrfc
C:\WINDOWS\nmtsr.exe
C:\WINDOWS\lemsbfr.exe
PATH=C:\WINDOWS;C:\DOS;C:\
SET TEMP=C:\TEMP
C:\WINDOWS\SMARTDRV.EXE /X
```

Sample NET.CFG

```
PROTOCOL ODINSUP
  BIND 3C509
  BUFFERED
LINK DRIVER 3c509
  port 300
  int 5
  FRAME ETHERNET_802.2
  FRAME ETHERNET_802.3
  FRAME ETHERNET_II
  FRAME ETHERNET_SNAP
  PROTOCOL IPX 0 ETHERNET_802.3
```

Sample SYSTEM.INI Sections

```
[386Enh]
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
netmisc=ndis.386,ndis2sup.386
transport=nwlink.386,nwnblink.386,netbeui.386
InDOSTolling=FALSE
secondnet=VNETWARE.386
OverlappedIO=off
device=vsockets.386
device=vbapi.386

[NetWare]
NWShareHandles=FALSE
RestoreDrives=TRUE

[network drivers]
devdir=C:\WINDOWS
LoadRMDrivers=Yes
netcard=
transport=*netbeui,ndishlp.sys,tcpdrv.dos,nemm.dos

[NWNBLINK]
LANABASE=1
```

Sample PROTOCOL.INI

```
[network.setup]
version=0x3110
netcard=ms$elnk3,1,MS$ELNK3,1
transport=ms$nwlinknb,NWLINK
transport=ms$netbeui,NETBEUI
transport=ms$ndishlp,MS$NDISHLP
transport=tcpip,TCPIP
lana0=ms$elnk3,1,ms$netbeui
lana1=ms$elnk3,1,ms$nwlinknb
lana2=ms$elnk3,1,ms$ndishlp
lana3=ms$elnk3,1,tcpip
```

```
[MS$ELNK3]
DriverName=ELNK3$
MAXTRANSMITS=6
```

```
[NWLINK]
BINDINGS=x3C509
```

```
[NETBEUI]
BINDINGS=x3C509
LANABASE=0
SESSIONS=10
NCBS=12
DriverName=netbeui$
```

```
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
```

```
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=x3C509
```

```
[TCPIP]
DefaultGateway0=130 25 0 1
SubNetMask0=255 255 0 0
IPAddress0=130 25 40 20
NBSessions=6
NetFiles=C:\WINDOWS
DriverName=TCPIP$
BINDINGS=x3C509
LANABASE=2
```

Installing the ODINSUP Driver for Use with Microsoft TCP/IP for NetWare 4.x

This section discusses the installation procedure for using the Microsoft TCP/IP for Windows for Workgroups protocol stack with ODI network adapter card drivers when the NetWare 4.x Workstation Shell is used.

Since this configuration requires the Novell IPXODI drivers, you must have your computers set up and attached to a Novell server using IPXODI.COM at MS-DOS before proceeding to the "Setup Instructions" below.

Be sure to back up your AUTOEXEC.BAT file so that you can restore this configuration later if necessary.

Setup Instructions

Note that this example uses the 3COM 3C509 network adapter card as an example.

1. Install Windows for Workgroups using the Custom Setup option. When you get to the Network Setup dialog box, choose the "Novell NetWare (Workstation Shell 4.0 and above)" entry as an additional network.

Then click on the "Drivers" button and choose the network adapter card driver for your network adapter card along with both the "NetBEUI" (NetBEUI is not required) and the "IPX/SPX Compatible Transport with NetBIOS" protocols.

Next, in the same "Network Drivers" box, click Setup and choose "Real Mode NDIS Driver". This is important because even though you are really running an ODI driver, with ODINSUP, Windows for Workgroups will think you are running on an NDIS driver. Choose OK and continue on with Setup. Just ignore the error messages about ODI drivers.

After Setup completes, you should restart your computer and start Windows, then install MS TCP/IP with WFW. You will probably get some error messages which you could suppress by using the **win /n** command to start Windows.

2. After completing MS TCP/IP setup, edit the SYSTEM.INI file and remove the NDIS 2.0 driver (<ELNK3.DOS>) from the netcard line of the **[Network Drivers]** section.

Note If you are using a different network adapter card, the NDIS network adapter card driver (for example, <ELINK3.DOS> in the above example for the 3Com 3C509 card) will be different.

3. Edit the AUTOEXEC.BAT file so that it contains the following lines:

Note If you are using the NETSTART.BAT file created by the NetWare 4.x client software, remove the **net start** line from your AUTOEXEC.BAT file and place it in the NETSTART.BAT file so the entries resemble the following lines.

```
SET NWLANGUAGE=ENGLISH
C:\WINDOWS\NET INIT      <==This loads protman and ndis protocols
C:\<NWPATH>\LSL.COM
C:\<NWPATH>\<your netcard's ODI MAC driver>.COM
C:\<NWPATH>\ODINSUP.COM
C:\WINDOWS\Net Start Netbind <==This binds the protocols to ODINSUP
C:\<NWPATH>\IPXODI.COM
C:\<NWPATH>\VLM.EXE
C:\WINDOWS\umb          <==The rest of these files are for MS TCP/IP
C:\WINDOWS\tcptsr
C:\WINDOWS\tinyrfc
C:\WINDOWS\nmtsr.exe
C:\WINDOWS\emsbfr.exe
```

4. Edit the NET.CFG file and verify that it contains the following lines. If these lines don't exist, add them to the appropriate sections of the NET.CFG file. If you do not have a NET.CFG file, create one using a text editor (such as Microsoft Windows Notepad), and save it in the directory that LSL.COM is executed from. Note that some of the lines in the NET.CFG file are indented and must be for them to work.

```

PROTOCOL ODINSUP
  BIND 3c509
  BUFFERED
LINK DRIVER 3c509 <== where 3C509 is the filename of your netcard's ODI
driver
  INT n <== where "n" is the one-digit interrupt number
  MEM nnnnn <== where "nnnnn" is the five-digit memory address
  PORT ### <== where "nnn" is the three-digit I/O port address
FRAME ETHERNET_802.2
FRAME ETHERNET_802.3
FRAME ETHERNET_II
FRAME ETHERNET_SNAP
PROTOCOL IPX 0 ETHERNET_802.3
First Network Drive = F

```

Note If you've been using ODI to attach to a Novell server at MS-DOS and you haven't specified the INT, MEM, PORT, DMA, SLOT, and so on, parameters in the NET.CFG file, you probably don't need to add them now. However, depending on the ODI MAC driver (Novell refers to this as the "MLID") you are using, you may need to place the INT, MEM, PORT, and so on, lines after the FRAME lines. Additionally, list your network's frame type FIRST in the list of "FRAME ETHERNET_xxx" entries. (This probably will be ETHERNET_802.3 or "ETHERNET_II.")

5. Edit the PROTOCOL.INI file as follows:

Replace the "**BINDINGS=**" lines in the [NWLINK], [NETBEUI], [MS\$NDISHLP], and [TCPIP] sections with the Novell ODI MAC driver (MLID) as follows.

Important If the ODI MLID filename begins with a numeral, you must preface the filename with an "x" in the **BINDINGS=** statement. For example, 3COM's 3C509 network adapter card uses an ODI MLID with a filename of "3C509.COM." In the PROTOCOL.INI file, the **BINDINGS=** statements would need to be:

```
BINDINGS=x3C509.COM
```

```
[NWLINK]
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the "x" in front.
```

```
[NETBEUI]
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with the "x" in front.
LANABASE=0
SESSIONS=10
NCBS=12
DriverName=netbeui$
```

```
[MS$NDISHLP]
DriverName=ndishlp$
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with
the "x" in front.
```

```
[TCP/IP]
DefaultGateway0=130 25 0 1
SubNetMask0=255 255 0 0
IPAddress0=130 25 40 20
NBSessions=6
NetFiles=C:\WINDOWS
DriverName=TCP/IP$
;BINDINGS=MS$ELNK3 <== NDIS MAC driver, ELINK3.DOS
BINDINGS=x3c509 <== ODI MLID driver, 3c509.COM with
the "x" in front.
LANABASE=2
```

Warning

After you make these modifications, do *not* make any changes in the Network Drivers section of Network Setup. If you do, the CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI files will be overwritten and the ODINSUP driver may not work properly.

Sample Configuration Files

Below are samples of modified CONFIG.SYS, AUTOEXEC.BAT, NET.CFG, and PROTOCOL.INI files as they appear if you are using Novell's ODINSUP with Windows for Workgroups 3.11 configured to use the Microsoft TCP/IP for Windows for Workgroups, NetBEUI and NWLink with NetBIOS protocols, on top of ODI network adapter card drivers.

Sample CONFIG.SYS

```
DEVICE=C:\WINDOWS\HIMEM.SYS
DOS=HIGH
BUFFERS=30
FILES=50
DEVICE=C:\DOS\SETVER.EXE
SHELL=C:\DOS\COMMAND.COM C:\DOS\ /p /e:2048
STACKS=9,256
LASTDRIVE=P
DOS=HIGH
DEVICE=C:\WINDOWS\IFSHLP.SYS
```

Sample AUTOEXEC.BAT

```
C:\WINDOWS\NET INIT
C:\NOVELL\LSL
C:\NOVELL\3C509
C:\NOVELL\ODINSUP
C:\WINDOWS\NET START NETBIND•
C:\NOVELL\IPXODI
C:\NOVELL\VLM
C:\WINDOWS\umb
C:\WINDOWS\tcptsr
C:\WINDOWS\tinyrfc
C:\WINDOWS\nmtsr.exe
C:\WINDOWS\emsbfr.exe
PATH=C:\WINDOWS;C:\DOS;C:\
SET TEMP=C:\TEMP
C:\WINDOWS\SMARTDRV.EXE /X
```

Sample NET.CFG

```
PROTOCOL ODINSUP
  BIND 3C509
  BUFFERED
LINK DRIVER 3c509
  port 300
  int 5
  FRAME ETHERNET_802.2
  FRAME ETHERNET_802.3
  FRAME ETHERNET_II
  FRAME ETHERNET_SNAP
  PROTOCOL IPX 0 ETHERNET_802.3
First Network Drive = F
```

Sample SYSTEM.INI Sections

```
[386Enh]
network=*vnetbios,*vwc,vnetsup.386,vredir.386,vserver.386
netmisc=ndis.386,ndis2sup.386
transport=nwlink.386,nwnblink.386,netbeui.386
InDOSPolling=FALSE
secondnet=VNETWARE.386
OverlappedIO=off
device=vsockets.386
device=vbapi.386
TimerCriticalSection=10000
ReflectDOSInt2A=TRUE
UniqueDosPSP=TRUE
PSPIncrement=5

[NetWare]
NWShareHandles=FALSE
RestoreDrives=TRUE

[network drivers]
devdir=C:\WINDOWS
LoadRMDrivers=Yes
netcard=
transport=*netbeui,ndishlp.sys,tcpdrv.dos,nemm.dos

[NWNBLINK]
LANABASE=1
```

Sample PROTOCOL.INI

```
[network.setup]
version=0x3110
netcard=ms$elnk3,1,MS$ELNK3,1
transport=ms$nwlinknb,NWLINK
transport=ms$netbeui,NETBEUI
transport=ms$ndishlp,MS$NDISHLP
transport=tcpip,TCPIP
lana0=ms$elnk3,1,ms$netbeui
lana1=ms$elnk3,1,ms$nwlinknb
lana2=ms$elnk3,1,ms$ndishlp
lana3=ms$elnk3,1,tcpip

[MS$ELNK3]
DriverName=ELNK3$
MAXTRANSMITS=6
```

```
[NWLINK]
BINDINGS=x3C509
```

```
[NETBEUI]
BINDINGS=x3C509
LANABASE=0
SESSIONS=10
NCBS=12
DriverName=netbeui$
```

```
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
```

```
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=x3C509
```

```
[TCP/IP]
DefaultGateway0=130 25 0 1
SubNetMask0=255 255 0 0
IPAddress0=130 25 40 20
NBSessions=6
NetFiles=C:\WINDOWS
DriverName=TCPIP$
BINDINGS=x3C509
LANABASE=2
```

Chapter
9

Integrating with Other Networks

In addition to providing support for integrating with Windows NT, Windows NT Advanced Server, and Novell NetWare, Windows for Workgroups 3.11 also supports networks such as Banyan VINES, SunSelect PC-NFS, and Artisoft LANtastic. This chapter provides specific information on using Windows for Workgroups 3.11 with other networks.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 1, “Windows for Workgroups 3.11 Architecture;” Chapter 2, “Windows for Workgroups 3.11 Setup and Installation;” Chapter 7, “Integrating with Windows NT and Windows NT Advanced Server;” Chapter 8, “Integrating with Novell NetWare;” Chapter 13, “Troubleshooting Windows for Workgroups 3.11.”
- Windows for Workgroups NETWORKS.WRI file

Contents of This Chapter

Summary of Network Support.....	9-2
Additional Network Support	9-2
Primary Network Support	9-3
For Additional Information	9-4
Microsoft LAN Manager.....	9-4
Banyan VINES	9-4
Support as an Additional Network	9-5
Support as a Primary Network	9-5
DEC PATHWORKS	9-6
Support as Microsoft Windows Network.....	9-6
Support as Additional Network.....	9-6
Windows 3.1-compatible Networks	9-7
Support for Network DDE	9-7
Artisoft LANtastic.....	9-10
SunSelect PC-NFS version 5.0.....	9-10
Novell NetWare.....	9-10

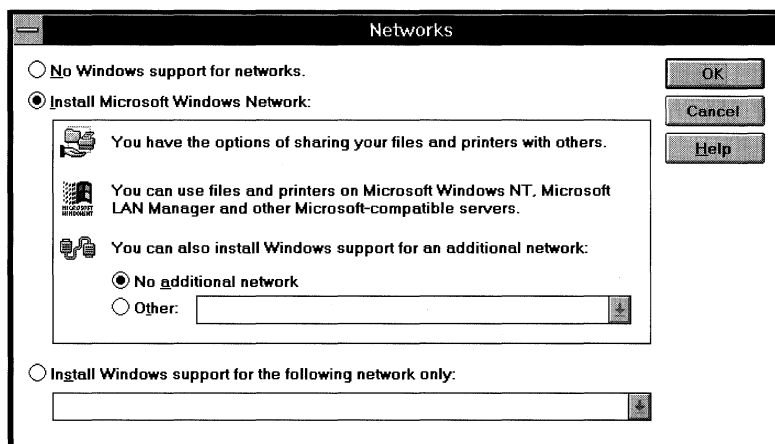
Summary of Network Support

As discussed in Chapter 2, “Windows for Workgroups 3.11 Setup and Installation,” Windows for Workgroups 3.11 supports several options for integrating with other networks:

- Installing only the Microsoft Windows Network to provide connectivity to other computers running Windows for Workgroups, Windows NT, Windows NT Advanced Server, Workgroup Add-on for MS-DOS, or Microsoft LAN Manager-compatible networks
- Configuring for an additional network in conjunction with the Microsoft Windows Network components
- Installing a Windows 3.1-compatible primary network without the Microsoft Windows Network components

Figure 9.1

The Networks dialog box for configuring network support in Windows for Workgroups 3.11



Additional Network Support

To configure a third-party network as an *additional* network, the user simply must select the “Install Microsoft Windows Network” option in the Networks dialog box and then select the “Other” option and choose one of the supported additional networks. Windows for Workgroups 3.11 provides support for running the following third-party network operating systems in conjunction with Windows for Workgroups 3.11:

- Banyan VINES version 4.11 (5), 5.00 (5), 5.52 (5)
- BW-NFS Network File System version 3.0c
- Novell NetWare Workstation Shell 3.x
- Novell NetWare Workstation Shell 4.0 and above
- SunSelect PC-NFS version 5.0

Note Windows for Workgroups 3.11 is not limited to working in conjunction with only the networks provided in the initial additional network list. Network vendors can supply a setup information file that provides information to configure Windows for Workgroups 3.11 to work with their networking products. If your network is not present in the list of networks that Windows for Workgroups 3.11 knows about, check with your network vendor to see if they support integration with Windows for Workgroups 3.11.

Primary Network Support

To configure a third-party network as an *primary* network, the user selects the “Install Windows support for the following network only” option in the Networks dialog box and chooses one of the supported Windows 3.1-compatible networks. Windows for Workgroups 3.11 provides support for running the on top of the following Windows 3.1-compatible networks:

- 100% MS-Net compatibles
- Artisoft LANtastic 3.x, 4.x, 5.x
- Banyan VINES 4.11 (5), 5.00 (5), 5.50 (5)
- BW-NFS Network File System (version 3.0)
- DEC PATHWORKS version 4.0, version 4.1 or higher
- IBM OS/2 LAN Server version 1.2 or 1.3, version 1.3 (CSD 5015/5050), version 2.0, without /API option
- Microsoft Windows Network version 3.11 Basic redirector,
- Novell NetWare Workstation shell 3.x, 4.0 and above
- TCS 10Net version 4.1x with DCA 1M card, version 4.1x, version 4.2 and above, version 5.0
- SunSelect PC-NFS version 5.0

Note Windows for Workgroups 3.11 is not limited to working in conjunction with only the networks provided in the initial Windows 3.1-compatible primary network list. Network vendors can supply a setup information file that provides information to configure Windows for Workgroups to work with their networking products. If your network is not present in the list of networks that Windows for Workgroups 3.11 knows about, check with your network vendor to see if they support integration with Windows for Workgroups 3.11.

This chapter will provide a discussion of some of the networks that are supported by Windows for Workgroups 3.11 and will discuss the relevant network functionality supported in an additional network or primary network configuration.

For Additional Information

For additional information as well as the most up-to-date information on integrating Windows for Workgroups 3.11 with other networks, sources include the NETWORKS.WRI file installed in your WINDOWS directory, the Microsoft Knowledge Base, and the Microsoft Workgroups forum on CompuServe (GO MSWRKGRP). In addition to these sources, check the source information provided in Appendix A, "Additional Support Information," for additional locations.

Microsoft LAN Manager

Windows for Workgroups 3.11 improves upon the LAN Manager connectivity supported by Windows for Workgroups 3.10. The improvements include full support for the LAN Manager 2.1 server message-based (SMB) protocol, support for home directories when a **net use** is performed from an MS-DOS command prompt including support from a login script, as well as support for the SMB messaging service.

The SMB messaging service allows Windows for Workgroups-based workstations to receive notification messages from LAN Manager servers and other client workstations to alert the user to events that occur on the network, such as the completion of a print job.

Support for connectivity to Microsoft LAN Manager is available when the Microsoft Windows Network is selected from the Networks dialog box.

Banyan VINES

Windows for Workgroups 3.11 supports Banyan VINES as both an additional network and as a primary network. Updated Banyan drivers for Windows are available with the revisions of VINES discussed in this section.

Support as an Additional Network

Windows for Workgroups 3.11 supports network integration with Banyan VINES by allowing users to take advantage of information-sharing capabilities in Windows while maintaining full access to Banyan's enterprise network services, including directory management, security, administration and messaging. Windows for Workgroups 3.11 allows users of Banyan VINES to take advantage of peer networking services while also providing connectivity to other computers running Windows for Workgroups, Windows NT, and Windows NT Advanced Server.

Vines 4.10

If your network runs VINES 4.10, you must upgrade to VINES 4.11 (5) before you install support for Windows for Workgroups 3.11.

Vines 4.11

If your network runs VINES 4.11 (5), your network administrator must apply the (5)-FW-1 and (5)-GN-1 software patches before you install support for Windows for Workgroups 3.11.

Vines 5.00

If your network runs VINES 5.00 (5), your network administrator must apply the (5)-EA-1 and (5)-ER-1 software patches before you install support for Windows for Workgroups 3.11.

Consult the NETWORKS.WRI file provided with Windows for Workgroups 3.11 for additional information.

VINES 5.52 (5) Networks

If your network runs VINES 5.52 (5), you must copy NDISBAN.COM to the local VINES directory that contains your VINES network client software. Use the PCCOPY command to copy this file from your VINES 5.52 (5) server to your workstation.

Support as a Primary Network

If you are using Banyan VINES as the primary network, be sure to upgrade to the latest revisions of the VINES network operating system as described in the preceding section.

Support for Network DDE

Network DDE is available when Banyan VINES is used as a primary network. It is necessary to load the VINES NetBIOS driver before starting Windows for Workgroups 3.11. Check your VINES documentation for more information.

DEC PATHWORKS

Windows for Workgroups 3.11 features improved support for DEC PATHWORKS connectivity from Windows for Workgroups 3.10, including support for long file names and other functionality supported by the PATHWORKS network redirector.

Support as Microsoft Windows Network

Windows for Workgroups 3.11 supports DEC PATHWORKS connectivity when the Microsoft Windows Network option is installed. In this case, it is only necessary to add the appropriate protocol (e.g., DECNet) to Windows for Workgroups 3.11 to access the PATHWORKS server.

Support as Additional Network

Support for DEC PATHWORKS as an additional network is not provided directly with Windows for Workgroups 3.11. Digital will provide setup software for their customers that will automate this configuration. Information on configuring DEC PATHWORKS as an additional network will be made available on Digital's CompuServe Forum, DECPCI, when it is completed.

Note that the existing 'PATHWORKS white paper' (available via CompuServe) for Windows for Workgroups 3.10 is not accurate for users of Windows for Workgroups 3.11.

Windows 3.1-compatible Networks

In addition to supporting the use of Windows for Workgroups 3.11 networking components along with networks such as Novell NetWare, Banyan VINES and Sun PC-NFS, Windows for Workgroups 3.11 provides support for running on top of networks that are supported by Windows 3.1. Support for Windows 3.1-compatible networks allows you to use Windows for Workgroups functionality such as Mail, Schedule+, and Microsoft At Work fax software in your existing environment without changing your desktop software. When Windows for Workgroups 3.11 is configured to run on top of a Windows 3.1-compatible network, this is referred to as using the Windows 3.1-compatible network as the *primary* network.

Using Windows for Workgroups 3.11 on top of a Windows 3.1-compatible network limits the network functionality to only offer the functions that are provided by the Windows 3.1-compatible network. Some Windows 3.1-compatible networks such as Artisoft® LANtastic® use proprietary network protocols to communicate and can not be integrated with other computers using Windows for Workgroups natively. When Windows for Workgroups 3.11 is configured to run on top of a Windows 3.1-compatible network, the peer services offered by Windows for Workgroups 3.11 are not available. Windows 3.1-compatible networks that provide NetBIOS services may also support the use of Network DDE to provide a means of dynamically exchanging information across the network using Dynamic Data Exchange, DDE.

Users of a Windows 3.1-compatible network that desire connectivity with Windows NT Advanced Server may need to use Windows for Workgroups 3.11 in place of the networking software that they run on their existing network.

Support for Network DDE

Windows for Workgroups 3.11 installs support for Network DDE on the following Windows 3.1-compatible networks:

- Artisoft LANtastic 3.x, 4.x, 5.x
- Banyan VINES 4.11 (5), 5.00 (5), 5.50 (5)
- BW-NFS Network File System (version 3.0)
- Microsoft Windows Network version 3.11 Basic redirector,
- Novell NetWare Workstation shell 3.x, 4.0 and above
- SunSelect PC-NFS version 5.0

For each of the above listed networks, either Microsoft or the respective network operating system vendor has tested Network DDE as supported by Windows for Workgroups 3.11 in conjunction with the vendor's NetBIOS services and verified that Network DDE operates properly.

When a third-party network is configured as a primary network, Network DDE requires a loaded NetBIOS driver in order to support NetBIOS services. The NetBIOS driver is normally referenced in the AUTOEXEC.BAT file and loads along with the other network redirector components.

When one of these Windows 3.1-compatible networks is selected as the primary network, the following Windows for Workgroups 3.11 components are installed:

Component	Description
NETDDEX.EXE	Initial Network DDE loader that checks for the presence of NetBIOS as well as a valid ComputerName= entry in the [network] section of SYSTEM.INI to be used to announce the NetBIOS name.
NETDDE.EXE	Network DDE resident application.
NDDENB.DLL	Network DDE API DLL.
WINCHAT.EXE	Chat application.

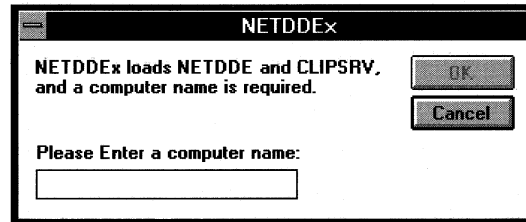
Note Hearts (MSHEARTS.EXE) and ClipBoard (CLIPBRD.EXE) also support Network DDE, if installed. Both MSHEARTS.EXE and CLIPBRD.EXE support stand-alone configurations and are installed by default by Windows for Workgroups 3.11 Setup.

The NETDDEX.EXE application is placed on the **load=** line of the **[Windows]** section of WIN.INI. NETDDEX.EXE is responsible for checking to see that NetBIOS is available on the computer (i.e., a NetBIOS provider has been loaded and is available to support NetBIOS services) and whether the NetBIOS provider has configured a valid computer name to use for NetBIOS. Network DDE requires a valid computer name to uniquely identify other computers on the network that can participate in Network DDE conversations.

The computer name for the workstation is specified by the **ComputerName=** entry in the **[network]** section of SYSTEM.INI file. If the **ComputerName=** entry is not present, NETDDEx displays a dialog, as shown in Figure 9.2, to prompt the user for the name of the computer to use and then places the response in the **[network]** section of the SYSTEM.INI file.

Figure 9.2

NETDDEx dialog box used to allow the user to specify the name of the computer for use in Network DDE conversations



A discussion of the support for Network DDE when third-party networking products are configured as the primary network is also provided in this chapter.

“Unsupported” Networks

It is possible to manually add Network DDE support for networks listed in the WINNET.INF network information file that provide NetBIOS services, but for which Windows for Workgroups 3.11 does not install Network DDE components. Some networks may not have been fully tested by Microsoft or by the network vendor, and thus the Network DDE components are not installed.

To install Network DDE in this scenario, it is necessary to expand and copy the NETDDEX.EX_ file from one of the Windows for Workgroups 3.11 or Workgroup Add-on for Windows disks and place this file in the WINDOWS directory. (The other Network DDE support files listed above are automatically installed by Windows for Workgroups 3.11 Setup.) It is also necessary to add a reference to the NETDDEX.EXE file on the **load=** line of the **[Windows]** section in the WIN.INI file.

If Network DDE services are not available after installing the NETDDEX.EXE application and loading the NetBIOS driver for your network before starting Windows for Workgroups 3.11 (e.g., try running Chat, WINCHAT.EXE, which will display an error message if the Network DDE service is not available), you can remove the NETDDEX.EXE file from the **load=** line in the **[Windows]** section of WIN.INI. If Network DDE services are not available, Network DDE won't be supported on your network.

Artisoft LANtastic

This section summarizes some of the known issues when running LANtastic as the primary network with Windows for Workgroups 3.11.

Support for Network DDE

When Artisoft LANtastic 3.x, 4.x, or 5.x, is installed as the primary network, Network DDE is available if the Artisoft AILANBIO.EXE NetBIOS driver is loaded prior to starting Windows for Workgroups 3.11.

SunSelect PC-NFS version 5.0

This section summarizes some of the known issues when running SunSelect PC-NFS version 5.0 as the primary network with Windows for Workgroups 3.11.

Support for Network DDE

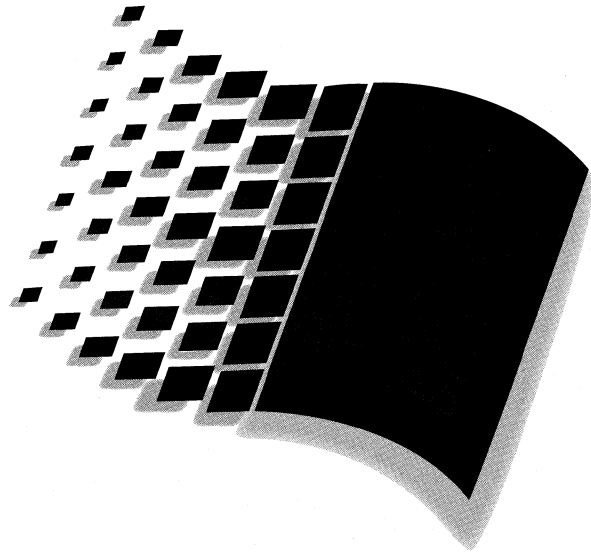
To support Network DDE on SunSelect PC-NFS version 5.0, it is necessary to load the NB.EXE NetBIOS layer on top of the TCP/IP provided with PC-NFS. The NB.EXE NetBIOS driver is located in the PC-NFS directory and must be started before Windows for Workgroups 3.11 loads.

Novell NetWare

This section summarizes some of the known issues when running Novell NetWare workstation shells as the primary network with Windows for Workgroups 3.11.

Support for Network DDE

To support Network DDE on Novell NetWare Workstation Shell 3.x, or 4.0 and above, it is necessary to load the NetWare NETBIOS.EXE TSR before starting Windows for Workgroups 3.11.



Using Windows for Workgroups 3.11

Part

4

Using Windows for Workgroups 3.11

Chapter 10

Microsoft At Work Fax

10-1

Overview of Microsoft At Work Fax Software.....	10-2
Sharing a Fax Modem Over the Network.....	10-5
Using the Advanced Dialing Feature.....	10-7
Using Security	10-10

Chapter
10

Microsoft At Work Fax

This chapter describes the capabilities offered by Microsoft At Work fax software included with Windows for Workgroups 3.11. Microsoft At Work fax software is the first implementation of the Microsoft At Work architecture and allows stand-alone and networked computers running Windows for Workgroups 3.11 to send and receive secure messages that include binary file attachments, or standard Group 3 facsimiles using the Microsoft Mail client or a mail-enabled application, and a compatible fax modem.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 3, "Windows for Workgroups 3.11 Files;" Chapter 4, "Windows for Workgroups 3.11 Initialization Files."
- On-line HELP for Microsoft At Work fax, MSFAX.HLP

Contents of This Chapter

Overview of Microsoft At Work Fax Software.....	10-2
Sharing a Fax Modem Over the Network.....	10-5
Using the Advanced Dialing Feature.....	10-7
Entering Your Fax Modem Number and Advanced Dialing Prefixes.....	10-7
Entering Fax Numbers in the Personal Address Book	10-9
Using Security	10-10
Protecting Messages with Key Encryption.....	10-10
Establishing and Maintaining Security.....	10-10

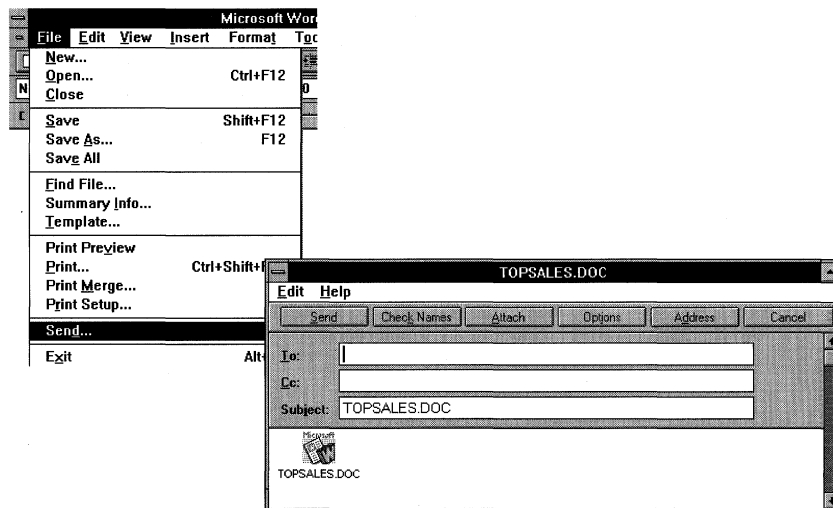
Overview of Microsoft At Work Fax Software

In June 1993, Microsoft unveiled a new software architecture to make a wide range of office tasks easier to perform and more cost-effective to accomplish. Microsoft At Work represents Microsoft's vision of the components necessary to tie together the digital office. Building on the existing business and technical infrastructure, the Microsoft At Work architecture focuses on creating digital connections between machines to allow information to flow freely throughout the workplace.

Windows for Workgroups 3.11 features the first PC-based implementation of the Microsoft At Work fax technology to simplify and improve communications for fax messaging. Microsoft At Work fax is integrated with the Windows environment and allows users to send fax messages from within Windows-based applications as easily as printing a document to a printer or sending an e-mail message.

Figure 10.1

To fax a message from within an application, simply choose *Print or Send* from the *File* menu.



Microsoft At Work fax provides many benefits over standard fax messaging, including the following:

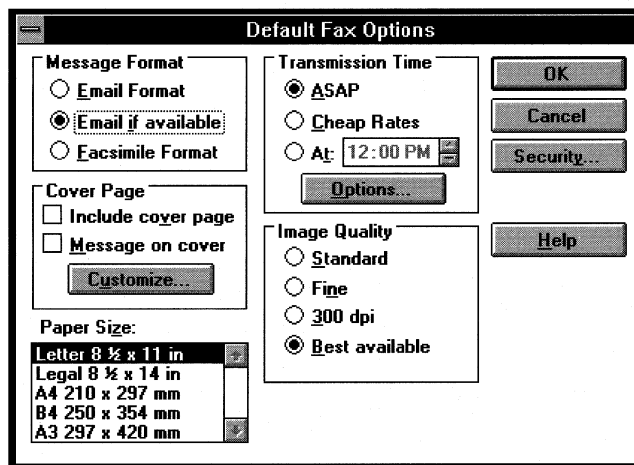
- **Extending the capabilities of fax by enabling the transmission of richer document formats**

Microsoft At Work fax allows users to send binary files, such as word processor files and spreadsheets, as easily as they send them via e-mail today. This capability will extend the workgroup to include anyone with Windows and a fax card. For example, Microsoft At Work fax will enable geographically separated groups to co-author and edit documents, or roll up financial statements. Companies can also use Microsoft At Work fax to automate mission critical tasks, such as automating the purchase order and

billing processes with subsidiaries. While a data communications package could be used to send binary information point-to-point, Microsoft At Work fax simplifies this exchange of information by using a familiar e-mail interface rather than a complex communications application.

Figure 10.2

Fax options that can be configured include identifying the time of transmission, cover page options, image quality, and security settings.



Microsoft At Work fax allows users to send messages with editable files, quality images, cover pages, and even specify the time of transmission.

- **Integrating fax into e-mail to create a single focal point for desktop messaging**

Microsoft At Work fax is fully integrated with the Windows for Workgroups Mail client. This will allow users to send documents either from Mail or from any Mail-Enabled Application (that uses the MAPI or CMC APIs). Windows for Workgroups users can use Microsoft At Work fax as a stand-alone fax application, or together with e-mail using the Workgroup Postoffice. Anyone using the Workgroup Postoffice or Microsoft Mail will be able to send information to e-mail users and fax users simultaneously. Fax addresses can be entered into the personal address book, and can be users with fax addresses can members of group aliases along with users of other types of e-mail addresses.

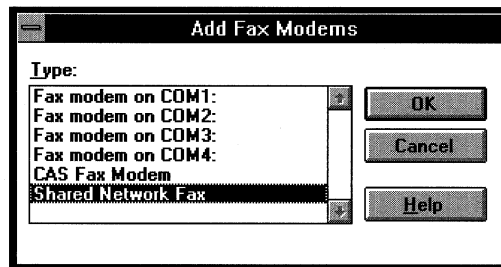
Received faxes go directly into the user's Mail inbox. For messages containing regular faxes, double clicking on the message brings up the fax viewer, where the user can view the fax, copy its contents to the clipboard, or print it out. The user can save received messages in private Mail folders and then share or in shared folders on the Postoffice. They can also forward or reply to received messages to both e-mail and fax recipients.

- **Sharing Fax boards in a workgroup environment**

Users of Windows for Workgroups can send messages via a fax board in their own computer, or multiple users can share a single fax board in one workstation on the network. Outbound faxes are automatically routed to the designated shared fax board. Inbound faxes are received by the machine with the shared fax board and are then automatically routed to the correct recipient's PC. Group 3 messages (those from a standard fax machine or most other types of PC fax software) are placed into the shared fax attendant's inbox, who must then forward the message to the designated recipient.

Figure 10.3

Fax modems can either be connected to a local communications port or shared on the network.



Windows for Workgroups users can share a fax modem for both sending and receiving fax messages.

- **Including tight security features, so users can confidently fax sensitive information**

Microsoft At Work fax includes a full security system. Users can encrypt documents to prevent others from reading them. They can require authentication of recipients before a message is delivered. They can also include a digital document signature that guarantees a document's contents has not been altered.

- **Complete compatibility with existing industry standard facsimile services**

Microsoft At Work fax is completely compatible with the 21 million installed Group 3 fax machines. Note that the advanced services described above (binary file transfer and security) are not available when communicating with Group 3 fax machines.

- **Compatibility with office equipment based on the Microsoft At Work architecture**

Microsoft At Work fax messaging will allow users to communicate directly with office devices, such as fax machines, servers and multifunctional peripherals that utilize the Microsoft At Work software. For example, from a Windows for Workgroups based PC, a user will be able to send a binary file to a Microsoft At Work-based fax machine that can automatically forward it to the appropriate recipient via the LAN.

Sharing a Fax Modem Over the Network

With Microsoft At Work fax, you can install a fax modem in one computer and share it with other computers on the same network. Individual computers can have their own fax modems installed and also use the shared fax modem.

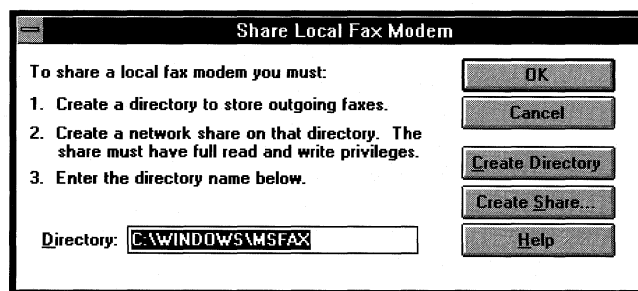
To share a fax modem with others on a network

1. From the Main group, choose the Control Panel icon, and then choose the Fax icon.
2. In the Fax Modems dialog box, verify that the modem you want to share with other users on the network is set as the active modem, and then choose the Share button.

Note The Share button changes to Stop Sharing when the default modem is shared.

Figure 10.4

Share Local Fax Modem dialog box for creating the directory where the fax queue will reside



3. In the Share Local Fax Modem dialog box, type the path of an empty shared directory that you want to use for the fax modem.
4. If you have not already created the directory, choose the Create Directory button to create the directory you have typed in the Directory box.

5. If you have not already shared the directory, choose the Create Share button and see the following procedure for creating a share.

If you are unable to create a share at this point, see your network documentation.

6. In the Fax Modems dialog box, choose the OK button.
The active modem is now shared.

Note If you change your shared active modem by selecting a modem on a different COM port, the new active modem becomes your shared modem. If you change your shared active modem by selecting a shared network fax modem, your new active modem will not be a shared modem.

To create a share

1. In the Share Local Fax Modem dialog box, choose the Create Share button. The Share Directory Dialog box appears.

Figure 10.5

The Share Directory dialog box is used to share the directory where the fax queue will reside on the network

2. In the Share Directory dialog box, type a name for the share in the Share Name box, or press TAB to accept the name of the directory as the share name.
3. The path of the directory you will be sharing appears in the Path box. Press TAB to proceed to the Comment field, or type the path of a different directory.
4. In the Comment field, type an optional description of the shared directory.
5. If you want the modem to be shared after restarting your computer, select the Re-Share At Startup check box.

6. Select either Full or Depends On Password for the Access Type.

Note You must change the Access Type from Read Only to Full when sharing the directory. If you leave the Access Type as read-only, other users will not be able to use your shared modem.

7. If you select Depends On Password, type the password in the Full Access Password box, and then choose the OK button twice.

Using the Advanced Dialing Feature

To enter a fax number into your Personal Address Book that can be used from anywhere in the world without changing any prefixes, use the advanced dialing feature. Microsoft At Work fax also uses the fax number to identify recipients to whom you will may send messages that have been digitally signed or encrypted for the purpose of security.

Three components make up the advanced dialing feature:

- Your fax modem number, including country and area codes
- The advanced dialing prefixes
- Recipient names and Fax numbers in your Personal Address Book entered in international format

Enter your fax modem number and the advanced dialing prefixes when you configure your fax modem.

Entering Your Fax Modem Number and Advanced Dialing Prefixes

Whenever you select a recipient with an internationally-formatted fax number from your Personal Address Book, Microsoft At Work fax reads your fax modem number and the advanced dialing prefixes to determine which numbers it must dial to connect. You entered your fax number and advanced dialing prefixes when you set up your modem. You can change this information at any time.

To change your fax modem number and add advanced dialing prefixes

1. In the Main group in Program Manager, choose the Control Panel icon, and then choose the Fax icon.
2. In the Fax Modems dialog box, choose the Setup button to open the Fax Setup dialog box.

Figure 10.6

Fax Setup dialog box

3. Type your complete fax modem number, including country code and area code.
4. Choose the Dialing button to open the Modem Dialing Options dialog box.

Figure 10.7

Modem Dialing Options dialog box

5. Type the appropriate prefixes:

Dialing Prefix: If you must dial a number to reach an outside line, type the number. For example, many business systems require "9."

Local Calls: Type any numbers required for local calls within your phone system. Most often, this setting is left blank.

Long Distance Calls: Type *all* the numbers required to reach an international line from your fax modem. For example, "9," if required, plus "011."

6. Choose the OK button three times, to close all open dialog boxes.

Note To use telephone calling cards with the prefix settings, you can enter the entire number in the *Dialing Prefix* setting using the following syntax:

9,<number to access long distance company>,,,<calling card number>,,,<destination number>

To increase the length of the pauses between numbers, increase the number of commas.

Entering Fax Numbers in the Personal Address Book

By entering fax numbers in your Personal Address Book in international format, you can take advantage of the advanced dialing feature and use your Personal Address book anywhere in the world without changes. The international format is:

recipient name@+countrycode-areacode-phonenummer

(Be sure to include the "+".)

To enter a fax number in international format in the Personal Address Book

1. In the Address Book dialog box, choose the Blank Card button.
2. In the New dialog box, select Microsoft At Work fax.
3. In the Fax number box type the fax number in international format.

When you select a recipient whose fax number is in international format, Microsoft At Work fax uses your fax modem number and the advanced dialing prefixes to determine what digits need to be dialed to complete the call.

For example, if you send a fax to a local recipient, Microsoft At Work fax determines that the country code and area code aren't required, so it doesn't dial them.

You can take your Personal Address Book to another country, connect to a new modem, and enter that modem's fax number and the advanced dialing prefixes. If you send a fax to the same recipient, Microsoft At Work fax determines that it now needs to dial the access code for an international line, then the country code and area code, and then the number.

Using Security

With Microsoft At Work fax, you can ensure the security of the faxes you send by *encrypting* them. An encrypted fax cannot be read by anyone except the intended recipient. You can also send a fax with a *digital signature*, which assures all recipients that only you could have sent it.

There are two ways to encrypt a fax—password encryption and key encryption. When you use password encryption, you type a password that locks the fax, and then tell the recipient what the password is. This method is less secure than key encryption, but it is sufficient for many situations.

Protecting Messages with Key Encryption

When you establish security, Microsoft At Work fax assigns to you two security keys—a private key and a public key. You can exchange public keys with anyone you choose. When you send a key-encrypted message, Microsoft At Work fax uses the recipient's public key and your private key to encrypt the message. When the message is received, Microsoft At Work fax uses your public key and the recipient's private key to *decrypt* it. Using your own private key ensures that the message could only have been sent by you. Using the recipient's public key ensures that only the recipient can unlock the message. (Both sender and recipient must be using Microsoft At Work fax software.)

You can also send a fax that is both digitally signed and encrypted.

Establishing and Maintaining Security

In order to send and receive secured faxes, and you must exchange public keys with your correspondents. You and your correspondents must all be using Microsoft At Work fax, must type your fax phone number in the fax setup dialog box in international format, and enable security.

You should disable security whenever you are not sending or reading secured faxes. The security system is password protected, and by disabling security you eliminate the possibility of someone using your private key either to read your encrypted messages or to send messages digitally signed by you.

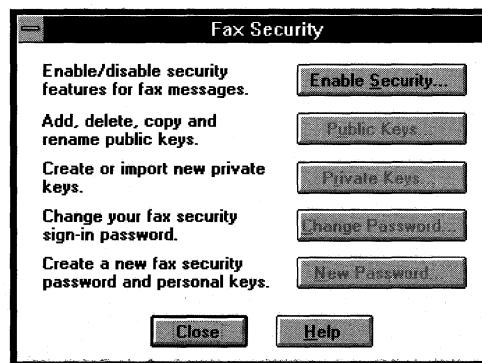
Important A digital signature is legally binding. Protect yourself from fraudulent use of your digital signature by disabling security when you are not using it. Never leave your computer while security is enabled.

To establish security

1. In Mail, choose Advanced Security from the Fax menu.
2. In the Fax Security dialog box, choose the Enable Security button.

Figure 10.8

The Fax Security dialog box used to configure At Work Fax security options



3. Microsoft At Work fax displays a message that you do not have an account and asks if you want to establish one. Choose the Yes button.
4. In the Password box, carefully type a password.
The characters you type do not appear on the screen.
5. In the Verify box, carefully type the password again, and then choose the OK button.
6. In the Fax Security dialog box, choose the Close button.

To enhance security, change your password periodically, using the Change Password button.

To disable security

1. In Mail, choose Advanced Security from the Fax menu.
2. In the Fax Security dialog box, choose the Disable Security button, and then choose the Close button.

To enable security

1. In Mail, choose Advanced Security from the Fax menu.
2. In the Fax Security dialog box, choose the Enable Security button.
3. In the Login dialog box, type your password, and then choose the OK button.

All the buttons except the New Password button are now available.

4. In the Fax Security dialog box, choose the Close button.

For information about sending a secured fax, see “Sending and Receiving Secured Faxes,” later in this chapter.

To change your password

1. When security is active, choose the Change Password button in the Fax Security dialog box.
2. In the Change Password dialog box, type your existing password in the Old Password box.

The characters you type will not appear on the screen.

3. In the New Password box, carefully type the new password.
4. In the Verify Password box, carefully type the new password again and then choose the OK button.

The purpose of verifying the password is to reduce the possibility of misspelling the password and locking yourself out of your own fax security.

5. In the Fax Security dialog box, choose the Close button.

To create a new password and change your personal keys

If you forget your password or suspect that your security has been breached, you can create a new password and change your personal keys to prevent the misuse of them by someone else. Changing your personal keys requires that you distribute your new public key to everyone who has your old one.

1. In Mail, choose Advanced Security from the Fax menu.
2. When security is disabled, in the Fax Security dialog box, choose the New Password button.

Microsoft At Work fax will display a warning. Choose the Yes button.

3. Carefully type the new password in the Password box, and then carefully type the password in the Verify box.
4. Choose the OK button.

Managing Personal Keys

The easiest way to exchange public keys is by exporting them to a floppy disk, and then exchanging disks with your correspondents. You can then import other people's public keys from the disks. You are safest if you only accept public keys directly from the owner, via registered mail, or from a third party who is well known and trusted by you. Otherwise you may receive a "signed" fax from an impostor, or you may send a secured fax that can be read by someone other than the intended recipient. If you receive a public key via registered mail, you can call the sender on the telephone to verify the contents.

You should always back up both of your personal keys so that you can restore them in the event of a computer failure. Exporting the keys to a floppy disk, and then locking the disk in a safe place is recommended. If you need to restore your personal keys, you can import them from the floppy disk.

Note The keys for security are stored in the file KEYFILE.DAT in your Windows directory.

Using Signed Keys

If you want a more secure method for exchanging public keys, you can create digitally signed keys. You can use this method to specify that all public keys imported by the users of your system must have the valid digital signature of a specified person. The owner of that signature verifies each public key before distributing the digitally signed key among users (via electronic mail or a network share, for instance). Each user then verifies the signature of the certifying person when using the Import Public Keys dialog to import the public key.

To create a signed key, first verify the authenticity of the key using the methods described earlier. Import the public key into your public key database and then use the Export Public Keys dialog to export it as a signed key. To export the key as signed, choose an .AWS extension for the name of the exported key file. Users who have already received your public key will be able to verify your signature on the key file and will feel confident that it contains valid public keys.

Not only do signed keys provide a more secure method of key distribution, they also make it easier to distribute keys to a large number of people. However, you should accept a key which has been signed by its owner only if you receive it directly or view the key and verify its contents with the owner. It is best use a trusted third party.

To export your private key to floppy disk

1. Insert a floppy disk into the disk drive.
2. When security is active, choose the Private Keys button in the Fax Security dialog box.
3. In the Private Key Management dialog box, choose the Export button.
4. In Filename box, type a name for the private key file.
The file name extension is .AWR.
5. Choose the floppy disk drive from the Drives list, and then choose the OK button.
6. In the Private Key Management box, choose the Close button.
Store your private key back-up in a secure location, such as a locked file cabinet, safe deposit box, or safe.

To import your private key from floppy disk

1. Insert the disk containing your private key into the disk drive.
2. When security is active, choose the Private Keys button in the Fax Security dialog box.
3. In the Private Key Management dialog box, choose the Import button.
4. Choose the floppy disk drive from the Drives list.
5. Select the .AWR file containing your private key from the list of files, or type the file name in the File Name box, and then choose the OK button.
6. In the Import Private Keys dialog box, type your password, and then choose the OK button.
7. In the Private Key Management dialog box, choose the Close button.

To export and import a public key

- Follow the procedures for exporting and importing private keys, but choose the Public Keys button in the Fax Security dialog box.

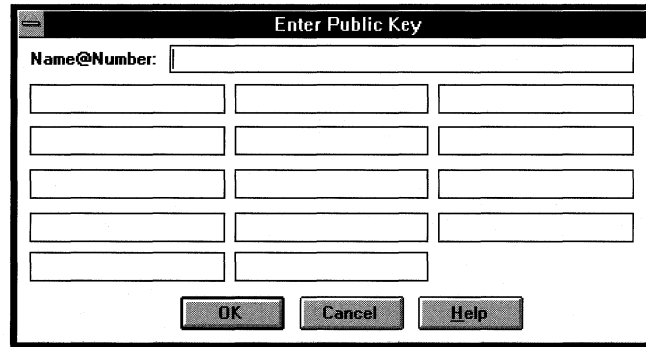
If someone gives you his or her public key on paper, you can enter the key into your system by simply entering it.

To type a public key

1. When security is active, choose the Public Keys button.
2. In the Public Keys dialog box, choose the Type In button.

Figure 10.9

The Enter Public Key dialog box



3. In the Name@Number box, type the recipient's name and fax number using the *name@number* format.

Note You must type the recipient's fax phone number in international format, which is:

recipient name@+countrycode-areacode-phonenumber

(Be sure to include the "+".)

4. Carefully type the contents of the key in the boxes, and then choose the OK button.

When security is enabled, you can view your or someone else's public key by choosing the View button in the Public Keys dialog box, and then selecting the key you want to view. To rename a public key, choose the Rename button. To copy a public key, choose the copy button.

Microsoft At Work fax uses the fax number included in the recipient's address to find the correct public key for that recipient. You should make certain that the fax number information included in the recipient's address is identical to the name of the key as it appears in the Public Keys dialog box.

Sending and Receiving Secured Faxes

When security is active you can send a key encrypted or digitally signed fax. You can also read a secured fax that you have received. You can set the key encrypt and sign options as global fax options.

You do not need to start security to send or read a password encrypted fax, however, you must select the password encrypt option for each password encrypted fax you send.

To send a password encrypted fax

1. In Mail, choose the Compose button
2. Choose the Options button on the Toolbar, and then choose the Fax button.
3. In the Fax Message Options dialog box, choose the Security button
4. Under Encrypt, choose the Password check box.
5. Carefully type the password in the Password box, and then carefully type the password in the Verify box.
6. Choose OK in the Fax Security dialog box, and then choose OK in the Options dialog box.
7. Address and send the fax as usual.
8. Notify the recipient of the password.

To send a key encrypted or digitally signed fax

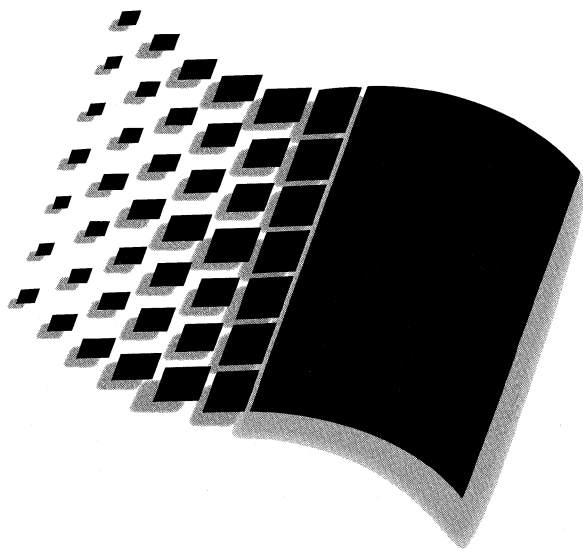
1. In Mail, choose Options from the Fax menu.
2. In the Default Fax Options dialog box, choose the Security button
3. In the Fax Security dialog box, select the option you want, and then choose the OK button.
4. In the Options dialog box, choose the OK button.
5. Send your fax as usual.

To read a secured fax

- With security active, read a secured fax exactly as you would any other fax or mail message.

If you have not started security, Microsoft At Work fax will notify you that you must do so before reading a secured fax.

Note When you are finished sending or reading secured faxes, disable security.



Configuring Windows for Workgroups 3.11

Part

5

***Configuring Windows for Workgroups
3.11***

Chapter 11 Tips for Optimizing Windows for Workgroups 3.11 **11-1**

Overview of Tips for Optimizing and Configuring	11-2
General Configuration Guidelines	11-2
Optimizing 32-bit File Access	11-7
Using Windows for Workgroups 3.11 as a Client Only	11-8
Using Windows for Workgroups 3.11 as a Client and Peer Server	11-12
Using Windows for Workgroups 3.11 as a “Dedicated” server	11-13

Chapter 12 Windows for Workgroups 3.11 Configuration Tips **12-1**

Overview of Configuration Tips	12-2
Tips for Sharing Resources	12-2
Windows for Workgroups Mail and Schedule+ Tips	12-3
Miscellaneous Configuration Tips	12-13

**Chapter
11**

Tips for Optimizing Windows for Workgroups 3.11

This chapter suggests tips for optimizing and configuring Windows for Workgroups 3.11 in order to achieve the best level of performance in different configuration scenarios.

Related information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 1, “Windows for Workgroups 3.11 Architecture;” Chapter 12, “Windows for Workgroups 3.11 Configuration Tips.”

Contents of This Chapter

Overview of Tips for Optimizing and Configuring	11-2
General Configuration Guidelines	11-2
SHARE.EXE	11-2
EMM386.EXE & Third-party Memory Managers	11-3
SMARTDRV.EXE	11-3
Optimizing 32-bit File Access	11-7
Using Windows for Workgroups 3.11 as a Client Only	11-8
General Guidelines	11-8
As a Client on a Microsoft Windows Network	11-9
As a Client on a Novell NetWare Network	11-11
Using Windows for Workgroups 3.11 as a Client and Peer Server	11-12
Adjust Server Priority as Needed	11-12
Use SmartDrive to Cache Shared CD-ROM drives	11-13
Using Windows for Workgroups 3.11 as a “Dedicated” server	11-13
Adjust Server Priority To “Resources Shared Fastest”	11-14
Increase 32-bit File Access Cache Size	11-15
Use SmartDrive to Cache Shared CD-ROM drives	11-15
Use NDIS 3 Network Card Driver if Available	11-16
Use a 32-bit Network Card	11-16
Don’t use a Screen Saver	11-16

Overview of Tips for Optimizing and Configuring

This chapter suggests tips for optimizing and configuring Windows for Workgroups 3.11 in the following scenarios:

- As a stand-alone no network configuration
- As a client where peer sharing is not enabled
- As a peer client and server
- As a “dedicated” server

In addition to discussing these configuration scenarios, we’ll also examine some general configuration guidelines that will help you to get the most out of Windows for Workgroups 3.11.

General Configuration Guidelines

Before getting into specifics suggestions for optimizing Windows for Workgroups 3.11, we’ll first define a base configuration.

When looking at your system configuration, you should check the following components to determine whether they are being used on your system and whether or not you can remove them to optimize your configuration.

SHARE.EXE

SHARE.EXE is an MS-DOS terminate and stay resident (TSR) program that provides file sharing and file locking support when you are running applications in MS-DOS.

Windows for Workgroups 3.11 provides a virtual device driver (VxD), called VSHARE.386, that provides the same functionality of SHARE.EXE without using any conventional memory. Removing SHARE.EXE will save approximately 6K of conventional memory.

Note It is only necessary to load SHARE.EXE when running applications from MS-DOS (i.e., without starting Windows for Workgroups) that require file sharing and file locking support. Check the documentation provided with your application to determine whether SHARE.EXE is necessary.

EMM386.EXE & Third-party Memory Managers

EMM386.EXE, included with Windows for Workgroups 3.11 and MS-DOS, provides access to upper memory and simulates expanded memory using extended memory. This is beneficial for MS-DOS-based applications that can use expanded memory. EMM386 also makes it possible to load programs and device drivers into upper memory blocks (UMBs). While this section discusses EMM386 specifically, the information is also relevant to the use of third-party memory management utilities that provide similar functionality.

Although EMM386 can provide more free conventional memory by loading programs and device drivers into UMBs, this only helps when running MS-DOS-based applications. Windows for Workgroups 3.11 uses extended (XMS) memory to run the Windows operating system and Windows-based applications.

Accessing device driver and application code from UMBs is slower than accessing the same code directly from conventional memory. To maximize the performance when accessing MS-DOS-based device drivers, it is recommended that EMM386 (or similar third-party memory managers) not be used.

In addition to possible performance penalties, EMM386.EXE will use approximately 150K of XMS (extended) memory to provide a mappable memory range for the UMA in which to load device drivers.

Note If you are not running MS-DOS-based applications that require more conventional memory than is available after loading the necessary device drivers and programs in conventional memory, and you are not using MS-DOS-based applications that require EMS memory, you may remove EMM386.EXE from your CONFIG.SYS file without adversely affecting the system.

SMARTDRV.EXE

SmartDrive provides disk caching support when Windows for Workgroups 3.11 is not running, when 32-bit File Access is disabled in Windows for Workgroups 3.11, or when 32-bit File Access is disabled on a given disk

volume. In order to provide more memory for use by Windows for Workgroups 3.11 when 32-bit File Access is enabled, you may either remove SMARTDRV.EXE from your AUTOEXEC.BAT file, or reduce the amount of memory that SmartDrive uses to provide disk caching support.

Note When the 32-bit File Access disk cache size is changed, the SMARTDRV.EXE line in your AUTOEXEC.BAT file is updated to reflect a smaller WinCacheSize value.

When 32-bit File Access is enabled, it may be necessary to continue to use SmartDrive to provide disk caching functionality in the following scenarios:

- MS-DOS 6.0 is running with DoubleSpace on a compressed volume
- Support for caching CD-ROM drives is desired
- Support for caching floppy disk drives is desired

To Identify Which Drives SmartDrive is Caching

When 32-bit File Access is enabled, the 32-bit File Access driver will disable SmartDrive from caching on disk volumes that the VFAT VxD mounts. To identify the disk volumes that SmartDrive is continuing to cache after VFAT loads, type "SMARTDRV" at the MS-DOS command prompt from within Windows for Workgroups 3.11 and observe the drive letters that are present. Drive letters that do not appear for physical drives in the system are either being cached by the 32-bit File Access driver, or are not being cached at all.

For example, the following SmartDrive disk cache report shows that drive C is not being cached by SmartDrive, but drive D, which is a CD-ROM drive, is being cached by SmartDrive (32-bit File Access is responsible for caching drive C in this scenario):

```
Microsoft SMARTDrive Disk Cache version 5.0
Copyright 1991,1993 Microsoft Corp.
```

```
Cache size: 262,144 bytes
Cache size while running Windows: 262,144 bytes
```

```

      Disk Caching Status
drive  read cache  write cache  buffering
-----
A:      yes        no           no
B:      yes        no           no
D:      yes        no           no
```

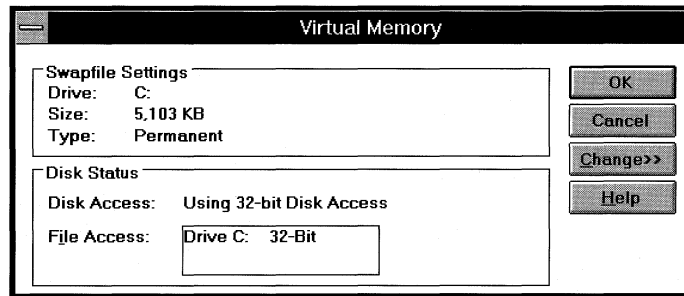
```
Write behind data will be committed before command prompt returns.
```


Identifying the drives that 32-bit File Access is caching

To identify which drives 32-bit File Access is being used on, double-click the Enhanced icon in Control Panel, and choose the Virtual Memory button. The Disk Status section of the Virtual Memory dialog box shows the status of Disk Access and File Access as shown in Figure 11.1.

Figure 11.1

Virtual Memory dialog box shows Disk Status of 32-bit support



For the disk volumes used on the system, File Access will either identify a drive as using 32-bit access or 16-bit access. If a given drive is shown as using 32-bit access, then the 32-bit File Access driver is caching the drive and SmartDrive kept from caching the drive. If a given drive is shown as using 16-bit access, then the 32-bit File Access driver is not caching the drive and SmartDrive is caching the drive, if SmartDrive is loaded.

Note When 32-bit File Access is enabled, you will want to increase the size of the cache used for the 32-bit File Access disk cache based on the amount of physical memory you have in your computer. Tips for optimizing the 32-bit File Access cache are discussed later in this chapter.

If 32-bit access is shown for all physical drives in the system, you may remove or reduce the memory size of the cache used when running Windows for Workgroups 3.11. The next two sections discuss removing and reducing the size of the SmartDrive disk cache.

Removing SMARTDRV.EXE

If you don't fit into one of the preceding scenarios, you can remove the line in your AUTOEXEC.BAT file that references SMARTDRV.EXE, or you can place "REM" at the beginning of the line that references SMARTDRV.EXE to remark it out and prevent it from being loaded. By removing SMARTDRV.EXE from your system, you can save both the XMS memory normally used by the cache, in addition to approximately 30 KB of conventional memory used by the SMARTDRV.EXE program.

If SMARTDRV.EXE is not loaded by the AUTOEXEC.BAT file, you can invoke SmartDrive manually by typing SMARTDRV (with the appropriate command line parameters) at the MS-DOS command prompt.

Reducing the Memory Used by SmartDrive

If you run MS-DOS–based applications from MS-DOS without starting Windows for Workgroups 3.11, you may wish to continue to use SmartDrive. However, if 32-bit File Access is enabled on all of your physical drives in your system, you may wish to reduce the size of the SmartDrive cache used when you are running Windows for Workgroups 3.11.

SmartDrive supports two different memory parameters when running in MS-DOS, InitCacheSize, and when running in Windows, WinCacheSize. If SmartDrive is loaded, when Windows starts SmartDrive will change the size of the cache from the InitCacheSize value to the WinCacheSize value. The following table identifies the default values used by SmartDrive in these two scenarios.

Total available XMS memory	InitCacheSize	WinCacheSize
1 MB	1 MB	0
2 MB	1 MB	256KB
4 MB	1 MB	512KB
6 MB	2 MB	1 MB
>= 8 MB	2 MB	2 MB

If 32-bit File Access is responsible for caching all physical drives, it can be observed that the WinCacheSize default memory value can use a substantial amount of physical memory unnecessarily.

You may want to reduce the size of the SmartDrive disk cache in the following scenarios rather than removing it from your AUTOEXEC.BAT file:

- You often operate in MS-DOS as well as within Windows for Workgroups, so it's convenient to always have SmartDrive loaded.
- You wish to continue to have SmartDrive load and available while within Windows for Workgroups to cache CD-ROM drives

To change the size of the SmartDrive cache, specify the value for the InitCacheSize and the value for the WinCacheSize parameters on the line in your AUTOEXEC.BAT file that references SMARTDRV.EXE. For example, the following sample entry for SMARTDRV.EXE assumes an 8 MB machine and sets InitCacheSize to 2048 KB (2 MB) and WinCacheSize to a minimal value of 128 KB — this frees up an additional 1920 KB (2048KB - 128KB) when Windows for Workgroups 3.11 runs.

Sample SMARTDRV.EXE Line in AUTOEXEC.BAT File

```
C:\WINDOWS\SMARTDRV.EXE 2048 128 /X
```

Optimizing 32-bit File Access

In general, it is best to use a cache size big enough to hold the data that you are reading or writing. If the cache size is large enough to hold the data you are reading, the system should be able to minimize the number of times required to access the disk and access the data directly from the cache. If the cache is too small to hold the data, the cache management routines will constantly have to throw data out of the cache in order to make room for new data read from disk. The optimal size of the cache is dependent upon the amount of physical memory available in the computer, as well as the size of data you will be reading or writing.

When 32-bit File Access is enabled, the cache size is set to the default values shown in the following table. Using a cache that is too small, will reduce the possible performance gains that 32-bit File Access can provide.

Total available memory	Default Cache Size
<= 4 MB	512 KB
<= 6 MB	1024 KB
<= 8 MB	2048 KB
<= 12 MB	3064 KB
> 12 MB	4096 KB

If you are using 32-bit File Access, check your AUTOEXEC.BAT file to verify that either SMARTDRV.EXE has been removed, or the SmartDrive WinCacheSize value has been reduced in size.

The different configuration scenarios presented in the following sections assume you are using the default cache size selected by the 32-bit File Access configuration routines, with the exception of using Windows for Workgroups 3.11 as a “dedicated” server.

Using Windows for Workgroups 3.11 as a Client Only

In this section, we'll discuss the different steps to optimize your Windows for Workgroups 3.11 configuration to work best as a client in several scenarios. It is assumed in this section that file sharing and printer sharing are not being used.

General Guidelines

There are some general guidelines that you should follow when using Windows for Workgroups 3.11 as a client to other network servers. The following recommendations apply when Windows for Workgroups 3.11 is used as a client to other servers on your network:

- Disable file sharing and printer sharing
- Choose the right network transport protocol
- Remove unnecessary network transport protocols
- Install Windows for Workgroups 3.11 on the local computer

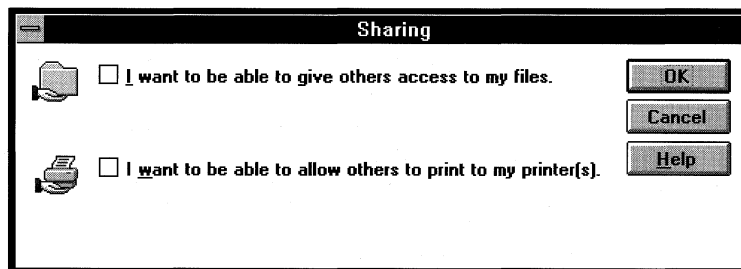
Disable File Sharing and Printer Sharing

Disabling file sharing and printer sharing will prevent the protect mode server from loading, thus providing more extended memory in which to run Windows-based and MS-DOS-based applications.

To disable file sharing and printer sharing, click the Sharing button in the Network Setup dialog box to display the Sharing dialog box as shown in Figure 11.2. Clear the two check boxes to disable file sharing and printer sharing.

Figure 11.2

Windows for Workgroups Sharing dialog box, which can be used to disable file and printer sharing



Choose the Correct Network Transport Protocol

While the network transport protocol used by a Windows for Workgroups 3.11 client is dependent upon the network protocols in use by the server, it is important to select the right network transport protocol based on the type of network activity. NetBEUI provides the fastest level of performance for big I/O activity including copying large files or blocks of information from a network server, and launching applications from a network server. The use of the 32-bit IPX/SPX compatible transport provides the best level of performance for transactional or small I/O requests.

Remove Unnecessary Network Transport Protocols

Each installed network transport protocol uses memory. Windows for Workgroups 3.11 will attempt to communicate over each network transport that is installed. Because of this, it is recommended to only install the network transport protocols necessary to communicate with server resources, in order to conserve memory and reduce overhead.

Install Windows for Workgroups 3.11 on the Local Computer

Generally, the amount of time it takes to access information from a local hard disk is smaller than the amount of time it takes to access information from a network server. To get the best level of performance when running Windows for Workgroups 3.11, it is recommended to install Windows for Workgroups 3.11 on the local computer rather than running it from a network server. If the available disk space is tight for installing Windows for Workgroups 3.11 locally, you can move some of the files that are not accessed frequently to the network server. These files may include readme files, certain accessories and their related help files. In addition to installing Windows for Workgroups 3.11 locally, it is best to store the swapfile on the local computer.

As a Client on a Microsoft Windows Network

When Windows for Workgroups 3.11 is used in a client-only configuration to communicate with other Windows for Workgroups, Windows NT, Windows NT Advanced Server, or computers running the Workgroup Add-on for MS-DOS, the following recommendations apply:

- Use NDIS 3 network card driver if available
- Select the appropriate network transport
- Enable ghosted connections

Use NDIS 3 Network Card Driver if Available

Using an NDIS 3 network card driver in conjunction with NDIS 3-compatible protect mode network transport protocols will provide the best level of performance. If an NDIS 3 network card driver is not provided in the Windows for Workgroups 3.11 box, check the Windows Driver Library (see Appendix A, "Additional Support Information" for more information on the WDL) to see if an NDIS 3 network card driver is available. If an NDIS 3 network card driver is not available for your network card, use an NDIS 2 network card driver.

Select the Appropriate Network Transport

Select the appropriate network transport protocol for use on Windows for Workgroups 3.11 depending on the type of network server you are accessing. The following table provides a summary of different scenarios and the associated network transport protocol you should use.

Type of Server to Access	Network Transport Protocol
Windows for Workgroups 3.10	NetBEUI
Windows for Workgroups 3.11 with Network DDE	IPX/SPX Compatible Transport with NetBIOS
Windows for Workgroups 3.11 without Network DDE	IPX/SPX Compatible Transport
Microsoft LAN Manager (or compatible)	NetBEUI
Workgroup Add-on for MS-DOS	NetBEUI
Windows NT or Windows NT Advanced Server	IPX/SPX Compatible Transport with NetBIOS

Enable Ghosted Connections

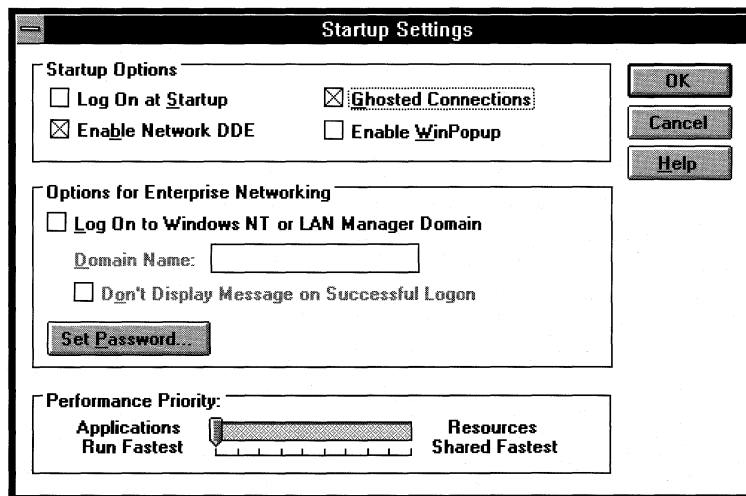
By default, ghosted connections are enabled. When the ghosted connections setting is enabled, Windows for Workgroups 3.11 will initialize data structures used to map local drives and local printer ports to network resources, but will not physically attach to the network resource until the user tries to access the resource.

By not physically attaching to a shared resource, Windows for Workgroups 3.11 can start up and can give the user control of the user interface faster than if the physical connection was made. Since the user may not be physically attached to a resource when the user, for example, clicks one of the drive icons in File Manager, the user may see a slight delay before the directory for the network drive is displayed. This slight delay is balanced with a possibly long start up time depending on the number of persistent network connections.

Ghosted connections can be enabled or disabled from the Startup icon in the Microsoft Windows Network section of Control Panel, as shown in Figure 11.3.

Figure 11.3

Startup Settings dialog box is used to enable/disable Ghosted Connections



As a Client on a Novell NetWare Network

When Windows for Workgroups 3.11 is used in conjunction with the Novell NetWare client software, the following recommendations apply:

- Remove the Novell NetBIOS TSR
- Remove NetBEUI if not needed

Remove the Novell NetBIOS TSR

If you are using the monolithic/dedicated IPX driver or have selected the IPX/SPX Compatible Transport with NetBIOS protocol, you may remove the Novell NetBIOS TSR driver from conventional memory. This will save approximately 30K of conventional memory.

Remove NetBEUI if Not Needed

If you do not need to communicate with a Windows for Workgroups 3.1 server (which doesn't support peer sharing over IPX and requires NetBEUI), Workgroup Add-on for MS-DOS peer server, or with a Microsoft LAN Manager (or compatible) server, remove the NetBEUI protocol from the Network Drivers dialog box in Network Setup. The NetBEUI protocol is not needed to support peer services unless you need connectivity to one of the above mentioned network servers.

Using Windows for Workgroups 3.11 as a Client and Peer Server

In this section, we'll discuss the different steps to optimize your Windows for Workgroups 3.11 configuration to work best as both a client and peer server in several scenarios. The optimization steps discussed in the previous section, "Using Windows for Workgroups as a Client Only," also apply when Windows for Workgroups 3.11 file sharing or printer sharing is enabled.

There are some guidelines that you should follow when using Windows for Workgroups 3.11 as a client and peer server on your network. When Windows for Workgroups 3.11 is used as a client to other servers on your network, the following recommendations apply:

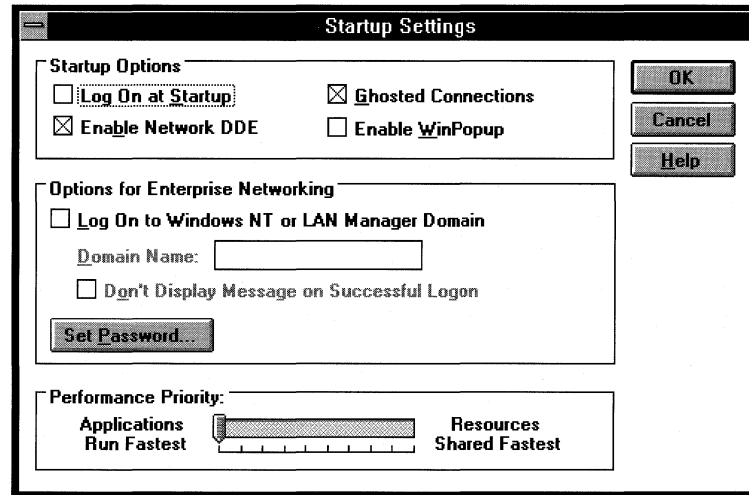
- Adjust server priority as needed
- Use SmartDrive to cache shared CD-ROM drives

Adjust Server Priority as Needed

Depending on the level of activity you experience when other users access resources shared on your computer, you may want to increase the Performance Priority slider bar that is located in the Startup Settings section of the Network icon in Control Panel. The Performance Priority slider bar controls the priority of the server process running under Windows for Workgroups 3.11 when users are accessing resources on your local computer. More priority is given to applications running in the system when the slider bar is to the left ("Applications Run Fastest"), whereas more priority is given to the server process when the slider bar is to the right ("Resources Shared Fastest").

Figure 11.4

Sliding the Performance Priority slider bar to "Applications Run Fastest" setting provides best performance for running applications on local computer



Use SmartDrive to Cache Shared CD-ROM drives

If you are sharing a CD-ROM drive, use SmartDrive to cache data read from the CD-ROM. Place the MSCDEX driver before SMARTDRV.EXE in your AUTOEXEC.BAT file using the "/s" parameter on MSCDEX.EXE to support sharing the CD-ROM drive.

The WinCacheSize value for SmartDrive will represent the size of the cache to use when SmartDrive caches read data from the CD-ROM. You may want to increase the size of the value listed in your AUTOEXEC.BAT file for the WinCacheSize parameter depending on the amount of memory available in your computer, the frequency at which users will be accessing the CD-ROM drive, and the type of data present on the CD-ROM drive.

Using Windows for Workgroups 3.11 as a "Dedicated" server

In this section, we'll discuss the different steps to optimize your Windows for Workgroups 3.11 configuration to work best as a "dedicated" server. A dedicated server is a computer that is only sharing resources, but does not need to access other shared resources on the network.

There are some guidelines that you should follow when using Windows for Workgroups as a dedicated server on your network. When Windows for Workgroups 3.11 is used as a dedicated server on your network the following recommendations apply:

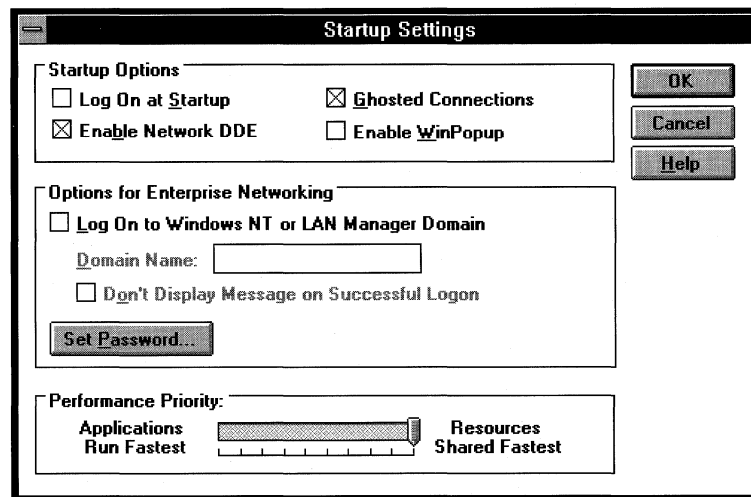
- Adjust server priority to “Resources Shared Fastest”
- Increase 32-bit File Access cache size
- Use SmartDrive to cache shared CD-ROM drives
- Use NDIS 3 network card driver if available
- Use a 32-bit network card
- Don’t use a screen saver

Adjust Server Priority To “Resources Shared Fastest”

To provide the highest priority to the server process, increase the Performance Priority located in the Startup Settings section of the Network icon in Control Panel. The Performance Priority slider bar controls the priority of the server process running under Windows for Workgroups 3.11 when users are accessing your local resources. Move the Performance Priority slider bar all the way to the right, as shown in Figure 11.5 to support sharing resources the fastest.

Figure 11.5

Sliding the Performance Priority slider bar to “Resources Shared Fastest” setting provides best performance for users accessing shared resources on your computer



Increase 32-bit File Access Cache Size

To provide the highest response rate to users accessing shared directories on your computer, increase the size of the 32-bit File Access cache above the default values. The default values assume that you will also be running applications on your system and are thus set to provide a balance between cache size and available physical memory in which to run applications.

Since you will be using the Windows for Workgroups computer as a dedicated server, you can maximize the cache size while minimizing the amount of available memory used to run applications on your system. The following table provides some recommendations on cache size depending on the amount of physical memory you have in your computer. A general rule is to use all but 4096K (4 MB) of total physical memory for the 32-bit cache size.

Total available memory	Cache Size to Use
<= 4 MB	512 KB
<= 6 MB	2048 KB
<= 8 MB	4096 KB
<= 12 MB	6144 - 8192 KB
> 12 MB	All but 4096 KB

Use SmartDrive to Cache Shared CD-ROM drives

If you are sharing a CD-ROM drive, use SmartDrive to cache data read from the CD-ROM. Place the MSCDEX driver before SMARTDRV.EXE in your AUTOEXEC.BAT file using the "/s" parameter on MSCDEX.EXE to support sharing the CD-ROM drive.

The WinCacheSize value for SmartDrive will represent the size of the cache to use when SmartDrive caches read data from the CD-ROM. Increase the size of the value listed in your AUTOEXEC.BAT file for the WinCacheSize parameter depending on the amount of memory available in your computer, the frequency at which users will access the CD-ROM drive, and the type of data present on the CD-ROM drive. Since the computer will be running Windows for Workgroups as a dedicated server, you may want to specify a 1MB or 2MB cache size.

It is important to note that SmartDrive will use the amount of memory identified by the WinCacheSize parameter, thus reducing the amount of available memory. You may need to adjust the size of the 32-bit File Access cache slightly in order to provide a balance of available memory.

Use NDIS 3 Network Card Driver if Available

Using an NDIS 3 network card driver in conjunction with NDIS 3-compatible protect mode network transport protocols will provide the best level of performance. If an NDIS 3 network card driver is not provided in the Windows for Workgroups 3.11 box, check the Windows Driver Library (see Appendix A, “Additional Support Information” for more information) to see if an NDIS 3 network card driver is available. Since this computer won’t be a client to another server, it is not necessary to use ODI drivers or load the NetWare client software.

Use a 32-bit Network Card

If your system supports a 32-bit adapter bus, use a 32-bit bus mastering or EISA network adapter card along with an NDIS 3 network card driver, if available. A 32-bit bus mastering or EISA network adapter card allows the network card to offload network I/O requests from the CPU of the computer to the network card itself, thus providing improved network I/O performance.

Examples of 32-bit network cards for which 32-bit NDIS 3 network card drivers are available include the Novell/Anthem NE3200, Compaq NetFlex, or Proteon 1990 network card. Check the Windows Driver Library for other available 32-bit NDIS 3 network card drivers.

Note Microsoft does not specifically recommend one network card over another—the network cards listed above are provided as an example only. Check with other sources for specific performance information.

Don’t use a Screen Saver

Screen savers can take away cycles from your CPU, thus providing a lower level of performance when sharing resources if the screen saver is active. In order to provide the best level of performance, either don’t use a screen saver or choose a screen saver that is not CPU intensive.

Chapter
12

**Windows for Workgroups 3.11
Configuration Tips**

This chapter provides a collection of tips and information on configuring and customizing Windows for Workgroups in various scenarios.

Related Information

- *Windows for Workgroups Resource Kit Addendum for version 3.11:* Chapter 2, “Windows for Workgroups 3.11 Setup and Installation.”
- *Microsoft Workgroup Add-on User’s Guide*, Appendix A, “Maintaining Mail.”
- Windows for Workgroups 3.11 Mail readme file, MAIL.WRI

Contents of This Chapter

Overview of Configuration Tips	12-2
Tips for Sharing Resources	12-2
Hiding Network Share Names.....	12-2
Sharing CD-ROM Drives	12-3
Windows for Workgroups Mail and Schedule+ Tips.....	12-3
Re-creating the Mail Initialization Procedure	12-4
Setting Up a Postoffice Across the Network	12-5
Using Mail with a NetWare Network.....	12-8
Moving a WGPO From One Computer To Another	12-8
Changing the WGPO Administrator	12-9
Allowing Multiple Users to Log On to Windows for Workgroups Mail on the Same Computer	12-10
Creating Global Address Groups for Users of Mail	12-12
Miscellaneous Configuration Tips.....	12-13
Quick Access to Network Section in Control Panel.....	12-13
Token Ring Cards and Local Addressing.....	12-13

Overview of Configuration Tips

This chapter provides a collection of tips for configuring Windows for Workgroups 3.11 in various scenarios. These configuration and installation tips are helpful for users, support organizations, value-added resellers (VARs) and system integrators.

The topics covered in this chapter include:

- “Tips for Sharing Resources” includes tips on how to restrict unauthorized access to network resources.
- “Windows for Workgroups Mail and Schedule+ Tips” provides tips on different configuration scenarios for installing and configuring Mail and Schedule+. In addition to new installation tips, tips are provided for modifying a Mail configuration after Mail has already been installed.

Tips for Sharing Resources

This section presents some tips for sharing resources using Windows for Workgroups 3.11.

Hiding Network Share Names

When sharing resources such as directories or printers using Windows for Workgroups 3.11, a dollar sign (“\$”) character can be appended to the end of a share name, keeping the share name from appearing in a browsed list of available shares on the server. This ability to “hide” a share name, prevents unauthorized users from browsing the list of available shares on network servers, and limits access to a given share by requiring that the network computer user know the exact share name in order to access the resource. This functionality enables a user to share a directory on his or her computer in a safe manner, without assigning a password.

For example, if drive C is shared as ROOT\$ on the computer named SERVER, then ROOT\$ does not appear in the Shared Directories or Shared Printer section of the Connect Network Drive or Connect Network Printer dialog boxes, respectively. The ROOT\$ share will also not appear if a user issues a NET VIEW from the MS-DOS command prompt. However, if a user enters \\SERVER\ROOT\$ as the path in the Connect Network Drive dialog box, the user can connect to the hidden server.

Sharing CD-ROM Drives

In order to share a CD-ROM drive, the Microsoft CD-ROM Extensions driver, MSCDEX.EXE version 2.21 or later, must be loaded and the /s option specified when the MSCDEX.EXE driver is invoked. The /s option is used to tell the system that the CD-ROM drive will be shared (if the /s option is not specified, the local user will be able to access the CD-ROM drive, however the user will not be able to share the drive from File Manager).

After the MSCDEX driver has been loaded and Windows for Workgroups has been started, the user can share directories on a given CD-ROM in the same manner as sharing directories on a local hard disk.

If you are using SmartDrive 5.0, you can also cache read access to the CD-ROM drive by placing the reference in your AUTOEXEC.BAT file to SMARTDRV.EXE *after* the reference to MSCDEX.EXE. If SmartDrive 5.0 detects that the MSCDEX.EXE driver is loaded, SmartDrive will attempt to cache read operations that are performed against the CD-ROM drive.

Sample AUTOEXEC.BAT file with MSCDEX configured for sharing a CD-ROM drive

```
C:\WINDOWS\net start

C:\WINDOWS\MSCDEX.EXE /S /d:cdrom1 /l:d

C:\WINDOWS\SMARTDRV.EXE /X
PROMPT $p$g
PATH C:\WINDOWS;C:\DOS
SET TEMP=C:\WINDOWS\TEMP
```

Windows for Workgroups Mail and Schedule+ Tips

This section is divided into the following topics:

- “Re-creating the Mail Initialization Procedure” outlines steps that should be taken if errors occur when initializing Mail for the first time. These procedures are useful if a user incorrectly specifies the option of connecting to an existing postoffice or becoming the Workgroup Postoffice (WGPO).
- “Setting up a Postoffice Across the Network” describes the steps for setting up and administering a postoffice on one computer while placing the WGPO on another computer. This section includes postoffice naming conventions and troubleshooting steps.

- “Using Mail with Novell NetWare” provides additional information needed to successfully set up a Novell NetWare Postoffice.
- “Moving a WGPO from One Computer to Another” describes steps for moving a Workgroup postoffice to a different server without transferring WGPO administration responsibilities.
- “Changing the WGPO Administrator” describes steps for transferring WGPO administration and management responsibilities from one person to another.
- “Allowing Multiple Users to Log On to Windows for Workgroups Mail on the Same Computer” explains how to set up one computer for multiple postoffice accounts.
- “Creating Global Address Groups for Users of Mail” explains the steps necessary for an administrator to define groups of mail users that can be used by all users of Mail.

Re-creating the Mail Initialization Procedure

When you first run Windows for Workgroups Mail, you are given the option to connect to an existing postoffice or create a new postoffice. After you make your selection, you cannot go back and change your selection.

Steps to Reinitialize Mail

If you want to change your initial selection, you must use the following steps to reinitialize Mail so that you can select the option you want.

1. Open the MSMAIL.INI file in an ASCII text editor, such as Microsoft Windows Notepad.
2. Disable the **ServerPath=** and the **login=** lines by typing a semicolon (;) at the beginning of each line.
3. Add or edit the **CustomInitHandler=** line so that it appears as follows:
CustomInitHandler=WGPOMGR.DLL,10
4. Run Mail. The initialization procedure begins.

How Mail Initialization Works

The initialization procedure is defined for Mail in the MSMAIL.INI file on the **CustomInitHandler=** line. This setting is defined as:

```
CustomInitHandler=WGPOMGR.DLL,<procedure #>
```

When you run Mail, it checks for the existence of the **CustomInitHandler=** line in the MSMAIL.INI file. If this line exists, Mail tries to run the procedure defined by this parameter setting. If this attempt fails because the dynamic link library (DLL) file WGPOMGR.DLL cannot be found or the procedure is undefined, Mail continues without reporting an error.

The procedure, located in WGPOMGR.DLL, displays the Connect Or Create dialog box to allow you to either connect to an existing remote postoffice or create a new Workgroup Postoffice.

- If you choose the Cancel button, WGPOMGR.DLL closes Mail.
- If you choose the OK button, WGPOMGR.DLL removes the **CustomInitHandler=** line from the MSMAIL.INI file and returns to Mail, automatically signing you in to the postoffice.

Setting Up a Postoffice Across the Network

With Windows for Workgroups Mail, the Workgroup Postoffice can be set up from one computer to another computer across the network.

For the example below, assume the following conditions are true:

- The postoffice is set up and administered from Computer1.
- The postoffice files are actually kept on Computer2.

Note The user on Computer1 is the Postoffice Manager, but the postoffice files are stored on Computer2.

- Computer1 is a Windows for Workgroups computer.
- Computer2 is a computer with server/sharing capabilities, such as a Windows for Workgroups computer, a LAN Manager 2.1 server, or a Novell server.

Note Novell servers require some special attention. Refer to “Using Mail with a NetWare Network” later in this chapter.

Steps to Connect to Other Computers

After Windows for Workgroups 3.11 setup is complete on Computer1, the designated administrator of the Workgroup Postoffice should take the following steps:

1. On Computer1, from the Main group, start Workgroups Mail.
2. Choose Create A New Workgroup Postoffice from the dialog box that is displayed.
3. To connect to Computer2, choose the Network button in the connect dialog box on Computer1.

If Computer2 is a Windows for Workgroups computer or a LAN Manager 2.1 server, type the server name and share name (that is, `\\server\share`) where you want the postoffice created, then choose OK.

Note You must have access rights to the server and the share.

If Computer2 is a Novell server, you must be logged onto the Novell server and have the correct permissions. Then, you should connect to the server and use one of these conventions:

```
server/share:directory
\\server\share\directory
remapped drive:\directory
```

For more information on the Novell naming conventions, check your Novell NetWare documentation. For more information on Windows for Workgroups naming conventions, see the "Windows for Workgroups Server, Share, and Mail Naming Conventions" section in this article.

4. After the Workgroup Postoffice is established, check to ensure that the postoffice is shared properly on Computer2.

Postoffice Naming Conventions

The following name length limitations exist in Microsoft Windows for Workgroups Mail:

Server Name:	15 characters
Share Name:	12 characters
Workgroup Postoffice Share:	8 characters

Windows for Workgroups Mail clients cannot connect to a Workgroup Postoffice if the share name contains more than eight characters, or if the Workgroup Postoffice server name or share name contains any spaces.

For example, the following are examples of invalid Workgroups Postoffice server or share names because of the use of spaces in the server or share names:

```
\\ser ver\wgpo  
\\server\wg po  
\\server\postoffice
```

The following is a valid Workgroups Postoffice server or share name:

```
\\server\wgpo
```

Note It is recommended that the share name “WGPO” be used for consistency across all Workgroup Postoffices.

Resolving Local Postoffice Connection Problems

If a Windows for Workgroups mail administrator sets up the Workgroup Postoffice (WGPO) on another workgroup user’s computer, that other user cannot connect to the postoffice and receives one of the following error messages:

The selected network path cannot be found.

This operation is not supported on this computer.

For example, if the mail administrator, working at a computer named “Admin,” creates the WGPO on a computer called “Computer1,” the user of Computer1 is unable to connect to the WGPO. To work around this problem, you must manually edit or create a new MSMAIL.INI file for Computer1.

Note Windows for Workgroups Mail defaults to universal naming conventions (UNC) to specify the location of the postoffice. UNC cannot be used to connect a user to a share on his/her local computer. Browsing for the WGPO share on the local computer results in the “not supported” error message. Manually typing in the UNC name of the share (<computername>\WGPO) results in the path not being found, as does typing in the local path (F:\WGPO).

Defining Connection to Local WGPO on WGPO Server

These steps will configure the MSMAIL.INI file on the local computer to be able to attach to the WGPO. When Mail is started for the first time, the user is prompted to connect to the WGPO automatically.

1. Copy the MSMAIL.INI file from a computer that is already connected to the WGPO.

2. Edit the MSMAIL.INI file for Computer1 as follows:
 - Change the **ServerPath=** statement to reflect the local path.
 - Change the **login=** statement to reflect the Computer1 mailbox (as set up by the Mail Administrator).
3. Copy the newly edited MSMAIL.INI file to the WINDOWS directory on Computer1.

Note that you can use the Mail Administrator's MSMAIL.INI file as the source for the MSMAIL.INI file for Computer1. If you use this file, be sure to remove all references to the WGPOMGR.DLL file.

Using Mail with a NetWare Network

To use Mail with a Novell NetWare network, you need to create a WGPO on a NetWare server and grant full trustee right to the WGPO directory.

To create a WGPO on a NetWare server

1. Create a directory on the NetWare server where the WGPO will be located.
2. Grant full trustee rights to this directory.
3. Log on to your NetWare server from the MS-DOS command prompt.
4. Start Windows for Workgroups 3.11.
5. Make sure that Windows for Workgroups 3.11 is configured to support Novell NetWare.

See Chapter 8, "Using Windows for Workgroups 3.11 with Novell NetWare" for further information

6. Use File Manager to map (assign) a drive letter to the NetWare directory where you want to create your WGPO.

For instructions consult your NetWare documentation.

7. Create the WGPO, as instructed in Appendix A of the *Microsoft Workgroup Add-on User's Guide*.

Moving a WGPO From One Computer To Another

If you need to transfer a WGPO from one server to another and you don't wish to transfer your administrator responsibilities, follow these steps:

1. Verify that you have full access to the share where the WGPO will be moved.
2. Verify that all users have exited Mail and signed out and are no longer connected to the WGPO.
3. Use File Manager to move the WGPO to its new location; be sure to move all subdirectories.
4. For each user and the WGPO Administrator, open the MSMAIL.INI file in a text editor (such as Notepad), and change the **ServerPath=** line so that it points to the new server. For example:

```
ServerPath=\\newserv\wgpo
```
5. Save your changes, and restart the system.

The WGPO administrator should be able to administer the postoffice and users should be able to connect to the WGPO as they did before.

Changing the WGPO Administrator

This section describes the procedure for transferring WGPO administrator responsibilities from one person to another. In this procedure, the following conventions are used:

- Admin1 is the current Postoffice Administrator.
- Admin2 will become the new Postoffice Administrator.

The following fields are required:

- Name
- Mailbox
- Password (You must know the passwords for Admin1 and Admin2.)

Steps to Change Administrators

1. Copy the MSMAIL.INI file from the WGPO computer to a floppy disk so that you can use it later when establishing the Admin2 account.
2. From Admin1's computer, sign on to Mail, select the Mail option, then select Postoffice Manager.
3. Select the Details option, and write down the required information for Admin1 and Admin2 (obtain the passwords from the Administrators; passwords don't appear in the details dialog box).

4. If Admin1 no longer needs a mail account, delete the user account for Admin2 and edit the details of the Admin1 account so that it matches the new Postoffice Administrator's account (Admin2).

NOTE: If you wish to move the administrative abilities without affecting the accounts of either user, skip this step and go to Step 5.

5. Open Admin1's MSMAIL.INI file in a text editor (such as Notepad) and remove the following two lines (instead of removing the lines, you can place a semi-colon preceding the line to remark it out, if desired):

```
WGPOMgr1=3.0;Mail;;13
WGPOMgr2=3.0;Mail;&Postoffice Manager...;14;WGPOMGR.DLL;0;;Manage
Workgroup Postoffice;MSMAIL.HLP;2870
```

Note These two lines will most likely be the last two lines of the [Custom Commands] section.

6. Admin1 should exit and sign out of Mail.
7. On Admin2's computer, open the MSMAIL.INI file that was copied to the floppy disk. Using a text editor (such as Notepad) cut the following two lines from this file:

```
WGPOMgr1=3.0;Mail;;13
WGPOMgr2=3.0;Mail;&Postoffice Manager...;14;WGPOMGR.DLL;0;;Manage
Workgroup Postoffice;MSMAIL.HLP;2870
```

Then, paste these two lines into the [Custom Commands] section of Admin2's MSMAIL.INI file (located in the WFW or Windows directory). Be sure that these lines are the last two lines in the [Custom Commands] section.

8. Save the changes made to the MSMAIL.INI file, then start Mail.

Note A message may appear that states mail was unable to find your .MMF file. A dialog box will then be displayed allowing you to select another .MMF file. Choose the .MMF for your user account, and choose OK to select the .MMF file found on the hard disk drive.

9. Open Mail and select the Mail option to verify the Postoffice Administrator option is now available on Admin2's computer.
10. If necessary, create a user account for Admin1.

Allowing Multiple Users to Log On to Windows for Workgroups Mail on the Same Computer

You can set up Windows for Workgroups Mail so that multiple users can log on with individual Mail files. In addition to Mail, multiple users can access

Schedule+ information. After following these configuration steps, users will also be able to access their mail messages and calendar information stored on the workgroup postoffice from any Windows for Workgroups workstation on the network.

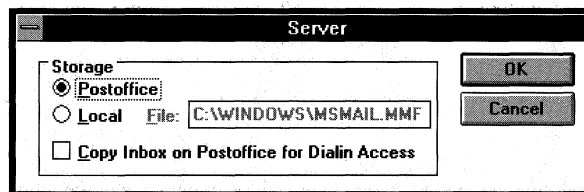
Note The MS-DOS-based Mail client provided with the Workgroup Add-on for MS-DOS stores mail messages on the workgroup postoffice, therefore no additional configuration is necessary to support multiple MS-DOS-based Mail users.

To establish multiple users

1. Run Mail on the workstation that the Postoffice Manager will use. When running Mail for the first time, create the workgroup postoffice (WGPO) by selecting the "Create a new Workgroup Postoffice" Postoffice Selection.
2. Create the postoffice manager account for the WGPO, and share the WGPO directory by using File Manager as instructed by the Mail program.
3. As the postoffice manager, create accounts for each of the users that will be on the WGPO. User accounts can be created by choosing the Postoffice Manager option from the Mail menu, and selecting the Add User button.
4. After user accounts have been created, start Windows for Workgroups Mail on the computer that multiple users will be using. If this is the first time you have started Mail, select the "Connect to an Existing Postoffice" Postoffice Selection and connect to the WGPO shared in step 2. Mail will ask you whether an account for the user has been created on the Postoffice, click the Yes button. Mail will connect to the remote WGPO and will create the MSMAIL.INI file on the local computer in the Windows directory.
5. Mail will prompt the user to sign in. Sign in to Mail by typing the mailbox name for one of the users that will be using Mail from this workstation.
6. We will now configure Mail to store the user's mail message file (MMF) on the postoffice, rather than the local workstation. Choose the Options item from the Mail menu. Select the Server button from the right-hand side of the Options dialog box. The Server dialog box will be displayed.

Figure 12.1

The Server dialog box



7. Change the Storage location to the Postoffice by selecting the Postoffice radio button as shown in Figure 12.1. Click the OK button. Mail will move the user's local MMF file to the WGPO. Close the Options dialog box by clicking the OK button.
8. Optionally, if you will be using Schedule+ you can start the Schedule+ application to create a local calendar file for the user. When Schedule+ is started the user will be prompted to enter his/her password. The user should enter the same password he/she is using for the Mail password. Schedule+ creates a local calendar file in the Windows directory for off-line use. Calendar information is also stored on the WGPO. The WGPO serves as the master location where calendar information is stored.
9. Exit and Sign out of Mail (and Schedule+ if you have started it).

Repeat steps 4 through 9 for each of the users that will be accessing mail messages from this workstation. The key steps in this process are steps 6 and 7, which are used to configure the WGPO to store the user's mail messages on the server where the WGPO resides.

Creating Global Address Groups for Users of Mail

Mail provided with Windows for Workgroups 3.11 allows individual users to create groups in their personal address books to send mail messages to a collection of users by referencing a single address book entry. However, Windows for Workgroups 3.11 Mail does not allow a system administrator to define global groups of Mail users that all users of Mail can access.

The Microsoft *Workgroup Postoffice Upgrade* upgrades a Windows for Workgroups or Windows NT workgroup postoffice to a Microsoft Mail postoffice and provides administrator tools and utilities to provide the following capabilities not provided by workgroup Mail:

- Ability to create global groups
- Ability for postoffices to support routing of mail messages across postoffices
- Support for mail gateways to access external mail systems included X.400, PROFS, and SMTP
- Client software for other operating system platforms including Macintosh and OS/2

For information on the *Workgroup Postoffice Upgrade*, contact your local reseller or Microsoft by calling 1-800-227-4679.

Miscellaneous Configuration Tips

This section provides several miscellaneous configuration tips that will help you to configure Windows for Workgroups 3.11 for your network environment.

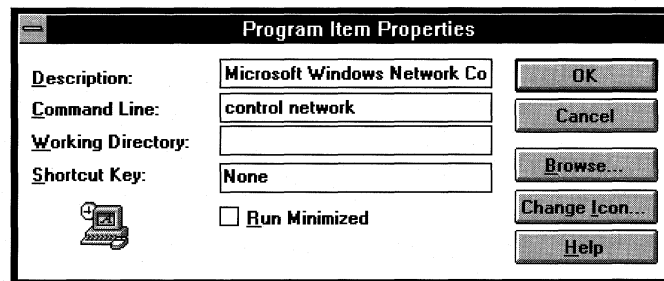
Quick Access to Network Section in Control Panel

To simplify the access to the Network section of Control Panel, you can create a Program Manager program item in the Network program group that allows you to double-click to gain access to the configuration options if you have Windows for Workgroups configured to use the Microsoft Windows Network networking components.

To do this, create a new program item by selecting the New item from the File menu in Program Manager and selecting the Program Item menu item. For the command line, type “**control network**” (without the quote marks), and click the OK button. Optionally, you can change the description for the program item. Figure 12.2 provides a sample Program Item Properties dialog box showing the information necessary for accessing the Network section of Control Panel.

Figure 12.2

Sample Program Item Properties dialog box



Token Ring Cards and Local Addressing

Some token ring network interface cards (NICs) can use a “local addressing” feature with Windows for Workgroups. This feature allows the network card’s internal network address to be bypassed and defined manually.

The local address is defined by placing the following line in the network card section of the PROTOCOL.INI file:

```
[MS$IBMTR1]           (Using the IBM Token Ring card)
Netaddress="<value>" (The quotation marks are required)
```

The value for the **Netaddress=** setting must be stated as a series of 12 hexadecimal digits within quotation marks, with no spaces separating the digits. There is no default for the **Netaddress=** setting.

The address must be within the range 400000000000 through 40007FFFFFFF; however, for strict IBM compatibility, use only decimal digits (0-9), as in "400001020304."

If the `Netaddress=` value is incorrectly entered (without quotation marks, for example), an error message may be displayed during startup. To correct these errors, verify that there are 12 digits, that they are within quotation marks, and that there are no spaces between entries.

You may also experience the following problems if there are duplicate computers on the network using the same `Netaddress=` value:

- Computers cannot connect to the network. (This problem occurs when the first computer to enter the ring causes another machine that is attempting to use the same `Netaddress=` value to fail.)

-or-

- Losing the connection to the ring when starting Windows for Workgroups or starting the real mode redirector.

-or-

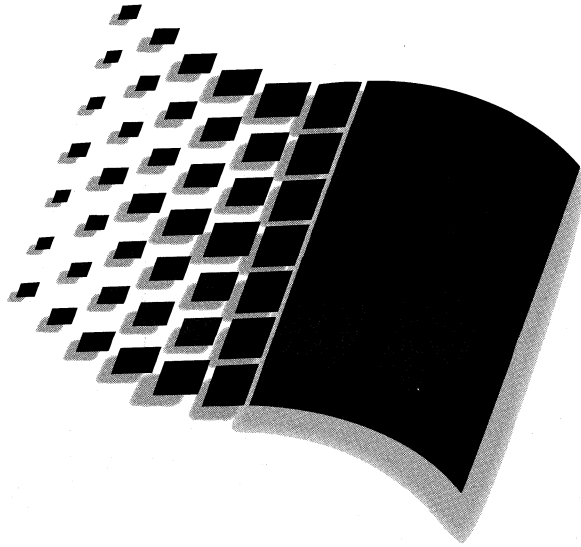
- Inability to browse or connect to other computers within Windows for Workgroups.

No error messages are displayed if you start a machine that is attempting to use a network address that is already in use, but network access problems, as described above, will occur.

To troubleshoot a possible network address conflict, remove the `Netaddress=` line in the `PROTOCOL.INI` by placing a semicolon at the beginning of that line. If problems persist, there may be some other conflict, such as IRQ, I/O address, or device driver.

The following token ring network cards are known to support local addressing with Windows for Workgroups (check your network card documentation or with your network card vendor to see if local addressing is supported with the network card you own):

Netcard	NDIS 2 Driver
ProNET-4/16 (P1892)	NDIS89XR.DOS
3Com TokenLink	TLNK.DOS
IBM Token-Ring Adapter	IBMTOK.DOS
IBM Token-Ring II	IBMTOK.DOS
IBM Token-Ring A	IBMTOK.DOS
IBM Token-Ring 16/4	IBMTOK.DOS
IBM Token-Ring 16/4 A	IBMTOK.DOS



Troubleshooting Windows for Workgroups 3.11

Part

6

Troubleshooting Windows for Workgroups 3.11

Chapter 13 ***Troubleshooting Windows for Workgroups 3.11*** 13-1

Troubleshooting Tools for Windows for Workgroups	13-4
Creating a Clean Configuration for Troubleshooting	13-9
Network Adapter Card Settings	13-10
Installation	13-13
How to Troubleshoot Network Connection Problems	13-17
Real Mode Network	13-27
Architecture and Configuration	13-30
Interoperability with LAN Manager, Windows NT, and Windows NT Advanced Server.....	13-31
Interoperability with Novell NetWare	13-33
Interoperability with Banyan VINES	13-37
Interoperability with SunSelect PC-NFS	13-39
Performance Enhancements	13-39
Other New Features	13-45
Microsoft At Work PC Fax	13-46
Remote Access Service (RAS) Client	13-48

Troubleshooting Windows for Workgroups 3.11

This chapter discusses how to troubleshoot possible problems that may occur while installing, configuring, starting, and running Windows for Workgroups 3.11.

Very often you can solve a problem by referring to online Help. You can access Help by choosing the Help button in a dialog box or pressing the F1 key on your keyboard.

If you encounter a problem, try to resolve it by also reading the information files that ship with Windows for Workgroups 3.11: README.WRI, MAIL.WRI, NETWORKS.WRI and PRINTER.WRI. These information files contain material not available in this book, in the *Microsoft Windows User's Guide*, in the *Microsoft Workgroup Add-on User's Guide* or in online Help. They contain important information for troubleshooting problems relating to specific hardware, software, and system configurations.

For further troubleshooting information and related flowcharts, refer to Chapter 14 in the *Windows for Workgroups Resource Kit for version 3.1*, "Troubleshooting Windows for Workgroups."

Related information

- *Microsoft Workgroup Add-on User's Guide*: Appendix A, "Troubleshooting."
- *Windows for Workgroups Resource Kit for version 3.1*: Chapter 14, "Troubleshooting Windows for Workgroups."
- On-line information files: README.WRI, NETWORKS.WRI, MAIL.WRI, PRINTER.WRI.
- *Windows for Workgroups Resource Kit Addendum for version 3.11*: Appendix A, "Additional Support Information."

Contents of This Chapter

Troubleshooting Tools for Windows for Workgroups	13-4
The Microsoft Diagnostic Tool (MSD)	13-4
Windows for Workgroups 3.11 Startup Switches	13-5
* CLN Files	13-6
Using Microsoft Network Diagnostics to identify network connectivity problems	13-7

Creating a Clean Configuration for Troubleshooting	13-9
Network Adapter Card Settings	13-10
Installation	13-13
Common Setup Issues	13-13
Windows Will Not Run	13-14
No Network Functionality In Windows	13-15
Using Multiple Configurations with Windows for Workgroups 3.11 ...	13-16
How to Troubleshoot Network Connection Problems.....	13-17
Initial Troubleshooting	13-18
Additional Troubleshooting.....	13-20
Duplicate Computernames	13-26
Shared Resources.....	13-26
Real Mode Network.....	13-27
Real Mode Network Will Not Start.....	13-27
Missing Real Mode Network Functionality	13-30
Architecture and Configuration	13-30
Common Configuration Issues	13-30
Interoperability with LAN Manager, Windows NT, and Windows NT Advanced Server.....	13-31
Windows NT Server Will Not Validate Logon of Machine Name with a Space Character In It	13-31
Time out of LAN Manager Logon Script Before Completion	13-31
User Account Issues	13-32
Using Lowercase Extended Characters for Passwords.....	13-32
Using International Characters in the Windows NT Share Name	13-32
Empty Server Browse List.....	13-32
Password Required For Chat - Network DDE.....	13-33
Interoperability with Novell NetWare	13-33
Machines across a NetWare Server or IPX Router are not visible	13-33
Can't access a NetWare Server	13-34
Setup recommended ODI but it won't work in real mode.....	13-34
My ODI Configuration No Longer Works After Installing Windows for Workgroups 3.11	13-35
I want to unload all ODI components.....	13-35
ODI Files Not Processing NET.CFG	13-35
I can't see NetBEUI servers when using ODI	13-36
I am having trouble running an IPX application	13-36
Interoperability with Banyan VINES	13-37
Load order of drivers in AUTOEXEC.BAT	13-37
Cannot Connect to a Banyan VINES Server	13-37
"Initban: Ban not installed or software mismatch"	13-37
"Unable to read PCCONFIG.DB configuration database"	13-37
"Cannot Start STDA Session: VINES error 157"	13-38
"Call to Undefined Dynalink"	13-38
"Cannot install protected mode mapping"	13-38
Environment Variables Overwritten.....	13-38
Problems Running Named Pipes Applications.....	13-38
Token-Ring Support with Banyan VINES	13-39

Interoperability with SunSelect PC-NFS.....	13-39
“NFS903F Missing or invalid PROTOCOL.INI data” Error When Starting SunSelect PC-NFS	13-39
Performance Enhancements	13-39
Ghosted Connection Issues	13-39
Problem browsing other servers on the network	13-40
32-bit file access is not enabled on a given disk drive	13-41
32-Bit File Access Troubleshooting	13-42
My system seems to have slowed down since I enabled 32-bit file access.	13-44
Incompatibilities with 32-bit file access and various Windows disk utilities	13-44
32-bit File Access cache related issues	13-44
Other New Features	13-45
Invalid or Damaged WFWSYS.CFG	13-45
Passwords for shared drives on the local machine are not visible.....	13-45
Microsoft At Work PC Fax	13-46
Errors with Faxes and Mail in the Outbox	13-46
Installing for Microsoft Mail after Installing for “Fax Only”	13-46
Can’t Send E-mail Format on a Class 1 Fax Modem	13-46
“Attachment type was not supported” Error	13-47
Can’t Fax to a Shared Fax Modem.....	13-47
I hear the modem answer the phone, but the Microsoft Fax status Indicator displays idle.....	13-48
Remote Access Service (RAS) Client	13-48
RAS connects to the server, but refuses to authenticate me.....	13-48
I have RAS services, however I am still unable to attach to a RAS server.	13-48

Troubleshooting Tools for Windows for Workgroups

The Microsoft Diagnostic Tool (MSD)

The Microsoft Diagnostic Tool (MSD) is an extremely useful tool for finding out information about computers and their environments. For example, just by loading MSD, you will be able to identify how memory is used in the range between 640KB and 1 MB to see if you have free blocks in the upper memory area to help avoid conflicts when loading device drivers into this range.

Once you load MSD, you will find many buttons that allow you to examine the machine's communications ports, memory, type of video card and disk drives, etc.. MSD will also allow you to view the contents of your configuration files such as the CONFIG.SYS, AUTOEXEC.BAT and all the Windows initialization files. In addition to this, you can print out a report with this information included.

When running MSD note the following:

- Because there is no standard for determining which IRQs are in use and by whom, the IRQ Status is not also going to be accurate.
- If you run MSD from inside of Windows, some of the information may not be as accurate as it would be outside of Windows.
- If you are running ODI, the Network section will give you information about your network configuration. It may also report the you have more than one MLID loaded, this may be incorrect.

MSD.EXE is automatically copied to a computer's hard drive when Windows for Workgroups 3.11 Setup program runs. MSD.EXE is located in the \Windows directory.

To run MSD.EXE

1. Exit Windows for Workgroups 3.11.

Although it is possible to run MSD.EXE from within Windows for Workgroups 3.11, the information may not be as accurate or complete. Therefore, running MSD.EXE while Windows is not running is recommended.

2. At the MS-DOS command prompt type:

C:\Windows\MSD

(If Windows for Workgroups 3.11 is installed in a directory other than "Windows" or on a drive other than "C:." make the necessary changes to the above.)

3. Read and follow the MSD instructions.

Windows for Workgroups 3.11 Startup Switches

Below are several switches that can be used to start Windows with different settings enabled. Many can be used together while troubleshooting. For example, starting Windows with the "Win /d:xsvfe" command would start Windows with all troubleshooting settings enabled. If your problem goes away after loading Windows this way, you can then try the switches one at a time or in different combinations to determine which one fixed the problem.

- **Win /d:x** Starts Windows for Workgroups 3.11 with the full upper memory area excluded. This is the same as adding "**emmexclude=a000-ffff**" to the **[386Enh]** section of the SYSTEM.INI. Use this switch if you suspect that Windows is overwriting a ROM device (such as a netcard) that is loaded in the upper memory area. If this switch fixes your problem, you should then add an **EMMExclude=** setting to the **[386Enh]** section of the SYSTEM.INI. You should adjust the setting to only exclude the ROM device that is being overwritten. Note that in order for this to work successfully, there must not be a UMB provider (Emm386, Qemm386, etc.) loaded in the CONFIG.SYS file.
- **Win /d:s** Starts Windows for Workgroups 3.11 with the **[386enh]** mode switch "**SystemROMBreakPoint=OFF**" set.. This is the same as adding "**SystemROMBreakPoint=OFF**" to the **[386Enh]** section of the SYSTEM.INI. For more information on the "**SystemROMBreakPoint=**" switch, see Chapter 4, "Windows for Workgroups 3.11 Initialization Files."

- **Win /d:v** Starts Windows for Workgroups 3.11 with the [386enh] mode switch “**VirtualHDirq=off**” set. This is the same as adding “**VirtualHDirq=off**” to the [386Enh] section of the SYSTEM.INI. For more information on the “**VirtualHDirq=**” switch, see Chapter 4, “Windows for Workgroups 3.11 Initialization Files.”
- **Win /d:f** This switch disables the WDCTL “32 Bit Disk Access” driver. This is the same thing as setting “**32bitdiskaccess=off**” to the [386enh] section of the SYSTEM.INI. Note that this will only apply to machines that have Western Digital 1003 compatible controllers in them.

The following switches are new to Windows for Workgroups 3.11:

- **Win /n** This switch starts Windows for Workgroups 3.11 with no Windows protect mode network drivers loaded. It is useful if you think one of the network drivers is causing your problem. You might also use this switch if you are using a portable computer when is not hooked up to a network card.
- **Win /d:t** This switch starts Windows in “troubleshooting” mode. Windows will start with no virtual device drivers (VxDs) loaded. This is a good switch to use if you suspect a VxD conflict. When running in this mode, MS-DOS applications can not run, communications applications can not run, and networking functionality is disabled unless you have started the real mode redirector.
- **win /d:c** This loads Windows without loading the 32-bit File Access driver, VFAT.386. This switch can be used to troubleshoot whether 32-bit File Access is the source of trouble. This is the same thing as setting removing the 32-bit File Access drivers from the [386enh] section of the SYSTEM.INI.

***.CLN Files**

Immediately after the Windows for Workgroups 3.11 Setup program is complete, Windows for Workgroups 3.11 creates backup versions of the SYSTEM.INI, WIN.INI, and PROTOCOL.INI and names them SYSTEM.CLN, WIN.CLN, and PROTOCOL.CLN.

These .CLN files can be extremely useful when trying to solve configuration problems on a machine that worked properly after completing Windows for Workgroups 3.11 Setup, but then stopped working, due to modifications made to the system either by changes to Windows Setup, or by newly installed software. It is recommended to use the MS-DOS **copy** command rather than simply renaming the .CLN file to the appropriate .INI file. Simply renaming the old .CLN file will leave you with no backup copy.

If Windows for Workgroups 3.11 was working properly and is not any longer

1. Exit Windows for Workgroups 3.11.
 2. Rename the currently troubled versions of SYSTEM.INI, PROTOCOL.INI, and WIN.INI to SYSTEM.BAK, PROTOCOL.BAK and WIN.BAK.
 3. Copy SYSTEM.CLN to SYSTEM.INI.
 4. Copy PROTOCOL.CLN to PROTOCOL.INI.
-

Note If you have modified the network setup for Windows for Workgroups, it may not be necessary to replace the WIN.INI with the WIN.CLN file. Replacing the WIN.INI file is recommended if you have difficulty after installing a new application or other Windows component.

5. Copy WIN.CLN to WIN.INI.
 6. Restart Windows for Workgroups 3.11.
-

Note Since Network configuration information is stored in the PROTOCOL.INI and SYSTEM.INI, any Network configuring that is done after running the Windows for Workgroups 3.11 Setup program will not be stored in the PROTOCOL.CLN and SYSTEM.CLN.

Using Microsoft Network Diagnostics to identify network connectivity problems

Microsoft Network Diagnostics is a network connectivity troubleshooting tool designed to assist a network administrator in isolating connectivity problems. Microsoft Network Diagnostics is useful when machines cannot communicate or “see” each other, or if the network behaves unreliably. Although Microsoft Network Diagnostics can be used while running Windows, optimal results will be achieved by exiting Windows and running the utility with only the required network drivers loaded.

Microsoft Network Diagnostics can perform diagnostics using either an IPX provider such as IPXODI.COM, or a NetBIOS provider such as Microsoft NetBEUI.

To Run Microsoft Network Diagnostics

1. Exit Windows.
2. Type "net diag" at the MS-DOS prompt.

Microsoft Network Diagnostics will identify the types of transports (protocols) that are currently installed. If you have both an IPX provider and a NetBIOS provider, you will have the option to choose which transport to use. Select the transport that is common to all machines that will be involved in the diagnostics.

Network Diagnostics then tries to detect a diagnostic server on the network. If it does not detect the diagnostic server you have set up, then the network cable may be faulty. Press Y to quit Network Diagnostics.

Note In the event that the cable is not faulty, there might be a problem with your network card or configuration.

3. The first machine that you run Microsoft Network Diagnostics on becomes the "diagnostic server" with which the other machines will attempt to communicate.
4. Run Microsoft Network Diagnostics on another workstation, which will then exchange information with the diagnostic server and print any problems out on the screen.

Optional switches available for Microsoft Network Diagnostics

DIAG /? will display a list of command line parameters.

DIAG /STATUS will invoke the NetBIOS adapter status function. Note that since this is a NetBIOS specific function it does not work with IPX, it requires a NetBIOS provider such as Microsoft NetBEUI. Use the adapter status function to view general information about the state of the adapter since it last powered-up. You can also use this tool to view the status of another workstation adapter by entering that workstation's computer name when prompted.

NET DIAG /NAMES allows you to change the NetBIOS name that Microsoft Network Diagnostics uses during diagnostic testing. This may be necessary if several people are independently running multiple diagnostic servers. This switch can only be used with the NetBIOS mode of Microsoft Network Diagnostics.

Creating a Clean Configuration for Troubleshooting

To begin troubleshooting a problem in Windows for Workgroups 3.11, always re-boot the system with a “clean” configuration. A clean configuration is the most simple configuration that enable Windows for Workgroups 3.11 and its networking components to load. If your problem no longer occurs in a cleanly booted configuration, re-create the original configuration line by line, in an attempt to determine what part of the original configuration is the source of the problem.

A clean configuration consists of a CONFIG.SYS and AUTOEXEC.BAT that look like the following examples.

Sample CONFIG.SYS file

```
FILES=45
BUFFERS=20
DEVICE=C:\<WFWG 3.11 dir>\HIMEM.SYS
<Third-party disk partitioner>
<Third-party disk compression driver>
<Other required third-party drivers>
SHELL=C:\<valid path>\COMMAND.COM /E:1024 /P
STACKS=9,256

DEVICE=C:\<WFWG 3.11 dir>\MFSHLP.SYS
```

Sample AUTOEXEC.BAT file

```
C:\<WFWG 3.11 dir>\Net Start
SET TEMP=C:\<valid path>
PATH=C:\<WFWG 3.11 dir>;C:\DOS;C:\
PROMPT $P$G
```

Exceptions

The following are examples of drivers that **SHOULD NOT** be removed; they are used when the computer is turned on to make the hard drive accessible. This is not a complete list, but it does include most of the commonly used drivers:

Hard Disk Drivers: SQY55.SYS, SSTBIO.SYS, SSTDRIVE.SYS, AH1544.SYS, ILIM386.SYS, ASPI4DOS.SYS, SCSIHA.SYS, SCSIDSK.EXE, SKYDRVI.SYS, ATDOSXL.SYS, NONSTD.SYS.

Disk Partitioners: DMDRVR.BIN, SSTOR.SYS, HARDRIVE.SYS, EDVR.SYS, FIXT_DRV.SYS, LDRIVE.SYS, ENHDISK.SYS.

Disk Compression Utilities: STACKER.COM, SSWAP.COM, SSTOR.EXE, DEVSWAP.COM

If the purpose of a device driver or program is unknown, **DO NOT** remove it. Most device drivers and programs will display a message describing their purpose when they are initialized.

A clean boot DOES NOT include:

- DOS=HIGH,UMB
- EMM386.EXE
- INSTALL=SHARE.EXE
- INSTALL=FASTOPEN.EXE
- Third-party memory managers
- RAM disk devices
- JOIN, GRAPHICS, PRINT, SUBST, APPEND
- MODE for printer redirection
- Multiple path statements
- MS-DOS-level mouse drivers
- Third-party disk caches
- Various third-party TSRs
- LOGIMENU, CLICK
- Virus checkers
- Drivers for scanners/fax
- Drivers for CD ROM/network
- Tape backup spoolers/redirectors/buffers
- Data acquisition units
- Keyboard accelerators/buffers

Network Adapter Card Settings

If your network adapter card can accept more than one type of cable, make sure that the card is configured for the cable that you are plugging into it. Refer to the documentation that came with the card for details.

When you configure the network adapter card, you must select the correct IRQ number, I/O port base address, and memory buffer address. On older network cards, you set jumpers or switches for each of these items; with newer cards, you can program them with the driver software using only the I/O port address. For information about the settings on specific network cards, see the file NETWORK.WRI or the Help file NTCARD.HLP, which is included on a diskette that ships with this book (in File Manager, double-click on NTCARD.HLP).

If you are not sure about which network card is installed in your computer or what its settings are, accept the defaults proposed by Windows for Workgroups Network Setup. After Setup is complete, you can use the Networks applet in Control Panel to install and configure network settings. For information about completing any options in the dialog boxes that appear during the network portion of Setup or when you run the Networks tool, use the Help button.

For the correct settings for your particular hardware, see the documentation for your network card and other devices such as SCSI adapters, or contact your hardware manufacturer.

You do not have to specify settings for built-in Ethernet capabilities on RISC-based computers from Acer, MIPS, and Olivetti.

Network Adapter Card Interrupts

The IRQ that you assign to a network adapter card should be unique; that is, it should not be used by any other device in the system. The standard assignments for IRQs in x86-based computers include the following:

IRQ	Used for	IRQ	Used for
0	Timer	8	Clock
1	Keyboard	9	—
2	(cascade)	10	—
3	COM2	11	—
4	COM1	12	—
5	LPT2	13	Math coprocessor
6	Floppy controller	14	Hard drive
7	LPT1	15	—

A network card should not be assigned an IRQ that is used by an active serial or parallel port, even if no device is currently attached to the port. Most newer Intel x86-based computers let you disable the built-in serial or parallel ports. After you disable a port, you can assign its associated IRQ to another device, such as a network card.

For example, if you use only a network printer, you can usually disable the built-in parallel printer ports for both LPT1 and LPT2. Network software does not use these interfaces when the underlying devices are redirected.

For information on disabling serial or parallel ports, see the documentation for your computer.

If you do not disable the serial ports, COM1 (IRQ 4) and COM2 (IRQ 3) are usually poor choices because most x86-based computers come with two active serial ports. For example, a typical computer with a mouse on COM1 and a modem on COM2 cannot use IRQ 3 or 4 for a network adapter card. IRQ 5 is often a safe choice, because x86-based computers usually do not have two parallel printer ports.

If you have two or more COM ports on your computer, you might find that a network adapter card (especially an EtherLink II card) will conflict with one port.

To change the interrupt of a network adapter card

1. Run the Networks Setup applet in the Network program group.
2. Double-click the correct entry in the list of Adapter Cards.
3. In the Configuration dialog box, change the interrupt number from its current value to an available interrupt, such as 5 or 10.

Make sure that the interrupt you choose is not being used by another device.

Assigning I/O Port Base Addresses

Most devices have unique default I/O port base addresses. In the rare case that an I/O port appears to be in conflict, it can usually be moved to another setting without harm. The following table shows some common I/O port addresses:

I/O address	Used for	I/O address	Used for
3F8	COM1	300	—
3BC	—	2F8	COM2
378	LPT1	278	LPT2

Refer to the documentation for your network adapter card and other hardware devices to find what I/O addresses are required or optional for your system.

Assigning Memory Buffer Addresses

No two devices can share memory buffers. Make sure that the network adapter card buffer address is not already used by another device, such as a SCSI adapter card or hard disk controller. Check the installation guide for your computer or peripherals to verify the setting of the memory buffer address.

Some SCSI and network adapters use conflicting memory addresses, such as an Adaptec or Future Domain SCSI adapter and a DEC EtherWORKS Turbo TP network adapter. This requires reconfiguring the hardware by changing jumpers.

You can use the **MSD** utility to check how memory buffers are being used.

Installation

Common Setup Issues

Enhanced mode only 3rd-party video drivers

Although Windows for Workgroups 3.11 runs in 386 Enhanced mode only, the Windows for Workgroups 3.11 setup program runs in a “simulated” Standard mode. This can cause a problem for several of the advanced video cards on the market that ship with drivers that run only in 386 Enhanced mode, and therefore can not run when Windows for Workgroups 3.11 is installing.

In previous versions of Windows and Windows for Workgroups, users running an Enhanced mode only video driver would get an error message during setup instructing them to exit setup, load the Windows standard VGA video driver, and then rerun setup.

This is not necessary with Windows for Workgroups 3.11. There is a section in the SETUP.INF file called, **[Setup Display]** that lists many of the 3rd party Enhanced-mode-only video drivers available. If your video driver is in this list, the Windows for Workgroups 3.11 setup program will automatically replace it with the Windows Standard VGA video driver for the duration of the setup program. When the Setup program is finished, it will reload the original 3rd party video driver. If you have an Enhanced-mode-only video driver that is not listed in the **[Setup Display]** section of the SETUP.INF file, you will have to remove your video driver and load the Windows Standard VGA video driver before running Setup.

No EGA or HERC Video Drivers

These drivers do not ship with Windows for Workgroups 3.11 but are present as part of the Windows Driver Library (WDL). The files from the WDL can be obtained from the Microsoft Download Service, CompuServe, or Microsoft Product Support Services. See Appendix A, "Additional Support Information," for more information on the Windows Driver Library.

To Regenerate Program Manager Groups

To regenerate the default Program Manager groups, choose Run from the Program Manager's File menu. On the command line, type:

```
WINSETUP /P
```

Express Setup: Incorrect card or settings detected

Express Setup will attempt to detect the netcard and its settings and does not prompt the user.

If the drivers and their settings are incorrect, Setup will complete successfully but the network functionality will be unavailable. Launch Windows for Workgroups 3.11 with the "WIN /N" switch and use Network Setup to check the netcard and its hardware settings. Some netcard specific settings such as "Transceiver Type" for cards that have multiple connectors may not be available in the advanced setup for the netcard. They will have to be set either with jumpers or through the software configuration program shipped with the netcard.

Windows Will Not Run

- Run Windows for Workgroups 3.11 in "Troubleshooting Mode" by typing:

```
WIN /D:T
```

When Windows is run in this mode, no VxD's or networking components are loaded.

- If Windows for Workgroups 3.11 loads with "WIN /D:T", then try "WIN /N" to load enhanced mode Windows for Workgroups 3.11 without the protect mode network components (focuses troubleshooting on network specific settings and VxDs).

- If Windows for Workgroups 3.11 loads with the “WIN /N”, try the troubleshooting steps for the “Cannot Get Network Functionality In Windows” described later in this chapter.
- Try standard Windows troubleshooting techniques (Clean Boot, IRQ/Base IO/UMA conflicts, 3rd Party Components, WIN /B, WIN /D:XSVFC, etc.).

No Network Functionality In Windows

Note If you are trying to troubleshoot a problem with network functionality, please refer to the section, “Interoperability with Novell NetWare,” later in this Troubleshooting chapter.)

- Verify Windows for Workgroups 3.11 system requirements: 80386, with at least 3072K of free XMS memory available to Windows for Workgroups 3.11.
- Run the real mode network to ensure the real mode drivers load and bind successfully. This step will verify the netcard settings in the PROTOCOL.INI and will verify that the real mode NetBEUI and redirector can load and work properly on the installed equipment.

Start the real mode network by typing “net start workstation.”

If this works, type “net stop /y,” this will stop the real mode network but leave the real mode drivers loaded. Now, start Windows for Workgroups 3.11 and see if the network works. If it does, the problem most likely is in the NDIS 3. network drivers.

- Launch Windows for Workgroups 3.11 with WIN /N to load without network functionality. Check the “Driver Type” for the netcard and make sure it is set for “Real Mode and Enhanced Mode NDIS Driver”. Check the NIC settings including IRQ, RAM address, I/O address, etc.
- Backup the SYSTEM.INI and PROTOCOL.INI files. Through the user interface, remove all protocols except for NetBEUI. If protect mode NetBEUI is functional, add the additional protocols back in one by one.

- If Windows for Workgroups 3.11 still will not load the network software, check the following settings:

Sample SYSTEM.INI File

```
[boot]
network.drv=wfwnet.drv
[386enh]
network=*vwc,*vnetbios,vnetsup.386,vredir.386,vserver.386
netcard= (depends on configuration)
transport= (depends on configuration)
netmisc= (depends on configuration)
secondnet= (depends on configuration)
```

Sample PROTOCOL.INI File

```
[<NDIS 3 netcard section name>]
Adapters=<NDIS 2 netcard section name>

[<NDIS 2 netcard section name>]
<netcard settings>
```

- Try standard Windows troubleshooting techniques (clean boot, IRQ/Base IO/UMA conflicts, 3rd-party components, **WIN /B**, **WIN /D:XSVFTC**, etc.).

Using Multiple Configurations with Windows for Workgroups 3.11

Windows for Workgroups 3.1 made it possible to construct multiple configurations (No-Net, Windows for Workgroups 3.1, NetWare, Windows for Workgroups 3.1 and NetWare) and use sections in both the CONFIG.SYS and AUTOEXEC.BAT to accomplish this.

With Windows for Workgroups 3.11, all lines except for IFSHLP.SYS and NET START have been moved to the SYSTEM.INI. Multiple configurations of Windows for Workgroups 3.11 requires multiple versions of the SYSTEM.INI and PROTOCOL.INI files. This will require some modification of your configuration. See Chapter 2, "Windows for Workgroups 3.11 Setup and Installation," for additional information on supporting multiple configurations. The IFSHLP.SYS driver should go in the [**Common**] section of CONFIG.SYS.

Sample CONFIG.SYS file in a multiple configuration environment

```
[Menu]
menuitem = WFW, Windows for Workgroups 3.11
menuitem = Clean, Clean Boot Configuration
menudefault=WFW,5

[Common]
BUFFERS = 20,0
FILES = 40
FCBS = 16,8
STACKS = 9,256
SHELL = C:\DOS\COMMAND.COM C:\DOS\ /p
DEVICE = C:\DOS\DBLSPACE.SYS /MOVE
DEVICE = C:\WINDOWS\IFSHLP.SYS

[WFW]
DEVICE = C:\DOS\HIMEM.SYS
DEVICE = C:\DOS\EMM386.EXE NOEMS

[CLEAN]
```

Sample AUTOEXEC.BAT file in a multiple configuration environment

```
PROMPT $p$g
C:\DOS\SMARTDRV.EXE 1024 128

goto %config%

:WFW
PATH C:\WINDOWS;C:\DOS;C:\NU
SET TEMP=C:\WINDOWS\TEMP
C:\WINDOWS\NET START
goto end

:clean

:end
```

How to Troubleshoot Network Connection Problems

When using Microsoft Windows for Workgroups 3.11, a variety of hardware- and software-related problems can cause one or more computers to lose the ability to browse or communicate with other computers. Problems range from no network functionality to random errors when transmitting data across the network. These problems have a variety of causes. (Terminate-and-stay-resident [TSR] programs in memory and shorts in connectors are two examples.)

Many factors must be considered when you troubleshoot this type of problem. Before you use the steps below, consider the following questions to help identify whether the problem is hardware or software related and possible causes of the problem:

- Has this configuration ever worked before?
- Did the problem just start happening?
- What has changed between the time this configuration was working and the time it stopped working?
- Is this problem occurring on one computer, several, or all of them?
- Has new hardware or software been added to a computer?
- Has cabling been moved or added?
- Have computers been added or removed from the network?
- Was this installation of Windows for Workgroups 3.11 upgraded from Windows 3.0 or 3.1, or Windows for Workgroups 3.1?
- Did you previously have other network software installed?
- Is the connection to the computer “live”? (If the card has transmit/receive data lights, are they active?)

Important Make a backup copy of the system configuration files (CONFIG.SYS, AUTOEXEC.BAT, PROTOCOL.INI, SYSTEM.INI, WIN.INI) before following any troubleshooting steps.

Initial Troubleshooting

- Make sure the network cabling is securely connected to both the computer you are using AND the computer you are trying to communicate with.
- Verify that the computer you are trying to view has sharing enabled. To check this, open Control Panel, choose Networks, and make sure the Sharing Enabled box is selected.
- Check for any error messages while the computer is booting. To prevent error messages from scrolling off the screen, place a PAUSE statement at the beginning and the end of your AUTOEXEC.BAT file.

-
- Run CHKDSK on the drive where Windows is installed. If Windows system files are corrupted, Windows is unstable and may need to be reinstalled. If CHKDSK shows errors, repair the errors by running CHKDSK with the /F parameter or by using a disk utility to repair the files on the hard disk drive. If there is data corruption, it may be necessary to reinstall Windows for Workgroups 3.11.
 - Clean boot each computer, as discussed in the “Creating a Clean Configuration for Troubleshooting” section of this chapter.
 - Verify that the network card settings in Network Setup are configured correctly.
 - If Windows for Workgroups 3.11 was installed over Windows 3.1 and another network (such as Novell NetWare), you may need to remove changes made by the previous network to Windows configuration files, particularly the SYSTEM.INI file.
 - Run a diagnostic test on the network card to ensure it is functioning correctly. If no diagnostic software is available for your network card, you may need to contact the network card manufacturer for information on performing diagnostic tests. Also, many diagnostic tests include functionality to test communication between computers on the network. This will test the network card and the cabling. If this low-level test does not allow two network cards to communicate, some type of hardware problem exists with a network card, cabling, or connectors. Contact your hardware vendor if either the network card diagnostic test or the network test fails.
 - If you have Intel EtherExpress network cards, you can use the Softset utility (available from the Microsoft Download Service [MSDL] or the Intel bulletin board service [BBS]) to troubleshoot the network card as well as the integrity of the network cabling (with the Test Network option).
 - If the network card is not on the supported network card list, contact the network card manufacturer to determine the correct emulation mode for the network card, or for an updated Media Access Control (MAC) network card driver. The manufacturer may also have information on jumpers and switches that may need reconfiguring for a particular emulation mode.
 - If removing or disabling new hardware and/or software causes the connectivity problem to disappear, there may be some parameter adjustments or special settings for the hardware or software when it is used on a network.

- If any network cabling has been moved, altered, or added, make sure it is working and properly connected. Most network problems are caused by faulty cabling and/or connectors. If you are using 10Base2 (Thin Ethernet), connect two computers together with a cable, T-connectors, and terminators that are known to work correctly. Also, make sure that you are using the right kind of cabling and/or connectors for your hardware.

Additional Troubleshooting

If the above techniques do not correct the problem, proceed with the following steps:

- Step 1. Run Microsoft Network Diagnostics, as described earlier in this chapter.
- Step 2. Try to view other computers on the network in File Manager. Choose the Connect Net Drive button or choose Connect Net Drive from the Disk menu, and type the computer name preceded by two backslashes (`\\computername`) in the Path box and press ENTER.

If you can view other computers on the network by manually entering computer names, several things may be causing this to occur, including that a "browse server" may not have been elected on the network. In Windows for Workgroups 3.11, a computer that maintains a list of Workgroups servers is selected. Sometimes this takes from 5-15 minutes to establish. If no browse server exists, you cannot browse servers on the network. Wait a few minutes, and try again.

If the local workstation name (but no other computer name) appears in the Show Shared Directories On dialog box, the network card is probably configured correctly. In this situation, the problem may be found in the network cabling or the other computer's network card configuration.

- Step 3. Check the cabling and connectors on each workstation. If the network is using Thin Ethernet, connect two computers together with a single cable, T-connectors, and terminators that are known to work properly. This isolates possible cabling and/or connector problems that may not be clearly visible. If the network topology is 10Base2 (Thin Ethernet or Thinwire), place a 50 Ohm terminator on the network card. If the local computer name now appears in the Show Shared Directories On dialog box (but not when the regular cabling is attached), some type of cabling and/or connector problem exists. Examples include an electrical short in the cabling,

improper termination, and using the wrong type of cabling. Check to ensure that each computer's T-connector is secured on each network card, that 50 Ohm terminators are at each end of the network, and that RG-58 cabling (not RG-59 or RG-62) is being used.

Note It may also be necessary to reroute network cabling away from sources of electrical interference (such as fluorescent lights).

If the local computer name does not appear in the Show Shared Directories On dialog box, the problem is with the local network card's configuration (either hardware or software). If your wiring is 10Base2 (Thin Ethernet), a quick test to see if the cabling is the problem is to remove the T-connector and place a terminator directly on the BNC connector on the network card. If doing so causes the machine to be able to "see itself" in File Manager, the problem is most likely with the existing cabling.

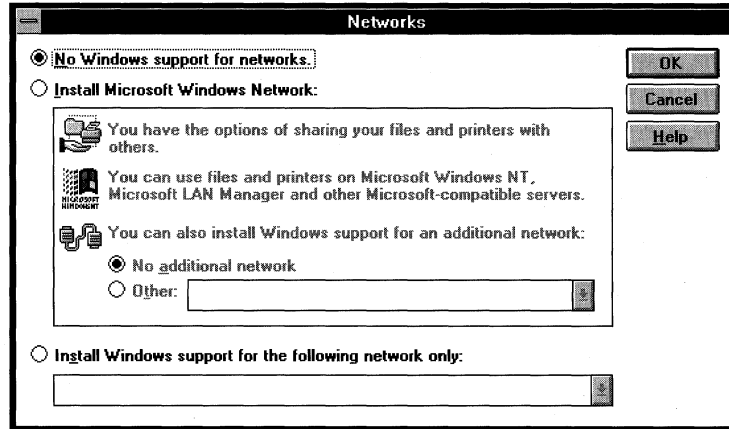
If placing a terminator on the network card doesn't identify the problem (or your cabling is other than 10Base2), try changing the IRQ and/or I/O address that the network card is using. With software-configurable network cards, this is done in the Network dialog box of Control Panel. Choose Adapters, and Setup, then select a different IRQ and/or I/O address. It may be necessary to try several selections if you do not know what your other hardware is configured to use.

Step 4. Try reinstalling the network card drivers. To do this:

- 1.) Start Windows for Workgroups 3.11 without any networking components by typing "Win /n" at the MS-DOS command prompt.
- 2.) Run Network Setup by double-clicking on the Network Setup icon in the Network program group. In the Network Setup dialog box, choose the Networks button.
- 3.) In the Networks dialog box, select the "No Windows support for networks" option.

Figure 13.1

The Networks dialog box, accessible through the Network Setup application.



- 4.) Choose OK to any open dialog boxes, and restart the machine when prompted to do so.
- 5.) Edit the SYSTEM.INI file and place a semi-colon (;) before each of the following entries in the [386Enh] section to make them inactive:


```
netcard=
netcard3=
secondnet=
transport=
netmisc=
network=
```
- 6.) Restart Windows.
- 7.) Run the Network Setup application again, making sure that file and/or printer sharing is enabled and that the network card settings are correct.

Note If the network card is hardware configurable (with jumpers or DIP switches), the settings on this screen need to match the actual settings of the jumpers or switches on the card, unless they say “Automatic or unused.” If the card is software configurable, it may be necessary to select a different IRQ, I/O Address, or RAM Address to resolve a connectivity problem. For example, some disk controllers come configured using I/O 300h, which is also the default for some network cards.

- 7.) Restart the computer and restart Windows. Attempt to communicate with other computers on the network.

- Step 5. Attempt to access another computer using the real mode redirector. This step identifies several possible problems, which are explained below. To start the real mode redirector, quit Windows and type “net start workstation” (without the quotation marks) at the MS-DOS command prompt. Next, try to view another computer (which must be in 386 enhanced mode) by typing the following:

```
net view \\<computername>
```

If the computer that you are trying to view is not currently sharing any directories, you will receive the message, “There are no entries in the list.”

If the error message “The specified computer cannot be found on the network” appears, there may still be cabling problems, an incorrect configuration on the remote (or the local) computer, or interference from some software (such as a TSR). If you can communicate with other computers using the real mode redirector, the problem may be an Upper Memory Block (UMB) conflict, a hardware conflict, or a virtual device driver (VxD) that is interfering with Windows for Workgroups 3.11. If you can view another computer’s shared resources using the real mode redirector, type “**net stop**” (without quotation marks) to stop the real mode redirector.

Edit the CONFIG.SYS file and remark out the line:

```
Device= C:\DOS\EMM386.EXE
```

Next, start Windows for Workgroups 3.11 by typing

```
WIN /D:X
```

Then try to view other computers in File Manager. If typing “WIN /D:X” corrects the problem, the network card’s memory address needs to be excluded with a UMB provider (such as EMM386.EXE) or by adding the line:

```
EMMEXCLUDE=memoryaddress
```

to the **[386Enh]** section of the SYSTEM.INI file.

For example, if your network uses a UMA address from C800-CFFF, add the following line to the **[386Enh]** section of your SYSTEM.INI file:

```
EMMExclude=C800-CFFF
```

If using the **WIN /D:X** command doesn't allow you to view any other computers in File Manager after restarting Windows but you could view other computers when you quit Windows and started the real mode redirector, there may be another problem. The problem may be caused by an IRQ, DMA channel, I/O, or RAM address conflict between the network card and another hardware device. Or, the problem may be that the settings in the Network dialog box of Control Panel do not match the actual hardware settings on the network card.

To change the IRQ, DMA, I/O, and/or RAM address settings, open Control Panel, choose Networks, choose Adapters, then choose Setup. Select a different setting (or the actual hardware setting) for your network card. With some network cards, you must also change jumpers or switch settings on the card to match the settings in Control Panel. For information about configuring jumpers and switches on your network card, check the documentation that came with the card or contact your manufacturer. If you cannot start Windows to open Control Panel, edit the **PROTOCOL.INI** file and change the settings for **Interrupt=**, **RamAddress=**, **DMAChannel=**, and **IOBase=** to unused values (for software-configurable cards) or to the actual hardware settings (for hardware-configurable cards).

Note When you change hardware settings (such as IRQ and I/O addresses) on software-configurable network cards (such as the Intel EtherExpress 16), you must either quit Windows, turn the computer completely off, and then restart it or select the Restart Computer option in Windows for the new settings to take effect.

- Step 6. If reinstalling the network card drivers does not enable the local computer to "see itself" in File Manager or view other computers on the network using the real mode redirector, there are several other possible steps to take:
- The correct Media Access Control (MAC) network card driver is not being used. If the card is emulating another card (such as the NE2000), it may be necessary to change jumpers or switches on the card to allow the driver to work properly. For more information on configuring the network card and obtaining updated drivers, contact your network card manufacturer.
 - The card may be in a slot that is functioning incorrectly. To verify this, try putting the network card in another slot in the computer or install the network card in another computer to determine if the card itself is defective.
 - The card could be in the wrong slot. For example, an ISA card may be in an EISA slot, or an EISA card may be in an ISA slot. Confirm that the correct card is in the correct slot.

- The network card may be malfunctioning. Try using a different network card or run diagnostic tests that may have come with the card.
- The bus speed on the computer may be too fast for the network card. Most network cards are designed to work at ISA (8.33 MHz) bus speed; setting the bus speed any faster may cause unreliable performance. The bus speed setting is usually changed in the computer's CMOS setup. Try lowering the computer's bus speed if intermittent problems occur.
- Some network cards, such as the Intel EtherExpress 16, come with a utility that checks the integrity of wiring and connectors between two computers. If one of these utilities is available, use it to determine whether or not the two computers are physically connected.

Another way to determine if two machines have a physical connection is to use the same computer name for two different computers on the network. Because each computer on the network must have a unique computer name, an error will result if two computers have the same computer name. To do this, change the value for Computername in the Networks dialog box of Control Panel, or edit the SYSTEM.INI file on one machine and change the setting for **ComputerName=** in the **[Network]** section to the name of another computer. When the computer reboots, the following error should appear, if the two computers are both on the network:

The following error occurred while loading protocol number 0.
Error 5123: The computer name you specified is already in use on the network.

Choose the Network icon in Control Panel to specify a different name. For more information, choose the Help button. If you do not receive this error message, a hardware problem exists with one or more of the following:

- The network card configuration is incorrect on one or more of the computers (hardware, I/O, IRQ, UMB conflict, and so on).
- One or more of the network cards is malfunctioning.
- There is some problem with the cabling or connectors. This could be an electrical short; interference; or a cable, connector, or terminator that is not the correct specification for your network topology.

To troubleshoot shorts and interference problems, either test the cabling with a testing device, or replace it with cables and connectors that are known to work correctly.

- Step 7. Check the SYSTEM.INI file for the following lines and remark them out if they exist. To remark out a line from the SYSTEM.INI file, place a semicolon (;) at the beginning of the line.

```
InDOPolling=True  
TimerCriticalSection=<any value>  
V86ModeLanas=<any value>
```

- Step 8. If Windows for Workgroups 3.11 is still not working after you complete the initial troubleshooting techniques and steps 1-5, and it has previously worked, the next step is to reinstall Windows for Workgroups 3.11 in another directory. Reinstalling Windows for Workgroups 3.11 in a clean directory should restore the configuration to the point at which it was working when first installed. When you start the Windows for Workgroups 3.11 Setup program, choose Custom Setup, and enter a new directory name, such as C:\WFWTEST. Once setup is complete, Windows for Workgroups 3.11 should work correctly.

If Windows for Workgroups 3.11 is still not working correctly, it is probably that some type of problem exists with your cabling, connectors, or network card. For more information on diagnosing problems with your network card or cabling, contact your hardware vendor.

Note Windows for Workgroups machines that have a space in their computername AND have a Windows NT machine in their workgroup will not be able to browse other computers on the network. The workaround for this situation is to remove spaces from the computername of the Windows for Workgroups machine.

Duplicate Computernames

Each computer on a network must have a unique name. If you specify a computername that is the same as another computer on the network or the same as a workgroup or a domain, the network will not start when you run Windows NT.

Shared Resources

If you can see the name of a shared resource, but cannot see or use its contents, you probably do not have sufficient permissions to access the resource. The owner of the resource can resolve this for you. It is also possible that the target server has just gone down or is having network problems.

If you cannot connect to a resource that you think you have permission to use, there are two likely possibilities:

- Your computer is not running a protocol that is running on the target computer.
- You logged on with a username that the target computer recognizes and a password that it doesn't recognize. A common example is to log on to your computer as Administrator and then try to connect to a server that has its own Administrator account established.

If you try to view the shared resource for a server that you know exists but receive a message that says it doesn't exist, there are several possibilities:

- The server is not running.
- The server is configured to be hidden from computer browsers.
- Your Browser service may not be started.
- The server is in a domain that is not in the list of domains to be browsed. Use the Network tool in Control Panel to reconfigure the Browser service.

Real Mode Network

Real Mode Network Will Not Start

NET START Fails

- Try re-booting the system with a clean configuration. See "Creating a Clean Configuration for Troubleshooting," at the beginning of this chapter. Remove the "Net start" command from the AUTOEXEC.BAT so that we can use it manually in the following steps.
- Type "net start netbind /v." If you are able to do this without errors, your netcard driver is binding successfully with your real mode protocol (NetBEUI).

If you do get errors here, there is either configuration problem with your netcard, netcard driver, or your protocol. Try to use the error message to narrow this down.

- If you are able to “bind” the network drivers, try loading the redirector with either of the following commands: “Net start basic” or “Net start full.”
- Real mode components (NIC driver, NetBEUI, Redirector) may be attempting to load high. Remark out EMM386.EXE (or any other UMB provider), if this wasn’t done when clean booting the system.
- Try NET START /NOHI. If NET START /NOHI works, put the “**LoadHigh=no**” switch in the [Network] section of SYSTEM.INI so that the user can just type NET START each time they need to run the real mode network instead of NET START /NOHI.
- Check the [Network Drivers] of SYSTEM.INI for any “<netcard>.DOS=LOW/HIGH” lines and change accordingly. The above /NOHI and “**Loadhigh=no**” switches will override the “<netcard>.DOS=HIGH” line.
- Memmaker will not optimize the UMBs with NET START components. If a user optimizes UMBs with MemMaker and then installs Windows for Workgroups 3.11 with the real mode net, they may find that some of the components that were previously loading high are now loading low because they occur in the AUTOEXEC.BAT *after* the NET START line. When NET START is run, the real mode components load into whatever UMBs are currently available, forcing TSRs that were previously configured to load into a particular memory region (using the MS-DOS 6.x /L and /S switches) to load low.

Step by Step Loading of the Real Mode Network

NET INIT

Loads NDIS NIC driver(s) and protocol(s) and PROTMAN.DOS. Files read: NET.EXE, WFWSYS.CFG, SYSTEM.INI, PROTMAN.DOS, PROTOCOL.INI, <netcard.DOS>, NDISHLP.SYS, NET.MSG.

NET START NETBIND

Performs Protocol Manager binding using PROTMAN.EXE. Files read: NET.EXE, WFWSYS.CFG, PROTMAN.EXE, SYSTEM.INI, NET.MSG.

NET START NETBEUI

Loads NetBEUI protocol. Files read: NET.EXE, WFWSYS.CFG, SYSTEM.INI, NET.MSG.

NET START BASIC/FULL

Loads BASIC or FULL redirector, logs user onto network, restores persistent connections. Files read: NET.EXE, WFWSYS.CFG, SYSTEM.INI, <username>.PWL, CONNECT.DAT, NET.MSG.

Verify Real Mode Network Components

The following files compose the Real Mode network. If you suspect that one of these files is corrupt, decompress the file off the Windows for Workgroups 3.11 installation disks.

NET.EXE
NET.MSG
NETH.MSG
PROTMAN.DOS
PROTMAN.EXE
IFSHLP.SYS
NDISHLP.SYS

NET START BASIC/FULL produces Error 7361

If a **NET START FULL** or **NET START BASIC** produces the error:

Error 7361: IPX or NetBIOS must be running in order to load the network services,

then there is no real mode protocol installed. If Novell's IPX is not installed, the easiest thing to do is to install NetBEUI or load the NetBEUI driver by typing **NET START NETBEUI** before starting the real mode network with **NET START BASIC/FULL**.

Missing Real Mode Network Functionality

- By default the real mode network loads the BASIC redirector which does not include support for named pipes and the network APIs. To automatically load the FULL redirector upon startup of Windows for Workgroups 3.11, add *Preferred redir=FULL* to the [network] section of the SYSTEM.INI.
- To enable the Disk Connections/Printer Connections popup TSR (NETPOP), the user can enter **NET START NETPOP** or add *Autostart=POPUP* to the [Network] section of SYSTEM.INI.

Architecture and Configuration

Common Configuration Issues

***When I type "Win," Windows for Workgroups hangs,
-or-
After typing "Win," I get dumped back to an MS-DOS
command prompt.***

Either of these problems indicate that there may be wrong entries in the PROTOCOL.INI or SYSTEM.INI files.

- Try to start Windows for Workgroups 3.11 by typing "Win /n", in an attempt to narrow down the type of problem. If Windows for Workgroups 3.11 loads, then the problem probably is centered around the network VxDs. If Windows for Workgroups 3.11 will not load, it is a much more generic Windows problem.
- Check the netcard and protocol configurations. Backup the SYSTEM.INI and PROTOCOL.INI files. Try the .CLN files first. If these files are still incorrect, then use Network Setup to install for no netcards. Exit all the way out to the "Restart Computer/Continue" dialog. Choose "Continue" and then use Network Setup to recreate the configuration and it will rewrite the PROTOCOL.INI and SYSTEM.INI files.

Resetting ROM settings on software configurable cards

- Check the netcard configurations and verify the proper settings with Network Setup. Exit out of Windows for Workgroups 3.11 and reboot. Some software configurable netcards will be reset by the NDIS 3 driver. Other software configurable netcards may require the NDIS 2 driver to load to reset the card (Example: the Intel EtherExpress 16). When in doubt, run the real mode network to load the NDIS 2 NIC driver to reset the card according to the new PROTOCOL.INI settings. If that does not seem to work, use the software configuration program shipped with the netcard to verify or change hardware settings.

If there is an I/O address conflict with another device in the machine, it may not be possible to configure the network adapter card without first removing the conflicting device. If it is not possible to remove the conflicting device, put the network card back into the first machine and run Network Setup.

Network Application Won't Run After Installing Windows for Workgroups 3.11

- Find out which protocol the application is using and use Network Setup to set that protocol as the "Default Protocol" (LANABASE=0).

Interoperability with LAN Manager, Windows NT, and Windows NT Advanced Server

Windows NT Server Will Not Validate Logon of Machine Name with a Space Character In It

- A Windows NT Advanced Server will not validate the logon of a Windows for Workgroups 3.11 client machine name if it has a space character in it. For example "JOHNDOE" as a machine name will work fine but "JOHN DOE" will not.

Time out of LAN Manager Logon Script Before Completion

- Logon scripts performed when logging onto a LAN Manager server must be completed within 30 seconds of starting or they will be aborted. This is a limitation of LAN Manager.

User Account Issues

“The Password Of This User Has Expired”

This error may appear if a Windows For Workgroups Client is attempting to access a Windows NT resource using a **net use** at a DOS prompt. The error occurs because the account being used in Windows for Workgroups matches an account on the Windows NT Server. The shared resource is only available to that Windows NT account and the administrator has selected ‘User Must Change Password at Next Logon’ for that user account.

“Network Error 2242”

This error may appear if a Windows For Workgroups client is attempting to access a Windows NT resource using File Manager. The error occurs because the account being used in Windows for Workgroups matches an account on the Windows NT Server. The shared resource is only available to that Windows NT account and the administrator has selected ‘User Must Change Password at Next Logon’ for that user account.

Using Lowercase Extended Characters for Passwords

Windows for Workgroups machines should not use lowercase extended characters for passwords on Windows NT servers. By convention, the down level client converts the password to uppercase before it is sent to Windows NT. Some of the international characters do not have an uppercase equivalent, which causes Windows NT to fail to validate the password.

Using International Characters in the Windows NT Share Name

If you try to connect to a Windows NT share that contains one or more international characters in the share name, you will receive an error message.

Empty Server Browse List

If a Windows For Workgroups machine is a backup browse master in a mixed Windows NT and Windows For Workgroups Domain, then the browser may return “Empty server list.”

The empty server list occurs because Windows For Workgroups uses the currently logged in user account for validation when connecting to shared resources. The server list is a shared resource on the Browse Master and all Backup Browse Masters connect to the Browse Master for updated server lists every fifteen minutes.

Since Windows NT will always be the Browse Master in the workgroup (NT has a higher priority in the election process), the Windows for Workgroups Backup Browse Master will have to retrieve the server list from a Windows NT machine. If the Windows for Workgroups machine does not have a valid account on the NT machine and the guest account is disabled, an empty server list will be returned.

To resolve the problem, disable browsing on the Windows For Workgroups machine by adding

“**MaintainServerList=no**” to the **[network]** section of the SYSTEM.INI file or enable the Guest account on all Windows NT machines in the workgroup.

Password Required For Chat - Network DDE

Windows for Workgroups machines are not able to chat a Windows NT machine if the Windows NT machine does not allow “Everyone,” or the logged in Windows for Workgroups user account rights to Chat.

Note Permissions for Chat and other DDE Shares can be checked and set using the DDESHARE.EXE utility provided with the Windows for Workgroups Resource Kit.

Interoperability with Novell NetWare

Machines across a NetWare Server or IPX Router are not visible

- Verify that both machines are running either the NWLink or “NWLink with NETBios Compatible” protocols. If one machine is running on either IPX.COM or Arcnet, the other machines will have to run the “NWLink with NETBios Compatible” protocol in order to connect to it.
- Check to see if the Windows for Workgroups 3.11 server can see other Windows for Workgroups 3.11 servers on its own segment of the network, and can also see the routing server.

Can't access a NetWare Server

- Verify that the user is running the real mode NetWare workstation shell and has logged in and can access NetWare servers in real mode.
- If the user can access NetWare servers in real mode but not in protect mode, verify that the user has selected Novell NetWare as a secondary network under Network Setup.
- Verify the following SYSTEM.INI settings:

```
[boot]
secondnet.drv=netware.drv
[386enh]
secondnet=vnetware.386
```

For monolithic and ODI ARCNet installations,

```
netcard3=nwsup.386,vipx.386,nwnblink.386
```

Note that for NDIS3, NDIS2 (MSIPX) and other ODI installations, VIPX.386 should never be loaded if NWLINK.386 is being used.

```
transport=nwlink.386,nwnblink.386
```

- Try installing Novell NetWare as the primary network under Network Setup. This configuration is basically Windows 3.1 with the NetWare network drivers installed. This configuration eliminates all Windows for Workgroups 3.11 real and protect mode network components. This configuration also provides access to NetWare server resources, as an interim solution.

Setup recommended ODI but it won't work in real mode

- Check NET.CFG for interrupt and port settings to confirm that they are setup correctly.
- Make sure that you have the latest NetWare files from Novell. DOSUP7 can be download from Novell's Bulletin Board Service or Novell's CompuServe forum. DOSUP7 has the latest LSL, IPXODI, and NETX. To confirm that you have the latest MLID, contact your netcard vendor.

My ODI Configuration No Longer Works After Installing Windows for Workgroups 3.11

Installing Windows for Workgroups 3.11 over a properly configured ODI setup should not affect the ODI configuration in any way.

- When installing Windows for Workgroups 3.11 over a Novell ODI drivers, Setup changes two things which should not interfere with an ODI setup.

ODIHLP.EXE is added to the AUTOEXEC.BAT. This TSR is a helper file that binds to LSL.COM. LSL.COM treats the TSR as an additional protocol and should not interfere with a previously configured ODI setup. To verify this, remove ODIHLP.EXE from the AUTOEXEC.BAT and see if ODI works. Note that this driver must be loaded After the ODI MLID driver.

Setup also modifies or creates a NET.CFG file. It adds some additional “Frame” settings which should not interfere with an ODI setup. Setup backs up the previous NET.CFG file as NET.nnn which you can restart to verify that Setup did not break the previously configured ODI setup.

A problem could occur if a NET.CFG did not exist before installing Windows for Workgroups 3.11. Windows for Workgroups 3.11 setup creates a generic NET.CFG with the four frame types listed. This could change the default frame type that the MLID driver is using to get to the Novell server.

I want to unload all ODI components

- All ODI components can be unloaded from memory at the command line with the “/U” switch (to unload NETX, type “NETX /U” at the command line). Note that ODIHLP.EXE must load after both the LSL.COM and the MLID. Because of this, if you are using ODIHLP.EXE you cannot unload ODIHLP.EXE, LSL.COM or the MLID.

ODI Files Not Processing NET.CFG

- LSL.COM looks for NET.CFG in the directory where LSL.COM is located and then the root directory. The other ODI components (IPXODI and the MLID) look at LSL loaded in memory to provide the location of the NET.CFG. When Windows for Workgroups 3.11 SETUP runs, it also looks at LSL for the NET.CFG location. If no NET.CFG file is found, Setup will create one and by default, place it in the Windows directory.

NETX.COM version 3.26 which ships with Windows 3.1 and Windows for Workgroups 3.1 does NOT look at LSL for the NET.CFG location and only looks in the current directory.

If you suspect that certain components are not reading the NET.CFG properly, change directories to where the ODI files (including NET.CFG) are located in the AUTOEXEC.BAT before running LSL.COM and the other ODI components. For example:

```
CD\NETWARE
LSL
IPXODI
EXP16ODI
NETX
```

I can't see NetBEUI servers when using ODI.

- Check the NET.CFG file for Frame 802.2 type.

I am having trouble running an IPX application

- NWLink (without the real mode IPX transport) does not provide for NETX (and SPX) bindery service. Bindery service may be necessary for some NetWare specific applications to communicate to NetWare servers (through NETX.)
- There may be LANABASE problems: The user may have both NWNBLink and NetBEUI or other protocols on the same LANABASE. Check the PROTOCOL.INI and SYSTEM.INI for the LANABASE settings for each protocol and verify that they are unique.
- Some NetBIOS applications require the NetBIOS transport to be located on Lana 0. Both NetBEUI and NWNBLINK provide NetBIOS services so you may need to make sure the transport you want your application to use is on Lana 0. You can do this by making the desired protocol the "Default" protocol in netcard setup.
- Some Windows applications access IPX using NetWare .DLLs. This functionality may not be part of NWLink.
- If you have a problem with an IPX/SPX application, such as Rconsole, confirm that both NWLINK.386 and VIPX.386 are not loading in the SYSTEM.INI file. Since NWLINK provides the virtual IPX services that VIPX.386 does, they should not be loaded together. The only time VIPX.386 should load is when you are running over IPX.COM or Arcnet.

Interoperability with Banyan VINES

Load order of drivers in AUTOEXEC.BAT

Most of the problems associated with Banyan Vines connectivity in Windows for Workgroups 3.11 can be found with files not loading or files loading out of order in the AUTOEXEC.BAT. The following is the correct order:

AUTOEXEC.BAT

```
c:\<Windows directory>\Net Initialize
cd <Banyan Files>
Ban /nc
NDISBAN or NDTOKBAN (Token Ring)
redirall
c:\<Windows directory>\net start
arswait
z:login
```

Note Banyan Systems also recommends having the login drive (Z:) in the path.

Cannot Connect to a Banyan VINES Server

Make sure that you can connect to a Banyan Vines server at DOS and that there are no error messages on boot up of the machine or as you get into Windows for Workgroups 3.11. If you can connect to a server at DOS and there are no error messages then make sure your supported version of Banyan Vines is installed in Windows for Workgroups 3.11 and that the SYSTEM.INI file has the line “Secondnet.driv=z:\VINES.DRV”

“Initban: Ban not installed or software mismatch”

This error message indicates that BAN.EXE was not loaded or did not load successfully when it got to NDISBAN. This may occur if NDISBAN is loaded before BAN in the AUTOEXEC.BAT or if BAN.EXE is not present.

“Unable to read PCCONFIG.DB configuration database”

The AUTOEXEC.BAT should contain the line “CD <Banyan files>”. If this line is deleted then this error message may be displayed during startup.

“Cannot Start STDA Session: VINES error 157”

This indicates that the server has gone down or the machine has been removed from the network while the client was in Windows for Workgroups 3.11.

“Call to Undefined Dynalink”

This error message may be displayed if the user is starting Windows for Workgroups from the login drive (Z:\).

“Cannot install protected mode mapping”

This error message is displayed when WFWNET.DRV cannot load VINES.DRV. This error message can be caused by a lack of available conventional memory. To work around this problem, try to increase the amount of free conventional memory.

Environment Variables Overwritten

If the VINES LOGIN command is placed before the PATH statement in the AUTOEXEC.BAT, then the Path (and other environment variables) in your VINES user profile may be overwritten by the environment variables in your AUTOEXEC.BAT file.

To work around this problem, either place all environment variables, including PATH, in your user profile only, or place all environment variables AFTER the LOGIN command in your AUTOEXEC.BAT file. If you want to add the user profile PATH environment variable to the PATH environment variable in your AUTOEXEC.BAT file, type %PATH% after the LOGIN command at the end of your AUTOEXEC.BAT file. For example, the following statement appends the user profile PATH values (%path%) to the existing PATH values (C:\;C:\WINWG) in the AUTOEXEC.BAT file:

```
Path=c:\;c:\winwg;%path%
```

Problems Running Named Pipes Applications

Applications written to the Named Pipes application programming interface (API) cannot run with the VINES protocol in the Windows for Workgroups environment; however, these applications are supported by the Windows for Workgroups NetBEUI protocol.

If it is necessary to just use the Vines protocol for named pipes then the Microsoft SQL NIK (Network Interface Kit) does allow Name Piped applications to run on the VINES protocol.

Token-Ring Support with Banyan VINES

Token Ring LAN's are currently only supported when running Windows for Workgroups 3.11 with VINES 5.52 (5).

Interoperability with SunSelect PC-NFS

“NFS903F Missing or invalid PROTOCOL.INI data” Error When Starting SunSelect PC-NFS

This error can be generated when trying to bind the SunSelect PC-NFS protocol to more than one Media Access Controller (MAC). To eliminate this error start Windows for Workgroups without network functionality by typing :

WIN /N

and pressing ENTER. Then open the Network group and double click on the Network Setup icon. Select Drivers and then highlight the PC-NFS Protocol listed under the network adapter to which you don't need to bind PC-NFS. Choose Remove and then click choose the close button. Follow the prompts and when asked, choose Restart Computer. This will allow the changes you have made to take effect.

Performance Enhancements

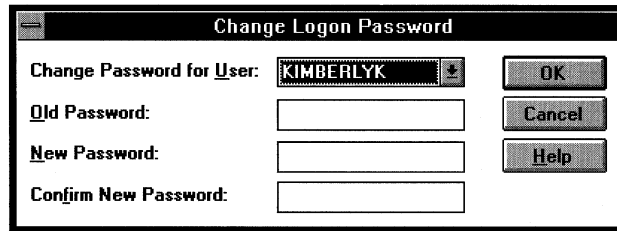
Ghosted Connection Issues

Network drives that are ghosted at startup may not display in the File-Open dialogs of some applications.

For user level passwords that are not cached, File Manager shows the drive icon, but when activated gives an error message about an invalid password and prompts the user to enter a valid password. The only workarounds are to set the Windows for Workgroups 3.11 login password to the same as the domain password, or to disable all ghosted connections. You can change your Login password in the Password section of the Network applet in Control Panel.

Figure 13.2

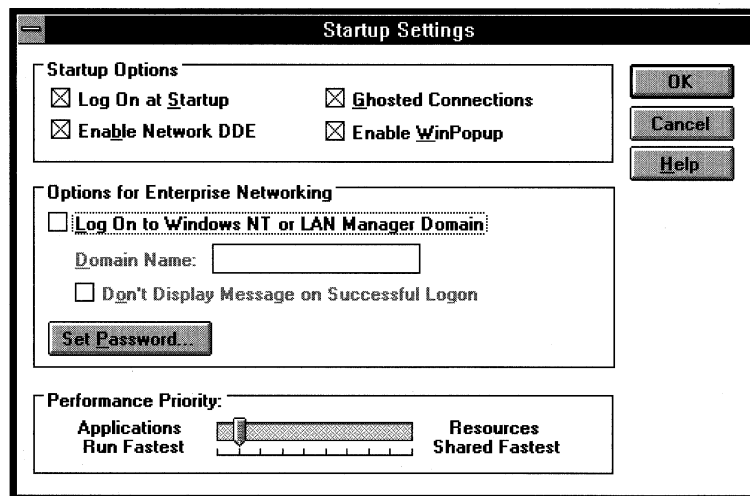
The Change Logon Password dialog box, accessible through the Network applet in Control Panel.



Some applications that are loaded by the Startup program group and are accessed across a network may have problems running when ghosted connections are enabled. Turning off ghosted connections should allow the application to run as expected, but may cause the startup time of Windows for Workgroupsto increase. You can disable ghosted connections in "Startup, Settings" section of the Network applet in Control Panel.

Figure 13.3

The Startup Settings dialog box, accessible through the Network applet in Control Panel.



Problem browsing other servers on the network

If you are getting no browse list or Windows for Workgroups 3.11 hangs when trying to browse, try exiting Windows, starting up the real mode network, and typing NET VIEW. If this does not allow you to view other servers, then the Master Browse Server is hung up and will need to be restarted. If successful at real mode, use the Browse Watcher tool included with this Resource Kit, to find the Backup Browse Servers and then restart them. If restarting the Master Browse Server and the Backup Browse Servers does not eliminate the problem, look for connection or hardware problems.

32-bit file access is not enabled on a given disk drive

Windows for Workgroups 3.11 implements 32-bit File Access in two different ways. One method is to run on top of a 32-bit Disk Access driver. Windows for Workgroups 3.11 ships with the same 32-bit Disk Access driver that shipped with Windows 3.1. It will work with any Western Digital 1003 compatible hard drive controller. It will not work on top of any SCSI drive. If your controller is not WD1003 compatible, check with your controller vendor to see if a driver is available for your controller. The second method is to a special driver called a "Real Mode Mapper." This drivers "maps" 32-bit File Access calls to 16-bit drivers and is required in order to run 32-bit File Access on any kind of compression software such as MS-DOS DoubleSpace or Stacker. Also note that if you are running MS-DOS DoubleSpace, you must be running MS-DOS 6.2 in order for 32-Bit File Access to load.

You can confirm whether or not 32-bit file access is enabled on a given disk drive by looking at the Control Panel Virtual Memory dialog. Control Panel queries VFAT for the status of each drive. If 32-bit disk access is not enabled on a drive, it will show "16-Bit" as the file access type for the drive.

Note Users of DoubleSpace require MS-DOS 6.2 to support 32-bit File Access on a DoubleSpace compressed volume. To obtain the MS-DOS 6.2 upgrade, contact Microsoft or your local reseller.

1) Is 32-Bit Disk Access functioning on the given volume? 32-bit file access requires either a 32-Bit Disk Access volume or a "Real Mode Mapper" volume in order to work. In order for a drive to be a 32-Bit Disk Access volume the controller needs to be Western Digital 1003 compatible (using *WDCTRL) or have a vendor supplied 32-Bit Disk Access driver. Microsoft makes no guarantees that 3rd party 32-Bit Disk Access drivers will work properly with 32-bit file access. If they do not have a 32-Bit Disk Access driver or are running disk compression software, they will need to use the real mode mapper (RMM.D32). To load this driver, you need to have IOS.386 (which replaces *BLOCKDEV) and VXDLDR.386 (which loads RMM.D32 on startup) loading in the [386Enh] section of SYSTEM.INI. Also, make sure that a "device=vfat.386" entry is in the [386enh] section of the SYSTEM.INI.

2) If #1 is satisfied and 32-bit File Access still is not enabled, check to ensure that the "minfilecache=" entry in the [vcache] section of the SYSTEM.INI is appropriate for the amount of memory in the system. For example, a 7MB cache on a 8MB system is far too large.

3) 32-bit File Access will not enable on a drive on which there are open files during the initialization process of 32-bit File Access. Because of this, 32-bit file access cannot be enabled through the Control Panel Virtual Memory dialog when using a temporary swap file. The temporary swap file is opened before 32-bit File Access initializes and 32-bit File Access will not be able to enable on the drive where the temporary swap file is located. There normally should not be any open files at the time when 32-bit File Access is initializing. If there are open files, they are probably the result of some real mode TSR or a 3rd-party VxD.

Note Users running SETUP /N from a NetWare server to install Windows for Workgroups 3.11 and are also loading a TSR in their logon script that is holding a file open during Windows for Workgroups 3.11 startup, will experience this problem.

4) 32-bit File Access will not be enabled if the user has started the real mode network (**NET START FULL** or **NET START BASIC**) and then started Windows for Workgroups 3.11. This is due to a design limitation in the IFS manager (IFSMGR.386). Users running Windows for Workgroups 3.11 through **SETUP /N** to an SMB server (LAN Manager, Windows for Workgroups 3.1, Windows for Workgroups 3.11 and Windows NT) will also experience this.

32-Bit File Access Troubleshooting

Possible symptoms of problems with 32-bit Files Access are: severe system instability, hang on startup, disk corruption, or disk utility compatibility problems. When troubleshooting a possible problem with 32-bit File Access, note that the following components are in use when 32-bit File Access is enabled:

VFAT.386: Needed for 32-bit File Access.

IOS.386/VXDLDR.386/RMM.D32: Needed for 32-bit file access to mount non-32-bit Disk Access and compressed drives.

***BLOCKDEV:** Needed for 32-bit Disk Access drives. Replaced by IOS.386 when there are any non-32-bit Disk Access or compressed drives present.

***WDCTRL/<3rd party Fastdisk Driver>.386:** Needed for 32-Bit Disk Access.

VCACHE.386: Used by VFAT.386 when 32-bit File Access is enabled to cache data.

32-bit file access Troubleshooting Strategy:

The basic strategy for troubleshooting 32-bit file access problems is a process of elimination of the following components: VFAT.386, IOS.386, VXD LDR.386, or RMM.D32, and Fastdisk drivers.

Remark the “**device=VFAT.386**” entry in the [386enh] section of SYSTEM.INI. Does the problem go away?

If no, re-enable the VFAT.386 entry in the SYSTEM.INI file. If using the Real Mode Mapper instead of using a Fastdisk driver, rename RMM.D32 in the SYSTEM directory and start Windows for Workgroups 3.11. If the problem goes away, then something is wrong with the IOS.386, VXD LDR.386 or RMM.D32, and you should expand these files from the original Windows for Workgroups 3.11 diskettes.

When using just Fastdisk, start Windows for Workgroups 3.11 with the **WIN /D:F** switch. If the problem goes away then it is the FastDisk driver that is causing problems. Try disabling the 32-bit Disk Access option and see what happens. This will enable the Real Mode Mapper on the drives, instead of the Fastdisk driver. If this works, check the documentation that came with the Fastdisk driver for proper installation instructions, or contact your Fastdisk driver vendor.

When using both IOS.386 and Fastdisk, try the above procedures for IOS.386 and Fastdisk while the other is disabled to identify which component is causing the problem.

Perform general troubleshooting, by removing TSRs, 3rd party components, etc.

If the problem persists, use the Control Panel Virtual Memory dialog to disable 32-bit File Access and 32-bit Disk Access, and see if the problem goes away.

Note WIN /D:F does not prevent 32-bit file access from mounting drives using RMM.D32. RMM.D32 is not a Fastdisk driver. Use WIN /D:C to disable 32-bit file access from mounting on any drives.

My system seems to have slowed down since I enabled 32-bit file access.

32-bit File Access does not use write behind caching on non MS-DOS 6.2 compressed volumes. Each user must weigh the efficiency and performance of 32-bit file access against SmartDrive. To increase performance you can increase the **minfilecache=** entry in the [**vcache**] section of the SYSTEM.INI. With SmartDrive the maximum cache size performance peak is at around 2Mb. (SmartDrive uses a linear searching method to find a possible cache entry.) VCACHE uses a more optimal hashing algorithm that works well with larger cache sizes. However, the more memory you give to VCACHE, the less memory available to Windows and the sooner you have to start paging to the swapfile.

Incompatibilities with 32-bit file access and various Windows disk utilities

Many Windows or non-Windows disk utilities may not work correctly with 32-bit file access enabled. These utilities will fail when attempting to do an INT26h (Absolute Disk Read). These type of utilities may give bizarre error messages such as "System Write Protect." If you need to run one of these utilities, disable 32-Bit File Access in the Virtual Memory-Disk dialog box and restart Windows for Workgroups 3.11 and then re-enable it when you are finished running the utility.

Utilities that make direct calls to the drive (such as Norton's Disk Doctor) must not be used in an MS-DOS box on a drive that is controlled by 32-bit file access. These utilities should be used outside of Windows.

Note Independent of whether 32-bit File Access is enabled, use of disk utilities in a MS-DOS box is not recommended. Applications or utilities that cannot install or run on a remote drive will fail if 32-bit File Access is enabled. DiskEdit, SpeedDisk and other similar types of Norton Utilities are applications that are not compatible with 32-bit File Access.

32-bit File Access cache related issues

If you suspect a problem with the 32-bit File Access disk cache, exit Windows for Workgroups, and restart by typing Win /d:c. This will disable VFAT.386. If you no longer experience the original problem, disable 32-File Access in the Virtual Memory dialog box in the Enhanced section of Control Panel.

Other New Features

Invalid or Damaged WFWSYS.CFG

Note For further information on the ADMINCFG.EXE or the WFWSYS.CFG, refer to Chapter 6, “Windows for Workgroups 3.11 Security Control Enhancements,” in this Windows for Workgroups Resource Kit Addendum.

WFWSYS.CFG exists in a stamped and unstamped form. WFWSYS.CFG is in an unstamped form immediately after running Setup. When Windows for Workgroups 3.11 is launched for the first time, WFWSYS.CFG is stamped by a unique ID for that computer. If you copy a stamped WFWSYS.CFG to another computer with a stamped WFWSYS.CFG, Windows for Workgroups 3.11 will not load with network functionality. Every machine **MUST** have the WFWSYS.CFG file in their \WINDOWS directory to have network functionality.

If the file gets deleted, damaged or copied from another machine you will not have any network functionality. If file is deleted, renamed or corrupted the user will not have network functionality. They must do one of the following:

- Have the administrator create a new unstamped WFWSYS.CFG using ADMINCFG.EXE.
- Delete the existing WFWSYS.CFG and then reinstall Windows for Workgroups 3.11 to have a new unstamped WFWSYS.CFG created.

Passwords for shared drives on the local machine are not visible

- Windows for Workgroups 3.1 shows the share password in the Share As... dialog by default, and Windows for Workgroups 3.11 by default has “Show Share Passwords in Sharing Dialogs” *disabled* by default in the WFWSYS.CFG.

In order to unhide the various passwords, run the ADMINCFG.EXE to enable the “Show Share Passwords in Sharing Dialogs” setting.

Note By default, Windows for Workgroups 3.11 does not cache user-level passwords, unlike Windows for Workgroups 3.1. This setting, “Allow Caching of User-Level Passwords,” can be enabled via the ADMINCFG.EXE, and is saved in the security settings file.

Microsoft At Work PC Fax

Errors with Faxes and Mail in the Outbox

- The Fax Manager loads and closes all items in the Outbox. The Fax system should not be toggled on and off with mixed faxes and mail in the Outbox. If the user selects NO at the “you have an unsent message, send message now” dialog, the faxes in the Outbox will come back as undeliverable mail.

Installing for Microsoft Mail after Installing for “Fax Only”

- If you install for FAX ONLY and then decide to install Mail, the MSMAIL.INI file should be renamed prior to the installation of Microsoft MAIL, otherwise the MSMAIL.INI transport information in the [providers] section will be wrong.

- Installed for “Fax Only”:

```
[Providers]
Transport=FAXSTUB
Name=PABNSP faxnsp
Logon=FAXSTUB
```

- Installed for “MS Mail and Fax”:

```
[Providers]
Name=PABNSP MSSFS Faxnsp
```

Can't Send E-mail Format on a Class 1 Fax Modem

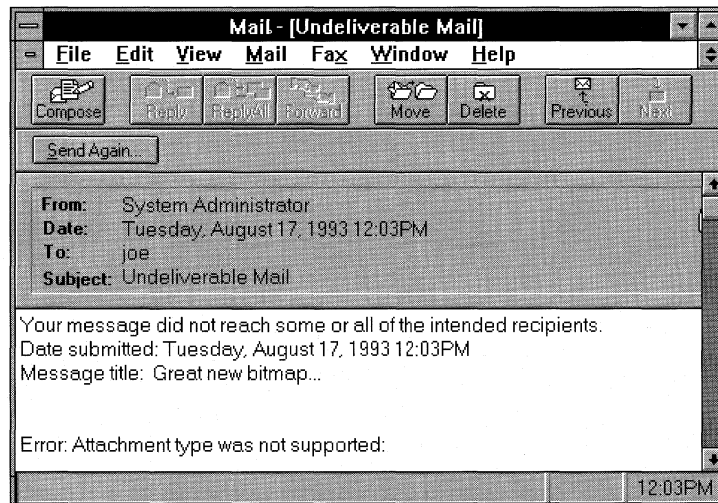
- If the E-mail Format transfer option is grayed out, the hardware didn't report back to Microsoft at Work Fax that it was in fact true Class 1 hardware. Try the modem command “AT+FCLASS=?” from Terminal to determine what Class fax modem is installed. Try removing and reinstalling the fax modem driver from the Fax Control Panel.

“Attachment type was not supported” Error

- When trying to send an attached file in facsimile format, Microsoft Fax will try to “print” the file by rendering it into facsimile format (DCX file). When it prints it just uses the attached file’s OLE server to print the document using the OLE Shell Print command stored in REG.DAT. If no OLE Shell Print command is registered for the attachment the user will get an Undeliverable Mail message with the error “Attachment type was not supported.”
- To test for this condition, drag and drop the file attempting to be sent from File Manager to Print Manager loaded as an icon on the desktop. To work around this error, have the user create the fax by doing a File-Print to the Microsoft Fax driver from within the application that created the file.
- This error will occur if an attempt is made to send a FAX message with an attachment that is not printable, such as an executable file or system file. This error will also occur if your modem is not class 1 compatible, or you are using a class 1 modem but have selected facsimile format. To determine the selected message type, from the Fax menu, choose Options.

Figure 13.4

To determine the selected message type, from the Fax menu, choose Options.



Can't Fax to a Shared Fax Modem

- If the user is on a PBX or other phone system which requires a prefix to reach an outside line, verify that the prefix is not being entered twice. For example, on the machine with the fax modem installed, check Control Panel-Fax for the prefix (it may say “9,” for the typical “dial 9 to get out”

PBX). Then, check the fax address of the user attempting to send the fax to the shared fax modem. If the fax address is “[fax:bob@9,555-1000]” then the prefix, “9”, is being entered twice resulting in misdialing of the destination phone number.

I hear the modem answer the phone, but the Microsoft Fax status Indicator displays idle.

- If you are using a CAS fax modem, this is completely normal behavior. CAS modems operate in the background and receive incoming faxes independent of Microsoft At Work Fax and new faxes are placed in a queue. Microsoft At Work Fax then checks for new fax messages by checking the queue at the interval set for Microsoft Mail to check for new messages.

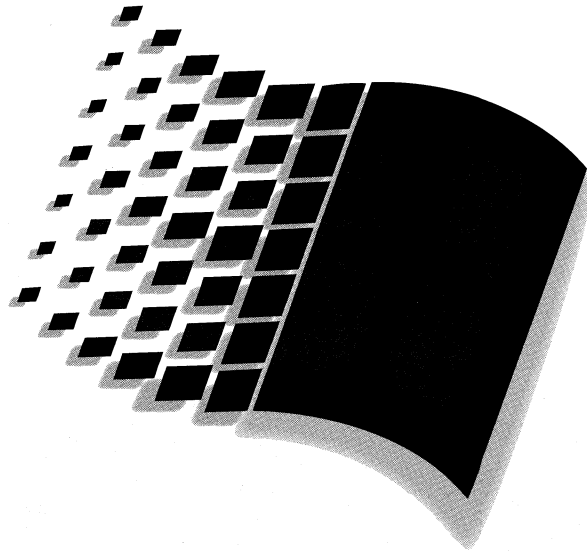
Remote Access Service (RAS) Client

RAS connects to the server, but refuses to authenticate me

- Verify with your NT system administrator that your NT account has RAS services enabled.
- If you are using a modem that is compatible, but not listed as a choice during setup, try selecting a lower initial baud rate or deselect the Enable Modem Compression option, by choosing Modem from the Edit menu.
- Disable software compression under the Options menu.

I have RAS services, however I am still unable to attach to a RAS server.

- Verify that the correct modem type and communications port are selected in RAS. To check this, from the Setup menu, choose Configure.
- Confirm that RAS is successfully communicating with the modem by entering Terminal (in the accessories group) and with the correct port selected, Type AT? and press the Enter key. You should receive an OK message if communications are successful.



Additional Information

Part
7

Additional Information

Appendix A

Additional Support Information

A-1

Getting Answers to Your Technical Questions	A-2
Sources for Support Information	A-4
Microsoft KnowledgeBase	A-11
Microsoft CompuServe Forums	A-18
Obtaining New and Updated Drivers and Information Electronically	A-20

Index

1

Additional Support Information

This appendix provides information on obtaining additional support and information for Windows for Workgroups 3.11. Information is provided on sources available for support from Microsoft, and also covers obtaining new and updated drivers, including drivers for network adapter cards not included in the Windows for Workgroups 3.11 box.

Contents of This Chapter

Getting Answers to Your Technical Questions	A-2
Windows for Workgroups SDK Information	A-3
Sources for Support Information	A-4
Microsoft TechNet	A-4
Microsoft Developer Network	A-7
Microsoft Solution Providers	A-9
Microsoft Certified Professional Program	A-9
Microsoft Consulting Services	A-10
Microsoft KnowledgeBase	A-11
Welcome to the Microsoft KnowledgeBase (MSKB)	A-11
How to Access the MSKB on CompuServe	A-12
Searching for Articles	A-13
The Microsoft Software Library	A-15
Searching with Expert Mode	A-16
Microsoft CompuServe Forums	A-18
Microsoft Connection - GO MICROSOFT	A-18
Information on Windows for Workgroups	A-18
Microsoft Forum Menu Structure	A-19
Obtaining New and Updated Drivers and Information Electronically	A-20
Windows Driver Library (WDL)	A-20
Microsoft Download Service (MSDL)	A-24

Getting Answers to Your Technical Questions

For answers to your questions and help with technical problems regarding Windows for Workgroups:

- First, check online Help (press the F1 key), the printed documentation set, and the information in the SETUP.TXT, README.WRI, NETWORKS.WRI, PRINTERS.WRI, and MAIL.WRI files.

Note If you are located outside the United States, contact your local Microsoft subsidiary for sales and support.

- For fast answers to common questions and a library of technical notes delivered by recording or fax, call Microsoft FastTips for Windows for Workgroups at (206) 635-7245, available seven days a week, 24 hours a day, including holidays. Microsoft FastTips is an automated system, accessible by touch-tone phone.
- Use CompuServe to interact with other users and Microsoft Product Support Services engineers, or access the Microsoft KnowledgeBase for product information. For CompuServe members, type **GO MSWRKGRP** to access the forum for Windows for Workgroups, or type **GO MSKB** to access the Microsoft Knowledge Base at any ! prompt. For an introductory CompuServe membership kit, call (800) 848-8199 and ask for operator 463.
- Use the Microsoft Download Service (MSDL) to access the latest technical notes on common support issues for Windows for Workgroups and to access the Windows Driver Library via modem. The MSDL is available via modem at (206) 936-6735, seven days a week, 24 hours a day, including holidays (1200, 2400, 9600, or 14400 baud; no parity, 8 data bits, 1 stop bit).
- Contact a Microsoft Solution Provider for installation services and follow-up product support. These companies have individuals who have been certified as Microsoft Certified Professionals on Windows for Workgroups. To be referred to a Microsoft Solution Provider in your area, please call Microsoft at (800) 227-4679.

- Get technical support from a Microsoft engineer. Microsoft offers the following support options to choose from:
 - Support is available for no charge from a Microsoft PSS engineer, via a toll line, for the first 90 days of using Windows for Workgroups. The 90-day period begins the day of your first call. Call (206) 637-7098 between 6:00 a.m. and 6:00 p.m. Pacific time, Monday through Friday, excluding national holidays. For support outside the United States, contact your local Microsoft subsidiary.
 - After your initial 90 days of free support have expired, support is available on a fee basis from a Microsoft PSS engineer. Support is available by calling (900) 555-2000 (\$2 per minute, \$25 cap) or (800) 936-5700 (\$25 per incident). For support outside the United States, contact your local Microsoft subsidiary.
 - Support for Microsoft TCP/IP for Windows for Workgroups is not available from the standard Windows for Workgroups Product Support Services phone line. If you have questions, please contact your Microsoft Solutions Channel member. Support for this product is also available through Microsoft's fee-based support plans. For information on locating a Solutions Channel member near you or about Microsoft's support options, call Microsoft Inside Sales at (800) 227-4679.
 - Microsoft Text Telephone (TT/TDD) services are available for people who are deaf or hard of hearing. Using a special TT/TDD modem, dial (206) 635-4948, between 6:00 a.m. and 6:00 p.m. Pacific time, Monday through Friday.

Windows for Workgroups SDK Information

Information on developing applications that use Windows for Workgroups functionality directly is available as part of the Windows 3.1 SDK Addendum. The Windows 3.1 SDK addendum is only available in electronic form in the Windows Extensions forum on CompuServe. The Windows Extensions forum can be found by typing **go winext** at a system prompt.

The Windows 3.1 SDK Addendum for Windows for Workgroups covers information on the Windows for Workgroups API calls including Network DDE and MAPI. Sample programs and the necessary SDK files are also available in the forum library.

Sources for Support Information

This section discusses the different Microsoft sources available for support and assistance to help you get the most out of using Microsoft products. These sources include Technet, the Microsoft Developer Network, Microsoft Solution Providers, the Microsoft Certified Professional program, and Microsoft Consulting Services.

Microsoft TechNet

Microsoft TechNet is the single comprehensive source of technical information for implementing and supporting Microsoft-based solutions. This worldwide information service is available to individuals on an annual subscription basis (\$295 per user, \$40 for each additional licensee) and is delivered through several advanced delivery mechanisms, including CD-ROM technology and a dedicated CompuServe forum.

Microsoft TechNet is designed for those who support or educate end-users, administer networks or databases, create automated solutions, and recommend or evaluate information technology solutions. Microsoft TechNet makes a wealth of in-depth technical information easily accessible so that subscribers can get fast, accurate answers directly and immediately from a single source. It's a great tool for in-house use by MIS and HELP Desks supporting multiple products in today's complex, integrated software environments as well as for companies providing support and integration services to their customers.

Details on each of the membership benefits follows:

The Microsoft TechNet CD-ROM (Monthly)

The Microsoft TechNet CD is packed with valuable and accessible technical information, and monthly editions are cumulative, adding fresh information. This worldwide CD includes:

- The Microsoft KnowledgeBase, which gives you answers to support questions by providing you easy access to the same extensive library of technical support information used by Microsoft Product Support Specialists every day. No need to call, no need to wait, saving you time and money.
- Resource Kits packed with technical references, troubleshooting information, utilities, and accessories to aid in installing and supporting Microsoft products. Would you like to know the optimal configuration for your network? The Resource Kits provide you with the answer.

- Technical information outlining how to get the most out of Microsoft products. Microsoft products are designed to be easy to use and very powerful; however, sometimes this “how to” information is hard to find. The TechNet CD gives you the “tips and tricks” you need to increase your productivity.
- Migration information that helps you move people in an organization from one product to another or from one environment to another. What are the issues involved in migrating from a mainframe based e-mail system to one that is LAN based? TechNet helps you.
- Product facts and features to assist you in evaluating Microsoft products. You can compare versions of products to better understand the advantages of upgrading.
- Educational materials such as tutorials, training guides and training session slides with notes. Windows for Workgroups and Windows NT training materials are included.
- Customer solution profiles that detail how your colleagues solve real information technology problems.
- Strategic information to keep you up-to-date on the direction Microsoft and its products are taking now and in the future. If you wonder about the overall direction that Microsoft is taking, or need more information on such topics as multimedia, ODBC, MAPI, or WOSA, TechNet brings you the information. Press releases are included.
- Conference session notes from key Microsoft conferences. As part of our effort to provide timely up-to-date information, the TechNet CD delivers technical information not found in a book or a magazine, but rather, straight from the technical professionals themselves. This allows you to stay one step ahead.
- The Software Library, which gives you drivers, utilities, macros and patches.

- The Microsoft Services Directory, a “one stop shop” technical services directory for those who develop, implement and support Microsoft-based solutions in the United States. This directory provides you with information on exactly where you need to go (or what you need to do) to get the following:

Training and certification on Microsoft products

Product support

Ongoing technical information

Third-party programs

Consulting services

Microsoft Press books

Other technical information on the CD includes:

- Using OLE and Word
- Ultimate Printer Manual
- Windows 3.1 and Networks
- Microsoft Excel Functions
- Word Setup and Troubleshooting Guide
- Works Troubleshooting Guide
- Windows Hyper Guide

The simple and easy-to-use interface for the Microsoft TechNet CD-ROM allows you to gain access to relevant information quickly:

- Instant look-up. A powerful, full-text Boolean search engine developed by Microsoft lets you look up the technical information that you need quickly and effortlessly. Simply type in a word or phrase on the information you want. You decide how specific or general you want the information to be, and the search engine will do the rest.
- Intuitive interface. The wealth of information contained on your Microsoft TechNet CD is easy to read, annotate, search, and browse because it's based on the Microsoft Multimedia Viewer. The intuitive Microsoft Windows-based interface allows you to view formatted text and graphics and print topics. A source index lists the CD contents hierarchically by information type, making it easy for you to browse documents on the CD.
- One source of information. No longer will you need to read through piles of papers, search through endless help files, and then cross-reference those same topics. Instead, the Microsoft TechNet CD gathers all the information in one place.

Dedicated Microsoft TechNet CompuServe Forum

The Microsoft TechNet forum on CompuServe (**go technet**) gives you up-to-the-minute news flashes, on-line connections to the Microsoft TechNet community, and the ability to download the latest technical information from Microsoft. You can also exchange information with other experts and peers across the country and around the world.

Membership in Microsoft

TechNet includes WinCIM, an easy-to-use Microsoft Windows-based front-end application to access CompuServe forums. This greatly simplifies the logon, viewing, and download process.

How to Order TechNet

Microsoft TechNet is priced at cost-of-goods and is an exceptional value, especially when compared to competing products. The fee for annual membership in Microsoft TechNet is \$295 (US), plus tax. Microsoft TechNet come with a 90-day, money-back guarantee. To enroll, using your credit card, call 1-800-344-2121 seven days a week, 24 hours a day.

For international orders, call (206) 936-8661 for local contact information.

Microsoft Developer Network

The Microsoft Developer Network is a club for all developers who write applications for the Microsoft Windows operating system or who use Microsoft tools for development purposes. The Microsoft Developer Network has two main goals: to write and publish information on programming for Windows, and to establish two-way communication with the development community. By joining the Microsoft Developer Network, you will become a registered developer with Microsoft and receive technical and strategic information through three channels: the Microsoft Developer Network CD, the Microsoft Developer Network News, and the Microsoft Developer Network Forum on CompuServe.

The Developer Network CD

The Microsoft Developer Network CD is a comprehensive source of information for developers of Windows-based applications. The CD provides new, in-depth articles on programming created in response to developers' inquiries.

To create the content for the Developer Network CD, we assembled a team of programmers, each experienced in specific areas of Windows (GDI, User, Kernel, Win32, multimedia, etc.), and asked them to document the architecture of Windows, addressing known areas of complexity.

The Developer Network CD uses a powerful, Windows-based search engine that lets you search the contents of the entire CD by source, by subject, or by keyword. You can create precise queries, print topics, and import source code into your application.

The Newspaper

The Microsoft Developer Network News is a quarterly newspaper with helpful, timely information for all programmers. The newspaper provides the latest news on Microsoft development tools, operating systems, and Windows functions, as well as programming tips, strategic information, and key Microsoft phone numbers.

The Forum

The Microsoft Developer Network posts all new technical articles and sample code on CompuServe, in the Microsoft Developer Network Forum. You can access this area by typing GO MSDNLIB at the CompuServe ! prompt. You can communicate with the Microsoft Developer Network through forum messages and electronic mail.

Enrollment Information

For more information, call the Microsoft Developer Services Team at (800) 227-4679, extension 11771, between 6:30 a.m. and 5:30 p.m. Pacific time. Outside the U.S., contact your Microsoft subsidiary or call (206) 936-8661 for local contact information.

Mail: Microsoft Developer Network
One Microsoft Way
Redmond, WA 98052-6399

Fax: (206) 936-7329, Attn: Developer Network

Internet: devnetwk@Microsoft.com

Microsoft Solution Providers

A key group of independent vendors have a business relationship with Microsoft to provide technical services centered around Microsoft products. Known as Microsoft Solution Providers, these companies collectively offer a wide variety of technical skills and products and services, such as product support and installation services, application development, vertical industry applications, integration services, project management, and consulting and training. To locate a Microsoft Solution Provider with the expertise to meet your needs, call Microsoft at (800) 227-4679.

Microsoft Certified Professional Program

This program is designed for support coordinators, system engineers, consultants, trainers, network administrators, or anyone who needs to demonstrate technical expertise and support Microsoft products. Upon successful completion of a series of standardized tests, you'll be recognized as a product expert and receive a Product Certification certificate, a camera-ready logo for your business, a membership card, and more. To get information about the program and how to prepare and sign up for exams, call Microsoft at (800) 227-4679. Or see MCP.ZIP from Section 1 of the "MS Windows Advanced Users" forum on CompuServe (**go winadv**).

Obtain recognition for your expertise on the Microsoft Windows operating system by becoming a Microsoft Certified Professional (MCP). The MCP Program supplies you with the guidelines to efficiently support your customers or your company's personnel on Microsoft products.

The Microsoft Certified Professional (MCP) Program certifies your ability to implement and support Microsoft products by passing a series of standardized exams. If you are a support coordinator, systems engineer, consultant, trainer, network administrator, or anyone else who must gain and display technical expertise concerning Microsoft Windows, you owe it to yourself and your company to become Microsoft Windows Support Certified. As an MCP, you will be recognized as a product expert and as a source for the latest information about Microsoft Windows.

To become Microsoft Windows Support Certified, you must register for and pass a closed-book exam that tests expertise and experience on Microsoft Windows.

You can register for the exam by calling Drake Training and Technologies at (800) 755-EXAM (3926). Each exam costs \$100 U.S. You may take the exam at a Drake Training and Technologies site near you. When you call Drake to register, be sure to ask about test sites in your area.

Upon successful completion of the exam(s), you will receive an MCP Program certificate, membership card, camera-ready logo for advertising purposes, access to up-to-date information from Microsoft and industry experts, a CompuServe Intro Kit, an invitation to be listed in the MCP Directory, discounts for the Technical Information Network, and invitations to technical conferences and forums.

Additional Benefits

Solutions Channels participants with Microsoft Certified Professionals on staff receive credits toward purchasing products and training videos, and are listed in the Solutions Channels Directory. Consulting Channels participants receive referrals, Microsoft Developer Network discounts, and more. VAR/Systems Integrator Channels participants may be authorized to resell Microsoft LAN Manager, SQL Server, and Microsoft Mail with the appropriate MCPs on staff. Training Channels participants may qualify their company to offer Microsoft University courses.

Call Microsoft at (800) 227-4679 for a complete copy of the Microsoft Certified Professional Program brochure or the Microsoft Certified Professional Corporate Backgrounder. The brochure contains detailed information on the current certifications, including Microsoft Windows, Microsoft Windows for Workgroups, Microsoft Windows NT Support, Microsoft LAN Manager, SQL Server, Microsoft Mail, Microsoft Excel for Windows and Macintosh, Microsoft Project for Windows and Macintosh, and Microsoft Word for Windows and Macintosh. The Microsoft Certified Professional Corporate Backgrounder explains how certification and periodic assessment of an individual's technical knowledge is essential to ensuring quality service and effective career development. You can obtain the latest copy of the Microsoft Certified Professional brochure electronically as MCP.ZIP from Section 1 of the "MS Windows Advanced Users" Forum on CompuServe (**go winadv**).

Microsoft Consulting Services

Microsoft Consulting Services (MCS) consultants are system architects with experience and expertise in Microsoft technology, methodologies, and tools, chartered to help organizations capitalize on the benefits of the most powerful platform for client-server computing — the Microsoft Windows NT operating system. MCS consultants focus on transferring knowledge and skills to corporations, government organizations, and third-party Microsoft Solution Providers worldwide. MCS, in conjunction with third-party solution providers, offer organizations a number of services customized to their unique information technology environment including planning, design, development, integration, and implementation. For more information about Microsoft Consulting Services, please call (800) 922-9446.

For more information about Microsoft Consulting Services, please contact an MCS office near you.

In the United States:	Canada (416) 568-0434
Central Region (708) 495-5550	Australia (61) (2) 870-2200
Northeast Region (617) 487-6500	France (33) (1) 6986-4480
South Region (214) 458-1739	Germany (49) (89) 3176-0
West Region (206) 635-1980	Italy (39) (2) 210-7361
	United Kingdom (44) (734) 270-001

Microsoft KnowledgeBase

Accessing the Microsoft KnowledgeBase on CompuServe

This section will help you understand how to use the Microsoft Knowledge Base (MSKB) on CompuServe and includes optimal searching techniques, tips on how to find articles quickly, an explanation of the various menu items in the Microsoft Knowledge Base (MSKB), and a description of the "Expert" search mode.

Note The following instructions also apply to the Microsoft Developers Knowledge Base (MDKB).

Much of this information is also contained in the online help associated with the MSKB.

Welcome to the Microsoft KnowledgeBase (MSKB)

The Microsoft Knowledge Base is a database that will enhance your use of Microsoft products by providing you with access to information previously available only to Microsoft support engineers. The Knowledge Base contains helpful articles on all kinds of subjects regarding various Microsoft Products. Using the Microsoft Knowledge Base is like having a Microsoft support engineer available to you day and night, and only a few keystrokes away. With access to these support files, you can quickly obtain answers to your software questions.

Finding the Answer

When you elect to search the Knowledge Base, you will find a generous array of options by which you can locate answers to your questions. Whether you are searching for general information on your product or just trying to find new developments that are on the way, you can use options that allow you to search by product name, version, or category. Once you specify a search term, the Knowledge Base will go to work for you, collecting all of the documents it can find related to the criteria you supplied.

By entering the product name, you can determine if there are further product developments or related articles on the product. If you want to check on current publications, supplying the publication date will locate documents published during the time frames you have specified.

The most notable feature of the Knowledge Base is its ability to quickly perform a search of the full text of all documents contained within the Knowledge Base. With this full-text search feature, you can find specific answers to your questions. If the subject of your question is mentioned in any of the over 25,000 documents on file within the Knowledge Base, this feature will locate these documents for your review. Nowhere else can you find such a feature that will give you the ability to receive immediate responses to your questions with such a minimal amount of work.

Software Library

Many Knowledge Base articles also refer to additional related files that are contained in the software library (GO MSL). The files are referenced by an S number (such as S12345). You can download these files by downloading the S number with a ZIP extension attached to it (S12345.ZIP, for example). A description of the Software Library can be found below in the section titled "The Microsoft Software Library."

How to Access the MSKB on CompuServe

To begin using the Knowledge Base on CompuServe, type GO MSKB at any CompuServe "!" prompt. From there, you'll see the following menu:

```
Knowledge Base      MSKB
Welcome to The Microsoft Knowledge Base
Copyright (c) 1990 Microsoft Corporation
```

- 1 What's New in the Knowledge Base
- 2 Description of Database
- 3 Online User's Guide
- 4 Search the Knowledge Base

The first three selections contain help screens that describe the Knowledge Base, as well as provide information on searching for articles in the Knowledge Base. Most of the information in these help screens is also contained in this users guide. To begin searching for articles, select option 4.

Searching for Articles

After selecting option 4 “Search the Knowledge Base” above, the following menu will be presented:

Knowledge Base

SELECT documents by searching for:

- 1 Words or phrases occurring anywhere in Documents
- 2 Words or phrases occurring anywhere in Document Titles only
- 3 Product Name
- 4 Product Version
- 5 Publication Date
- 6 Document Identification Number
- 7 Operating Environment of Product
- 8 Bugs, Fixes, and Documentation Errors
- 9 Press Releases
- 10 Expert Mode

Articles in the Knowledge Base can be searched for by selecting any of the menu items. The following is a description of each menu item, and how it can be used to find articles:

1. Words or Phrases Occurring Anywhere in Documents

This is the full-text search option that is the “most powerful” search available. You may enter an entire word or phrase that you want to locate. Once you have entered your searching criteria, the full text of each article is searched to locate all occurrences of your criteria. Choose this method when you need the broadest searching capability. Be aware that you may locate articles that do not directly relate to your interest. This search is not case sensitive, so don’t worry about the case of your query.

2. Words or Phrases Occurring Anywhere In Document Titles Only

As stated in this menu choice, the search is limited to document titles only. Your search criteria may contain as many or few letters or words as you desire. This search method allows you to limit the search to a particular field of interest without the need for input of specific search criteria.

3. Product Name

This choice leads to a menu of product categories. After you select a category, a menu of specific product names will appear.

4. Product Version

The prompt for version number is divided into two prompts: one for the major number and one for the minor number. The version 3.2 contains the major number 3 and the minor number 2. This allows for some flexibility of input. To receive all minor numbers of a specific major number, enter a carriage return (CR) at the minor number prompt. Note: Be explicit in specifying minor version numbers. For example, a minor version number of "0" is NOT the same as "00."

5. Publication Date

The menu choice for publication date allows a specific date to be entered, and provides the choice of receiving articles published BEFORE or AFTER the date entered.

6. Document Identification Number

This document number is unique for each article and is assigned by Microsoft. This number is sometimes referred to as the "Q" number of an article (Q75223, for example).

7. Operating Environment of Product

You may enter the operating system in which you are interested from a menu of valid operating systems.

8. Bugs, Fixes, and Documentation Errors

All articles relating to known bugs, fixes for known bugs, and documentation errors can be located with this selection.

9. Press Releases

A list of press releases is available by selecting this option. All Microsoft press releases are now posted to the Microsoft Knowledge Base instead of the "What's New at Microsoft" menu option in the Microsoft Connection area.

10. Expert Mode

This method of searching allows more experienced users to input their search criteria independent of the menu searches. Valid search terms and operators may be obtained by typing /HELP or /H at the Expert mode prompt. An explanation of Expert mode is also contained below under the heading "Searching with Expert Mode."

Article Searching Tips

The following tips will help you to quickly find what you are looking for, and will give you hints about what to do if you cannot find an article. These tips have been provided by support engineers at Microsoft who use the Knowledge Base daily.

- Use the full-text search feature whenever possible. This is the most powerful of the search options, but it also has the possibility of providing you with the most number of articles. Provide as many appropriate keywords as possible in a single search. If the resulting list of articles does not contain what you are looking for, try eliminating one or more keywords and search again. Remember that in the full-text search mode, the articles must contain at least one of every keyword you list in order for them to be found.
- Try different combinations of words and phrases. The Knowledge Base does not compensate for plural words, words with different endings, etc. If the word you search for is not contained in the article verbatim, your search will not find it. For instance, if you are searching for “bitmap” and you don’t find anything, try “bitmaps.” If “scroll” doesn’t work, try “scrolls,” “scrolling,” or “scrolled.”
- Narrow your searches using the product name. If the subject you are searching on is generating a large number of articles (for instance, “file” is one of those topics), you need to narrow your search. Begin by first selecting the correct product name, then narrow your search using the full-text search feature (or, if you are using Expert mode searching, you can select product and text search in one command). This will eliminate all the articles that pertain to other Microsoft products.

The Microsoft Software Library

The Microsoft Software Library contains many of the files available for downloading by CompuServe users. These are the official files currently available from Microsoft Product Support Services. These Microsoft files include printer drivers for MS Word, Works, and Windows; various patches; demos; application notes; sample code and programs; and utilities. All new Microsoft files will be posted here.

The Software Library uses exactly the same file commands used in the regular forum data libraries. The keyword list for each file includes the "S" number (or filename) given in the Knowledge Base article that refers to it. Every file has a Knowledge Base article pointing to it. These are exactly the same files that are available by mail from Microsoft Product Support Services. The easiest way to access the Software Library is by typing GO MSL at any CompuServe "!" prompt.

If you know that something is in the Software Library but don't know the "S" number or filename, the quickest way to find it is to look in the Knowledge Base for the article that refers to it. Query on topics relating to the file, and include the keyword "softlib." Most of the pointer articles for the Software Library files contain the keyword "software library" or "softlib." For instance, if you know that there is a file in the Software Library containing information about performing an ILS landing using Flight Simulator 4.0, you might query on "ils landing software library," and from this query, find an article that lists filename S12634 as containing additional information. Then, you can GO MSL, and download file S12634.ZIP.

Searching with Expert Mode

The Expert search mode is a powerful method that you can use to quickly find articles in the Knowledge Base without selecting multiple menu items to set up your search. This mode is named "Expert" because it requires knowledge of the query language and search fields used in the database.

The Expert mode of the Knowledge Base allows you to search the following "fields":

TEXT	"Full text search" on all words in the articles
TITLEKEY	Article titles only
PCODE	Product name
VER	Version number
PDATE	Publication date
DOCID	Microsoft document identifier
OPSYST	Operating system
DOCTYPE	Document type

The following relational operators/logicals are valid:

<u>Type of Search</u>	<u>Valid Relational Operators</u>
Numeric	EQ, NE, BEG, GT, GE, LT, LE
Term(s)	EQ, NE, BEG
Phrase	EQ, NE

Where EQ = equal to, NE = not equal to, BEG = begins with, GT = greater than, GE = greater than or equal to, LT = less than, LE = less than or equal to. In addition, you may use the logical operators “AND” and “OR” to specify exactly which articles you want to locate. Parentheses can be used to group expressions.

To set up your search, combine a keyword from above with a logical operator, then a value. If your value contains more than one word or any special characters, enclose it in single quotation marks. Acceptable values for each of the fields change from time-to-time, and can be found online on CompuServe by typing /HELP once you are in Expert search mode. Another method of learning the Expert Mode commands and field names is to perform your search using the standard menu interface, and notice the query string that is generated by the system. The valid field names, as well as some sample values, are listed below:

<u>Key Field</u>	<u>Sample Values</u>
TITLEKEY	Any text in the article title or “PR” for Microsoft press releases
TEXT	Any text in the entire article
PCODE	WINSDK Windows Software Development Kit EXCEL Microsoft Excel WINWORD Microsoft Word for Windows
VER	3.0, 2.11, 1.12, 3.1
PDATE	Dec 1 1991, Jan 4 1992
DOCID	Q82843, Q00234, Q11734
OPSYST	MSDOS, OS2, MACINTOSH, WINDOWS
DOCTYPE	BUGLIST Articles listing known bugs
FIXLIST	Articles listing fixes to known bugs
DOCERR	Articles listing documentation errors

Sample Expert Mode Search Expressions

Note: Search values containing spaces or special characters must be enclosed in single quotation marks. If you do not specify a “search field” (that is, TEXT, PROD, TITLE, and so on), TEXT will be assumed. In addition, a relational operator of EQ is assumed unless otherwise specified.

<u>User Enters</u>	<u>Search Performed</u>
apple and printer	(text eq apple) and (text eq printer)
'apple and printer'	text eq 'apple and printer'
text eq basic interpreter	(text eq basic) or (text eq interpreter)
pcode eq winsdk and text eq printer	(pcode eq winsdk) and (text eq printer)
doctype eq docerr and pcode eq excel	(doctype eq docerr) and (pcode eq excel)
pdate ge 'apr 12 1989' and ver '2.5'	(pdate ge 'apr 12 1989') and (ver ge '2.5')
docid eq q11736	docid eq q11736

Microsoft CompuServe Forums

In addition to the other Microsoft services and support mechanisms described earlier in this chapter, Microsoft also maintains several forums on the CompuServe Information Service. These forums represent excellent sources of information on the use of Microsoft products.

Microsoft Connection - GO MICROSOFT

Microsoft is committed to providing a broad range of services that meet the diverse needs of our customers worldwide. The Microsoft Connection is a key component of these services.

The Connection contains an extensive set of technical information including the Microsoft Knowledge Base with over 40,000 technical articles, the Microsoft Software Library, with sample applications, drivers, patches etc. and numerous forum libraries with Microsoft and customer uploaded files. Microsoft sponsors a variety of Microsoft-moderated forums where customers can exchange tips, tricks, and technical questions and answers with a worldwide community of Microsoft users. The forums in the U.S. area of the Connection are organized into eight categories; Information on Microsoft, Microsoft Services, Desktop Applications, Personal Operating Systems, Development Products, Advanced Systems, Windows Shareware Forums, and Windows Vendor Forums. For a detailed map of the service please download MENU.ZIP from Library 1 of any forum in the Microsoft Connection.

Consistent with our commitment to our customers worldwide, we've expanded the connection by creating the Microsoft Benelux, Central Europe, Italy, Spain/Latin America, and Sweden forums. Customers can communicate with each other and with Microsoft representatives in their local language(s) in many of these forums.

Information regarding forums and services is available within the specific US and international areas.

Information on Windows for Workgroups

Information on Windows for Workgroups can be accessed in the Microsoft Workgroup forum. Type **go mswrkgrp** at any CompuServe command prompt to access the Workgroup forum.

Microsoft Forum Menu Structure

The menu structure for the Microsoft forums on CompuServe is defined as follows:

```
MICROSOFT CONNECTION
MENU STRUCTURE AS OF 10/1/93

MICROSOFT CONNECTION <GO MICROSOFT> or <GO MSCON>
-- ABOUT THE MICROSOFT CONNECTION
-- MICROSOFT BENELUX <GO MSBEN>
-- MICROSOFT CENTRAL EUROPE <GO MSEURO>
-- MICROSOFT ITALY <GO MSITALY>
-- MICROSOFT SPAIN/LATIN AMERICA <GO MSSPAIN>
-- MICROSOFT SWEDEN <GO MSSWEDEN>
-- MICROSOFT U.S.
  -- INFORMATION ON MICROSOFT
    -- About the Microsoft Support Network
    -- About Consumer Customer Service
    -- Authorized Training Centers
    -- Microsoft Address and Phone Numbers
  -- MICROSOFT KNOWLEDGE BASE <GO MSKB>
  -- MICROSOFT SOFTWARE LIBRARY <GO MSL>
  -- MICROSOFT SERVICES
    -- Microsoft Developer Services <GO MSDS>
      -- About Microsoft Developer Services
      -- Developer Network Forum <GO MSDNLIB>
      -- Microsoft DevCast Froum <GO DEVCAST>
      -- Microsoft Development Products Forums
      -- Microsoft Developer Knowledge Base <GO MDKB>
      -- Microsoft Software Library <GO MSL>
      -- Update MSDS Registration Information
      -- MSDN Version of WinCIM Download Area
    -- Microsoft TechNet Services <GO TECHNET>
      -- About MS TechNet Services
      -- Other MS Forums
      -- MS TechNet Forum
      -- Microsoft Knowledge Base <GO MSKB>
      -- Microsoft Software Library <GO MSL>
      -- Update TechNet Registration Information
      -- TechNet version of WinCIM Download Areas

  -- MICROSOFT DESKTOP APPLICATIONS
    -- Microsoft Knowledge Base <GO MSKB>
    -- Microsoft Software Library <GO MSL>
    -- Microsoft Office
      -- Microsoft Office Setup <GO MSEXCEL>
      -- Microsoft Word Forum <GO MSWORD>
      -- Microsoft Excel Forum <GO MSEXCEL>
      -- Microsoft Access Forum (Office Prof) <GO MSACCESS>
      -- Microsoft Apps Forum w/ MS PowerPoint <GO MSAPP>
      -- Microsoft Workgroup Forum w/ MS Mail <GO MSWRKGRP>
    -- Microsoft Word Forum <GO MSWORD>
    -- Microsoft Excel Forum <GO MSEXCEL>
    -- Microsoft Access Forum <GO MSACCESS>
    -- Microsoft FoxPro Forum <GO FOXFORUM>
    -- Microsoft Applications Forum <GO MSAPP>
    -- Microsoft Workgroup Forum <GO MSWRKGRP>
    -- Microsoft Programming Applications Forum <GO PROGMSA>
```

```
-- MICROSOFT PERSONAL OPERATING SYSTEMS
-- Microsoft Knowledge Base <GO MSKB>
-- Microsoft Software Library <GO MSL>
-- MS-DOS Forum <GO MSDOS>
-- Microsoft Windows Forum <GO MSWIN>
-- Microsoft Workgroups Forum <GO MSWRKGRP>

-- MICROSOFT DEVELOPMENT PRODUCTS
-- Microsoft Developer Knowledge Base <GO MDKB>
-- Microsoft Software Library <GO MSL>
-- Microsoft Developer Network Forum <GO MSDNLIB>
-- Microsoft Basic Forum <GO MSBASIC>
-- Microsoft Languages Forum <GO MSLANG>
-- Microsoft 32 Bit Languages Forum <GO MSLNG32>
-- Microsoft Windows SDK Forum <GO WINSDK>
-- Microsoft Win32 SDK for NT Forum <GO MSWIN32>
-- Microsoft Windows Extensions Forum <GO WINEXT>
-- Microsoft Windows Objects Forum <GO WINOBJ>
-- Microsoft Programming Applications Forum <GO PROGMSA>
-- Microsoft Windows Multimedia Developer Forum <WINMM>

-- MICROSOFT ADVANCED SYSTEMS
-- Microsoft Knowledge Base <GO MSKB>
-- Microsoft Software Library <GO MSL>
-- Microsoft Windows NT Forum <GO WINNT>
-- Microsoft Client Svr Computing Forum <GO MSNETWORKS>
-- Microsoft SQL Server Forum <GO MSSQL>
-- Microsoft Workgroups Forum <GO MSWORKGRP>

-- WINDOWS SHAREWARE FORUMS
-- Windows Shareware Forum <GO WINSHARE>
-- Windows Games Forum <GO WINFUN>

-- WINDOWS VENDOR FORUMS
-- Windows 3rd Party Applications A Forum <GO WINAPA>
-- Windows 3rd Party Applications B Forum <GO WINAPB>
-- Windows 3rd Party Applications C Forum <GO WINAPC>
-- Windows 3rd Party Applications D Forum <GO WINAPD>
```

Obtaining New and Updated Drivers and Information Electronically

Windows Driver Library (WDL)

The Windows Driver Library (WDL) is a collection of new and updated printer, display, sound, and network drivers for use with Microsoft Windows. Network drivers on the WDL include NDIS 2 and NDIS 3 drivers for network adapter cards not included in the Windows for Workgroups 3.11 retail box. As new and updated files become available they are added to the WDL.

If you have a modem, the drivers are available at no charge on CompuServe, GENie, Microsoft OnLine and the Microsoft Download Service (MSDL). However, note that standard connect time fees and long-distance telephone charges, if any, apply when you download files. When you connect to any of these services, please read the WDL.TXT for a complete list of the devices the WDL supports.

If you do not have access to a modem, you can obtain an individual driver from the WDL on a disk by calling Microsoft Product Support Services at (206) 637-7098.

Instructions for Downloading a file from the Microsoft Software Library

1. Locate the device in the WDL.TXT. Note the name of the file listed next to the device. You need to download this file from your download service.
2. If you are downloading to a floppy disk you need to have a formatted blank disk. If you are downloading to your hard disk, create a new subdirectory in which you will place the files.

Important Do not download files directly into your Windows directory. Doing so could overwrite files essential to the proper operation of your system.

3. Follow the downloading procedure used by your downloading service. The file you download is the executable (.EXE) file that you identified in step 1. This file contains all the files you need to support your device.

Download the .EXE file to your floppy disk or to the new subdirectory you created on your hard disk.

4. Change to the floppy disk drive (or the subdirectory on your hard disk) that contains the .EXE file. At the MS-DOS prompt, type the file name and then press enter.

When the .EXE file finishes running, all the files you need to support your device such as a .DRV (WDL) file and the OEMSETUP.INF file are set up. You are also provided with a .TXT file that contains instructions for installing the device drivers or (other software) and a licensing agreement.

If you have problems extracting files try downloading the files again.

Accessing the WDL from COMPUSERVE

If you are using WinCIM:

1. From the Services Menu select 'GO'.
2. Type MSL in the GO Dialog box.
3. Select '2' to scan.
4. Search for WDL to view the whole WDL list or another key word to view specific files.

If you are not using WinCIM:

1. Logon to CompuServe and type 'GO MSL'.
2. Follow steps 3 and 4 listed above, in the "If you are using WinCIM" section.

Accessing the WDL from Microsoft Online

1. Logon to OnLine.
2. From the Database Menu select the option to 'Select DB'.
3. Choose the "Software Library" option.
4. From the Software Library option select the option "Host Items".
5. In the Query box type WDL to review the whole WDL list or another key work to view a specific file.

To get more information on a specific file, highlight the file with the cursor and press <enter>. This brings up more details about the file.

Accessing the WDL from Genie

1. Logon to Genie.
2. From the main menu select option 5 - Computing Services.
3. From the Computing Services menu select option 6 - IBM PC/TANDY Roundtables.
4. From the IBM PC/TANDY Roundtables menu select option 3 - Software Libraries.
5. From the Software Libraries Menu select option 3 - Search File Directory.
6. Type WDL in as the search string to view the word WDL list or any; other key word to view a specific file.

Accessing the WDL from Microsoft Download Service

More information on the Microsoft Download Service is discussed in the next section.

1. Log onto MSDL by calling (206) 936-MSDL (6735).
2. Enter name and location.
3. from the main menu press F for File index.
4. Select 1 for Windows & DOS.
5. Select 2 for Windows 3.1 Driver Library.
6. Select L to list the whole WDL list or E to examine a specific file.

Searching for WDL Files/Drivers

The following is a list of some of the Key words to use for the search for WDL and WNTDL drivers:

S# (if known)
Q# (if known)
storage
printer
display
netcard
misc
audio
mips
x86
manufacturers name (ie. Compaq, IBM, Cornerstone, Epson ...etc.)

Microsoft Download Service (MSDL)

Microsoft Download Service (MSDL) operates like any MS-DOS-based computer bulletin board system (BBS). The MSDL contains Application Notes from Microsoft Product Support Services (PSS), as well as driver files and other types of support files for download. To use the MSDL, you must have a computer with a modem and a terminal package. Any terminal package, such as Microsoft Works, Windows Terminal, Procomm, or Crosstalk®, will work with the MSDL. If you experience difficulty while you are working with the MSDL, try calling a local BBS so you can avoid paying long-distance charges while trying to determine the cause of the problem.

Please note that technical support is not available on the MSDL.

To Connect to the MSDL

The MSDL supports 1200, 2400, 9600, and 14400 baud rates (V.32 and V.42), with 8 data bits, 1 stop bit, and no parity. Make sure the terminal software is configured to operate with these settings. After you have chosen these settings, you can begin the session as follows:

1. Call the MSDL at (206) 936-MSDL (6735).
2. Enter your full name and the location you are calling from.

The MSDL will list some basic instructions and information and then display the Main menu:

```
*****
****   Microsoft Download Service   ****
****                               ****
****                               ****
*****
[D]ownload File
[F]ile Index
[I]nstructions on Using This Service
[W]indows 3.1 Driver Library Update
[N]ew Files & Complete File Listing
[M]icrosoft Information
[A]lter User Settings
[U]tilities - Comments
[L]ength of Call
[E]xit - Logoff the System
[H]elp - System Instructions
Command:
```

Downloading Files

If you already know the exact name of the file to download, follow the steps below. If you do not know the filename, see the following section, “How to Search for Files.”

1. At the Main menu, press D for Download.
2. Press D again and press the ENTER key.
3. When asked for the filename, type the name of the file you want to download. Be sure to include the correct extension (usually .EXE); also be sure to differentiate between the letter “O” and the number 0 (zero) in filenames.

Tip If you see a “-More-” prompt at the bottom of the screen, you can press the SPACEBAR to see more files.

4. When asked which protocol you would like to use, enter any protocol supported by your terminal package (check your software manual for more information). If you are unsure, press X for Xmodem.
5. The MSDL will then display the “Awaiting Start Signal” message. When you see this message, start the download process with your terminal software. For example, if you are using Windows Terminal, choose Receive Binary File from the Transfers menu.
6. If you don’t start the process, the transfer will fail, and you’ll need to start again at step 2.
7. Once your transfer is complete and you want to exit the MSDL, choose Exit from the menu by pressing E.

Searching for Files

If you do not know the exact name of the file to download or you simply want to find out what files are available, do the following:

1. At the Main menu, press F for the File Index.
2. Press F for File Search.

3. You will be prompted to enter the text to search on. For example, if you want to search for a Hewlett-Packard® (HP) LaserJet® printer driver, type “hp laserjet” and press the ENTER key.

The matching filenames will be displayed in a list.

Tip If you see a “-More-” prompt at the bottom of the screen, you can press the SPACEBAR to see more files.

If you don't find what you are looking for, see the following section, “How to Use the File Index,” for instructions on how to use the file index.

4. Once you see the file that you want, write down the filename so you can download the file later.
5. Press the ENTER key to quit the search option.

See “How to Download Files” above, for instructions on how to download the file.

Using the File Index

1. At the Main menu, press F for File Index.
2. In the next screen (the File menu), choose the number that matches the application you are looking for.
3. Continue to select the appropriate number from the menus that appear until you see a list of files displayed on screen.

For example, if you are looking for a Windows 3.1 printer driver, do the following:

- a. Press F at the Main menu.
 - b. Press 1 for Windows and MS-DOS.
 - c. Press 2 for Windows 3.1 Driver Library.
 - d. Press 2 for Windows 3.1 Printer Drivers.
4. A list of files will be displayed on the screen. Read through the list to see if the file you need is displayed.

Tip If you see a “-More-” prompt at the bottom of the screen, you can press the SPACEBAR to see more files.

5. Once you locate the file, write down the name. Press the SPACEBAR until you see the following at the bottom of the screen:

<D>ownload, <P>rotocol, <E>xamine, <N>ew, <L>ist, or <H>elp

Selection or <CR> to exit:

6. To download the file, press D, then follow steps 3-6 in "How to Download Files" above.

Using the File Once It Is Downloaded

You now have your file. If the file has an .EXE extension, run the file by typing its name at the MS-DOS command prompt. The .EXE file will extract its contents and the resulting files are then ready to be installed. Please refer to any text files that have been extracted for exact instructions on using the downloaded file or files.

Troubleshooting Guide to the MSDL

You may encounter one or more of the following problems when using the MSDL:

- Your connection fails.
- Your attempt to download a file results in the message: "Awaiting Start Signal."
- Your attempt to download a file fails.
- Your connection succeeds but everything is displayed on one line.

Procedures for correcting these problems follow, but remember that if for some reason you cannot correct them, you can always receive MSDL files by downloading them from CompuServe®, GENie™, and America Online®, or by calling Microsoft Product Support Services at (206) 454-2030 or Microsoft Consumer Sales at (800) 426-9400.

Your Connection Fails

If you cannot connect to the MSDL, or you have connected but nothing happens, try the following steps in order:

1. Check your communications protocol software and make sure data bits is set to 8, parity to none, and stop bits to 1--(8,N,1).
2. Select a lower baud rate. Doing this will result in slower data transfers, but it may allow you to get the files you need. If you still cannot connect or must use a higher baud rate, try step 3.
3. Disable modem data compression, specifically V.32bis and V.42bis, and try connecting again. There are different types of data compression, so make sure you disable ALL types on your modem.

Data compression is intended to allow higher data transfer rates, but most MSDL files are already compressed. In fact, the transfer rate can be slower if your modem instructs the MSDL-side modem to compress files that are already compressed before sending them.

To disable data compression, you must modify your terminal software Originate string. For example, most Courier modems require the addition of "&K0" to the Originate string. In Windows Terminal, choose Modem Commands from the Settings menu, and modify the Originate string ATQ0V1E1S0=0 to read ATQ0V1E1S0=0&K0. Data compression will be disabled the next time the modem is dialed. If you do not have a Courier modem, see your modem manufacturer's documentation for instructions.

Check your modem manufacturer's documentation to determine exactly how to disable compression for your model. If you disable all compression and still cannot connect to the MSDL, proceed to step 4.

4. Disable error correction. There are different types of error correction, so make sure you disable all levels. To disable error correction for Courier modems, add "&M0" to the terminal software Originate string. If you do not have a Courier modem, see your modem manufacturer's documentation for instructions.
5. If none of these steps corrects the problem, try a different modem. If the connection still fails, access the files by one of the other means available to you.

Your Attempt to Download a File Results in an “Awaiting Start Signal” Message

To correct this problem, you must start the Receive File process in your communications software. For example, in Windows Terminal, choose Receive Binary File from the Transfers menu. The MSDL cannot send data until it receives this signal.

This information is also listed in the MSDL Main menu under Help.

Your Attempt to Download a File Fails

If your download attempt fails, try these procedures:

1. Make sure you have selected the same protocol in your communications software and from the MSDL.
2. Switch to a different protocol.
3. Disable data compression on your modem. (See step 3 under “Your Connection Fails.”)
4. Try a lower baud rate or connect to the MSDL again. This often corrects problems caused by bad phone connections or noisy phone lines.

If the download still fails, access the files by one of the other means available to you. If you need further assistance, call Microsoft Product Support Services at (206) 454-2030.

Your Connection Succeeds but Everything Is Displayed on One Line

After you connect to the MSDL and type your name, you may not be able to read anything because the display is collapsed onto one line.

Usually, this problem is the result of selecting “No Line Feeds” when you log on to the MSDL. There are two ways to correct this problem:

1. Turn on linefeeds or incoming carriage returns in your communications software, then log on again. For example, in Windows Terminal, choose Terminal Preferences from the Settings menu, and select the Inbound check box under CR->CR/LF.
2. Log on again with a new name and select Yes for linefeeds.

Index

Note Index entries with a “W-” indicate the entry can be found in the *Windows for Workgroups Resource Kit for Version 3.1* and are unchanged from Windows for Workgroups 3.1. Index entries not preceded with a “W-” indicate the entry can be found in this *Windows for Workgroups Resource Kit Addendum for Version 3.11*.

- 16-bit network adapter drivers, support for 1-6
- 32bitdiskaccess entry, SYSTEM.INI file 1-19
- 32-bit Disk Access
 - 386 enhanced mode virtual device drivers 1-19
 - components of the system 1-18 to 1-19
 - configuration scenarios 1-30 to 1-33
 - disabled by default 1-13
 - disabling when starting Windows for Workgroups 13-6
 - enabling 1-15
 - hard disk access
 - under MS-DOS 1-16
 - under Windows with 32-bit Disk Access 1-18
 - under Windows without 32-bit Disk Access 1-17
 - overlapped I/O 1-15
 - overview 1-12 to 1-14
 - performance 1-14
- 32-bit disk caching
 - compared with SmartDrive 1-25
 - compressed disk volumes, using with 1-28
 - identifying drives being cached 11-5
 - optimizing 32-bit File Access 11-7
 - overview 1-26 to 1-27
 - role of VCACHE.386, illustrated 1-26
 - SmartDrive, removing or reconfiguring 1-28
 - troubleshooting 13-44
- 32-bit File Access
 - See also* 32-bit disk caching
 - configuration scenarios
 - non-32-bit disk access 1-30
 - non-VFAT mounted volume 1-30
 - VFAT mounted on a compressed non-32-bit Disk Access volume 1-32
 - VFAT mounted on a compressed WDCTRL 32-bit Disk Access volume 1-33
 - VFAT mounted on non-32-bit Disk Access volume 1-31
 - VFAT mounted on WDCTRL 32-bit Disk Access volume 1-31
 - WDCTRL 32-bit Disk Access volume 1-30
 - disabled by default 1-20
- 32-bit File Access (*continued*)
 - disabling when starting Windows 13-6
 - enabling 1-20
 - IFS Manager 1-24
 - optimizing 11-7
 - overview 1-20
 - real-mode mapper 1-22
 - requirements for 1-22
 - troubleshooting
 - 32-bit File Access not available on a drive 13-41
 - cache problems 13-44
 - incompatible disk utilities 13-44
 - slow system 13-44
 - strategy for troubleshooting 13-43
 - symptoms, described 13-42
- 32-bit network adapter drivers, support for 1-8
- 32-bit network cards 11-16
- 386 enhanced mode
 - files loaded by WIN386.EXE 3-15
 - grabber files 3-14
 - network drivers, listed 3-22
 - virtual device drivers 1-19
 - WINOA386.MOD 3-14
- [386enh] section in SYSTEM.INI
 - entries 4-7 to 4-9, W-6-30 to W-6-56
 - installed network adapter device driver W-5-59 to W-5-61
 - installed protocol device driver W-5-60 to W-5-61
 - modified at system installation W-3-12, W-5-39 to W-5-40
 - optimizing MS-DOS-based applications W-9-6
 - page-mapping conflicts W-14-44
 - timer interrupts W-7-21
 - UMB conflict troubleshooting W-14-27 to W-14-29
 - VGA cards requiring additional memory W-14-18
 - virtual device drivers W-2-9 to W-2-11
 - virtual device support files 4-8
 - Virtual Display Device file version W-14-17 to W-14-18
- 386SPART.PAR file, caution against deleting 3-24

A

- Access validation, Windows NT 5-8
- Accessories
 - ClipBook Viewer W-10-6 to W-10-9, W-11-13, W-11-16 to W-11-18
 - Net Watcher W-10-9 to W-10-11
 - WinMeter W-10-12
- Adapters, network *See* Network adapter cards; Network adapter drivers
- adaptrate entry, PROTOCOL.INI file 6-36
- Add/Remove Files dialog box W-3-14
- [Address Book] section in MSMAIL.INI W-6-82
- ADMINCFG.EXE file
 - See also* Administrator Configuration Utility
 - expanding the compressed file 5-10
 - removing 2-7
- Administrative setup (setup /a) 2-6
- Administrator Configuration Utility
 - disabling file sharing for all users 5-15
 - handling exceptions for security settings 5-17
 - removing 2-7
- Advanced dialing feature, Microsoft At Work Fax 10-7
- Advanced Power Management (APM) W-10-13
- Advanced Power Management driver 3-6
- Allow Caching of User-level Passwords setting 5-6
- AlwaysEncrypt entry, EFAXPUMP.INI file 4-32
- AlwaysLogin entry, EFAXPUMP.INI file 4-32
- AlwaysSign entry, EFAXPUMP.INI file 4-32
- ANSI entry, WRKGRP.INI file 2-9
- AnswerMode entry, EFAXPUMP.INI file 4-22
- Applications
 - See also* MS-DOS-based applications; Windows applications
 - 386 enhanced mode W-2-6 to W-2-11, W-2-15 to W-2-19
 - Application Programming Interface (API) W-2-2 to W-2-4
 - common dialog boxes W-10-2 to W-10-4
 - errors W-14-45
 - exclusive mode W-6-31
 - filename extension W-6-26
 - files, listed 3-15
 - font files 3-12
 - function libraries W-2-4 to W-2-5
 - layer
 - IEEE networking model W-1-9
 - OSI networking model W-1-7
 - pathname W-6-19
 - private initialization files W-6-7
 - processing time statistics W-10-12 to W-10-13
 - Program Manager group W-5-72
 - scheduling (appointment) applications W-13-9
- Applications (*continued*)
 - starting
 - automatically W-3-2, W-3-31, W-6-22
 - disabling automatic start W-7-17
 - from Mail W-12-15
 - with document file W-6-10 to W-6-11
 - swap file W-9-5
 - temporary (.TMP) files W-9-3
 - UNC directory searches W-10-4 to W-10-5
 - working directory W-5-73
- Application Programming Interface (API)
 - described W-2-2 to W-2-4
 - messaging interface (MAPI) W-6-15, W-12-13, W-12-26 to W-12-27
 - Network DDE W-11-24
 - Network DDE library W-11-12
 - parameter validation W-14-43
- APPS.INF
 - described W-5-3
 - editing W-5-5
 - information file format W-5-4 to W-5-5
 - sections
 - [dontfind] W-5-42
 - [pif] W-5-43 to W-5-47, W-5-73 to W-5-74
 - list of W-5-42
- Architecture of Windows for Workgroups 3.11
 - 32-bit Disk Access
 - components of the system 1-18 to 1-19
 - enabling 1-15
 - hard disk access scenarios 1-16 to 1-18
 - overlapped I/O 1-15
 - overview 1-12 to 1-14
 - performance 1-14
 - 32-bit File Access
 - bit disk caching 1-25 to 1-29
 - configuration scenarios 1-29 to 1-33
 - enabling 1-20
 - IFS Manager 1-24
 - overview 1-20
 - real-mode mapper 1-22
 - requirements for 1-22
 - boot sequence 1-33 to 1-35
 - differences from previous version, described 1-3
 - driver configuration
 - Windows for Workgroups 3.10 1-36 to 1-37
 - Windows for Workgroups 3.11 1-37 to 1-40
 - enhanced system drivers and utilities 1-47 to 1-48
 - illustrations
 - components of the 32-bit Disk Access system 1-18
 - configuration using NDIS 2.0 drivers 1-6
 - configuration using NDIS 3.0 drivers 1-8
 - disk access under MS-DOS 1-16
 - disk access under Windows with 32-bit Disk Access 1-18

- Architecture of Windows for Workgroups 3.11 (*continued*)
 - illustrations (*continued*)
 - disk access under Windows without 32-bit Disk Access 1-17
 - disk-access scenarios 1-30 to 1-33
 - role of IFS Manager 1-24
 - role of VCACHE.386 1-26
 - network browsing
 - adding computers to the browse list 1-44
 - browse list, described 1-42
 - designating a browse server 1-43
 - how user requests are handled 1-45
 - identifying browse servers 1-45
 - LAN Manager 2.x domains 1-46
 - master and backup browse servers 1-43
 - net view command 1-45
 - overview 1-41
 - removing computers from the browse list 1-44
 - role of the browse server 1-42
 - slow network connections 1-45
 - networking component enhancements
 - alerts and notifications through the Messenger service 1-11
 - network protocols 1-10
 - overview 1-5
 - support for 16-bit network adapter drivers 1-5
 - support for 32-bit network adapter drivers 1-8
 - support for ODI drivers 1-10
 - ARCNet configuration using ODI drivers, illustrated 8-20
 - ARCNet network adapters, NetWare integration using 8-19
 - AreaCode entry, EFAXPUMP.INI file 4-22
 - Artisoft LANtastic 2-6, 9-10
 - At Work Fax *See* Microsoft At Work Fax
 - AUDIT.LOG file 5-20
 - AuditEnabled entry, SYSTEM.INI file 4-10
 - AuditEvents entry, SYSTEM.INI file 4-10
 - Auditing network events
 - using Event Log 5-20 to 5-22
 - using Net Watcher 5-19
 - AuditLog entry, SYSTEM.INI file 4-10
 - AuditLogon entry, SYSTEM.INI file 4-10
 - AUTOEXEC.BAT file
 - driver configuration
 - Windows for Workgroups 3.10 1-37
 - Windows for Workgroups 3.11 1-38
 - editing 4-5
 - EMM386.EXE 11-3
 - ODI configuration for Novell NetWare 8-12
 - sample configurations
 - monolithic IPX configuration 8-34
 - MSIPX configuration 8-37
 - multi-configuration file 2-14
 - ODINSUP configuration 8-43, 8-49
 - Open Datalink configuration 8-31
 - AUTOEXEC.BAT file (*continued*)
 - SET TEMP statement W-14-34
 - SHARE.EXE 11-2, W-2-19
 - SMARTDRV.EXE, removing 1-29
 - troubleshooting with a clean configuration 13-9
 - AutoStart entry, SYSTEM.INI file 4-11
- ## B
- Backup browse server, described 1-43
 - Backup versions of initialization files (.CLN files) 13-6
 - Banner, logon 5-6
 - Banyan VINES
 - installing network support 2-5
 - network support for 2-6, 9-4 to 9-6
 - troubleshooting 13-37 to 13-39
 - Base memory address W-1-29
 - Baseband transmission W-1-17 to W-1-18
 - bcastaddr entry, PROTOCOL.INI file 6-20
 - bindings entry, PROTOCOL.INI file 6-21, 6-37
 - Bitmap files for wallpaper
 - deleting 3-25
 - listed 3-19
 - Blind and low vision users W-D-4
 - BlindDial entry, EFAXPUMP.INI file 4-23
 - Boot sequence 1-33 to 1-35
 - [boot.description] section in SYSTEM.INI W-6-59
 - [boot] section in SYSTEM.INI
 - 386 grabber file version W-14-17 to W-14-18
 - disabling file-handle caching W-7-20
 - entries W-6-57 to W-6-59
 - modified at system installation W-3-11 to W-3-12
 - secondary network added to W-5-60 to W-5-61
 - Windows boot shell W-3-13
 - Booting the system with a clean configuration for troubleshooting 13-9
 - Broadband transmission W-1-17 to W-1-18
 - Browsing network resources
 - adding computers to the browse list 1-44
 - browse list, described 1-42
 - designating a browse server 1-43
 - how user requests are handled 1-45
 - identifying browse servers 1-45
 - LAN Manager 2.x domains 1-46
 - master and backup browse servers 1-43
 - net view command 1-45
 - overview 1-41
 - removing computers from the browse list 1-44
 - role of the browse server 1-42
 - slow network connections 1-45
 - troubleshooting 13-27, 13-32, 13-40
 - bufqelements entry, PROTOCOL.INI file 6-37
 - Bus topology W-1-10 to W-1-11
 - BW-NFS Network File System 2-5, 2-6

C

Cables

- ArcNet network W-1-23
 - connectors W-1-25 to W-1-26
 - Ethernet networks W-1-20
 - specifications W-1-24
 - token-ring network W-1-22 to W-1-23
 - transmission techniques W-1-17 to W-1-18
 - troubleshooting network problems W-14-38, W-14-40
 - types of W-1-13 to W-1-17
- Cache flushing, SmartDrive 5.0 1-47
- Cache, disk *See* Disk caching
- CacheThisPassword entry, SYSTEM.INI file 4-11
- Caching shared CD-ROM drives 11-13, 11-15
- Calendering software. *See* Schedule+
- CasModem entry, EFAXPUMP.INI file 4-31
- CD-ROM drives
- caching by using SmartDrive 11-13, 11-15
 - caching support, described 1-47
 - CD-ROM player W-7-13 to W-7-14, W-14-46 to W-14-47
- Central file server network W-1-37 to W-1-38
- Certified Professional Program, Microsoft A-9
- Chat password 13-33
- CheapTimeEnds entry, EFAXPUMP.INI file 4-28
- CheapTimeStarts entry, EFAXPUMP.INI file 4-28
- Checksum, TCP packets 6-8
- CHKDSK utility 13-18, W-9-4
- Class entry, EFAXPUMP.INI file 4-23
- Class0ModemID entry, EFAXPUMP.INI file 4-23
- class1timeout entry, PROTOCOL.INI file 6-37
- Class2ModemID entry, EFAXPUMP.INI file 4-23
- Clean boot
- defined 13-9
 - what not to include 13-10
- Clipboard
- ClipBook Viewer W-10-6
 - DDE data exchange W-11-4
 - Link clipboard W-11-8
 - metafile support W-10-18
 - Network DDE conversations W-11-13
- ClipBook Server
- described W-10-7
 - Network DDE conversations W-11-16 to W-11-18
 - Network DDE example W-11-18 to W-11-22
- ClipBook Viewer
- maximum pages W-10-6
 - Network DDE
 - conversation interface W-11-13
 - DDE share W-11-16
 - example W-11-18 to W-11-22
 - system component W-11-12
 - pasting Clipboard data W-10-6
 - sharing pages W-10-6 to W-10-9
- [ClipShares] section in SYSTEM.INI W-6-60
- CLIPSRV.EXE 1-35
- .CLN files 13-6, 2-8
- Coaxial cable
- connectors W-1-25 to W-1-26
 - Thicknet network W-1-20, W-1-21 to W-1-22
 - Thinnet network W-1-20 to W-1-21
 - types of W-1-13 to W-1-15
- [colors] section in WIN.INI W-6-7
- CommaDelay entry, EFAXPUMP.INI file 4-23
- commands entry, PROTOCOL.INI file 6-37
- comment entry, SYSTEM.INI file 4-11
- Common configuration block, CONFIG.SYS file 2-12
- Common Dialogs DLL
- described W-10-2
 - NetWare button W-10-3 to W-10-4
 - Network button W-10-3
 - UNC directory searches W-10-4 to W-10-5
- Communications driver file 3-6
- [COMn] section, EFAXPUMP.INI file 4-22 to 4-28
- Compressed disk volumes *See* Disk compression
- CompuServe forums, Microsoft
- information on Windows for Workgroups A-18
 - menu structure A-18
 - Microsoft Connection A-18
 - Microsoft Developer Network A-8
 - Microsoft Knowledge Base, accessing A-12
 - Microsoft TechNet A-7
- ComputerName entry, SYSTEM.INI file 4-11
- Computernames, duplicate 13-26
- CONFIG.SYS file
- buffer statement W-9-3
 - driver configuration
 - Windows for Workgroups 3.10 1-36
 - Windows for Workgroups 3.11 1-37
 - editing 4-5
 - environment space setting W-9-4
 - expanded memory driver entry W-9-2 to W-9-3
 - files statements W-9-3
 - LastDrive entry 8-29
 - memory settings W-14-20
 - MSIPX configuration, upgrading from 8-36
 - multiple system configurations 2-11 to 2-14
 - sample configurations
 - monolithic IPX configuration 8-34
 - ODINSUP configuration 8-43, 8-49
 - Open Datalink configuration 8-31
 - troubleshooting with a clean configuration 13-9
- CONFIG.WIN file 2-12
- Configurable peer networking 5-2 to 5-4
- Configuration files *See* Initialization files
- Configuring Windows for Workgroups *See* Optimizing Windows for Workgroups; Setting up Windows for Workgroups
- CONNECT.DAT file 1-35

- Connect Network Drive dialog box W-10-3
 - Connection problems
 - duplicate computernames 13-26
 - how to troubleshoot 13-17
 - identifying 13-7
 - shared resources 13-26
 - troubleshooting techniques 13-18 to 13-26
 - Connections to servers, auditing 5-21
 - Consulting Services, Microsoft A-10
 - Control Panel
 - 32-bit Disk Access, enabling 1-15
 - 32-bit File Access, enabling 1-21
 - customizing Windows for Workgroups W-3-5
 - information file *See* CONTROL.INF W-5-3
 - Network icon
 - Change Password button W-8-12
 - computer name W-1-35
 - maintaining settings W-3-31
 - workstation optimization W-9-16 to W-9-17
 - current printer driver W-14-34
 - CONTROL.INF
 - described W-5-48
 - editing W-5-5
 - information file format W-5-4 to W-5-5
 - removing drivers from W-5-69 to W-5-70
 - sections W-5-48 to W-5-49
 - CONTROL.INI
 - editing W-6-3 to W-6-4
 - sections W-6-79
 - source file W-6-5
 - Copying files to a network share W-7-17 to W-7-19
 - CopyQualityCheckLevel entry, EFAXPUMP.INI file 4-23
 - Core files 3-3
 - CountryCode entry, EFAXPUMP.INI file 4-23
 - Currency defaults W-6-11 to W-6-14
 - [Custom Commands] section
 - MSMAIL.INI W-6-82 to W-6-83, W-12-15 to W-6-16
 - SHARED.INI W-6-94, W-12-16 to W-12-19
 - Custom message types
 - customizing Mail with W-12-13
 - described W-12-19 to W-12-21
 - help request sample W-12-23 to W-12-25
 - installing in Mail W-12-21 to W-12-23
 - maximum number installed W-12-20
 - Schedule+ W-12-21, W-13-7 to W-13-9
 - Schedule+ initialization file W-13-3
 - [Custom Messages] section
 - MSMAIL.INI
 - initialization file entries W-6-83 to W-6-84
 - installing custom messages W-12-21
 - Schedule+ predefined message types W-13-7
 - SHARED.INI
 - initialization file description W-6-94
 - installing custom messages W-12-22
 - installing help request forms W-12-25
 - Custom Separator File W-10-18 to W-10-20
 - Customer support *See* Product Support Services; Resource directory
- ## D
- Data frame W-1-5 to W-1-6, W-1-7
 - Data Link Control *See* Microsoft DLC protocol
 - Date defaults W-6-11 to W-6-14
 - [DDEShares] section in SYSTEM.INI W-6-60, W-11-14
 - DDE *See* Dynamic data exchange; Network DDE
 - Deaf and hard-of-hearing, text telephone service A-3, W-D-2
 - DEC Etherworks Turbo/TP network adapter 8-33, 8-37
 - DEC PATHWORKS 2-6, 9-6
 - Default gateway
 - defined 6-9
 - specifying 6-14
 - DefaultFax entry, EFAXPUMP.INI file 4-31
 - defaultgateway0 entry, PROTOCOL.INI file 6-21
 - DeferBrowsing entry, SYSTEM.INI file 4-12
 - Deleting Windows for Workgroups files 3-24 to 3-25
 - DeliveryFormat entry, EFAXPUMP.INI file 4-28
 - denysaps entry, PROTOCOL.INI file 6-37
 - Desktop configuration W-14-11
 - [desktop] section in WIN.INI W-6-8 to W-6-9
 - DevDir entry, SYSTEM.INI file 1-39, 4-18
 - Developer Network, Microsoft
 - described A-7
 - Developer Network CD A-7
 - enrollment information A-8
 - forum on CompuServe A-8
 - newspaper A-8
 - Developer Services Team, Microsoft A-8
 - Developers Knowledge Base, Microsoft A-11
 - Device drivers *See* Drivers
 - Dialog boxes
 - Add/Remove Files W-3-14
 - Common Dialogs DLL W-10-2 to W-10-5
 - Compatible Networks W-8-4 to W-8-5, W-8-13
 - Connect Network Drive W-10-3
 - File Open W-7-17, W-10-2, W-10-4 to W-10-5
 - File Save As W-7-17 to W-7-19, W-10-2
 - NetWare button W-10-3 to W-10-4
 - Network button W-10-3
 - Network Settings W-7-14 to W-7-15, W-9-17 to W-9-18
 - Paste W-10-6
 - Separator Pages W-10-15 to W-10-17
 - Share Clipbook Page W-10-7
 - Diagnostics tool (MSD) 13-4, 13-7
 - Digitally signed faxes, sending 10-16
 - Direct hosting and IPX 1-11
 - DirectHosting entry, SYSTEM.INI file 4-12
 - Disable File Sharing setting 5-3
 - Disable Network DDE Sharing setting 5-4
 - Disable Password Caching setting 5-5

- Disable Print Sharing setting 5-4
 - DisableECM entry, EFAXPUMP.INI file 4-24
 - DisableVFATWarning entry, SYSTEM.INI file 4-7
 - Disk access *See* 32-bit Disk Access
 - Disk caching, 32-bit
 - compared with SmartDrive 1-25
 - compressed disk volumes, using with 1-28
 - identifying drives being cached 11-5
 - illustration of the role of VCACHE.386 1-26
 - optimizing 32-bit File Access 11-7
 - overview of 1-26 to 1-27
 - SmartDrive, removing or reconfiguring 1-28
 - troubleshooting 13-44
 - Disk compression
 - disk caching, using with 1-28
 - forcing lazy writing on compressed disk volumes 1-28
 - virtual memory, using with W-9-16
 - utilities, caution against removing 13-9
 - VFAT support 1-24
 - Disk partitioners, caution against removing 13-9
 - Disk space
 - administrative setup of Windows for Workgroups 2-7
 - freeing by deleting files 3-24 to 3-25
 - Mail postoffice W-12-38
 - shared copy setup of Windows for Workgroups 2-8
 - Display driver
 - files, listed 3-6
 - incompatible adapter chip W-14-11
 - troubleshooting display problems W-14-15 to W-14-20
 - troubleshooting fonts W-14-32 to W-14-33
 - Display fonts
 - loaded at startup W-6-14
 - MS-DOS-based application W-6-32
 - DLC *See* Microsoft DLC protocol
 - DLL (dynamic link library)
 - Common Dialogs DLL W-10-2 to W-10-5
 - described W-2-4 to W-2-5
 - language libraries
 - Mail custom commands W-12-14 to W-12-15
 - Windows 3.1 extensions W-2-2 to W-2-4, W-2-3
 - DMA (direct memory access) W-6-36, W-6-39
 - [dnr] section, TCPUTILS.INI file 6-24
 - DNS domains 6-16
 - domain entry, TCPUTILS.INI file 6-25
 - Domains
 - DNS domains 6-16
 - LAN Manager 2.x 1-46
 - security in a Windows NT environment 7-4
 - DOS *See* MS-DOS
 - DOS client files for Novell NetWare 8-5
 - DOSUP7.EXE 8-5, 8-6
 - DoubleSpace drives, mounting VFAT.386 1-24
 - Download Service, Microsoft (MSDL)
 - connecting to A-24
 - downloading files A-25
 - Download Service, Microsoft (MSDL) (*continued*)
 - connecting to A-24
 - overview A-24
 - searching for files A-25
 - troubleshooting A-28 to A-29
 - using downloaded files A-27
 - Drake Training and Technologies A-9
 - Driver Library, Windows A-20 to A-23
 - drivename entry
 - PROTOCOL.INI file 6-21, 6-37
 - TCPUTILS.INI file 6-24, 6-25
 - Drivers
 - 16-bit network adapter drivers 1-5
 - 32-bit network adapter drivers 1-7
 - 386 enhanced mode virtual device drivers 1-19
 - binding to Protocol Manager 1-40
 - boot sequence, described 1-34
 - caution against removing certain drivers 13-9
 - files, listed
 - Advanced Power Management driver 3-6
 - communications driver 3-6
 - display drivers 3-6
 - enhanced mode network drivers 3-22
 - keyboard drivers 3-5
 - mouse drivers 3-6
 - MS-DOS drivers 3-13
 - multimedia drivers 3-9
 - network drivers 3-20
 - printer drivers 3-7
 - system driver 3-5
 - IPX.COM 8-10
 - IPXODI.COM and LSL.COM 8-10
 - NDIS 2.0
 - described 1-6
 - listed 3-21
 - NDIS 3.0
 - described 1-8
 - listed 3-23
 - network transport protocol drivers 3-22
 - NDIS2SUP.386 1-7
 - NetBEUI.386 1-9
 - Novell drivers
 - listed 8-6, 8-7
 - monolithic IPX configuration 8-19
 - ODI IPX configuration 8-15
 - ODI drivers *See* Open Datalink Interface (ODI) 8-39
 - RMM.D32 (real-mode mapper) 1-23
 - SmartDrive 5.0, described 1-47 to 1-48
 - third-party network drivers, loading 1-40
 - WDCTRL 1-12 to 1-14
 - Windows for Workgroups 3.10 configuration 1-36 to 1-37
 - Windows for Workgroups 3.11 configuration 1-37 to 1-40
- [drivers] section in SYSTEM.INI W-6-60

Dynamic binding W-2-5
 Dynamic data exchange (DDE)
 application W-11-7
 client application W-11-6
 Clipboard transfers W-11-4
 conversation W-11-3, W-11-6 to W-11-8
 data hierarchy W-11-6 to W-11-7
 data item W-11-7
 data links W-11-8
 DDE Management Library W-11-3 to W-11-4
 described W-11-3
 example uses W-11-6 to W-11-7
 global atom/shared-memory handle W-11-4
 messages W-11-3 to W-11-4, W-11-8 to W-11-10
 networks. *See* Network DDE
 OLE comparison W-11-10 to W-11-11
 server application W-11-6 to W-11-7
 server name service W-11-3
 topic W-11-7
 transferring Mail messages W-12-15 to W-12-16
 Windows messages W-11-4
 Dynamic link library *See* DLL
 Duplicate computernames, troubleshooting 13-26

E

Edit MSMAIL.INI command W-12-15
 [EFAX Transport] section, MSMAIL.INI file 4-21
 [EFAXPump] section, EFAXPUMP.INI file 4-28
 EFAXPUMP.INI file
 [COMn] section 4-22 to 4-28
 editing 4-4 to 4-5
 [EFAXPump] section 4-28
 format of 4-3
 [Message] section 4-28 to 4-30
 [Modem] section 4-31
 [Network] section 4-31
 overview 4-2, 4-22
 [security] section 4-32
 [embedding] section in WIN.INI W-6-10
 EMM386.EXE
 configuration guidelines 11-3
 optimizing configuration W-9-8, W-9-11
 Empty Wastebasket Mail command W-12-18 to W-12-19
 Empty server browse list, troubleshooting 13-32
 Environment space W-9-3
 EnableSharing entry, SYSTEM.INI file 4-12
 EnableSharingPopUps entry, SYSTEM.INI file 4-8
 EnableV17Recv entry, EFAXPUMP.INI file 4-24
 EnableV17Send entry, EFAXPUMP.INI file 4-24
 Encrypted security file (WFWSYS.CFG)
 creating 5-11
 described 5-3
 installing 5-12
 password protecting 5-11

Enhanced-mode-only video drivers, troubleshooting 13-13
 Ethernet
 cabling connectors W-1-25 to W-1-26
 described W-1-19 to W-1-20
 specifications W-1-24
 Thicknet W-1-21
 Thinnet W-1-20
 troubleshooting W-14-40
 twisted-pair W-1-22
 EVEN_PACKETS entry, PROTOCOL.INI file 6-6
 Event Log, auditing network events 5-20 to 5-22
 Exclude entry, SYSTEM.INI file 4-12
 Exclusive mode, running MS-DOS-based applications in
 W-7-20 to W-7-21
 ExitCommand entry, EFAXPUMP.INI file 4-24
 Expanded memory
 386 enhanced mode settings W-6-30 to W-6-56
 allocating UMBs W-9-8 to W-9-16
 expansion board configuration W-9-2 to W-9-3
 optimizing EMM386.EXE W-9-11 to W-9-13
 troubleshooting
 EMM386 adapter conflict W-14-23
 invalid path W-14-23
 out-of-memory message W-14-24
 Extended lowercase characters in passwords 13-32
 Extended memory
 386 enhanced mode W-2-7
 adding W-14-26
 expansion board configuration W-9-2 to W-9-3
 HIMEM.SYS driver W-2-5 to W-2-6
 memory manager for setup W-3-13
 RAM drive size W-14-25, W-14-27
 RAMDrive W-9-3
 SMARTDrive W-3-16
 Extensions for Windows for Workgroups
 Mail extensions W-12-29 to W-12-35
 Schedule+ extensions W-13-17
 [extensions] section in WIN.INI W-6-10 to W-6-11

F

FastDisk *See* 32-bit Disk Access
 FastTips for Windows for Workgroups A-2
 Fax boards, sharing 10-3
 Fax modems
 changing your fax modem number 10-8
 sharing over the network 10-5 to 10-7
 Fax security *See* Microsoft At Work Fax
 Fax software *See* Microsoft At Work Fax
 File Manager
 Connect dialog W-7-8
 described W-10-14
 file sharing interface W-7-4 to W-7-5
 Mail user interface W-12-27

File Manager (*continued*)

- MRU network drive connections W-10-15 to W-10-17
- network connections W-2-17, W-8-22
- toolbar W-10-14
- UNC redirection W-7-17 to W-7-19
- WINFILE.INI entries W-6-80 to W-6-81

File Open dialog box

- accessing shared resources W-10-2 to W-10-4
- UNC directory searches W-10-4 to W-10-5
- UNC redirection W-7-17 to W-7-19

File Save As dialog box W-7-17 to W-7-19, W-10-2, W-10-4 to W-10-5

File sharing

- Disable File Sharing setting 5-3
- disabling for a protected mode server 11-8
- disabling for all users 5-15

File-handle caching W-7-20

Files

- application files 3-15
- bitmap files for wallpaper 3-19
- core files 3-3
- deleting Windows for Workgroups files 3-24 to 3-25
- DOSUP7.EXE files, listed 8-6
- driver files
 - Advanced Power Management driver 3-6
 - communications driver 3-6
 - display drivers 3-6
 - keyboard drivers 3-5
 - mouse drivers 3-6
 - multimedia drivers 3-9
 - overview 3-4
 - printer drivers 3-7
 - system driver 3-5
- font files
 - MS-DOS-based applications 3-12
 - raster fonts 3-11
 - system fonts 3-10
 - TrueType fonts 3-11
 - vector fonts 3-11
- games files 3-16
- hardware support files 3-19
- installed on local workstation by Setup 2-8
- international support files 3-13
- Mail files 3-17
- Microsoft At Work Fax files 3-18
- MS-DOS support files
 - files for 386 enhanced mode 3-15
 - MS-DOS drivers 3-13
 - WinOldAp and Grabber files 3-14
- NetWare support files for Windows 8-4
- NetWare workstation configuration files 8-21
- network files used for Microsoft Windows Network
 - enhanced mode network drivers 3-22
 - NDIS 2.0 network adapter drivers 3-21
 - NDIS 3.0 network adapter drivers 3-23

Files (*continued*)

- network files (*continued*)
 - NDIS 3.0 network transport protocol drivers 3-22
 - network driver files 3-20
 - real mode network support files 3-21
 - Remote Access Service client files 3-23
- Novell drivers 8-6, 8-7
- Novell Files forum 8-5
- README files 3-19
- Schedule+ files 3-18
- screensaver files 3-19
- Setup-related files 3-3
- VLMUP1.EXE files, listed 8-8
- wave-form sound files 3-19
- WIN.COM 3-2
- WINUP7.EXE files, listed 8-7
- FileSharing entry, SYSTEM.INI file 4-13
- FixModemClass entry, EFAXPUMP.INI file 4-24
- FixSerialSpeed entry, EFAXPUMP.INI file 4-24
- Font files
 - boot sequence, described 1-35
 - fixed-font files 3-10
 - MS-DOS-based applications 3-12
 - raster fonts 3-11
 - system fonts 3-10
 - TrueType fonts 3-11
 - vector fonts 3-11
- [fonts] section in WIN.INI W-6-14
- [FontSubstitutes] section in WIN.INI W-6-15
- Frame postamble W-1-7
- Frame preamble W-1-7
- Force Alphanumeric Passwords setting 5-6
- ForceLazyOff entry, SYSTEM.INI file 4-21
- ForceLazyOn entry, SYSTEM.INI file 1-28, 4-20
- Forums on CompuServe *See* Microsoft forums on CompuServe
- FRAME entry, PROTOCOL.INI file 6-6
- Frame formats 6-5

G

Games

- deleting to free disk space 3-25
- files 3-16
- Hearts W-6-11, W-10-14
- Gateway, default for TCP/IP
 - defined 6-9
 - specifying 6-14
- Gateways, Mail W-12-30 to W-12-31, W-B-17, W-B-24 to W-B-48
- GDI (Graphics Device Interface)
 - 386 enhanced mode W-2-7
 - described W-2-3
 - GDI.EXE 1-35, 3-3
 - metafile W-10-18 to W-10-20

General Protection (GP) faults W-14-42 to W-14-45
 Ghosted connections
 enabling 11-10
 troubleshooting 13-39
 Global atom W-11-4
 Global shared-memory handle W-11-4
 Grabber files 3-14
 Graphics Device Interface. *See* GDI
 Group accounts, described 7-5
 Guest accounts, described 7-5

H

HangupDelay entry, EFAXPUMP.INI file 4-24
 Hard disk
 disk space requirements
 administrative setup 2-7
 Mail postoffice W-12-38
 shared copy setup 2-8
 drivers, caution against removing 13-9
 fragmented W-9-4
 freeing disk space
 archiving server calendar data W-13-6
 deleting application files W-9-4
 deleting swap files W-9-4 to W-9-5
 disk compression software W-9-16
 minimizing necessary files 3-24 to 3-25
 RAMDrive W-9-2, W-9-8
 swap file W-9-8
 interleave W-9-2
 Hard-of-hearing, text telephone service for A-3
 Hardware support files, listed 3-19
 Hearing impaired, text telephone service A-3
 Hearts game W-6-11, W-10-14
 [Hearts] section in WIN.INI W-6-11
 Help files, deleting 3-25
 Help on network card settings 13-11
 Help Request Mail command W-12-23 to W-12-25
 Help window WIN.INI entries W-6-27 to W-6-28
 High memory area (HMA), MS-DOS in W-9-8 to W-9-9
 HighestSendSpeed entry, EFAXPUMP.INI file 4-25
 HIMEM.SYS driver W-2-5 to W-2-6, W-2-7, W-9-3, W-9-14
 Host ID, defined 6-9
 host name entry, TCPUTILS.INI file 6-26
 Hosting, defined 1-11

I

I/O port base addresses, assigning 13-12
 I/O system W-1-28, W-2-3
 IBM OS/2 LAN Server 2-6
 IBM Token Ring 16/4 network adapter 8-33, 8-34
 IEEE 802 networking model W-1-8

IFS Manager (IFSMGR.386)
 boot sequence 1-34
 described 1-24
 IFSHLP.SYS file 1-37
 IFSMGR.386 (IFS Manager)
 boot sequence 1-34
 described 1-24
 ImageQuality entry, EFAXPUMP.INI file 4-29
 IncludeCover entry, EFAXPUMP.INI file 4-29
 .INI files *See* Initialization files
 Initialization files
 See also EFAXPUMP.INI file; MSMAIL.INI file;
 PROTOCOL.INI file; SCHDPLUS.INI file;
 SYSTEM.INI file; WIN.INI file; WRKGRP.INI file
 backup versions of (.CLN files) 13-6
 editing 4-4 to 4-5
 format of 4-3
 last known clean files 2-8
 overview 4-2
 .SRC files, editing 4-6
 Installation *See* Setting up Windows for Workgroups
 Installation information (.INF) files
 See also individual filename
 APPS.INF W-5-42 to W-5-47
 CONTROL.INF W-5-48 to W-5-49
 custom installations W-5-69 to W-5-74
 editing W-5-5, W-6-3 to W-6-4
 file descriptions W-5-3 to W-5-4
 format W-5-4 to W-5-5, W-6-2 to W-6-3
 list of W-6-2
 NETWORK.INF W-5-50 to W-5-63
 OEMSETUP.INF W-5-64 to W-5-68
 SETUP.INF
 sections W-5-8 to W-5-41
 specifying pathname W-3-4
 source files W-6-5
 Institute of Electrical and Electronic Engineers *See* IEEE
 Integrated services digital network (ISDN) 7-13
 Interchange scheduling file format W-13-10 to W-13-17
 Interleave, hard disk W-9-2
 InterLink utility 2-19
 Internal-stack-overflow error W-14-29
 International characters in the Windows NT share
 name 13-32
 International support files, listed 3-13
 InternationalPrefix entry, EFAXPUMP.INI file 4-25
 Interrupt
 COM W-6-33
 conflicts W-14-37
 IRQ settings for network adapters 13-11
 keyboard W-6-31
 request lines W-1-27
 timer W-7-21
 virtual devices W-2-8

[intl] section in WIN.INI W-6-11 to W-6-14
IOS.386 1-34
IP address
 overview of 6-9
 specifying 6-14
IP protocol
 See also TCP/IP protocol
 overview of 6-8
ipackets entry, PROTOCOL.INI file 6-37
ipaddress0 entry, PROTOCOL.INI file 6-21
IPX applications, trouble running 13-36
IPX.COM 8-10, 8-16
IPX/SPX compatible transport
 See also NWLink protocol
 installing 6-5, 8-28 to 8-29
IPXODI.COM 8-10, 8-12
IRQ *See* Interrupt
ISDN *See* Integrated services digital network

K

KeepConn entry, SYSTEM.INI file 4-13
Key encryption for faxes
 described 10-10
 sending key-encrypted faxes 10-16
Keyboard driver files, listed 3-5
[keyboard] section in SYSTEM.INI W-3-12, W-6-61 to W-6-62
Knowledge Base, Microsoft
 accessing on CompuServe A-12
 overview A-11
 searching for articles A-13 to A-15
 searching with Expert mode A-16 to A-17
 software library A-12, A-15
KRNL386.EXE 1-34, 3-3

L

LAN
 ArcNet network W-1-23
 cabling media W-1-13 to W-1-17
 compatible with Windows for Workgroups W-8-3 to W-8-4
 data transmission through cables W-1-17 to W-1-18
 dual-net environment W-1-33 to W-1-34
 Ethernet W-1-19 to W-1-22
 network adapter cards W-1-25 to W-1-29
 protocols W-1-31 to W-1-34
 security W-1-39
 specifications W-1-24
 token ring W-1-22 to W-1-23
 topologies W-1-10 to W-1-13

LAN Manager
 integrating Windows for Workgroups with 9-4
 troubleshooting 13-31 to 13-33
LAN Manager 2.x domains 1-46
LAN Manager Messenger service 1-11
LANA numbers
 defined W-7-9 to W-7-10
 in SYSTEM.INI file 1-45
lanas# entry, PROTOCOL.INI file 6-35
lanabase entry
 PROTOCOL.INI file 6-21
 SYSTEM.INI file 4-20
LANAs entry, SYSTEM.INI file 4-13
Language libraries
 listed 3-13
 SYSTEM.INF entries W-5-41
 WIN.INI entry W-6-13
Laptop computer, using to set up Windows for Workgroups on local workstations 2-19
Last known clean configuration files 2-8
LastDrive parameter, CONFIG.SYS file 8-29
LastLogoFile1 entry, EFAXPUMP.INI file 4-29
LastLogoFile2 entry, EFAXPUMP.INI file 4-29
LastLogoFile3 entry, EFAXPUMP.INI file 4-29
LastLogoFile4 entry, EFAXPUMP.INI file 4-29
LastLogoFile5 entry, EFAXPUMP.INI file 4-30
Layers, in networking models
 IEEE W-802 networking model W-1-8 to W-1-10
 OSI networking model W-1-3 to W-1-8
Lazy writing
 defined 1-27
 forcing on compressed disk volumes 1-28
Link Driver section, NET.CFG file 8-24
Listing network resources *See* Browsing network resources
LMAnnounce entry, SYSTEM.INI file 1-46, 4-13
LMLogon entry, SYSTEM.INI file 4-14
load entry, PROTOCOL.INI file 6-37
LoadHigh entry, SYSTEM.INI file 4-14, W-9-9, W-9-15, W-14-21
LoadNetDDE entry, SYSTEM.INI file 4-14
LoadRMDrivers entry, SYSTEM.INI file 1-39, 4-19
Local area network *See* LAN
LocalFax entry, MSMAIL.INI file 4-21
LocalNumber entry, EFAXPUMP.INI file 4-25
LocalPrefix entry, EFAXPUMP.INI file 4-25
Log entry, EFAXPUMP.INI file 4-25
Logging network events 5-20 to 5-22
Logging on to NetWare servers before starting Windows 8-31
LogoFile entry, EFAXPUMP.INI file 4-30
Logon
 banner 5-6
 settings for logon restrictions 5-9
 troubleshooting 13-31

Logon Password Expiration setting 5-6
 Logon validation, Windows NT 5-8
 LogonDisconnected entry, SYSTEM.INI file 4-14
 LogonDomain entry, SYSTEM.INI file 4-15
 LogonValidated entry, SYSTEM.INI file 4-15
 LongDistancePrefix entry, EFAXPUMP.INI file 4-25
 looppackets entry, PROTOCOL.INI file 6-38
 Lowercase extended characters in passwords 13-32
 LowestSendSpeed entry, EFAXPUMP.INI file 4-25
 LPT ports W-7-20
 LSL.COM driver 8-10

M

Macintosh as a Mail client W-12-32
 Mail
 files, listed 3-17
 Microsoft At Work Fax, integrating with 10-3
 removing from Windows for Workgroups Setup 2-15
 Mail application
 client workstation
 Edit MSMAIL.INI command W-12-15 to W-12-16
 installing commands W-12-15
 installing custom message types W-12-21 to W-12-22
 View Schedule button W-13-3
 compared to Microsoft Mail W-12-28
 connectivity enhancements
 Extensions for Windows for Workgroups W-12-29 to W-12-35
 FAX Gateway W-B-17
 Wide Area Network W-B-23, W-B-26
 X.400 Gateway W-B-28 to W-B-32
 PROFS W-B-34 to W-B-39
 custom commands W-12-14 to W-12-19
 customization options W-12-13
 described W-12-3
 disk space W-12-38
 Help Request command W-12-23 to W-12-25
 mail server W-12-3
 mail session manager W-12-12
 messages
 address book W-12-5
 attachments W-12-4 to W-12-5, W-12-38 to W-12-39
 composing offline W-12-7 to W-12-8
 custom message types W-12-19 to W-12-22
 deleted W-12-39
 embedded objects W-12-4 to W-12-5
 exporting W-12-8
 folders W-12-6 to W-12-7
 forms W-12-4, W-12-23 to W-12-25, W-13-7 to W-13-9
 local outbox W-12-8
 notification W-12-12 to W-12-13
 Mail application (*continued*)
 messages (*continued*)
 packaged object W-12-37 to W-12-38
 Schedule+ W-13-7 to W-13-9
 searching for W-12-6 to W-12-7, W-12-39
 sending with Send Mail W-12-27
 text editor W-12-4
 names service W-12-12 to W-12-13
 notification engine W-12-12
 postoffice
 administrator W-12-10, W-12-36 to W-12-37
 custom commands W-12-15 to W-12-18
 custom message types W-12-22 to W-12-23
 described W-12-3
 directory structure W-12-8 to W-12-9
 disk space W-12-38
 Empty Wastebasket command W-12-18 to W-12-19
 Help Request form W-12-23 to W-12-25
 mail server W-12-3
 pathname in MSMAIL.INI W-12-36, W-12-39
 session manager W-12-12
 shared folders W-12-6
 SHARED.INI file W-12-16
 reinitializing W-12-36
 resource accounts W-13-6 to W-13-7
 Schedule+
 messaging W-13-2
 starting from Mail W-13-3
 user accounts W-13-6 to W-13-7
 spooler W-12-11
 starting an application from W-12-15
 system modules W-12-11
 transport W-12-11
 MAIL.WRI file 1-2
 [Mail] section in WIN.INI W-6-15
 MaintainServerList entry, SYSTEM.INI file 1-44, 4-15
 MAPI *See* Messaging Application Program Interface
 Master browse server, described 1-43
 MAX_CONNECTIONS entry, PROTOCOL.INI file 6-6
 MAX_SOCKETS entry, PROTOCOL.INI file 6-6
 maxgroup entry, PROTOCOL.INI file 6-38
 maxin entry, PROTOCOL.INI file 6-38
 maxmember entry, PROTOCOL.INI file 6-38
 maxout entry, PROTOCOL.INI file 6-38
 MaxRetries entry, EFAXPUMP.INI file 4-28
 maxsendsize entry, TCPUTILS.INI file 6-24
 [mci extensions] section in WIN.INI W-6-16
 [mci] section in SYSTEM.INI W-6-62
 MCP Program certificate, obtaining A-9
 Memory buffer addresses, assigning 13-13
 Memory managers, configuration guidelines 11-3
 Memory used by SmartDrive, reducing 11-6
 [menu] keyword section, CONFIG.SYS file 2-11
 [Message] section, EFAXPUMP.INI file 4-28 to 4-30

- Messaging Application Program Interface (MAPI)
 - customizing Mail with W-12-13
 - described W-12-26
 - detecting on a workstation W-6-15
 - functions W-12-27
- Messenger service, LAN Manager 1-11
- Metafile W-10-18 to W-10-20
- Microsoft At Work Fax
 - advanced dialing feature 10-7
 - changing your fax modem number 10-8
 - files, listed 3-18
 - overview 10-2 to 10-5
 - Personal Address Book, entering fax numbers in 10-9
 - prefixes, adding 10-8
 - removing from Windows for Workgroups Setup 2-15
 - security
 - disabling 10-11
 - enabling 10-12
 - establishing 10-10
 - key encryption 10-10
 - overview 10-10
 - password, changing 10-12
 - personal keys, changing 10-12
 - personal keys, managing 10-13
 - private keys, exporting and importing 10-14
 - public keys, exporting and importing 10-14
 - public keys, typing 10-15
 - reading secured faxes 10-16
 - sending digitally signed faxes 10-16
 - sending key-encrypted faxes 10-16
 - sending password-encrypted faxes 10-16
 - signed keys, using 10-13
 - sharing fax modems over the network 10-5 to 10-7
 - troubleshooting 13-46 to 13-48
- Microsoft CD-ROM Extensions 12-3, W-7-13 to W-7-14
- Microsoft Certified Professional Program A-9
- Microsoft Connection, forums on CompuServe A-18
- Microsoft Consulting Services A-10
- Microsoft Developer Network
 - described A-7
 - Developer Network CD A-7
 - enrollment information A-8
 - forum on CompuServe A-8
 - newspaper A-8
- Microsoft Developer Services Team A-8
- Microsoft Developers Knowledge Base A-11
- Microsoft Diagnostics (MSD) tool 13-4, 13-7
- Microsoft DLC protocol
 - configuring 6-30 to 6-31
 - installing 6-27 to 6-30
 - overview 6-26 to 6-27
 - parameters 6-32 to 6-34
 - PROTOCOL.INI parameters 6-34 to 6-43
- Microsoft Download Service (MSDL)
 - connecting to A-24
 - downloading files A-25
 - overview A-24
 - searching for files A-25
 - troubleshooting A-28 to A-29
 - using downloaded files A-27
- Microsoft Draw W-10-18
- Microsoft Excel for Windows W-11-18, W-11-23, W-12-27
- Microsoft FastTips for Windows for Workgroups A-2
- Microsoft forums on CompuServe
 - information on Windows for Workgroups A-18
 - menu structure A-18
 - Microsoft Connection A-18
- Microsoft Inside Sales A-3
- Microsoft Knowledge Base
 - accessing on CompuServe A-12
 - overview A-11
 - searching for articles A-13 to A-15
 - searching with Expert mode A-16 to A-17
 - software library A-12, A-15
- Microsoft LAN Manager *See* LAN Manager
- Microsoft Mail
 - See also* Mail; Mail application
 - Add Paks W-12-35
 - connectivity map W-B-10 to W-B-12
 - configuring W-B-1 to W-B-50
 - File Format API (FFAPI) W-13-9 to W-13-10
 - gateways W-12-30 to W-12-31
 - Microsoft Mail for PC LANs W-12-28
 - Remote Workstation software W-7-11
 - [Microsoft Mail] section in MSMAIL.INI W-6-85 to W-6-91, W-12-16, W-12-25, W-12-36
- Microsoft Product Support Services
 - See also* Resource directory
 - support from Microsoft PSS engineers A-2
 - [Microsoft Schedule] sections in SCHDPLUS.INI W-6-95 to W-6-100
- Microsoft Solution Providers A-2, A-9
- Microsoft Solutions Channel A-3
- Microsoft TechNet
 - forum on CompuServe A-7
 - monthly CD A-4
 - ordering A-7
 - overview A-4
 - WinCIM A-7
- Microsoft Windows Network
 - files
 - enhanced mode network drivers 3-22
 - NDIS 2.0 network adapter drivers 3-21
 - NDIS 3.0 network adapter drivers 3-23
 - NDIS 3.0 network transport protocol drivers 3-22
 - network drivers 3-20
 - real mode network support files 3-21
 - Remote Access Service client files 3-23

- Microsoft Windows Network (*continued*)
 installing support for 2-4
 using Windows for Workgroups as a client only 11-9
- Microsoft Word for Windows W-11-23, W-12-27
- MinFileCache entry, SYSTEM.INI file 4-20
- Minimum Password Length setting 5-6
- MinutesBetweenRetries entry, EFAXPUMP.INI file 4-30
- [MMF] section in MSMAIL.INI W-6-92 to W-6-93
- [Modem] section, EFAXPUMP.INI file 4-31
- MODEM.INF file 7-8
- ModemFaxClasses entry, EFAXPUMP.INI file 4-25
- ModemID entry, EFAXPUMP.INI file 4-26
- ModemIDCmd entry, EFAXPUMP.INI file 4-26
- ModemRecvSpeeds entry, EFAXPUMP.INI file 4-26
- Modems
See also NULL modem
 compatibility and speed 7-10
 sharing fax modems over the network 10-5 to 10-7
 troubleshooting
 shared fax modems 13-47
 supported modems 7-8
 unsupported modems
 configuring 7-9
 industry standards for modems 7-9
 testing compatibility of 7-9
 testing with Terminal 7-10
- ModemSendSpeeds entry, EFAXPUMP.INI file 4-26
- Monitoring network events
 using Event Log 5-20 to 5-22
 using Net Watcher 5-19
- Monolithic protocol stack W-1-31
- Monolithic IPX configuration
 default configuration 8-18
 driver versions 8-19
 overview 8-16
 sample configuration files 8-34
 testing the network before installing Windows for Workgroups 8-17
- Most recently used (MRU) connections
 file W-10-15 to W-10-17
 printer W-10-21
 stored in WIN.INI W-6-16
- Mouse driver files, listed 3-6
- Moving files to a network share W-7-17 to W-7-19
- [MRU_Files] section in WIN.INI W-6-16, W-10-15 to W-10-17
- [MRU_Printers] section in WIN.INI W-6-16, W-10-21
- MS-DOS
 applications *See MS-DOS-based applications*
 configuration troubleshooting W-14-20 to W-14-24
 device drivers W-2-9
 InterLink utility 2-19
 OEM versions W-14-44
- MS-DOS (*continued*)
 version W-2-19, W-3-9, W-9-3
 Windows for Workgroups support files 3-13 to 3-15
 workstation *See* Workgroup Connection for DOS
- MS-DOS-based applications
 386 enhanced mode W-2-6 to W-2-11, W-2-16 to W-2-17
 exclusive mode W-7-20 to W-7-21
 font files 3-12
 multitasking support W-2-9
 network processing time statistics W-10-12 to W-10-13
 optimizing performance W-9-6
 out-of-memory message W-14-24
 PIFs W-5-43 to W-5-47, W-7-17 to W-7-19
 scheduling programs W-13-17
 screen display access W-6-32
 timer interrupts W-7-21
 troubleshooting
 386 enhanced mode W-14-31
 incompatible grabber W-14-16
 README files W-14-32
 UNC redirection W-7-17 to W-7-19
 virtual machine W-2-7 to W-2-8
- MS-DOS support files
 MS-DOS drivers 3-13, 3-15
 WinOldAp and Grabber files 3-14
- MSCDEX.EXE 1-47, 11-13, 11-15
- MSD.EXE (Microsoft Diagnostics tool) 13-4, 13-7
- [msdlc] section, PROTOCOL.INI file 6-35 to 6-43
- [msdlc_xif] section, PROTOCOL.INI file 6-35
- msdlcretries entry, PROTOCOL.INI file 6-38
- MSIPX configuration 8-36
- MSKB *See* Microsoft Knowledge Base
- MSMAIL.INI
 administrator name W-12-36 to W-12-37
 custom message types W-12-21 to W-12-25, W-13-7 to W-13-9
 Edit MSMAIL.INI command W-12-15 to W-12-16
 editing 4-4 to 4-5, W-6-3 to W-6-4
 format of 4-3
 installing Help Request form W-12-23 to W-12-25
 overview 4-2
 Schedule+ usage W-13-3
 sections
 [Address Book] W-6-82
 [CustomCommands] W-6-82 to W-6-83
 [CustomMessages] W-6-83 to W-6-84
 [EFAX Transport] 4-21
 [Microsoft Mail] W-6-85 to W-6-91
 [MMF] W-6-92 to W-6-93
 list of W-6-82
 server custom commands W-12-15 to W-12-18
 server pathname W-12-36, W-12-39
 workstation custom commands W-12-14 to W-12-19

Multitasking
 386 enhanced mode W-2-6 to W-2-7
 foreground application priority W-14-30
 Multimedia driver files, listed 3-9
 Multinet entry, SYSTEM.INI file 4-15
 Multiple system configurations
 setting up Windows for Workgroups 2-11 to 2-14
 troubleshooting installation problems 13-16

N

Named pipe applications, trouble running 13-38
 Names of computers, duplicate 13-26
 nameserver0 entry, TCPUTILS.INI file 6-25
 nameserver1 entry, TCPUTILS.INI file 6-25
 nbssessions entry, PROTOCOL.INI file 6-21
 NDIS 2.0 drivers
 described 1-6
 listed 3-21
 SYSTEM.INI file entries 1-39
 NDIS 2.0 protocols on ODI drivers
 installing the ODINSUP driver 8-39 to 8-49
 overview 8-39
 NDIS 3.0 drivers
 described 1-8
 listed 3-23
 SYSTEM.INI file entries 1-38
 NDIS 3.0 IPX/SPX protocol *See* NWLink protocol
 NDIS.386, described 1-9
 NDIS2SUP.386 driver 1-7
 NDISHLP.SYS driver 1-7
 NDISLOG.TXT file 1-34
 NE2000 network adapter 8-34
 net init command 1-40
 net start command
 placement in the AUTOEXEC.BAT file 1-37, 1-38
 troubleshooting 13-27 to 13-29
 net start netbind command 1-40
 net stop command 1-7
 net view command 1-45
 Net Watcher accessory
 auditing network events 5-19
 identifying workstation connections W-10-9 to W-1010
 terminating connections W-10-9 to W-10-11
 NetBEUI protocol, overview of 6-2
 NetBEUI.386 virtual device, described 1-9, W-2-16 to
 W-2-17
 NetBIOS interface
 described W-1-35
 implementing W-2-11 to W-2-13
 lana numbers W-7-9 to W-7-10
 Novell NetBIOS W-8-19
 virtual device driver W-2-16 to W-2-17
 NetBIOS services over IPX 8-28 to 8-29
 NETBIOS.EXE 8-28
 NetCard entry, SYSTEM.INI file 1-38, 1-39, 4-19, 4-8
 [netcard] section in PROTOCOL.INI W-6-74 to W-6-75
 Netcard3 entry, SYSTEM.INI file 1-38, 4-8
 NET.CFG file
 Link Driver parameters 8-24
 sample configurations
 ODINSUP configuration 8-43, 8-49
 Open Datalink configuration 8-34
 settings for ODI 8-23
 [net.cfg] section, SYSTEM.INI file 4-9
 NETDDE.EXE 1-35
 netfiles entry, PROTOCOL.INI file 6-21
 NetMisc entry, SYSTEM.INI file 1-38, 4-8
 Network adapter cards
 base I/O port address W-1-28
 base memory address W-1-29
 changing settings W-6-73
 configuring W-1-26
 described W-1-25
 detected by Setup W-3-2
 installable W-5-52 to W-5-56
 interface connectors W-1-25 to W-1-26
 interrupt request lines W-1-27 to W-1-30
 NDIS card driver W-1-29, W-2-11 to W-2-13,
 OEM (original equipment manufacturer) W-5-64 to
 W-5-68
 PROTOCOL.INI W-6-73
 removing from Setup W-5-69 to W-5-70
 troubleshooting 13-10 to 13-13, W-14-37 to W-14-39
 Network adapter drivers
 ARCNet driver 8-19
 NDIS 2.0 drivers
 driver files, listed 3-21
 support for 1-6
 NDIS 3.0 drivers
 driver files, listed 3-23
 support for 1-8
 Novell NetWare drivers, specifying 8-10
 third-party drivers, loading 1-40
 Network browsing *See* Browsing network resources
 Network cards, 32-bit 11-16
 Network connections, troubleshooting *See* Connection
 problems
 Network DDE
 386 enhanced mode W-2-16
 API W-11-24
 application macros W-11-16 to W-11-18
 ClipBook Viewer example W-11-18 to W-11-22
 ClipBook Viewer interface W-11-13
 data exchange with ClipBook W-10-6 to W-10-9
 DDE links W-11-16 to W-11-18
 DDE shares W-6-60, W-11-11 to W-11-12, W-11-14 to
 W-11-16
 described W-11-11
 direct network example W-11-22 to W-11-23

- Network DDE (*continued*)
 - Hearts game W-10-14
 - identifying conversations W-10-9 to W-10-10
 - loading W-11-24
 - preventing sharing 5-4
 - other network support for 9-7 to 9-9
 - system components W-11-12 to W-11-13
 - terminating conversations W-10-10 to W-10-11
 - Windows 3.1 W-11-25
 - workstation connections W-10-8 to W-10-9
- Network Device Interface Specification *See* NDIS
- Network drivers
 - driver files, listed 3-20
 - NETWORK.INF entries W-5-50 to W-5-63
 - SETUP.INF entries W-5-20 to W-5-23
- [network drivers] section, SYSTEM.INI file 4-18 to 4-19
- Network entry, SYSTEM.INI file 4-8
- Network functionality, troubleshooting
 - Banyan VINES 13-37 to 13-39
 - no network functionality in Windows 13-15
 - Novell NetWare 13-33 to 13-36
 - real mode network problems
 - missing network functionality 13-30
 - network will not start 13-27
 - SunSelect PC-NFS 13-39
 - Windows NT and Windows NT Advanced Server 13-31 to 13-33
- Network ID, defined 6-9
- Network protocols *See* Protocols
- NETWORK.INF
 - described W-5-4, W-5-50
 - editing W-5-5
 - entries used in PROTOCOL.INI W-6-73
 - information file format W-5-4 to W-5-5
 - removing drivers from W-5-69 to W-5-70
 - sections
 - [multinet] W-5-57 to W-5-58
 - [multinet_install] W-5-58 to W-5-61
 - [netcard] W-5-52 to W-5-54
 - [netcard_install] W-5-54, W-5-59 to W-5-61
 - [netcard_protocol] W-5-54, W-5-62 to W-5-63
 - [nwddata] W-5-51
 - [protman] W-5-52
 - [protman_install] W-5-52
 - [transport] W-5-55 to W-5-56
 - [transport_install] W-5-56, W-5-59 to W-5-61
 - [transport_protocol] W-5-57, W-5-62 to W-5-63
 - [workgroup] W-5-51 to W-5-52
 - list of W-5-50
 - values used in SETUP.SHH W-3-23 to W-3-24
- [network] section in EFAXPUMP.INI 4-31
- [network] section in SYSTEM.INI
 - computer name W-1-35
 - disabling resource sharing W-7-5
 - entries 4-10 to 4-18, W-6-64 to W-6-70
- [network] section in SYSTEM.INI (*continued*)
 - workgroup W-8-7 to W-8-8
 - workstation broadcasting W-8-7
- [network.setup] section in PROTOCOL.INI 6-35, W-6-74, W-7-9 to W-7-10
- Network Setup icon 2-3
- Network support
 - See also* Novell NetWare
 - Banyan VINES 9-4 to 9-6
 - configuring an additional network 9-2
 - configuring the primary network 9-3
 - DEC PATHWORKS 9-6
 - Microsoft LAN Manager 9-4
 - networks supported as additional networks 9-2
 - networks supported as primary networks 9-3
 - obtaining information about other networks 9-4
 - options
 - Microsoft Windows Network 2-4
 - overview of options 9-2
 - standalone configuration 2-4
 - Windows 3.1-compatible network support 2-5
 - Windows 3.1-compatible networks
 - Artisoft LANtastic 9-10
 - overview 9-7
 - SunSelect PC-NFS version 5.0 9-10
 - support for Network DDE 9-7 to 9-9
- NETWORK.WRI file 13-11
- Networking component enhancements
 - alerts and notifications through the Messenger service 1-11
 - illustrations
 - configuration using NDIS 2.0 drivers 1-6
 - configuration using NDIS 3.0 drivers 1-8
 - network protocols 1-10
 - overview 1-5
 - support for 16-bit network adapter drivers 1-5
 - support for 32-bit network adapter drivers 1-8
 - support for ODI drivers 1-10
- NetworkNamenn entry, EFAXPUMP.INI file 4-31
- Networks dialog box 2-4
- NETWORKS.WRI file 1-2
- NETX.EXE 6-4
- Non-Windows applications *See* MS-DOS-based applications
- [NonWindowsApp] section in SYSTEM.INI W-6-62 to W-6-64, W-9-5
- Novell Files forum 8-5
- Novell NetWare
 - illustrations
 - ARCNet configuration using ODI drivers 8-20
 - default monolithic IPX configuration 8-18
 - default ODI IPX configuration 8-13
 - flow of IPX information 8-26
 - monolithic IPX model 8-16

- Novell NetWare (*continued*)
- illustrations (*continued*)
 - ODI driver model 8-11
 - ODINSUP configuration 8-39
 - installing for monolithic IPX configuration
 - default configuration 8-18
 - driver versions 8-19
 - overview 8-16
 - testing the network before installing Windows for Workgroups 8-17
 - installing for ODI configuration
 - default configuration 8-13
 - driver versions 8-15
 - ODI support files for Windows for Workgroups 8-15
 - overview of ODI 8-11
 - testing the network before installing Windows for Workgroups 8-12
 - installing support for
 - ARCNet network adapters 8-19
 - configuring Windows for Workgroups 8-9 to 8-10
 - obtaining required files 8-5 to 8-8
 - overview 8-4
 - support files for Windows 8-4
 - installing Windows for Workgroups from a NetWare network 2-18
 - NDIS 2.0 protocols on ODI drivers
 - installing the ODINSUP driver 8-39 to 8-49
 - overview 8-39
 - NetBIOS services over IPX 8-28 to 8-29
 - NetWare dialog box button W-10-2, W-10-3 to W-10-4
 - Network DDE support 9-10
 - NWLink protocol
 - choosing the right configuration 8-27
 - connectivity 8-27
 - overview 8-25
 - overview of enhanced support 8-3
 - resources, connecting to W-8-23
 - sample configurations
 - monolithic IPX configuration 8-34
 - MSIPX configuration 8-36
 - ODINSUP configuration 8-43, 8-49
 - Open Datalink configuration 8-31
 - token ring card W-8-18
 - troubleshooting 13-33 to 13-36
 - using client software with Windows for Workgroups
 - LastDrive parameter in CONFIG.SYS 8-29
 - log on to NetWare server before starting Windows 8-31
 - using Windows for Workgroups as a client on a NetWare network 11-11
 - workstation configuration files
 - NET.CFG and MLID settings 8-23
 - NET.CFG Link Driver parameters 8-24
 - overview 8-21
 - special settings 8-23
 - NTCARD.HLP file 13-11
 - NULL modem
 - cable wiring for 7-11
 - configuring for direct serial connections 7-11
 - NumBigBuf entry, SYSTEM.INI file 4-16
 - numnames entry, PROTOCOL.INI file 6-21
 - NumRings entry, EFAXPUMP.INI file 4-26
 - numsockets entry, TCPUTILS.INI file 6-24
 - NWLink protocol
 - default NWLink stack 6-5
 - installing 6-5
 - integrating Novell NetWare with Windows for Workgroups 8-25 to 8-27
 - Novell NetWare connectivity 6-4, 8-27
 - NWNBLink provider 6-4
 - overview 6-3
 - PROTOCOL.INI parameters 6-6
 - supported frame types 6-5
 - NWNBLink 6-4, 8-28 to 8-29
 - [NWNBLink] section, SYSTEM.INI file 4-20
- ## O
- Object Linking and Embedding (OLE)
 - described W-11-10 to W-11-11
 - Mail messages W-12-5
 - Microsoft Draw program W-10-21
 - OLE links W-11-17, W-11-25
 - troubleshooting W-C-39
 - WIN.INI [embedding] section W-6-10
 - Object Packager utility W-12-37 to W-12-38
 - ODI *See* Open Datalink Interface
 - ODIHLP.EXE 8-15
 - ODINSUP driver
 - installing 8-40 to 8-49
 - ODINSUP configuration, illustrated 8-39
 - OEM font files, listed 3-10
 - OEMSETUP.INF
 - described 1-37, W-5-4, W-5-64
 - directory W-5-64
 - editing W-5-5
 - entries used in PROTOCOL.INI W-6-73
 - example file W-5-68
 - information file format W-5-4 to W-5-5
 - sections
 - [disk] W-5-64
 - [multinet] W-5-67
 - [multinet_install] W-5-67
 - [netcard] W-5-65
 - [netcard_install] W-5-65
 - [netcard_protocol] W-5-65 to W-5-66
 - [transport] W-5-66
 - [transport_install] W-5-66
 - [transport_protocol] W-5-67

- Open Datalink Interface (ODI)
 - ARCNet configuration using ODI drivers 8-20
 - default IPX ODI configuration 8-13
 - driver versions 8-15
 - IPXODI.COM 8-12
 - Link Support Layer (LSL) 8-11
 - Multiple Link Interface Driver (MLID) 8-12
 - NDIS 2.0 protocols on ODI Drivers
 - installing the ODINSUP driver 8-39 to 8-49
 - overview 8-39
 - ODI driver model, illustrated 8-11
 - ODI support files for Windows for Workgroups 8-15
 - sample configurations 8-31
 - support for ODI drivers 1-10
 - troubleshooting 13-34
 - Open System Interconnection *See* OSI
 - Optical fiber
 - data transmission W-1-17 to W-1-18
 - described W-1-16 to W-1-17
 - Optimizing Windows for Workgroups
 - 32-bit File Access, optimizing 11-7
 - client and peer server configuration
 - adjusting server priority 11-12
 - caching shared CD-ROM drives 11-13
 - client configuration
 - choosing protocols 11-9
 - disabling file and printer sharing 11-8
 - installing on the local computer 11-9
 - Microsoft Windows Network 11-9
 - Novell NetWare network 11-11
 - removing unnecessary protocols 11-9
 - dedicated server configuration
 - 32-bit File Access cache size, increasing 11-15
 - 32-bit network card 11-16
 - avoiding screen savers 11-16
 - caching shared CD-ROM drives 11-15
 - NDIS 3 network adapter driver 11-16
 - server priority, adjusting 11-14
 - EMM386.EXE and other memory managers 11-3
 - SHARE.EXE 11-2
 - SmartDrive
 - identifying drives being cached 11-4
 - identifying drives cached by 32-bit File Access 11-5
 - overview 11-3
 - reducing memory used by 11-6
 - removing SMARTDRV.EXE 11-5
 - size of cache, changing 11-6
 - [Options] section, WRKGRP.INI file 2-9
 - OSI networking model
 - Application layer W-1-7, W-1-34
 - Data Link layer W-1-5 to W-1-6, W-1-29 to W-1-30
 - described W-1-3
 - interface W-1-5
 - layer numbers W-1-3
 - NDIS interface W-1-29 to W-1-30
 - OSI networking model (*continued*)
 - NetBIOS interface W-1-35
 - Network layer W-1-6, W-1-31 to W-1-34
 - Physical layer W-1-5, W-1-10
 - Presentation layer W-1-34
 - protocol W-1-4 to W-1-5
 - sending data W-1-4 to W-1-5, W-1-7 to W-1-8
 - Session layer W-1-6 to W-1-7, W-1-34
 - structure W-1-4
 - Transport layer W-1-6, W-1-7, W-1-31 to W-1-34
 - Overlapped I/O, 32-bit Disk Access 1-15
 - OverlappedIO entry, SYSTEM.INI file 4-9
- ## P
- Page swapping W-6-48 to W-6-49
 - Page-mapping conflict W-14-44
 - Pageswap device W-2-10
 - Paging W-9-8
 - PaperSize entry, EFAXPUMP.INI file 4-30
 - Parallel ports W-7-20
 - [Password Lists] section
 - WIN.INI W-7-7 to W-7-8
 - SYSTEM.INI W-6-70
 - Password-encrypted faxes, sending 10-16
 - Password validation *See* Logon validation
 - Passwords
 - Chat permissions 13-33
 - fax security password, changing 10-12
 - lowercase extended characters, using 13-32
 - security settings file, protecting 5-11
 - settings 5-5 to 5-6
 - troubleshooting 13-45
 - Paste dialog box W-10-6
 - Paste Link command W-11-8, W-11-16 to W-11-18, W-11-20
 - Paste Special command W-11-17
 - Peer-to-peer network W-1-37 to W-1-39
 - path entry, SYSTEM.INI file 4-9
 - PATHWORKS, DEC 9-6
 - PC Fax *See* Microsoft At Work Fax
 - Peer networking, configurable 5-2 to 5-4
 - Performance
 - improvements, described 1-3
 - screen savers, effect of 11-16
 - server priority, adjusting 11-12, 11-14
 - Performance Priority setting 11-12, 11-14
 - Permanent swap file W-9-4 to W-9-5, W-9-8
 - disk drive location W-6-49
 - size W-6-49
 - Permissions *See* Passwords; Security
 - Personal Address Book, entering fax numbers in 10-9
 - PIF (program information file)
 - directory location W-5-43 to W-5-47
 - foreground application priority W-14-30

- PIF (program information file) (*continued*)
 - identical executable filenames W-5-42, W-5-73
 - Lotus W-1-2-3 W-3.1 W-14-31
 - Memory Locked options W-14-31
 - run application in exclusive mode W-7-20 to W-7-21
 - setup information W-5-43
 - UNC redirection W-7-17 to W-7-19
 - Video Memory option W-14-31
- ping utility 6-18
- poolsize entry, TCPUTILS.INI file 6-24
- Ports
 - base I/O port addresses W-1-28, W-14-37
 - configuring COM ports W-14-34
 - network-redirection printer port W-14-35
 - parallel W-7-20
 - serial port adapter setting W-6-33
 - serial printer settings W-14-35
 - WIN.INI printer entries W-6-17 to W-6-19
- [ports] section in WIN.INI W-6-17 to W-6-18, W-7-20
- Postoffice *See* Mail application
- PreAnswer entry, EFAXPUMP.INI file 4-26
- PreDialCommand entry, EFAXPUMP.INI file 4-27
- Print jobs, monitoring 5-22
- Print Manager
 - Connect dialog W-7-8
 - dedicated print server W-9-5
 - processing time statistics W-10-12 to W-10-13
 - separator pages W-9-5, W-10-17 to W-10-20
 - WIN.INI [spooler] section W-6-20 to W-6-21
- PrintBufTime entry, SYSTEM.INI file 4-16
- Printer driver files, listed 3-7
- Printers
 - disabling sharing 11-8
 - preventing sharing 5-4
- PRINTERS.WRI file 1-2
- PrinterSharing entry, SYSTEM.INI file 4-16
- Printing, notification of completed print jobs 1-11
- priority entry, SYSTEM.INI file 4-16
- Priority of server, adjusting 11-12, 11-14
- Product accessibility
 - deaf and hard of hearing users W-D-2
 - single-handed users W-D-3
 - blind and low vision users W-D-4
- Product Support Services
 - See also* Resource directory
 - support from Microsoft PSS engineers A-2
- PROGMAN.EXE 1-35
- PROGMAN.INI
 - described W-6-76
 - editing W-6-3 to W-6-4
 - sections
 - [groups] W-6-77
 - [restrictions] W-6-77 to W-6-78
 - [settings] W-6-76
 - updating group pathname W-14-11
- Program Manager
 - application directory W-5-73
 - boot sequence, described 1-35
 - creating groups W-3-31
 - custom groups W-5-72 to W-5-73
 - customizing Windows for Workgroups W-3-5
 - initialization file *See* PROGMAN.INI
 - installation defaults W-5-28 to W-5-31
 - installed groups W-5-72 to W-5-73
 - invalid or damaged group W-14-11
 - regenerating groups 13-14
 - Setup shell W-5-12
 - Startup Group W-3-2, W-3-31, W-7-17
 - UNC redirection W-7-17 to W-7-19
- [programs] section in WIN.INI W-6-19
- [protmat] section in PROTOCOL.INI W-6-74
- Protected mode
 - See also* Real mode
 - NDIS 3.0 network adapter drivers 1-7
 - VREDIR.386 redirector 1-10
 - VSERVER.386 server virtual device 1-10
- PROTMAN.DOS (Protocol Manager driver) 1-36
- PROTOCOL.INI file
 - described W-6-73
 - editing 4-5, W-6-3 to W-6-4, W-6-73
 - Microsoft DLC parameters 6-34 to 6-43
 - NWLink protocol parameters 6-6
 - sample configurations
 - monolithic IPX configuration 8-34
 - MSIPX configuration 8-37
 - ODINSUP configuration 8-43, 8-49
 - Open Datalink configuration 8-33
 - sections
 - [netcard] W-6-74
 - [netcard_protocol] W-5-54, W-5-62 to W-5-63, W-5-65 to W-5-66
 - [network.setup] W-6-74
 - [protman] W-5-52, W-6-74
 - [protocol] W-6-75
 - [transport_protocol] W-5-57, W-5-62 to W-5-63, W-5-67
 - TCP/IP parameters 6-19 to 6-22
 - troubleshooting 13-30
 - used by Protocol Manager W-2-11
- Protocol Manager, described W-1-30
- [protocol] section in PROTOCOL.INI W-6-75
- Protocols
 - choosing according to network activities 11-9
 - illustrations
 - components of the default NWLink stack 6-5
 - NetBEUI in relation to the OSI model 6-3
 - stack comparisons of OSI, IEEE 802, and DLC 6-26
- IPX.COM 8-16
- IPX/SPX Compatible Transport with NetBIOS 8-29
- IPXODI.COM 8-12

Protocols (*continued*)

- Microsoft DLC
 - configuring 6-30 to 6-31
 - installing 6-27 to 6-30
 - overview 6-26 to 6-27
 - parameters 6-32 to 6-34
 - PROTOCOL.INI parameters 6-34 to 6-43
- NetBEUI 6-2
- NWLink
 - default NWLink stack 6-5
 - installing 6-5
 - Novell NetWare connectivity 6-4, 8-27
 - NWNBLink provider 6-4
 - overview 6-3, 8-25
 - PROTOCOL.INI parameters 6-6
 - supported frame types 6-5
- overview 1-10
- removing unnecessary protocols 11-9
- support for Windows NT and Windows NT Advanced Server 7-3
- support for, described 6-2
- TCP/IP
 - configuring 6-14 to 6-17
 - how IP works 6-8
 - how TCP works 6-8
 - installing 6-11 to 6-14
 - overview 6-7
 - PROTOCOL.INI parameters 6-19 to 6-22
 - TCPUTILS.INI parameters 6-23 to 6-26
 - troubleshooting TCP/IP connections 6-18
 - Windows Sockets 6-10 to 6-11
- PSS *See* Product Support Services
- PulseDial entry, EFAXPUMP.INI file 4-27

R

- RAM *See* Random access memory
- Random access memory (RAM) and disk
 - caching 1-26 to 1-27
- Raster font files, listed 3-11
- Read-ahead caching, described 1-27
- README files
 - deleting 3-25
 - listed 3-19
- README.WRI file 1-2
- Real mode
 - See also* Protected mode
 - NDIS 2.0 network adapter drivers 1-6
 - network support files 3-21
 - stopping the real-mode network 1-7
 - troubleshooting real mode network problems
 - missing network functionality 13-30
 - network will not start 13-27
- Real-mode mapper (RMM.D32)
 - boot sequence 1-34
 - described 1-23
- Rebooting with a clean configuration for
 - troubleshooting 13-9
- reconnect entry, SYSTEM.INI file 4-17
- Redirectors
 - protected mode 1-10
 - real mode 1-7
- Registration database W-11-21
- Remote Access Service (RAS)
 - accessing the Remote Access server 7-6
 - client files, listed 3-23
 - direct serial connections 7-11
 - features of the Remote Access Server 7-7
 - modem, choosing and configuring 7-8 to 7-11
 - overview 7-6
 - security features 7-13
 - support for ISDN 7-13
 - troubleshooting 13-48
- Removing Windows for Workgroups files 3-24 to 3-25
- Required Validated Logon setting 5-6
- Required= entry, WRKGRP.INI file 2-10
- reshare entry, SYSTEM.INI file 4-17
- Resource directory
 - answers to technical questions A-2 to A-3
 - Microsoft Certified Professional Program A-9
 - Microsoft Consulting Services A-10
 - Microsoft Developer Network
 - described A-7
 - Developer Network CD A-7
 - enrollment information A-8
 - forum on CompuServe A-8
 - newspaper A-8
 - Microsoft Developers Knowledge Base A-11
 - Microsoft Download Service (MSDL)
 - connecting to A-24
 - downloading files A-25
 - overview A-24
 - searching for files A-25
 - troubleshooting A-28 to A-29
 - using downloaded files A-27
 - Microsoft FastTips for Windows for Workgroups A-2
 - Microsoft forums on CompuServe
 - information about Windows for Workgroups A-18
 - menu structure A-18
 - Microsoft Connection A-18
 - Microsoft Knowledge Base
 - accessing on CompuServe A-12
 - overview A-11
 - searching for articles A-13 to A-15
 - searching with Expert mode A-16 to A-17
 - software library A-12, A-15
 - Microsoft Solution Providers A-2, A-9

Resource directory (*continued*)

- Microsoft TechNet
 - forum on CompuServe A-7
 - monthly CD A-4
 - ordering A-7
 - overview A-4
 - WinCIM A-7
- overview A-2 to A-3
- Windows Driver Library (WDL) A-20 to A-23
- Windows for Workgroups SDK information A-3

Restricted logon settings 5-9

[restrictions] section

- PROGMAN.INI W-6-77 to W-6-78

WINFILE.INI

- initialization file, described W-6-81
- disabling file sharing W-7-5, W-10-15

RMM.D32 (real-mode mapper)

- boot sequence 1-34
- described 1-23

ROM settings on software configurable cards, troubleshooting 13-31

S

saps entry, PROTOCOL.INI file 6-39

SCHDPLUS.INI file

- described W-13-3
- editing 4-5, W-6-3 to W-6-4
- sections W-6-95 to W-6-100

Schedule+

- appointment notification W-13-2, W-13-18
- archiving calendars W-13-6
- auto-pick searches W-13-18
- custom message types W-12-21, W-13-7 to W-13-9
- data exchange with other schedulers W-13-9
- date and time format W-13-18
- described W-13-2
- Extensions for Windows for Workgroups W-12-29 to W-12-35
- files, listed 3-18
- forms W-13-8 to W-13-9
- initialization file W-6-95 to W-6-100, W-13-3
- Interchange file format W-13-10 to W-13-17
- Microsoft Mail File Format API (FFAPI) W-13-9
- multi-server network W-13-20
- offline calendar
 - copying to another computer W-13-6
 - file extension W-13-3
 - saving changes to W-13-2
- online calendar
 - access privileges W-13-3, W-13-19
 - file location W-13-2
 - filename W-13-3
 - scheduling appointments W-13-3 to W-13-4, W-13-19

Schedule+ (*continued*)

- print sizes W-13-19
- recurring appointments W-13-18
- removing from Windows for Workgroups Setup 2-15
- resource accounts W-13-6 to W-13-7
- Schedule+ Add Paks W-12-35
- standalone or networked W-13-2
- starting from Mail W-13-3
- synchronizing calendars W-13-4 to W-13-5
- upgrading with Extensions W-13-17
- user accounts W-13-6 to W-13-7
- user assistant W-13-19
- user license W-13-19

ScheduledTransmitTime entry, EFAXPUMP.INI file 4-30

scope entry, PROTOCOL.INI file 6-21

Scope ID, defined 6-15

Screen savers

- deleting 3-25
- effect on performance 11-16
- files, listed 3-19

SDK information for Windows for Workgroups A-3

SecondNet entry, SYSTEM.INI file 4-8

Security control enhancements

- administration of security settings 5-4
- Administrator Configuration Utility 5-10
- auditing network events
 - using Event Log 5-20 to 5-22
 - using Net Watcher 5-19
- banner options 5-6
- configurable peer networking 5-2 to 5-4
- example security scenarios
 - disabling file sharing for all users 5-15
 - handling exceptions for security settings 5-16
 - settings for a group of workstations 5-18 to 5-19
- overview 5-2
- password settings 5-5 to 5-6
- remote update of security settings 5-13 to 5-14
- security settings file
 - creating 5-11
 - installing 5-12
 - password protection 5-11
- Windows NT environment
 - domain support 7-4
 - overview 7-4
 - share-level security 7-4
 - support for security features 5-7 to 5-9
 - user and group accounts 7-5
 - user-level security 7-4

Security features of Remote Access Service 7-13

Security of faxes

- disabling 10-11
- enabling 10-12
- establishing 10-10
- key encryption 10-10
- managing personal keys 10-13

- Security of faxes (*continued*)
 - overview 10-10
 - password, changing 10-12
 - personal keys, changing 10-12
 - private keys, exporting and importing 10-14
 - public keys, exporting and importing 10-14
 - public keys, typing 10-15
 - reading secured faxes 10-16
 - sending digitally signed faxes 10-16
 - sending key-encrypted faxes 10-16
 - sending password-encrypted faxes 10-16
 - signed keys, using 10-13
- [security] section, EFAXPUMP.INI file 4-32
- Separator pages (printing) W-9-5, W-10-17 to W-10-20
- Server priority, adjusting 11-12, 11-14
- Server startup or shutdown, auditing 5-21
- Setting up Windows for Workgroups 3.1
 - administrative setup 2-6, W-3-18, W-3-19 to W-3-20
 - automated setup W-3-18, W-3-20, W-3-21 to W-3-23
 - custom setup W-3-6 to W-3-7
 - express setup W-3-6
 - information files *See* Installation information files
 - maintaining Windows for Workgroups W-5-1
 - MS-DOS mode setup 2-3, W-3-7, W-3-9 to W-3-13
 - reconfiguring system W-6-3 to W-6-5
 - removing devices from W-5-69 to W-5-70
 - removing initialization files W-7-4
 - startup switches 2-6, W-3-5
 - System Information screen W-3-10 to W-3-11
 - troubleshooting
 - causes of failure W-14-7
 - failure while installing W-3-13
 - general W-C-1 to W-C-10
 - memory-resident software W-14-8 to W-14-9
 - MS-DOS mode setup W-14-9 to W-14-10
 - pop-up programs W-7-2
 - Windows mode setup W-14-10
 - Windows mode setup 2-3, W-3-7, W-3-13 to W-3-17
- Setting up Windows for Workgroups 3.11
 - See also* Configuring Windows for Workgroups; Setup program
 - administrative setup (setup /a) 2-6
 - default workgroups for users with WRKGRP.INI 2-9 to 2-11
 - last known clean configuration files 2-8
 - multiple system configurations 2-11 to 2-14
 - network support options
 - Microsoft Windows Network 2-4
 - standalone configuration 2-4
 - Windows 3.1-compatible network support 2-5
 - quick installations
 - network installation 2-17 to 2-19
 - overview 2-16
 - using the MS-DOS InterLink utility 2-19
 - Setting up Windows for Workgroups 3.11 (*continued*)
 - removing Mail, Schedule+, and Microsoft At Work Fax 2-15
 - shared copy setup (setup /n) 2-7
 - setup /a command (administrative setup) 2-6
 - setup /n command (shared copy setup) 2-7
 - Setup program
 - MS-DOS mode 2-3
 - Setup-related files 3-3
 - troubleshooting 13-14
 - Windows mode 2-3
 - SETUP.INF file
 - described W-5-3, W-5-6
 - editing W-5-5
 - information file format W-5-4 to W-5-5
 - pathname W-3-4
 - removing drivers from W-5-69 to W-5-70
 - sections
 - blowaway W-3-13
 - code page W-5-15 to W-5-18
 - copy-files W-5-24 to W-5-28, W-5-71 to W-5-72
 - display driver W-5-12 to W-5-15
 - fonts W-5-32 to W-5-33
 - general installation W-5-8 to W-5-12
 - incompatible drivers W-5-33 to W-5-34
 - keyboard W-5-15 to W-5-18
 - list of W-5-6 to W-5-7
 - miscellaneous W-5-34 to W-5-37
 - mouse driver W-5-18 to W-5-19
 - network installation W-5-20 to W-5-23
 - Program Manager W-5-72 to W-5-73
 - Program Manager groups W-5-28 to W-5-31
 - system configuration W-5-38 to W-5-41
 - system fonts W-5-23
 - TSR information W-14-9
 - values used in SETUP.SHH W-3-23 to W-3-24
- SETUP.EXE 2-3
- SETUP.SHH system settings file W-3-23 to W-3-30
- SETUP.TXT file 1-2
- SetupCommand entry, EFAXPUMP.INI file 4-27
- Share ClipBook Page dialog box W-10-7
- Share-level security in a Windows NT environment 7-4
- Share passwords, troubleshooting 13-45
- Share TSR (MS-DOS) W-9-4
- SHARE.EXE, configuration guidelines 11-2
- SHARED.INI file
 - custom commands W-12-15 to W-12-19
 - custom message types W-12-21 to W-12-25
 - described W-6-94
 - editing W-6-3 to W-6-4
 - sections W-6-94
- Sharing directories
 - Disable File Sharing setting 5-3
 - disabling file sharing for all users 5-15

- Sharing directories (*continued*)
 - disabling sharing for a protected mode server 11-8
 - troubleshooting connection problems 13-26
- Sharing fax boards 10-3
- Sharing fax modems over the network 10-5 to 10-7
- Sharing printers
 - Disable Print Sharing setting 5-4
 - disabling sharing for a protected mode server 11-8
 - troubleshooting connection problems 13-26
- SHELL.CFG file 8-34
- Show Share Passwords in Sharing Dialogs setting 5-6
- Shutdown of servers, auditing 5-21
- Single-handed users W-D-3
- SlowLanas entry, SYSTEM.INI file 1-45, 4-17
- SmallFrameECM entry, EFAXPUMP.INI file 4-27
- SmartDrive
 - cache size, changing 1-28, 11-6
 - caching shared CD-ROM drives 11-13
 - command line switches 1-48
 - compared with 32-bit disk caching 1-25
 - identifying drives being cached 11-4
 - identifying drives cached by 32-bit File Access 11-5
 - new features, described 1-47
 - overview 11-3
 - reducing memory used by 11-6
 - removing 11-5
- SMARTDRV.EXE *See* SmartDrive
- SMB (Server Message Block) protocol W-1-35 to W-1-36, W-8-3
- SMODISUP.386 8-15
- Sockets *See* Windows Sockets
- [Sockets] section, TCPUTILS.INI file 6-23
- Soft-font installers, listed 3-8
- Softset utility 13-19
- Software library, Microsoft Knowledge Base A-12, A-15
- Solution Providers, Microsoft A-2, A-9
- Sound files
 - deleting 3-25
 - listed 3-19
- [sounds] section in WIN.INI W-6-19 to W-6-20
- SOURCE_ROUTING entry, PROTOCOL.INI file 6-7
- SPART.PAR file, caution against deleting 3-24
- SpeakerMode entry, EFAXPUMP.INI file 4-27
- Speed of system, troubleshooting 32-bit File Access 13-44
- SpoolDirectory entry, EFAXPUMP.INI file 4-28
- [spooler] section in WIN.INI W-6-20 to W-6-21, W-7-5
- .SRC files, editing 4-6
- stacksize entry, PROTOCOL.INI file 6-39
- Star bus topology W-1-11 to W-1-12
- Starting Windows for Workgroups
 - applications
 - automatic startup W-3-2, W-3-31, W-6-22
 - from Mail W-12-13
 - with document file W-6-10 to W-6-11
 - logging on to NetWare servers first 8-31
- Starting Windows for Workgroups (*continued*)
 - starting in troubleshooting mode 13-6
 - switches for the win command 13-5
 - troubleshooting 13-14, 13-30
- StartMessaging entry, SYSTEM.INI file 4-17
- Startup group 1-35, W-3-2, W-3-31, W-7-17
- Startup of servers, auditing 5-21
- Static binding W-2-5
- stations entry, PROTOCOL.INI file 6-39
- Subnet mask
 - defined 6-9
 - specifying 6-14
- subnetmask0 entry, PROTOCOL.INI file 6-22
- SunSelect PC-NFS
 - installing network support 2-5
 - network support for 2-6, 9-10
 - troubleshooting 13-39
- Support services *See* Resource directory
- Swap file
 - application swap file setting W-9-5
 - deleting 3-24
 - disk drive location W-6-48 to W-6-49
 - disk-compression software W-9-16
 - network drive W-9-6
 - permanent, creating W-9-4 to W-9-5
 - size W-6-49, W-9-8
 - temporary swap file setting W-9-5
 - virtual device W-2-10
- swap entry, PROTOCOL.INI file 6-39
- System driver file 3-5
- System Editor, using to modify .INI files 4-5
- System font files, listed 3-10
- SYSTEM.DRV 3-5
- SYSTEM.INI file
 - 32-bit Disk Access entries 1-19
 - browse server entry 1-44
 - editing 4-4 to 4-5
 - format of 4-3
 - LANA numbers 1-45
 - NDIS 2.0 configuration 1-39
 - NDIS 3.0 configuration 1-38
 - overview 4-2, 4-6
 - real-mode mapper entries 1-23
 - sample configurations
 - monolithic IPX configuration 8-34
 - MSIPX configuration 8-37
 - ODINSUP configuration 8-43, 8-49
 - Open Datalink configuration 8-31
 - sections
 - [386enh] 4-7 to 4-9, W-6-30
 - [boot.description] W-6-59
 - [boot] W-6-57 to W-6-59
 - [ClipShares] W-6-60
 - [DDEShares] W-6-60, W-11-14
 - [drivers] W-6-60

SYSTEM.INI file (*continued*)sections (*continued*)

- [keyboard] W-6-61 to W-6-62
- [mci] W-6-62
- [net.cfg] 4-9
- [network drivers] 4-18 to 4-19
- [network] 4-10 to 4-18
- [NonWindowsApp] W-6-62 to W-6-64
- [NWNBLink] 4-20
- [PasswordLists] W-6-70
- [vcache] 4-20 to 4-21
- troubleshooting 13-30

T

TCP headers 6-8

TCP/IP product support, obtaining A-3

TCP/IP protocol

- configuring 6-14 to 6-17
- how IP works 6-8
- how TCP works 6-8
- installing the ODINSUP driver 8-40 to 8-49
- installing 6-11 to 6-14
- overview 6-7
- PROTOCOL.INI parameters 6-19 to 6-22
- TCPUTILS.INI parameters 6-23 to 6-26
- troubleshooting TCP/IP connections 6-18
- Windows Sockets 6-10 to 6-11
- tcpconnections entry, PROTOCOL.INI file 6-22
- tcpconntimeout entry, PROTOCOL.INI file 6-22
- [tcpglobal] section, TCPUTILS.INI file 6-26
- tcpkeepalive entry, PROTOCOL.INI file 6-22
- tcpsegmentsize entry, PROTOCOL.INI file 6-22
- TCPUTILS.INI file
 - [dnr] section 6-24
 - overview 6-23
 - [sockets] section 6-23
 - [tcpglobal] section 6-26
- tcpwindowsize entry, PROTOCOL.INI file 6-22
- TCS 10Net 2-6
- TechNet
 - forum on CompuServe A-7
 - monthly CD A-4
 - ordering A-7
 - overview A-4
 - WinCIM A-7
- Technical support *See* Resource directory
- Telephone numbers
 - CompuServe membership kit A-2
 - Drake Training and Technologies A-9
 - Microsoft Certified Professional Program A-9
 - Microsoft Consulting Services A-10
 - Microsoft Developer Services Team A-8
 - Microsoft Download Service (MSDL) A-24

Telephone numbers (*continued*)

- Microsoft FastTips for Windows for Workgroups A-2
- Microsoft Inside Sales A-3
- Microsoft Solution Provider referral A-2, A-9
- text telephone (TT/TDD) service A-3
- TEMP directory, deleting files from 3-24
- Terminal application, testing modems with 7-10
- Text telephone (TT/TDD) service A-3
- Thicknet
 - cabling connectors W-1-25 to W-1-26
 - coaxial cable W-1-14
 - network W-1-20, W-1-21 to W-1-22
 - specifications W-1-24
- Thinnet
 - cabling connectors W-1-25 to W-1-26
 - coaxial cable W-1-14
 - network W-1-20 to W-1-21
 - specifications W-1-24
 - troubleshooting W-14-40
- Time-of-day logon restrictions 5-9
- timers entry, PROTOCOL.INI file 6-41
- .TMP files, deleting 3-24
- Token-ring network
 - described W-1-12 to W-1-13, W-1-22 to W-1-23
 - Novell NetWare network W-8-18
 - specifications W-1-24
 - support with Banyan VINES 13-39
- Topologies
 - bus W-1-10 to W-1-11
 - defined W-1-10
 - star bus W-1-11 to W-1-12
 - token ring W-1-12 to W-1-13
- Transport
 - defined W-1-31 to W-1-32
 - layer
 - IEEE networking model W-1-9
 - OSI networking model W-1-7, W-1-31
- Transport protocols *See* Protocols
- TransmitPriority entry, EFAXPUMP.INI file 4-30
- Transport entry
 - PROTOCOL.INI file 6-35
 - SYSTEM.INI file 1-38, 1-39, 4-9, 4-19
- Troubleshooting
 - 32-bit File Access
 - cache problems 13-44
 - incompatible disk utilities 13-44
 - not available on a given drive 13-41
 - slow system 13-44
 - strategy for troubleshooting 13-43
 - symptoms, described 13-42
 - 386 enhanced mode W-14-27 to W-14-30
 - Banyan VINES 13-37 to 13-39
 - browsing network servers 13-40
 - clean configuration, creating 13-9
 - configuration problems 13-30

Troubleshooting (*continued*)

- connection problems
 - duplicate computernames 13-26
 - identifying 13-7
 - overview 13-17
 - troubleshooting techniques 13-18 to 13-26
 - using shared resources 13-26
 - desktop configuration W-14-11
 - fonts W-14-32 to W-14-33, W-C-20 to W-C-23
 - General Protection (GP) faults W-14-42 to W-14-45
 - ghosted connections 13-39
 - hardware W-C-11 to W-C-19
 - incompatible TSRs W-14-7 to W-14-9, W-14-11
 - installation problems
 - Express Setup detects incorrect settings 13-14
 - multiple configurations 13-16
 - no network functionality in Windows 13-15
 - Program Manager groups, regenerating 13-14
 - video drivers 13-13, 13-14
 - Windows will not run 13-14
 - Microsoft At Work Fax 13-46 to 13-48
 - modems 7-8
 - MS-DOS configuration W-14-20 to W-14-24
 - MS-DOS-based applications W-14-30
 - multi-boot programs W-7-4
 - multimedia W-14-45 to W-14-48, W-C-40 to W-C-45
 - network adapter settings 13-10 to 13-13
 - Novell NetWare 13-33 to 13-36
 - operating problems W-C-28 to W-C-39
 - options W-14-3 to W-14-4
 - printing W-14-33 to W-14-37, W-C-24 to W-C-39
 - passwords for shared drives 13-45
 - real mode network problems
 - missing network functionality 13-30
 - network will not start 13-27
 - Remote Access Service (RAS) client 13-48
 - starting Windows for Workgroups 13-14, 13-30
 - starting Windows in troubleshooting mode 13-6
 - SunSelect PC-NFS 13-39
 - TCP/IP connections 6-18
 - tools
 - CLN files 13-6
 - Microsoft Diagnostics (MSD) tool 13-4, 13-7
 - switches for starting Windows 13-5
 - video display problems W-14-15 to W-14-20
 - WFWSYS.CFG file 13-45
 - Windows NT and Windows NT Advanced Server 13-31 to 13-33
- TrueType fonts
- font files 3-11
 - video display problems W-14-32 to W-14-33
 - WIN.INI entries W-6-21
- [TrueType] section in WIN.INI W-6-18
- trxbuffers entry, PROTOCOL.INI file 6-41
 - trxbuFSIZE entry, PROTOCOL.INI file 6-41

TT/TDD (text telephone) service A-3

Twisted-pair cable

- cabling connectors W-1-25 to W-1-26
- described W-1-15 to W-1-16
- Ethernet network W-1-20, W-1-22
- network specifications W-1-24
- Topologies W-1-20

U

- uiipackets entry, PROTOCOL.INI file 6-43
- unload entry, PROTOCOL.INI file 6-43
- UNC (universal naming conventions)
 - described W-7-17 to W-7-19
 - directory searches W-10-4 to W-10-5
 - password-protected resources W-10-5
 - pointers in Mail W-12-37 to W-12-38
- usedix entry, PROTOCOL.INI file 6-43
- User accounts, described 7-5
- User-level security 5-8, 7-4
- USER.EXE 1-35, 3-3
- username entry
 - SYSTEM.INI file 4-18
 - TCPUTILS.INI file 6-26
- Utilization statistics W-10-12 to W-10-13

V

- V86 memory manager W-2-10
- V86ModeLANAs entry, SYSTEM.INI file 4-9
- Validated logon to Windows NT 5-8
- ValidNetConns entry, EFAXPUMP.INI file 4-32
- ValidPorts entry, EFAXPUMP.INI file 4-31
- [vcache] section, SYSTEM.INI file 4-20 to 4-21
- VCACHE.386 1-25, 1-26
- Vector font files, listed 3-11
- VFAT.386
 - See also* 32-bit File Access
 - disk-access scenarios
 - VFAT mounted on a compressed non-32-bit Disk Access volume 1-32
 - VFAT mounted on a compressed WDCTRL 32-bit Disk Access volume 1-33
 - VFAT mounted on non-32-bit Disk Access volume 1-31
 - VFAT mounted on WDCTRL 32-bit Disk Access volume 1-31
 - mounting on DoubleSpace drives 1-24
 - real-mode mapper 1-22
- Video drivers, troubleshooting
 - enhanced-mode-only video drivers 13-13
 - no EGA or HERC video drivers 13-14
- VINES, Banyan *See* Banyan VINES
- VIPX.386 8-4, W-8-14

- Virtual Loadable Module (VLM) components for
 - NetWare 8-8
 - Virtual Machine Manager W-2-8
 - Virtual memory options
 - 32-bit Disk Access, enabling 1-15
 - 32-bit File Access, enabling 1-21
 - Virtual memory page swapping, SYSTEM.INI entries for 4-7
 - VLMUP1.EXE 8-8
 - VNB.386 driver 1-9
 - VNETBIOS virtual device 1-9
 - VNETSUP.386 1-34
 - Volume entry, EFAXPUMP.INI file 4-27
 - VREDIR.386 1-10, 1-34, W-2-16 to W-2-17, W-7-10
 - VSERVER.386 1-10, 1-35, W-2-16 to W-2-17, W-7-13
 - VSHARE.386 W-2-16, W-2-18
 - VXDLDR.386 1-34
- W**
- Wallpaper bitmap files
 - deleting 3-25
 - listed 3-19
 - Warning beep setting W-6-22
 - Wave-form sound files
 - deleting 3-25
 - listed 3-19
 - WDCTRL 32-bit Disk Access driver
 - described 1-12 to 1-14
 - disk-access scenarios
 - VFAT mounted on a compressed non-32-bit Disk Access volume 1-32
 - VFAT mounted on a compressed WDCTRL 32-bit Disk Access volume 1-33
 - VFAT mounted on non-32-bit Disk Access volume 1-31
 - VFAT mounted on WDCTRL 32-bit Disk Access volume 1-31
 - WDCTRL 32-bit Disk Access volume 1-30
 - WDCTRL virtual device driver 1-14
 - WDL (Windows Driver Library) A-20 to A-23
 - WFWNET.DRV 1-35
 - WFWSYS.CFG file
 - allowing exceptions to the default file 5-16
 - creating 5-11
 - described 5-3
 - installing 5-12
 - password protecting 5-11
 - troubleshooting 13-45
 - win /d:c command 13-6
 - win /d:f command 13-6
 - win /d:s command 13-5
 - win /d:t command 13-6
 - win /d:v command 13-6
 - win /d:x command 13-5
 - win /n command 13-6
 - WIN.COM file 1-34, 3-2
 - WIN.INI file
 - boot sequence for Load and Run lines 1-35
 - described W-6-6
 - disable printer sharing W-10-20 to W-10-21
 - editing
 - entries W-6-3 to W-6-4
 - source file W-6-5
 - with system files W-6-4 to W-6-5
 - modified at system installation W-5-37
 - sections
 - [colors] W-6-7
 - [desktop] W-6-8 to W-6-9
 - [devices] W-6-9
 - [embedding] W-6-10 to W-6-11
 - [extensions] W-6-10
 - [fonts] W-6-14
 - [FontSubstitutes] W-6-15
 - [Hearts] W-6-11
 - [intl] W-6-11 to W-6-14
 - list of W-6-6 to W-6-7
 - [Mail] W-6-15
 - [mci extensions] W-6-16
 - [MRU_Files] W-6-16, W-10-15 to W-10-17
 - [MRU_Printers] W-6-16, W-10-21
 - [network] W-6-16 to W-6-17
 - [ports] W-6-17 to W-6-18
 - [PrinterPorts] W-6-18 to W-6-19
 - [programs] W-6-19
 - [sounds] W-6-19 to W-6-20
 - [spooler] W-6-20 to W-6-21
 - [TrueType] W-6-21
 - [Windows] W-6-22 to W-6-27
 - [WindowsHelp] W-6-27 to W-6-28
 - values used in SETUP.SHH W-3-23 to W-3-24
 - Windows 3.0 W-3-15
 - WIN386.EXE 1-34
 - WIN386.SWP file, deleting 3-24
 - WinCIM A-7
 - windowerrors entry, PROTOCOL.INI file 6-43
 - Windows 3.1-compatible networks
 - Artisoft LANtastic 9-10
 - listed 2-6
 - Novell NetWare 9-10
 - overview 9-7
 - SunSelect PC-NFS version 5.0 9-10
 - support for Network DDE 9-7 to 9-9
 - Windows applications
 - See also Applications; MS-DOS-based applications*
 - 386 enhanced mode W-2-8 to W-2-11, W-2-16 to W-2-17
 - adding mail-enabled features W-12-13
 - APIs W-2-2 to W-2-4

Windows applications (*continued*)

data exchange

Clipboard W-11-4

ClipBook Viewer W-10-6 to W-10-9, W-11-13,
W-11-16 to W-11-18

dynamic data exchange (DDE) W-11-3 to W-11-9

macros with DDE W-11-23 to W-11-24

MS-DOS-based application

Network DDE W-11-11 to W-11-25

Object Linking and Embedding (OLE) W-11-10 to
W-11-11, W-11-25

Paste Link command W-11-8

General Protection (GP) faults W-14-42 to W-14-45

mail-enabled features

adding with macros W-12-27

adding with MAPI functions W-12-23 to W-12-25

detecting Mail functionality W-6-15

user interface W-12-27

optimizing performance W-9-2

processing time priority values W-7-13 to W-7-17

user preferences W-6-6 to W-6-7

video display problems W-14-16

Windows Driver Library (WDL) A-20 to A-23

Windows for Workgroups

See also Architecture of Windows for Workgroups;

Troubleshooting

configuration block, CONFIG.SYS file 2-12

SDK information A-3

Windows mode setup, described W-2-3

Windows NT

integrating with Windows for Workgroups

overview 7-2

protocol support 7-3

Remote Access Service (RAS) client

accessing the Remote Access server 7-6

direct serial connections 7-11

features of the Remote Access Server 7-7

modem, choosing and configuring 7-8 to 7-11

overview 7-6

security features 7-13

support for ISDN 7-13

security features

domain support 7-4

overview 7-4

share-level security 7-4

user and group accounts 7-5

user-level security 7-4

troubleshooting 13-31 to 13-33

Windows NT Advanced Server

integrating with Windows for Workgroups

overview 7-2

protocol support 7-3

Windows NT Advanced Server (*continued*)

Remote Access Service (RAS) client

accessing the Remote Access server 7-6

direct serial connections 7-11

features of the Remote Access Server 7-7

modem, choosing and configuring 7-8 to 7-11

overview 7-6

security features 7-13

support for ISDN 7-13

security features

domain support 7-4

overview 7-4

share-level security 7-4

user and group accounts 7-5

user-level security 7-4

security features, support for 5-7 to 5-9

troubleshooting 13-31 to 13-33

[Windows] section in WIN.INI W-6-22 to W-6-27

[WindowsHelp] section in WIN.INI W-6-27

Windows Sockets 6-10 to 6-11

WINFILE.INI

editing W-6-3 to W-6-4

resource sharing restriction entry W-10-15, W-7-5

sections W-6-73 to W-6-74

WinMeter accessory W-10-12 to W-10-13

WinNet entry, SYSTEM.INI file 4-18

WINOA386.MOD file 3-14

WinOldAp file 3-14

WINPOPUP.EXE 1-11

WINSETUP.EXE 2-3

WINUP7.EXE 8-7

WorkGroup entry, SYSTEM.INI file 4-18

[Workgroups] section, WRKGRP.INI file 2-9, 2-10

WORKGRP.SYS 1-36

Workstation configuration files for Novell NetWare

NET.CFG and MLID settings 8-23

NET.CFG Link Driver parameters 8-24

overview 8-21

special settings 8-23

Write caching, SmartDrive 5.0 1-47

Write-behind caching, defined 1-27

WRKGRP.INI file

defining default workgroups 2-9

implementing 2-11

sample entries 2-10

X

xsaps0 entry, PROTOCOL.INI file 6-43

xsaps1 entry, PROTOCOL.INI file 6-43

xstations0 entry, PROTOCOL.INI file 6-43

xstations1 entry, PROTOCOL.INI file 6-43