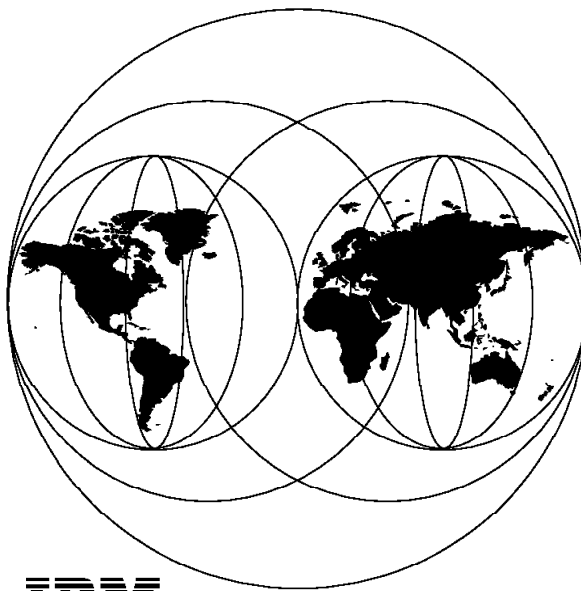


SG24-2008-00

OS/2 Warp Server Functional Enhancements, Part 1

September 1997



IBM

**International Technical Support Organization
Austin Center**

SG24-2008-00

International Technical Support Organization

OS/2 Warp Server Functional Enhancements, Part 1

September 1997



Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, "Special Notices" on page 191.

First Edition (September 1997)

This edition applies to Version 4.0 of OS/2 Warp Server and OS/2 Warp Server SMP.

Comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

© Copyright International Business Machines Corporation 1997. All rights reserved.

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

| | |
|---|------|
| Figures | vii |
| Tables | xi |
| Preface | xiii |
| The Team That Wrote This Redbook | xiii |
| Comments Welcome | xiv |
| Chapter 1. OS/2 Warp Server Introduction | 1 |
| 1.1 Positioning OS/2 Warp Server | 2 |
| 1.1.1 OS/2 Warp Server FirstStep and OS/2 Warp Server Version 4 | 2 |
| 1.1.2 IBM OS/2 Warp Server Advanced Version 4 | 2 |
| 1.1.3 Licensing of IBM OS/2 Warp Server | 3 |
| 1.1.4 IBM OS/2 Warp Server Client Support | 4 |
| 1.1.5 OS/2 Warp Server Integration | 4 |
| 1.2 Service and Function Overview | 5 |
| 1.2.1 File and Print Services | 5 |
| 1.2.2 Remote Initial Program Load (RIPL) | 9 |
| 1.2.3 SystemView System Management | 9 |
| 1.2.4 Backup and Recovery | 15 |
| 1.2.5 Remote Access | 16 |
| 1.2.6 Advanced Function Printing | 16 |
| 1.2.7 NetWare File and Print Gateway Services | 17 |
| 1.2.8 Enhanced TCP/IP Connectivity | 17 |
| 1.2.9 IBM Neighborhood Browser Enabler | 19 |
| 1.2.10 Multiprotocol Transport Services | 19 |
| 1.3 New Enhancements | 21 |
| 1.3.1 Software Choice | 21 |
| 1.3.2 IBM Enhanced Remote Access | 21 |
| 1.3.3 32-bit CHKDSK | 21 |
| 1.3.4 TCP/IP Functions | 21 |
| 1.4 Possible Enhancements of OS/2 Warp Server | 21 |
| Chapter 2. A Better Choice—Software Choice | 23 |
| 2.1 Overview | 23 |
| 2.2 Introduction to Software Choice | 24 |
| 2.3 Benefits | 26 |
| 2.4 Items Available through Software Choice | 27 |
| 2.5 Language Support | 27 |
| 2.6 Accessing the Software Choice Home Page | 29 |
| 2.7 Subscribing to Software Choice | 37 |

| | |
|---|--------|
| 2.8 Software Choice Scenarios and Integration | 38 |
| 2.9 Introducing Feature Installer | 40 |
| 2.9.1 Hardware Prerequisites | 41 |
| 2.9.2 Software | 41 |
| 2.10 Software Choice Feature Installation - Java for OS/2 | 41 |
| 2.11 Integration with TME 10 NetFinity Server for OS/2 4.0 | 45 |
| 2.11.1 Introduction | 45 |
| 2.11.2 Prerequisites | 45 |
| 2.11.3 Integration | 46 |
| 2.11.4 Distribution | 51 |
| 2.12 Integration with NetView Distribution Manager for OS/2 2.11 | 57 |
| 2.12.1 Introduction | 57 |
| 2.12.2 Prerequisites | 58 |
| 2.12.3 Integration | 58 |
| 2.12.4 Distribution | 60 |
| 2.13 Integration with Tivoli Software Distribution for OS/2 | 62 |
| 2.13.1 Introduction | 62 |
| 2.13.2 Prerequisites | 62 |
| 2.13.3 Integration | 63 |
| 2.13.4 Distribution | 65 |
| 2.14 Installing Features to RIPL Clients | 68 |
| 2.14.1 Removing Features from RIPL Clients | 69 |
| Chapter 3. IBM Enhanced Remote Access for OS/2 Warp Server | 71 |
| 3.1 Enhancements | 71 |
| 3.2 Overview and Concepts | 72 |
| 3.2.1 IBM Enhanced Remote Access Environments | 72 |
| 3.2.2 PPP Support | 75 |
| 3.2.3 Client Support | 75 |
| 3.3 System Requirements | 76 |
| 3.3.1 IBM Enhanced Remote Access for OS/2 Warp Server System Requirements | 76 |
| 3.3.2 Remote Client System Requirements | 78 |
| 3.4 Installing IBM Enhanced Remote Access | 80 |
| 3.4.1 Installing Remote Access Services in OS/2 Warp Server | 81 |
| 3.4.2 Upgrading to IBM Enhanced Remote Access | 87 |
| 3.5 Configuring IBM Enhanced Remote Access | 91 |
| 3.5.1 Configuring PPP Support on the Connection Server | 92 |
| 3.5.2 Remote Client | 100 |
| 3.5.3 Windows 95 PPP Clients | 100 |
| 3.5.4 Windows NT Version 4 PPP Clients | 121 |
| 3.5.5 OS/2 Warp PPP Clients | 122 |
| 3.6 Administration | 134 |
| 3.6.1 Changing Passphrases after Migration | 134 |

| | |
|--|------------|
| 3.6.2 Recovering the Administrator Passphrase | 135 |
| 3.6.3 PPP Security | 136 |
| 3.6.4 IP Address Configuration | 137 |
| 3.7 Problem Determination | 137 |
| 3.8 IBM Enhanced Remote Access PPP Internal Architecture | 139 |
| 3.8.1 Reference Information | 143 |
| Chapter 4. IBM Neighborhood Browser Enabler | 145 |
| 4.1 Prerequisites | 145 |
| 4.2 IBM Neighborhood Browser Enabler Architecture | 146 |
| 4.2.1 Browser Types | 147 |
| 4.2.2 IBM Neighborhood Browser Enabler NetBIOS Name Registration | 147 |
| 4.2.3 Browser Communication Process | 150 |
| 4.2.4 Updating Browser Information | 151 |
| 4.2.5 Browser Election Process | 152 |
| 4.2.6 IBM Neighborhood Browser Enabler Installation | 153 |
| 4.2.7 Uninstalling the IBM Neighborhood Browser Enabler | 155 |
| Chapter 5. File Systems Overview and CHKDSK Enhancements | 157 |
| 5.1 CHKDSK Overview | 157 |
| 5.1.1 32-bit CHKDSK System Requirements | 157 |
| 5.1.2 Benefits | 158 |
| 5.2 Enhanced CHKDSK Design | 159 |
| 5.2.1 Installing the 32-bit CHKDSK | 159 |
| 5.2.2 AUTOCHECK Function | 160 |
| 5.2.3 Using CHKDSK | 161 |
| 5.2.4 Uninstalling the 32-bit CHKDSK | 162 |
| 5.3 FAT and HPFS File System Design | 163 |
| 5.3.1 File Allocation Table (FAT) | 163 |
| 5.3.2 High Performance File System (HPFS) | 166 |
| 5.3.3 HPFS386 Architecture | 171 |
| 5.3.4 Enhanced High Performance File System (HPFS) File Recovery | 174 |
| Chapter 6. TCP/IP Enhanced New Functions | 175 |
| 6.1 Obtaining TCP/IP Updates | 175 |
| 6.2 TCP/IP Aliasing | 175 |
| 6.2.1 Configuring TCP/IP Aliasing | 176 |
| 6.3 Subnet Masking | 177 |
| 6.4 Variable Length Subnet Masks | 178 |
| Appendix A. Sharing Microsoft Office 97 and Lotus SmartSuite 97 from OS/2 Warp Server | 183 |
| A.1 Sharing Microsoft Office 97 | 183 |

| | |
|---|-----|
| A.2 Sharing Lotus SmartSuite 97 | 186 |
| Appendix B. Special Notices | 191 |
| Appendix C. Related Publications | 193 |
| C.1 International Technical Support Organization Publications | 193 |
| C.2 Redbooks on CD-ROMs | 193 |
| How To Get ITSO Redbooks | 195 |
| How IBM Employees Can Get ITSO Redbooks | 195 |
| How Customers Can Get ITSO Redbooks | 196 |
| IBM Redbook Order Form | 197 |
| List of Abbreviations | 199 |
| Index | 201 |
| ITSO Redbook Evaluation | 203 |

Figures

| | | |
|-----|--|----|
| 1. | LAN Services File and Print Folder | 6 |
| 2. | SystemView Service Manager | 10 |
| 3. | Adapter and Protocol Services and Multiprotocol Transport Services Overview | 20 |
| 4. | Software Choice Logo | 24 |
| 5. | Software Choice Integration | 25 |
| 6. | Software Choice Features | 27 |
| 7. | Software Choice Description Page | 30 |
| 8. | Software Choice Welcome Page | 31 |
| 9. | Software Choice Home Page | 32 |
| 10. | Software Choice Catalog | 33 |
| 11. | Software Choice Java for OS/2 Product Information | 34 |
| 12. | Java for OS/2 License Agreement | 35 |
| 13. | Java for OS/2 Feature Language Preference | 36 |
| 14. | Software Choice Java for OS/2 Download Page | 37 |
| 15. | Java for OS/2 Browser-based Installation | 43 |
| 16. | Java for OS/2 Advanced Path Installation | 44 |
| 17. | TME 10 NetFinity Server SYSLEVEL Information | 46 |
| 18. | Java for OS/2 Response File | 47 |
| 19. | TME 10 NetFinity Server New Software Library Entry | 48 |
| 20. | Software Library Entry Name and Definition File | 48 |
| 21. | Software Library New Configuration | 49 |
| 22. | Java for OS/2 Configuration Panel | 50 |
| 23. | Configuration with Code Server Response File | 51 |
| 24. | Schedule New Event | 52 |
| 25. | Schedule Targets | 53 |
| 26. | Schedule - Software Distribution Catalog | 53 |
| 27. | Schedule Install | 54 |
| 28. | Schedule Date and Time | 55 |
| 29. | TME 10 NetFinity Server Logfile | 56 |
| 30. | NetView DM/2 SYSLEVEL Information | 58 |
| 31. | Java for OS/2 Profile | 59 |
| 32. | Catalog a Profile | 60 |
| 33. | Install a Change File | 61 |
| 34. | NetView DM/2 Local Message Log | 62 |
| 35. | Software Distribution for OS/2 SYSLEVEL Information | 63 |
| 36. | Software Library New Configuration | 64 |
| 37. | Configuration with Code Server Response File | 65 |
| 38. | SD/2 Install Change File | 66 |
| 39. | SD/2 Schedule Install Change File | 67 |
| 40. | Common IBM Enhanced Remote Access Environments | 74 |

| | | |
|-----|---|-----|
| 41. | Output from MODE COM1 Command | 78 |
| 42. | OS/2 Warp Server Setup and Installation Window | 82 |
| 43. | Remote Access Services Configuration Window | 83 |
| 44. | Remote Access Services Configuration Options Window | 84 |
| 45. | Remote Access Services Administrator Configuration Window | 85 |
| 46. | Installation Window | 89 |
| 47. | Upgrade Warning Window | 90 |
| 48. | Installation Upgrade Complete Window | 91 |
| 49. | IBM Enhanced Remote Access Logon Option | 92 |
| 50. | MPTS Configuration Window - Binding TCP/IP to LAN Adapter | 95 |
| 51. | Configuration for a Token-Ring Adapter | 96 |
| 52. | Configuration for an Ethernet Adapter | 96 |
| 53. | PPP Section of the \WAL\WCLLOCAL.INI Configuration File | 97 |
| 54. | \WAL\WCLIPADR.INI IBM Enhanced Remote Access Configuration File | 99 |
| 55. | Opening the Windows 95 Control Panel | 101 |
| 56. | Windows 95 Control Panel | 102 |
| 57. | Windows 95 Network Configuration Window | 103 |
| 58. | Adding a Network Adapter | 104 |
| 59. | Adding the Dial-Up Adapter | 105 |
| 60. | Default Protocols for Dial-Up Adapter | 106 |
| 61. | Adding a Protocol to Dial-Up Adapter | 107 |
| 62. | Adding TCP/IP Protocol to Dial-Up Adapter Configuration | 108 |
| 63. | Dial-Up Adapter Configuration with TCP/IP Installed Protocol | 109 |
| 64. | Prompt to Restart Windows 95 | 110 |
| 65. | Dial-Up Networking New Connection | 110 |
| 66. | Make New Connection Configuration | 111 |
| 67. | Selected Modem Properties | 112 |
| 68. | Connection Server Modem Number and Country Code Entry | 113 |
| 69. | Dial-Up Networking with New Entry | 114 |
| 70. | Selecting Dial-Up Networking Properties | 115 |
| 71. | Configure Server Type Window | 116 |
| 72. | Dial-Up Server Settings | 117 |
| 73. | Dial-Up Networking TCP/IP Configuration | 118 |
| 74. | Server Types Configuration Window | 119 |
| 75. | Connect To Window | 120 |
| 76. | Connecting to Enhanced Remote Access Services | 120 |
| 77. | Connected to Window | 121 |
| 78. | Programs Folder Contents | 122 |
| 79. | Internet (Modem) Folder Contents | 122 |
| 80. | Internet Dialer New Entry | 123 |
| 81. | Login Info Tab of the Add Entry Dialog | 124 |
| 82. | Connect Info Tab of the Add Entry Dialog | 125 |
| 83. | Server Info Tab of the Add Entry Dialog | 126 |

| | | |
|------|--|-----|
| 84. | Modem Info Tab of the Add Entry Dialog | 127 |
| 85. | Closing Dial Configuration Confirmation Window | 128 |
| 86. | IBM Dial-Up for TCP/IP Window with New Entry | 129 |
| 87. | Connecting to an IBM Enhanced Remote Access Connection Server | 130 |
| 88. | Installation Directory for DIALs Client | 131 |
| 89. | Modem and Port Selection for DIALs Client | 131 |
| 90. | IBM 8235 DIALs Installation Complete Window | 132 |
| 91. | DIALs/2 Folder Contents | 132 |
| 92. | DIALs/2 Connection Information | 133 |
| 93. | CMPROCES Utility Database Merge | 136 |
| 94. | IBM Enhanced Remote Access Protocol Architecture | 139 |
| 95. | IBM Neighborhood Browser Enabler Service Level | 146 |
| 96. | Standard NetBIOS Name Table Entries | 148 |
| 97. | IBM Neighborhood Browser Enabler NetBIOS Name Table Entries | 149 |
| 98. | Browser Communication Process | 150 |
| 99. | Updating the Browser Server List | 151 |
| 100. | Master Browser Election Process | 152 |
| 101. | IBM Neighborhood Browser Enabler Files | 153 |
| 102. | CHKDSK Flow during AUTOCHECK Processing | 159 |
| 103. | FAT Partition Data Structures | 165 |
| 104. | High Performance File System (HPFS) Data Structure | 167 |
| 105. | HPFS File and Directory Organization | 169 |
| 106. | HPFS Dirty Bit | 170 |
| 107. | Using IP Aliasing during System Consolidation | 176 |
| 108. | SETUP.CMD for IP Address Aliasing | 177 |

Tables

| | | |
|-----|--|-----|
| 1. | Software Choice Language Support | 28 |
| 2. | Product Information Details | 34 |
| 3. | CONFIG.SYS Modifications During Connection Server Installation | 86 |
| 4. | IBM Enhanced Remote Access Configuration Files | 88 |
| 5. | Security Authentication | 142 |
| 6. | Compatibility Among Components | 142 |
| 7. | IBM Neighborhood Browser Types | 147 |
| 8. | NetBIOS Name Table Entries for Neighborhood Browser | 149 |
| 9. | CHKDSK Installation Changes | 160 |
| 10. | CHKDSK /F: Parameter Options | 161 |
| 11. | Relationship between Cluster Size and Partition Size | 164 |
| 12. | FAT Advantages and Disadvantages | 166 |

Preface

This ITSO redbook assists those individuals who need information on IBM's latest enhancements for OS/2 Warp Server, including Software Choice, Point-to-Point Protocol (PPP) dial support, Network Neighborhood enablement, enhanced disk checking, and improvements in TCP/IP.

We provide a brief overview of OS/2 Warp Server functions and features, including client support and licensing. Through examples, we describe Software Choice, IBM's new Web-based software-delivery offering that allows companies to download new components from any browser and implement them more quickly than traditional shrink-wrap software. Integration with NetFinity, NetView Distribution Manager and Tivoli Software Distribution is addressed.

We explore the architecture and implementation of Enhanced Remote Access for OS/2 Warp Server, which adds support for any PPP client, including the IBM 8235 DIALs clients, Windows 95 and NT, and Shiva.

The Network Neighborhood Browser Enabler allows Windows 95 and Window NT clients to find OS/2 Warp Server resources through their Network Neighborhood icon. We describe the browser architecture and added functionality.

The function of the new 32-bit CHKDSK program, a critical component of any OS/2 server, is explained in detail, including a comparison of file systems such as FAT, HPFS and HPFS386.

We describe the basic configuration and usage of the minor enhancements in the TCP/IP stack, such as variable subnet masking and aliasing, that are available for OS/2 Warp Server.

Microsoft Office 97 and Lotus SmartSuite 97 are very popular application suites. We describe the installation steps of these suites for the administrator of Windows 95 and NT clients.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Oscar Cepeda is a Staff Software Engineer at the International Technical Support Organization, Austin Center. He conducts ITSO Workshops in OS/2

Warp Server and DSS. Before joining the ITSO, Oscar was an I/T Specialist in IBM U.S. Availability Services. He has nine years of experience with IBM.

Franz-Stefan Hinner is a Technical Specialist in IBM Germany. With IBM for 10 years, his areas of expertise include desktop and server systems, DOS, Windows, and OS/2. He has experience in both defect and non-defect support.

Robert Jones is a LAN Systems Administrator in ISSC Australia. He has nine years experience in OS/2 and Warp environments as well as two years experience in OS/2 LAN Server and Remote Access Services. He has worked at ISSC Australia for 10 years. His areas of expertise include Remote Access Services, OS/2 Warp Server and ADSM.

Oliver Mark is a Systems Management specialist in IBM Germany. He has six years of experience in OS/2 and Warp environments as well as experience with OS/2 Warp Server, CID Installation, NetFinity, and Remote Access Services. He is an IBM Certified Warp Engineer and an IBM Certified Warp Server Engineer.

Thanks to the following people for their invaluable contributions to this project:

IBM Austin

Janet Callaway
Gary Hunt
Bob Jones
Jay Leiserson
Garry Lewis
Velma Pavlasek
Jack Spencer
James Wahlig

IBM Raleigh

Sanjay Khanna

International Technical Support Organization, Raleigh Center

Martin Murhammer

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. OS/2 Warp Server Introduction

The IBM OS/2 Warp Server Version 4 is the next generation of the popular IBM OS/2 LAN Server product. It demonstrates a change of the IBM server strategy from file and print serving to a complete networking strategy. The major enhancements to OS/2 Warp Server are the combination of additional functions which were formerly separate products. IBM combined these products for use in small, medium and large business networks that need an affordable, reliable product that integrates the following functions:

- OS/2 Warp Base operating system
- File and Print Services
- Remote Initial Program Load (RIPL)
- System and Resource Management Services
- Backup and Recovery functions including an ADSM/2 Client
- Remote Access Services
- Advanced Function Printing (AFP) and bidirectional printer support
- NetWare Gateway Services
- TCP/IP Services
- IBM Neighborhood Browser Enabler Service
- AnyNet protocol support

All components that ship with OS/2 Warp Server are installable by a single installation routine. Inherited from OS/2 LAN Server 4.0, OS/2 Warp Server includes a sophisticated set of network capabilities, including a graphical, object-oriented administration model which simplifies setup, installation and administration.

To accommodate the requirements of NetWare environments, OS/2 Warp Server includes a NetWare File and Print Gateway that allows smooth and transparent integration with NetWare servers.

OS/2 Warp Server's flexible security design allows access control privileges to be assigned to specific files on the server in order to fit the business needs of small, medium and large company networks. In the Advanced version of OS/2 Warp Server, these access control privileges are combined with HPFS386, a highly optimized Ring 0 extension of the High Performance File System (HPFS) that stores access rights directly at the file level.

In the following sections, we provide a short overview of the various services included in OS/2 Warp Server.

1.1 Positioning OS/2 Warp Server

The IBM strategy of combining the needed server functions in a single installation complements the strategy to address the different business networks with different products. Therefore, IBM packages OS/2 Warp Server in three offerings to fit the requirements of small, medium and large networks. The base for these offerings is OS/2 Warp Server. The offerings are called:

OS/2 Warp Server FirstStep
OS/2 Warp Server Version 4
OS/2 Warp Server Advanced Version 4

1.1.1 OS/2 Warp Server FirstStep and OS/2 Warp Server Version 4

OS/2 Warp Server FirstStep is a specially designed offering which packages OS/2 Warp Server Version 4 with 10 Client licenses, making it ideal for the small business. Because this server is identical to the stand-alone OS/2 Warp Server Version 4, you have the same capabilities to manage your server and your network, share files, printers and serial devices, remote access, enhanced TCP/IP services, Backup and Recovery, Advanced Print Services, and NetWare File and Print Gateway Services. OS/2 Warp Server possesses the same 32-bit preemptive multitasking capabilities of IBM's reliable, powerful and battle-tested OS/2 Warp operating system, which offers crash protection and runs OS/2, DOS and Windows applications.

1.1.2 IBM OS/2 Warp Server Advanced Version 4

IBM OS/2 Warp Server Advanced Version 4 addresses medium and large network customers. It enhances the performance, functionality and capacity of IBM OS/2 Warp Server.

To increase performance, IBM implemented HPFS386 in the Advanced server. Unlike file operations in HPFS, the HPFS386 file system runs at the same privilege level as the OS/2 kernel. Whereas OS/2 Warp Server (which can use HPFS) stores access controls in the NET.ACC file, OS/2 Warp Server Advanced (which can use HPFS386) puts the access control structure in the file system. This allows access control checking without unnecessary head movements and CPU ring transitions. Also implemented in HPFS386 is the ability to implement limitations for user disk space.

In addition to HPFS386, IBM implemented Local Security to OS/2 Warp Server Advanced, which allows the administrator to protect local system access and grant rights to files and directories only after the user has been locally validated and logged on successfully.

In addition, the Fault Tolerance System is also delivered with OS/2 Warp Server Advanced. It allows you to implement disk mirroring and duplexing, which reduces the chance of server downtime if a hard drive or drive controller fails.

Also included in the OS/2 Warp Server Advanced is code for Pentium optimization. If a Pentium-class CPU is found, OS/2 Warp Server uses Pentium-specific processor instructions whenever possible, which results in modest enhancements in performance.

1.1.3 Licensing of IBM OS/2 Warp Server

In general, you need a Use-Based Feature (UBF) for each user that will access any of the chargeable services of OS/2 Warp Server. The chargeable services are:

- File and Print Services
- Systems Management Services
- Remote Access Services

In the past, IBM charged for the client code, but this is no longer the case. Now, a UBF is required for a user to access the chargeable features of OS/2 Warp Server. The following information may also be helpful to the administrator:

- A single UBF allows a user to access any and all OS/2 Warp Servers in that enterprise. UBFs are not required for each server.
- OS/2 Warp Server does not currently implement a UBF licensing enforcement mechanism to access its features, but may do so in the future.
- Maintaining compliance with the license terms and agreements is the responsibility of the administrator.

If you have OS/2 Warp Connect Version 3.0 or OS/2 Warp Version 4.0, a UBF license is included for that user. DOS/Windows system users require a UBF to connect to a server. Windows 95 and Windows NT systems do not require IBM client code to access OS/2 Warp Server, but a UBF is also required for those users. In general, the administrator should ensure that a UBF has been purchased for each *employee*, not necessarily for each machine. If 50 employees share 30 machines, 50 UBFs are required. If 10 of the machines run OS/2 Warp Connect and 20 machines run DOS/Windows or Windows 95, then only 40 additional UBFs are required.

Each copy of OS/2 Warp Server includes one UBF, which can be subtracted from the total user count required (this is true in the United States; check in

your country to see if this is still true). So, for the example of 50 employees above, if five servers are installed, the total number of UBFs needed is:

50 employees
- 10 UBFs (from OS/2 Warp Connect)
- 5 UBFs (from five servers)

35 UBFs to be purchased

Note: OS/2 Warp 4 does not currently include a UBF for access to OS/2 Warp Server. However, after December 31, 1997, OS/2 Warp 4 will include a UBF in the purchase price.

1.1.4 IBM OS/2 Warp Server Client Support

One of the major reasons for the success of OS/2 Warp Server and OS/2 LAN Server is the broad variety of clients that can utilize the functions of the server. These clients include:

- DOS Version 6.1 and higher with DOS LAN Services
- DOS PC LAN Program (PCLP) Version 1.31 or later
- OS/2 Version 1.3
- OS/2 Version 2.x
- OS/2 WARP Version 3.x
- OS/2 WARP Connect Version 3.x
- OS/2 WARP Version 4.0
- Microsoft Windows 3.X
- Microsoft Windows for Workgroups
- Microsoft Windows 95
- Microsoft Windows NT

In addition, you can support Macintosh clients and AIX clients with the following products:

- LAN Server for Macintosh
- IBM PC Connection for AIX

LAN Server for Macintosh and PC Connection for AIX are purchased separately. For more detailed information on client support for OS/2 Warp Server, refer to the IBM Redbook titled *Network Clients for OS/2 Warp Server: OS/2 Warp 4, DOS/Windows, Windows 95/NT, and Apple Macintosh*, SG24-2009.

1.1.5 OS/2 Warp Server Integration

OS/2 Warp Server is backward-compatible with previous OS/2 LAN Server clients and servers. This allows OS/2 Warp servers to be incrementally added to an existing LAN Server network and provide the customer with

excellent compatibility between systems. It also allows a smooth migration from older versions of OS/2 LAN Server.

To simplify the migration of Novell NetWare servers to OS/2 Warp Server, a Novell NetWare Gateway is integrated into OS/2 Warp Server. This is actually the NetWare Client for OS/2 running on OS/2 Warp Server. Having the NetWare client on the server allows NetWare file and print resources to be shared with OS/2 Warp Server clients without requiring the NetWare requester code on these clients.

1.2 Service and Function Overview

The following sections provide a short overview of the different services, functions and features of OS/2 Warp Server. For more detailed information, refer to *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*, SG24-4602, and *Inside OS/2 Warp Server, Volume 2: System Management, Backup/Recovery and Advanced Print Services*, SG24-4702.

1.2.1 File and Print Services

The OS/2 Warp Server File and Print Services is the Local Area Network (LAN) component that allows you to share hardware and software resources located on that server. The following resources can be shared:

- Files and Directories
- Printers
- Serial Devices

Note: Be aware that DOS-based clients (including Windows) may not access shared serial devices unless they are redirected to LPT ports for output only, for example to serially attached printers and plotters.

After connecting to the server, network resources are used like local resources.

OS/2 Warp Server has one unique specialty. It allows an administrator to build up a network folder, called Public Applications, that includes applications the user may use. This folder is dynamic in that it is rebuilt at every logon. This allows the administrator to enable application sharing quickly and easily.

When you open the LAN Services File and Print folder, the following functions are available:

able to access files on a partition that is HPFS386-formatted. The HPFS386 startup diskette, with the HPFS386 Installable File System (IFS) driver loaded, allows access to the HPFS386 file system. If you must access a system that does not have a valid CONFIG.SYS file, you need to boot from the OS/2 Warp Installation Diskettes and a modified OS/2 Warp Diskette 1. This utility allows you to automatically modify Diskette 1 to add support for HPFS386.

- FT Administration

OS/2 Warp Server provides you with a utility to manage fault tolerance on the server. You can check the status of mirrored drives and repair broken mirrors.

Note: Fault tolerance is only available with OS/2 Warp Server Advanced package.

- FT Setup

Fault tolerance provides you with the functions to mirror and duplex drives. The FTSETUP command allows you to set up fault tolerance for the first time. It allows you to implement RAID 0 (disk striping) software functionality. The fault tolerance features are:

- Disk mirroring

Enables the ability to duplicate a single logical drive or volume on two partitions which are on different disks on the same disk controller. This protects you against a single disk failure.

- Disk duplexing

Gives you the capability of further protecting your installation by imposing a restriction that the two disks on which the partitions reside are controlled by two different disk controllers. This protects you against both single drive failure and single disk controller failure.

- LAN Server Administration

OS/2 Warp Server provides the same Graphical User Interface (GUI) that you are already familiar with from LAN Server Version 4.0. It allows easy, drag-and-drop, object-oriented administration.

It allows you to administer by dragging and dropping objects to manage users, groups, applications, servers, and shared resources. All defined users or groups are objects, which enables the administrator to create a very dynamic network.

- LAN Server Audit Log Utility

To audit specific events, you can use the audit log utility. As an enhancement to LAN Server 4.0, changes made to the sort order are saved and retrieved every time you view the audit log.

- LAN Server Error Log Utility

The LAN Server Error Log Utility is used to display errors that have been logged, either on the workstation or server. The logfile can be printed and cleared.

Changes made to the sort order will be saved and retrieved every time you view the error log, unlike LAN Server 4.0.

- Logoff

The graphical interface allows you to log off the domain or the local workstation.

Note: Logging off a domain terminates all network applications and associations.

- Logon

Logon allows you to perform a local or domain logon.

- Network DDE and Clipboard

The Network Clipboard is used to exchange clipboard data over the network and allows you to cut and paste data into or from other applications across a network. This is done by using Dynamic Data Exchange (DDE) and clipboard functions.

- Network Messaging

The Network Messaging service allows you to exchange messages with other users and receive messages from resources like printers finishing a print job.

- OS/2 LAN Services Installation/Configuration

Use this function to reinstall, remove or reconfigure File and Print Services. It also provides you with the option to create response files for Configuration, Installation and Distribution (CID) environments.

- Start Server

Select this object to start the File and Print Sharing Services on the server workstation if you did not select to automatically start the server using the changes applied to STARTUP.CMD as part of the installation process.

- IBM OS/2 Warp Server Tuning Assistant

This provides you with the automatic tuning and configuration of your OS/2 Warp Server.

OS/2 Warp Server does not dynamically retune itself as you add more requesters. If you have a growing client base, you should run this utility at regular intervals to verify that your OS/2 Warp Server configuration can efficiently support the number of users connected to resources and provide optimum performance.

In addition, you will find two text files, README.DOC and ERROR.TXT, inside the folder that provide details on late changes, installation information and a listing of all error codes related to OS/2 Warp Server.

1.2.2 Remote Initial Program Load (RIPL)

The Remote Initial Program Load (RIPL) functions are a part of the File and Print Services and offer you the capability to load the complete client software environment from a centrally-located server.

It follows a concept based on easy administration since all maintenance is done locally on the server and the client machines are not affected. Also, since the client hardware performs a generic function, it can be exchanged with identical hardware. This is a fundamental concept for the IBM Network Station. The OS/2 Warp Server implementation is based on IEEE802.2 and NetBEUI protocols.

1.2.3 SystemView System Management

One of the basic requirements of local area networks is to better manage and control software and hardware resources. To achieve this, IBM integrated into OS/2 Warp Server the SystemView package with additional enhancements from the Distributed Console Access Facility (DCAF). The following functions are part of the OS/2 Warp Server SystemView component:

- Error and Alert management
- Software and CID software preparation
- Critical file monitoring
- Event scheduling
- Process management
- Remote system access and remote session
- Serial control
- Software and hardware inventory
- Partition and Redundant Array of Independent Disks (RAID) management
- System monitoring

These functions can be accessed locally or remotely, which gives the administrator greater flexibility. To avoid unauthorized usage, there is also integrated security that allows you to set up different users with varying levels of application access. In particular, the critical file monitor, error and alert management, remote system access, and software/hardware inventory help to support user helpdesk functions. Opening the SystemView Service Manager, you find the folder shown in Figure 2, dependent on the rights granted and on your machine type; so, for example, you will not find the RAID management within a non-RAID machine.

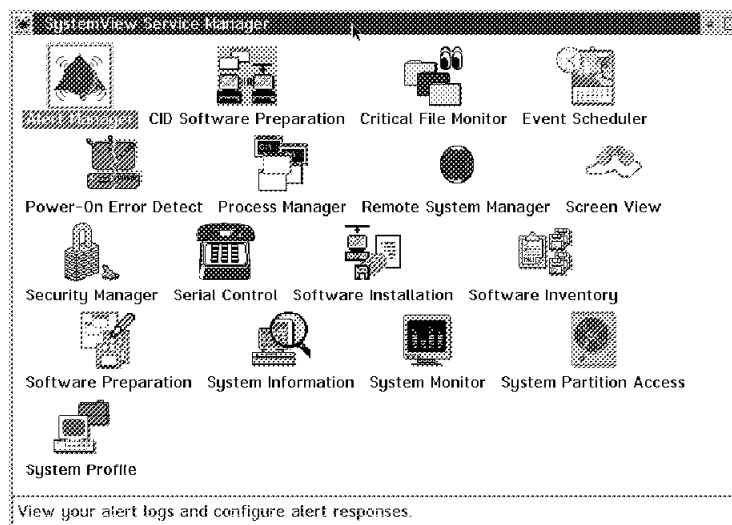


Figure 2. SystemView Service Manager

To give you a general overview over the functions integrated in OS/2 Warp Server SystemView System Management, we provide a short description of the functions:

- Alert Manager

The Alert Manager is the extendable facility that allows receipt and processing of application-generated alerts. In response to alerts, a variety of actions can be taken, including alert logging, pop-up user notification, forwarding the alert to another system, program execution and application-defined action. Features of this service include:

- Simplifies application use and processing of alerts
- Provides standard responses to alerts
- Provides extensively configurable alert management and action generation

- CID Software Preparation

CID Software Preparation is used to prepare a CID-enabled software product for distribution to and installation on an unattended remote workstation.

- Critical File Monitor

This service enables you to be warned whenever critical system files on the systems in your network are deleted or altered.

The Critical File Monitor service makes it simple for you to generate alerts when information in an important system file (such as CONFIG.SYS) changes, such as date, time, size or is deleted when it was previously present. You can also define an alert when a file is created.

The Critical File Monitor can also be used to monitor any other file that resides on a SystemView-enabled system as well.

- Event Scheduler

To easily automate many hardware system management tasks, use the Event Scheduler. You can create scheduled events, execute these events automatically on multiple remote systems or entire system groups, and maintain detailed logs of the results of these scheduled events.

- Power-On Error Detect

When a Power-On Error Detect-enabled remote system encounters a Power-On-Self-Test (POST) error, the system sends an alert message out onto the LAN. The Power-On Error Detect service enables you to receive these messages, determine the identity of the system that generated the message, and diagnose the POST problem that causes the error to begin with, before you have even left your desk. This minimizes system downtime and loss of productivity through rapid problem determination and recovery.

All information received by the Power-On Error Detect service is kept in the Power-On Error Detect log. Typically, IBM Microchannel systems are enabled for Power-On Error Detect.

- Process Manager

To view detailed information about all processes that are currently active on a system, you can use the Process Manager service. It enables you to execute commands on the system and to close individual processes by initiating a kill command. Finally, Process Manager will monitor any process that you have specified and can generate a process alert if the process is started, stops, or fails to start within a specified amount of time from startup.

- Remote System Manager

The Remote System Manager service enables a manager to link with and remotely access SystemView services installed on managed systems within the manager's network. Managed systems are divided into administrator-specified logical groups.

This enables the manager to take over the entire system, including desktop control. Any function that the local system offers can also be accessed remotely when the correct access rights are granted.

- Screen View

The Screen View service enables you to view a snapshot of any managed system's current display, in conjunction with the Remote System Manager. The managed system's desktop is converted into a bitmap file and is then compressed and transmitted to the system manager, which then displays a scalable window depiction of the managed system's desktop. This is particularly useful for remote system troubleshooting and user helpdesk functionality.

Note: When this service runs locally, it will create a bitmap of your local display. After this bitmap has been created, you can save the bitmap and load previously saved bitmaps. This is helpful for screen captures to be used in documentation.

- Security Manager

This service manages the incoming and outgoing controls of security. By using the incoming passwords and outgoing password you can control which services are accessible to outside users.

Note: Be aware that by default, no security is present. This means everybody with manager functionality can access the machine and take over desktop control.

- Serial Control

Serial Control service is used to configure the SystemView functions for serial access by adding or changing serial connection entries.

- Software Installation

The Software Installation service is used to manage and install the software objects already cataloged on the server. It is used to create and manage groups of software objects to be distributed.

Basically, the groups allow you to have filtered views of the distribution server catalog. Two groups are already defined by default:

- Software Products

All software product objects, including CID and non-CID objects.

- Shared Applications

All objects of the shared application type.

- Software Inventory

Software Inventory enables you to quickly and easily scan any managed system for the presence of installed software products. Its flexible scanning methods enable you to search for specific products, types of products, or just complete a record of all recognized software on a system. A report can be printed to a file, sent to your printer, or exported to a database.

In addition, you can enhance this service to identify products by the presence of specific file names or by the presence of a SYSLEVEL file.

- Software Preparation Profiles

The Software Preparation feature is used to prepare software and files for distribution. To prepare configuration, installation and distribution (CID)-enabled products, use the CID Software Preparation services.

To define them, you enter all the information required to package a software object in your local software profile and then build the actual software object and store it in the distribution server catalog.

To manage and install the software objects already cataloged on the server, open the Software Installation services.

- System Information

The System Information Tool provides a function to gather and display a variety of information about the hardware and software configuration of your system.

In addition to operating as a Presentation Manager application, the System Information utility can generate output to a file or printer by using command line options or menu selections.

The System Information Tool provides information on the following topics:

- Adapter identity
- Drive information
- Power management information
- Error log display and interpretation
- Keyboard information
- Memory configuration
- Mouse type and settings
- Operating system information
- Model and processor information
- Parallel and serial port configuration
- PCI bus configuration

- PCMCIA bus configuration
 - Printer configuration
 - SCSI, ESDI, IDE/ST506 or other disk adapters
 - System security features
 - Video system information
 - Viral Product Data (VPD)
- System Monitor Service
- To provide administrators with a convenient method of charting and monitoring the activity of a number of components in the system, the System Monitor Service was implemented. It includes the following features:
- Continuous monitoring of a variety of systems, including:
 - Locked memory usage
 - Virtual memory usage
 - CPU usage
 - DASD space available and space remaining
 - DASD utilization
 - TCP/IP protocol functions
 - Processes running
 - Threads running
 - Pentium processor computations
 - RAID device attributes
 - Read/write errors (only in manager)
 - Ability to export System Monitor data to a database
 - User-definable thresholds that will generate alerts when exceeded
 - Detachable, sizable, scalable, and user-configurable monitors
 - Choice of line graph, text and real-time graphic representations of system activity
- The System Monitor Service uses a data handling technique that allows for both long-term system activity profiles and short-term, high-resolution system activity monitoring.
- System Partition Access
- Partition access allows for greatly simplified system partition file handling on PS/2 computers, both locally and remotely. This service features:
- Extensive file-level handling
 - Initial Machine Load (IML) image updating
 - Adapter Description Program (ADP), Adapter Description File (ADF) and Diagnostic Generation System (DGS) updating
 - Set configuration program updating

- User confirmation security to prevent accidental deletion of system partition
- Services previously available only through use of the reference diskette
- System Profile

The System Profile service provides you with an easy to organize repository for a variety of system- and user-specific information that might not be readily available otherwise. The System Profile notebook comes with many predefined fields to help simplify organization and entry of this data. The System Profile notebook also features many user-definable fields to help you customize the System Profile to meet your individual needs.

System Profile's data can be saved to an ASCII file. This data can also be gathered by the SystemView Manager and exported to a database. The combination of System Information Tool and Software Inventory's sophisticated information-gathering abilities with System Profile's extensive selection of system- and user-specific data fields results in a extraordinarily flexible and useful system inventory and information facility.

1.2.4 Backup and Recovery

OS/2 Warp Server Backup and Recovery provides features which enable you to safeguard your system against possible loss of information by taking backups of your OS/2 files and folders. This can be done automatically or manually, and also allows a selective restore of these files.

OS/2 Warp Server Backup and Recovery has the following features:

- Supports backup and recovery of files and Access Control Lists (ACL).
- Backup media supported are:
 - diskette
 - tape
 - optical disk
 - hard disk
 - LAN drives (using ALIAS name, not UNC name)
- Used in conjunction with IBM ADSTAR Distributed Storage Manager (ADSM), backups can be sent to a separate server using the communication protocols available.
- Supports a wide range of popular SCSI tape drives.
- Allows scheduled backups.
- Compresses backup data.

- Manages backup volumes without the need of creating an administration system for backups.
- Includes a disaster recovery utility.
- Interface is multimedia-enabled and can be customized.
- Features object-oriented, drag-and-drop technology.

1.2.5 Remote Access

Today, connectivity is required for nearly all businesses of any size. OS/2 Warp Server includes a full set of remote access capabilities. This helps you on business trips to easily access important data in your network and continue working just as if you were attached to your LAN, including all functions and abilities offered in your local network. Also, it offers small businesses with two or more sites the ability to easily connect and share important data.

With OS/2 Warp Server remote node capability, users are able to log onto the network and upload and download data and print documents to other facilities. Offices are able to quickly share information by linking to their corporate network and other sites via a high-speed modem line, X.25 or ISDN.

Remote Access Services, together with the new PPP Server support (available as a separate download), supports the following clients:

- OS/2 2.11
- OS/2 Warp
- DOS/Windows 3.x
- Windows for Workgroups
- Windows 95
- Windows NT

For more information on Remote Access Services, refer to Chapter 3, "IBM Enhanced Remote Access for OS/2 Warp Server" on page 71.

1.2.6 Advanced Function Printing

To address various customer printing requirements, IBM included the Advanced Function Printing (AFP) in OS/2 Warp Server. Advanced Function Printing enhances OS/2 Warp Server by enabling access to non-PostScript printers and high-capacity host printers.

To enable access to non-PostScript laser printers such as LexMark and Hewlett-Packard, users are able to send PostScript documents using OS/2 Warp Server's PostScript printer emulation.

OS/2 Warp Server also has advanced printer functionality that is compatible with high-speed printers in a mainframe-connected environment. This compatibility assists organizations by protecting their investments in high-capacity host printers. A corporate customer can easily introduce OS/2 Warp Server into the network and configure this advanced business network solution to drive 700-page-per-minute printers.

1.2.7 NetWare File and Print Gateway Services

To protect your investment in existing NetWare servers, OS/2 Warp Server can act as a File and Print Gateway using the NetWare File and Print Gateway Services. This means OS/2 Warp Server can share logical drives or print queues that reside on a NetWare server. Requesters connected to the OS/2 Warp Server can use these NetWare resources without having the NetWare client code installed on their machines.

This allows you to smoothly migrate to a OS/2 Warp Server environment. It can also help to reduce the administrative cost associated in maintaining NetWare client code on each machine. This conserves workstation resources such as RAM and disk space. It makes your life as administrator easier because you have only to maintain one client environment. A reduction in the number of connections used on the NetWare server is another beneficial effect. The integration of NetWare servers into your corporate network enables a single point of logon, and this is what makes OS/2 Warp Server the open road to networking in your corporate environment.

1.2.8 Enhanced TCP/IP Connectivity

Many functions are included the TCP/IP component of OS/2 Warp Server, including the following:

- Dynamic Host Configuration Protocol service
- Dynamic Domain Name Server service
- Aliasing
- Variable Subnet Routing

Network administrators face a host of challenges building and maintaining their TCP/IP networks. Typically, they must assign IP addresses, host names and other network information at individual computers. This forces them to track changes every time a computer is either added, removed or relocated in the network. Subnet routing and aliasing of addresses are also an issue in TCP/IP networks. These allow routing between subnets and enable addressing one adapter with multiple addresses. All these functions are included in the TCP/IP enhancements. Other TCP/IP applications, such as FTP, Telnet and remote shell and execution are also included.

These tasks are time-consuming, error prone, and can disrupt network operations. IBM addresses these challenges with a new networking technology called Dynamic IP. IBM introduced Dynamic IP in OS/2 Warp Server, implementing a true TCP/IP plug-and-go network solution, greatly simplifying both IP network access and IP network administration. Dynamic IP is well suited for networking mobile hosts and is fully compatible and interoperable with existing IP network hosts and routers.

Dynamic IP is the integration of the Dynamic Host Configuration Protocol and Dynamic Domain Name Server. Both Dynamic Host Configuration Protocol and Dynamic Domain Name Server are new features to OS/2 Warp Server.

Dynamic Domain Name Server and Dynamic Host Configuration Protocol are complementary open networking standards developed by the Internet Engineering Task Force, the group that assures compatibility with clients and servers on other operating systems, including UNIX, Microsoft Windows NT and Microsoft Windows 95. The Dynamic Host Configuration Protocol protocol centralizes and automates the configuration of IP hosts, including IP addresses, while the Dynamic Domain Name Server protocols automatically record the association between IP hosts and their Dynamic Host Configuration Protocol-assigned addresses. The Dynamic IP clients needed to operate Dynamic Host Configuration Protocol- and Dynamic Domain Name Server-server are also included in OS/2 Warp Server.

A new function called variable subnet routing allows you to implement a subnet router to address separated subnets over a single adapter. This also includes IP address aliasing. This function is especially helpful when you must temporarily remove a machine from the network and enable another server or client to be reached by the same address. This takes away the fear of migrating large networks running the TCPBEUI protocol from different servers to one server.

The TCPBEUI, or NetBIOS over TCP/IP, interface of OS/2 Warp Server supports up to 1000 sessions on a single adapter. Adapter and Protocol Services provides a full TCP/IP protocol stack and a TCPBEUI protocol stack that is a ring 0 implementation of RFC 1001/1002. RFC 1001/1002 is not an encapsulation technique, but rather builds special packets and sends them out via User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). For example, once a NetBIOS session has been established, TCPBEUI will use sockets-send commands over a TCP connection to send NetBIOS session data. TCPBEUI builds a four-byte session header that precedes the actual user data. Thus, a NetBIOS Chain Send of 128 KB would have an overhead of only four bytes.

TCPBEUI allows peer-to-peer communication over the TCP/IP network with other computers that have compatible services.

1.2.9 IBM Neighborhood Browser Enabler

To maintain a centralized list of available resources and servers in your domain, the IBM Neighborhood Browser Enabler service for Microsoft Windows Client was developed. This enables Microsoft clients, such as Windows 95 and Windows NT, to more easily utilize OS/2 Warp Server resources.

To eliminate the network traffic required for every Microsoft Windows Client to maintain a list of shared network resources, the IBM Neighborhood Browser Enabler service builds the server lists to address the resource requests directly. This lowers the network traffic required to build and maintain the list and also frees the CPU time each Microsoft Windows Client would otherwise need to create a network resource list.

For additional information on the IBM Neighborhood Browser Enabler, refer to Chapter 4, "IBM Neighborhood Browser Enabler" on page 145.

1.2.10 Multiprotocol Transport Services

OS/2 Warp Server provides you with a wide range of supported networking protocols and communication adapters you may use in many combinations to suit your requirements for a server system. Adapter and Protocol Services may be called the communications engine of OS/2 Warp Server since it provides the AnyNet communications support for all other components of this product.

In order to support the variety of network applications and services that come with OS/2 Warp Server, and to support many additional networking products, Adapter and Protocol Services provide a very complete set of networking protocols that can be used in a LAN environment as well as for wide area networking.

Originally, Adapter and Protocol Services was called LAN Adapter and Protocol Services, but since it now also includes drivers for Wide Area Networking adapters, the word LAN was dropped, but it kept the familiar acronym LAPS. LAPS includes the following networking protocols based on the Network Driver Interface Specification standard:

- NetBIOS
- TCP/IP
- IEEE 802.2
- IPX/SPX over NDIS support
- TCPBEUI (NetBios over TCP/IP)

- NetBIOS over IPX support

Adapter and Protocol Services also includes virtual IEEE 802.2 and NetBIOS support for DOS and Windows applications running on your OS/2 Warp Server system. The Adapter and Protocol Services can be divided into two parts:

- Adapter and Protocol Services (LAPS)
- Multiprotocol Transport Services (MPTS)

For an overview of both, refer to Figure 3.

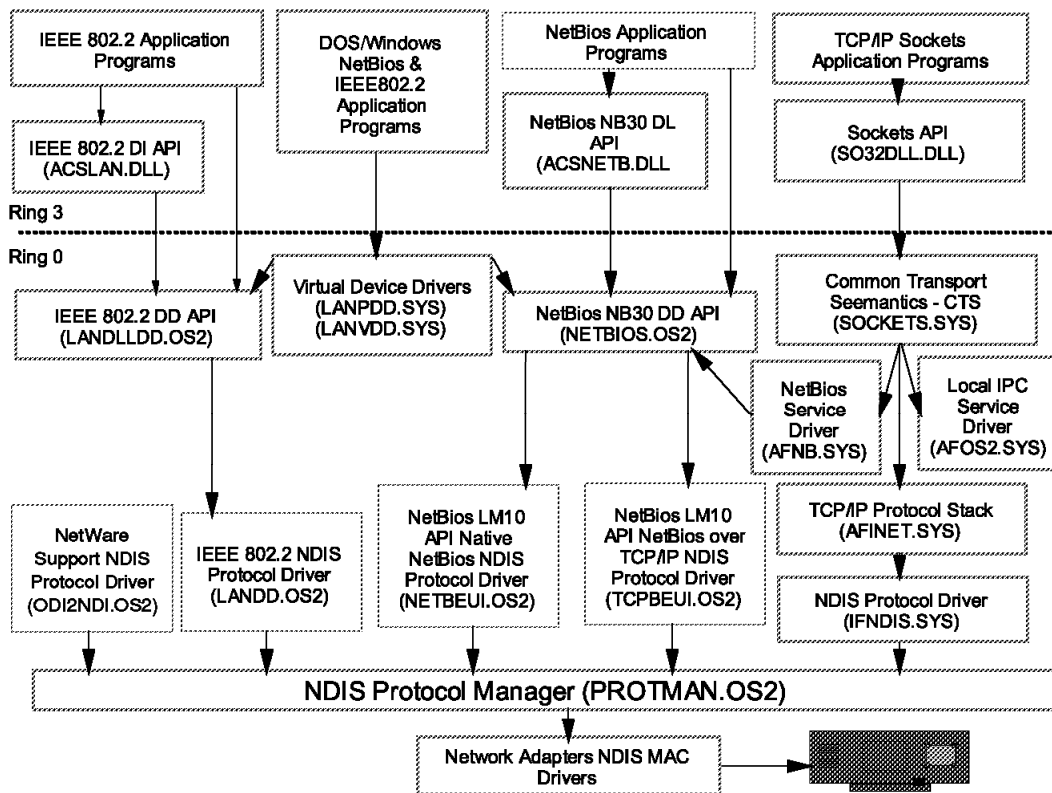


Figure 3. Adapter and Protocol Services and Multiprotocol Transport Services Overview

1.3 New Enhancements

The remainder of this redbook describes some of the enhancements that IBM has prepared for OS/2 Warp Server. They are very briefly described below.

1.3.1 Software Choice

IBM has introduced a new mechanism to deliver applications and new functions to the customer called Software Choice. It is a Website repository containing the newest software components for IBM products. The components may be available several months before the shrinkwrap version of the product. The Web site is located at:

<http://www.software.ibm.com/os/warp/swchoice/>

This site offers you earlier, easier access to new features. Today, the ability to evaluate the latest information technology is so important, and it is a great advantage to get the newest features for your products immediately.

1.3.2 IBM Enhanced Remote Access

Many customers have used OS/2 LAN Distance and the Remote Access Services component of OS/2 Warp Server. IBM Enhanced Remote Access adds the ability to support existing PPP clients, such as Windows 95, Windows NT, 8235 DIALs OS/2 Client, 8235 DIALs Windows Client, and the Shiva PPP client.

1.3.3 32-bit CHKDSK

Another new feature is the enhanced 32-bit CHKDSK for HPFS. It is a faster, enhanced version of CHKDSK that detects and corrects file system errors on your HPFS- and HPFS386-enabled hard disks. This new version allows you to check a very large disk (greater than 8 GB) in a much shorter time.

1.3.4 TCP/IP Functions

Two minor enhancements for OS/2 Warp Server in the area of TCP/IP are IP aliasing and variable subnet masking. These functions simplify resource availability and enhance usability in a complex network environment.

1.4 Possible Enhancements of OS/2 Warp Server

There are many enhancements being considered for delivery for OS/2 Warp Server in the near future, which shows that IBM is strongly committed to its network operating system. These enhancements are:

- Lightweight Directory Access Protocol (LDAP) (RFC 1777,1823)

LDAP is an open, industry standard protocol for directory services that runs over TCP/IP. LDAP allows the infrastructure to be built for clients, applications and servers of multiple vendors to access information in a single directory database in a consistent manner. This may enable a single network logon for all network resources across multiple vendors and platforms.

- 32-Bit TCP/IP

This new version of TCP/IP is substantially faster than the current 16-bit implementation and is BSD 4.4 compliant. Enhancements to DHCP and DDNS servers and clients, Java-based browser enablement, fully CID-enabled installation, as well as many new protocol parameters will be available. This version of TCP/IP will be the subject of a future redbook.

- IBM Network Station Support

The IBM Network Station is a desktop network computer, commonly known as a thin client, that communicates with the IBM AS/400, RS/6000, and System/390 computers. It also has World Wide Web browsing capability and can run Java applications. OS/2 Warp Server may include support for this computer in the near future, which gives OS/2 Warp Server customers yet another low-cost, manageable client alternative.

- Workspace on Demand Support

The WorkSpace On-Demand client obtains all software from OS/2 Warp Server, functioning as a thin client. Users can run DOS, Windows 3.x, OS/2 and Java applications from this client. This client obtains all system and application configuration information from the server, which greatly simplifies the tasks of setup and management. Many customers are interested in reducing their cost of computing without sacrificing application compatibility and control. WorkSpace On-Demand is an ideal solution for these customers.

Note: The list above is not a commitment by IBM to deliver these functions, but these and others are in consideration. IBM needs your input, through your marketing representatives, to determine which features are most important to deliver to your business.

Chapter 2. A Better Choice—Software Choice

In today's Information Systems (I/S) environment, most companies are growing their network infrastructure and connectivity to the Internet, increasing their internal support capabilities, and providing the latest hardware and software technology to their end-users. The potential benefit is that this easily-accessed and managed information will give the company a competitive advantage in its particular industry. As a result, the I/S administrator or professional has an increasingly difficult task of keeping abreast of the latest technology and determining if and how to implement this new technology.

2.1 Overview

For many companies, there is a long list of product and functional enhancements requested of the vendors they work with and, often times, a long waiting period until those enhancements are seen in newly-released products. The enhancements are usually delivered when the next shrink-wrap version of a product is available, which can vary widely between versions. For IBM OS/2, a major version may be released once a year.

Many companies wish they had earlier access to new software technology as a component so they could evaluate it sooner and implement it in a quick, yet prudent, manner. Normally, when a new version of a product is released, many larger companies must go through a formal process of testing and validation with their end-users and test compatibility with customized applications, which can delay the rollout by several months.

IBM has listened to many customer requests and has modified its software delivery strategy to effectively satisfy these increasingly demanding customer needs. The new delivery strategy is embodied in an offering called Software Choice.

This chapter describes the following items:

- Software Choice—the new mechanism for IBM workstation software delivery to customers.
- Software Choice Catalog Overview—a deeper look into the types of software available on the Software Choice Web page.
- Integrating Software Choice—a description of how to integrate Software Choice features into existing NetFinity, NetView Distribution Manager/2 and TME Software Distribution environments.
- Adding features to OS/2 Remote Initial Program Load (RIPL) clients.

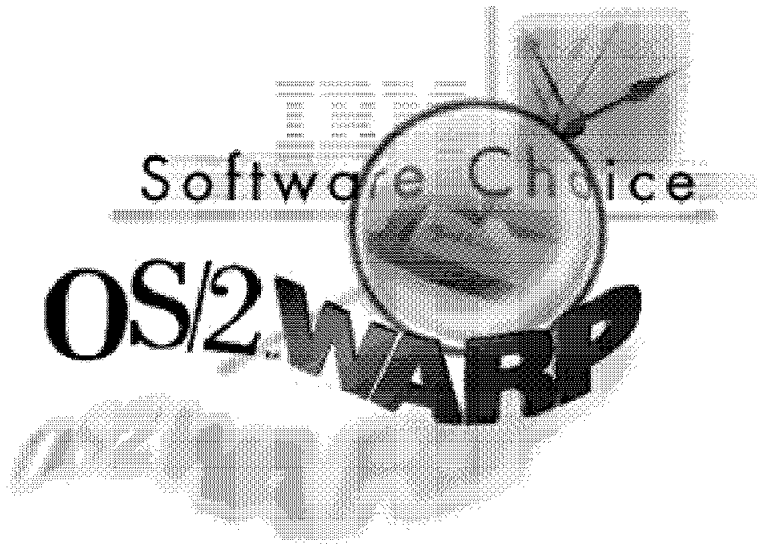


Figure 4. Software Choice Logo

2.2 Introduction to Software Choice

Software Choice is a new approach to providing early, easy access to features and updates in advance of the regular product releases. Initially, Software Choice offers new functionality for OS/2 Warp Version 4 and OS/2 Warp Server.

These software features and components are being released as manageable, "application-style" features to minimize implementation cost. Delivery of these features will be accomplished through the World Wide Web (WWW), which will speed up the general availability of the features. The alternative, diskette distribution, is more expensive and less productive, since most customers have some access to the WWW these days.

Some features are available for free to anyone with WWW access, and other features will be available on a subscription basis. The subscription-based features will also be accessible through the WWW to those customers who have purchased an eligible Upgrade Protection Option (UPO) under a Software Advantage contract or Strategic Account Offering.

All Software Choice features will also be distributed on a CD-ROM that will be released periodically. Eventually, these features will be integrated into

new-version shrinkwrap releases of products as appropriate. The Software Choice page begins at the following URL:

<http://www.software.ibm.com/os/warp/swchoice>

Refer to section 2.6, “Accessing the Software Choice Home Page” on page 29, for more specific pages within the Software Choice site. The full text of the Software Choice Announcement is available in the IBM announcement letter #297-133.

As shown in Figure 5, Software Choice can be integrated into an existing customer environment.

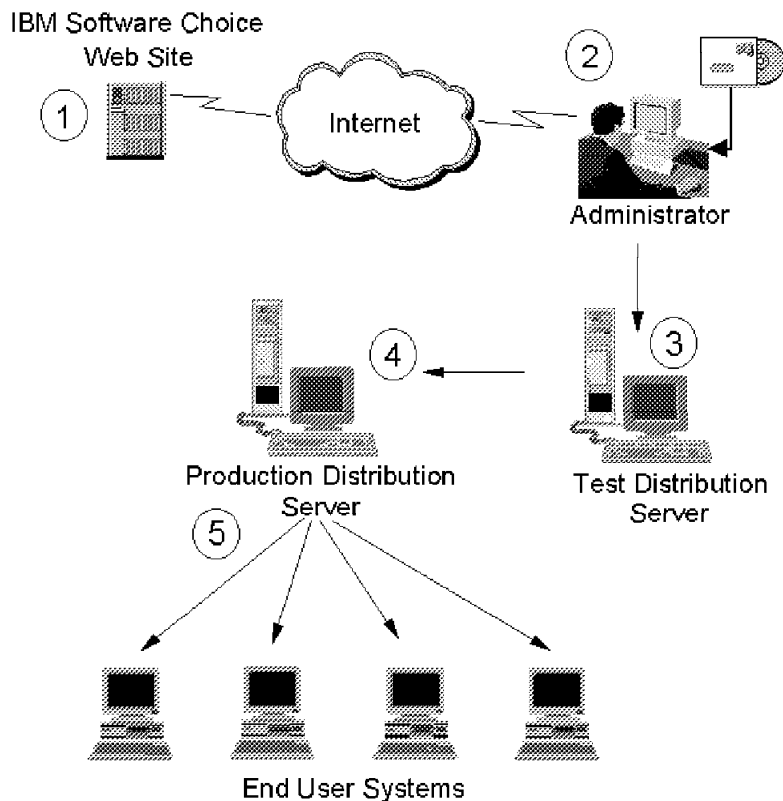


Figure 5. Software Choice Integration

The features available from the Software Choice Website can be downloaded and integrated into the existing enterprise software distribution infrastructure. An explanation of Figure 5 follows:

1. IBM develops a new component and places it as a free or subscription-based item in the Software Choice catalog.
2. Administrators access the Software Choice Website using any browser, such as Netscape Navigator or Microsoft Internet Explorer. Since only files are being downloaded, the operating system being used for the download can be Windows 95 or Windows NT even if OS/2 components are within the download files.

Since a CD-ROM is also distributed periodically, the administrator might also use this as an additional source of components to implement.
3. Usually, the administrators will want to put the new component on a test server and execute some sample scenarios to verify the new function and its compatibility with the customer application environment. The appropriate response files are created, and the component is prepared based on the type of software distribution manager, such as Tivoli Software Distribution, NetView Distribution Manager, or TME 10 NetFinity Software Distribution.
4. Once the component has passed the company's internal testing phase, the component is moved onto the production software distribution mechanism. This server schedules and installs the component onto the end-user systems.
5. The component is distributed to the target clients using one of the software distribution managers mentioned previously. The component is now installed on the end-user's system and is available for use.

2.3 Benefits

The key benefits of Software Choice are:

- Allows delivery of network computing capabilities for OS/2 on a "Web Year" schedule.
- Allows OS/2 users to move to network computing at their own pace.
- Delivers components when they are available rather than waiting for the next release.
- Concurrent availability world wide for all National Language Versions of a feature (some features may have only a subset of languages available).
- Reduces the cost of implementing network computing capabilities on OS/2.
- Delivered as "application-like" enhancements. No need to wait for and install a new version of the operating system to get a new feature.

- Ability to download and install desired features without downloading undesired features.

2.4 Items Available through Software Choice

The Software Choice home page will have more and more features over time. For 1997, many features are announced to be available through the Software Choice home page. This list is subject to change at any time, and the page may look different than the examples shown in Figure 6.

| <u>Feature</u> | <u>Shipment</u> | |
|---|-----------------|---------------|
| JAVA 1.0.2 | Free | 1Q 97 |
| Netscape Navigator 2.02 | Free | |
| Netscape Navigator Plug-in Pack | Free | |
| Neighborhood Browser Enabler for OS/2 Warp Server | Free | |
| Network Client for Windows 95 | Free | 2Q 97 |
| Coordinated Logon Client for Windows NT | Free | |
| Primary Logon Client for Windows NT | Free | |
| Enhanced Remote Access Support | Subscription | And beyond... |
| Java 1.1 | Subscription | |
| TCP/IP Enhancements | Subscription | |
| IBM Network Station Support | Subscription | |
| LDAP Support | Subscription | |
| PLUS ... | | |
| Hardware Support/DD Pak | | |
| Service Info/FixPaks | | |

Figure 6. Software Choice Features

2.5 Language Support

The features discussed in this redbook and the features actually available may differ in the number of language versions supported. Table 1 on page 28 shows all Software Choice supported languages as well as some features.

Table 1. Software Choice Language Support

| Languages Supported by Web Site | Neighborhood Enabler | Java 1.02 | Navigator 2.02 | Remote Access |
|--|-----------------------------|------------------|-----------------------|----------------------|
| English | Y | Y | Y | Y |
| French | Y | E | Y | Y |
| Canadian French | Y | E | Y | Y |
| German | Y | E | Y | Y |
| Italian | Y | E | Y | Y |
| Portuguese | Y | E | Y | E |
| Brazilian Portuguese | Y | E | Y | Y |
| Spanish | Y | E | Y | Y |
| Danish | Y | E | Y | Y |
| Dutch | Y | E | Y | Y |
| Finnish | Y | E | E | Y |
| Norwegian | Y | E | E | Y |
| Swedish | Y | E | Y | Y |
| Hungarian | E | E | E | E |
| Czech | E | E | E | E |
| Polish | E | E | E | E |
| Russian | E | E | E | E |
| Greek | E | E | E | E |
| Turkish | E | E | E | E |
| Arabic | E | E | E | E |
| Hebrew | E | E | E | E |
| Japanese | Y | E | Y | Y |
| Korean | Y | E | Y | Y |
| S. Chinese | Y | E | E | Y |
| T. Chinese | Y | E | E | E |
| Thai | E | E | E | E |

Note: Y indicates that the function is supported in that particular language. E indicates that the function is supported over the U.S. English base.

2.6 Accessing the Software Choice Home Page

This section describes the content of the Software Choice Website and how to access it. In doing so, we use the example of downloading and installing Java for OS/2.

There are a few levels in the hierarchy of information in the Software Choice Website. Instead of having a single home page, there is a Software Choice home page for each of the supported languages listed in Table 1 on page 28. For example, the Software Choice home page for U.S. English is:

http://service.boulder.ibm.com/asd-bin/doc/en_us/home.htm

A description of the levels follows:

1. IBM Software Choice Description Page (shown in Figure 7 on page 30) is available at:

<http://www.software.ibm.com/os/warp/swchoice>

This page provides a general description of Software Choice and also lists some of the features that are available from the catalog. If you have never accessed Software Choice before, you can visit this page to read some basic information about Software Choice. To go to the language selection page, click anywhere on the graphic in the bitmap near the top.

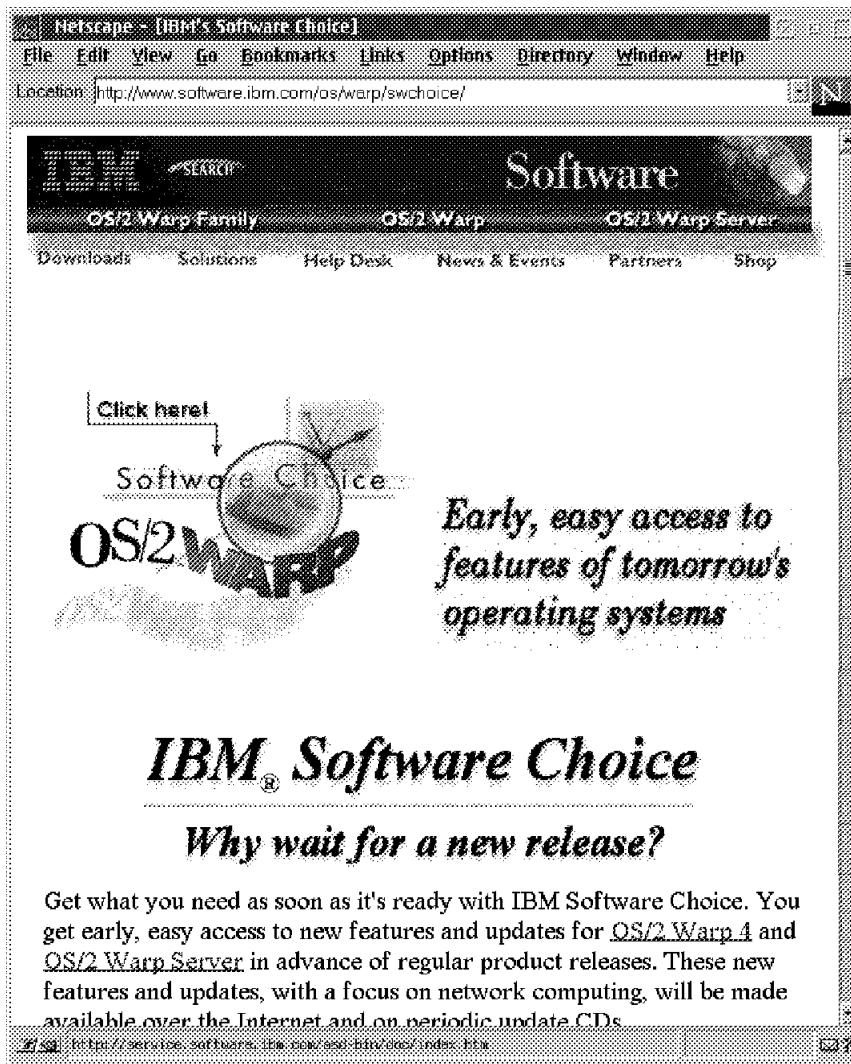


Figure 7. Software Choice Description Page

2. IBM Software Choice welcome page (shown in Figure 8 on page 31) is available at:

<http://service.software.ibm.com/asd-bin/doc/index.htm>

This page allows you to select your preferred language to read the Software Choice Web information. Select a language from the drop-down list box and click on the **GO** button to reach the Software Choice home page in that language.

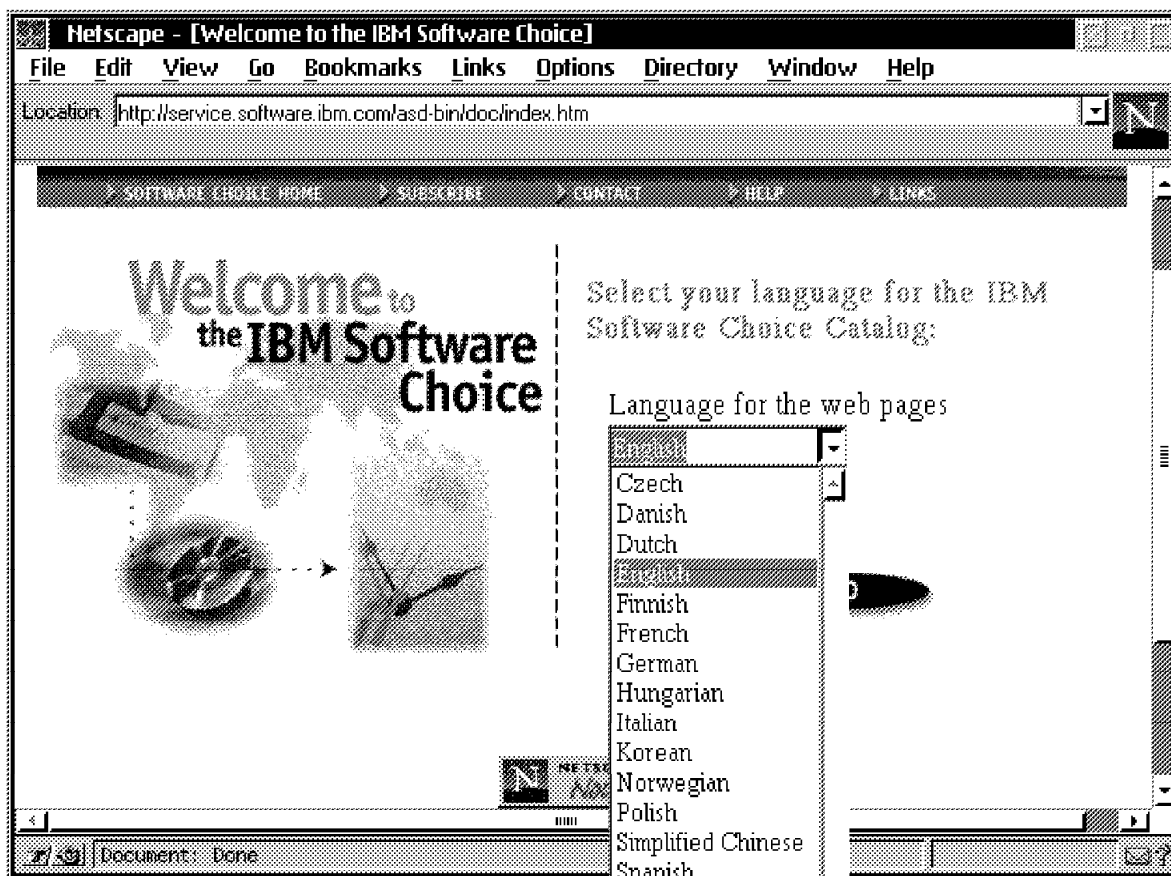


Figure 8. Software Choice Welcome Page

3. Software Choice home page (shown in Figure 9 on page 32) is available at:

http://service.boulder.ibm.com/asd-bin/doc/en_us/home.htm

The example shown is for U.S. English. The part in **bold** varies based on the language you selected. The Brazilian Portuguese home page, for example, is at:

http://service.boulder.ibm.com/asd-bin/doc/pt_br/home.htm

The home page has a link to the Software Choice catalog in your selected language. Click on the link called **IBM Software Choice Catalog** to view the list of features available for download.

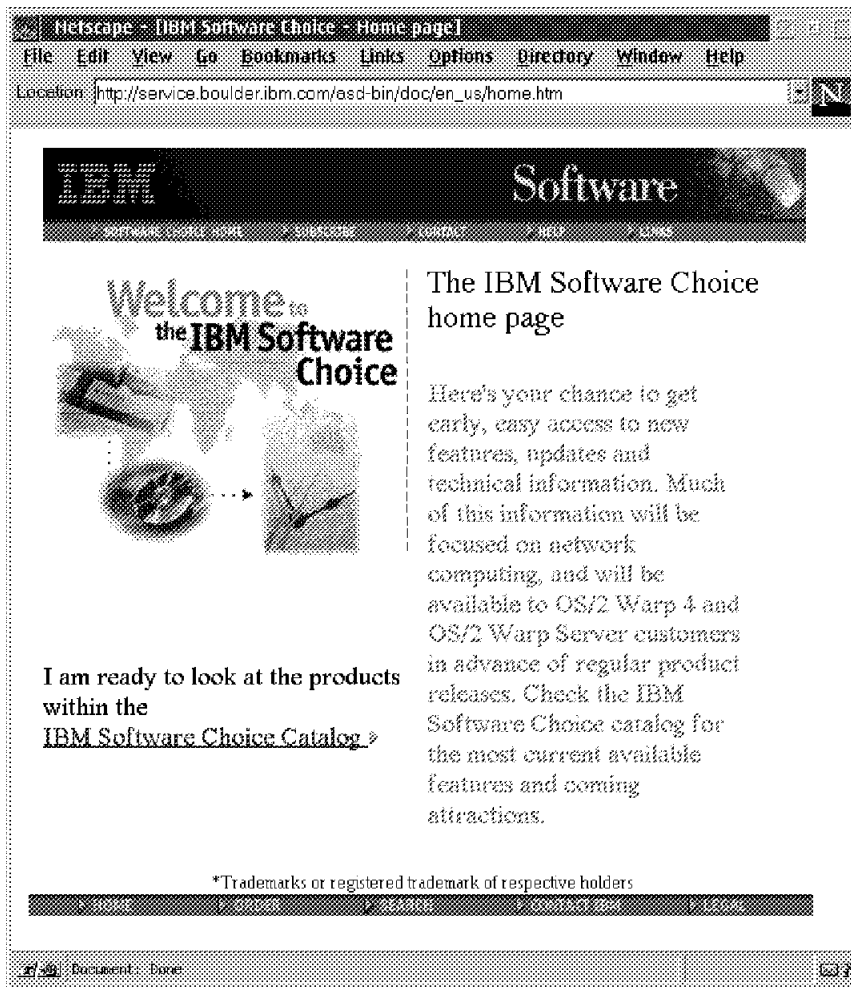


Figure 9. Software Choice Home Page

4. Software Choice catalog page is available at:

http://service.boulder.ibm.com/asd-bin/doc/en_us/catalog.htm

The example shown in Figure 10 on page 33 is for U.S. English. This page contains a list and the corresponding links to the latest Software Choice features that are available for download. You should place a bookmark in your browser for this page.

Note: You will reach the Software Choice catalog in the language you previously selected. This does not necessarily mean that the listed features are available in your selected language.

IBM employees can also reach the Software Choice home page inside the IBM firewall at the following URL:

<http://antero.boulder.ibm.com/asd-bin/doc>

Once your preferred language is selected, you will get the IBM internal Software Choice home page. Click on **IBM Software Choice Catalog** to see the list of features. IBM employees can download all Software Choice items, including subscription-based items. This is the page to add to your bookmarks.



Figure 10. Software Choice Catalog

Let's assume we are interested in the Java for OS/2 feature. To download this feature, we continue the steps we began in the previous pages. From the Software Choice Catalog, select **Java for OS/2**.



Figure 11. Software Choice Java for OS/2 Product Information

The product pages provide general information about the product and provide links to other pages for additional information, such as an overview, technical information, and so on. The information is described in Table 2.

| Table 2 (Page 1 of 2). Product Information Details | |
|--|--|
| Overview | Describes the enhancements contained in the feature and its major functions and may also include links to other areas for additional detail. |
| Technical information | Describes the functions in greater technical detail than the Overview and may also include links to other information. |
| Trademarks | Lists the trademarks for names used in the product and corresponding documentation. |
| Installation requirements | Lists the supported environments, hardware and software requirements, size of download file, and size of the decompressed file. |
| README | May describe the basic contents of the README file and how to access it, or may include the entire text of the README file, depending on the feature chosen, and may also include links to additional information. |
| Service and Support | Describes how the feature is supported and the means of contacting IBM to obtain such support and may include links to to a forum where the product is discussed. |

Table 2 (Page 2 of 2). Product Information Details

| | |
|----------|---|
| Download | Download the product. If the feature is available only on a subscription basis, you need to enter a user ID and password previously supplied to you by IBM. After agreeing to the license terms and selecting the desired language for the feature, you will see a download page with file information. |
|----------|---|

Clicking on **Download** shows you the license agreement for downloading and using the particular feature. The license agreement may differ depending on the product. Accepting the license agreement is a prerequisite for downloading and using the product.



Figure 12. Java for OS/2 License Agreement

Once you have accepted the license agreement, at the bottom of the page, click on **Yes, I agree with the license. Download this product**. You will be asked for the language of the feature to download.

As mentioned before, not all features are available in every language. For example, Java for OS/2 is available only in U.S. English. Select the desired language from the pull-down menu and click **GO**, as shown in Figure 13.

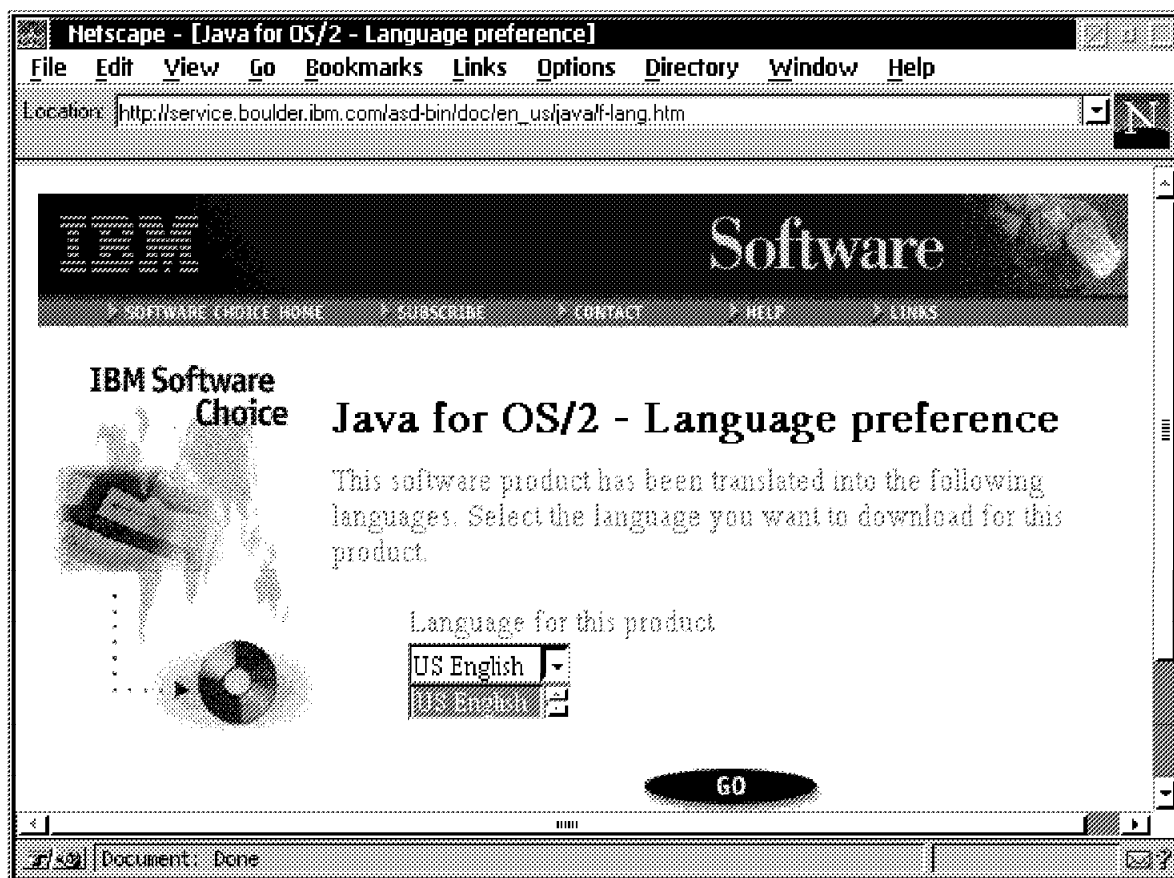


Figure 13. Java for OS/2 Feature Language Preference

You now see some information about the size of package you are going to download, a rough estimate of how long it the download might take, and a choice of servers (either FTP or HTTP) from where you can download the product. After selecting the target path, the product is downloaded to your system. Note that the process of downloading the product does NOT install the product. The feature is now available to be unzipped and installed. See section 2.10, "Software Choice Feature Installation - Java for OS/2" on

page 41, for more detailed information on installing Software Choice features.



Figure 14. Software Choice Java for OS/2 Download Page

2.7 Subscribing to Software Choice

Software Choice in general is accessible by everyone. All information is provided for free, as are many other pages of the IBM Warp Family home page.

Some features are protected by user ID and password, and the code is accessible only for customers with UPO and Software Advantage. Those customers should have received a user ID and password from IBM in the mail. However, anyone can read about these features, including all items

listed in Table 2 on page 34. Only the actual download from the FTP or HTTP server is restricted.

Subscription Changes

Although Software Choice subscription-based items originally required either a UPO or Software Advantage contract, a new two-year subscription offering is now available to those customers who do not have an active UPO or Software Advantage contract. Please refer to IBM Announcement Letter 297-332 for details.

Here are more specific details for UPO and Software Advantage customers:

- User IDs and passwords are provided to customers who purchased the appropriate upgrade protection prior to announcement, via letter, no later than May 30, 1997.
- Customers with existing Software Advantage contracts who sign new contracts prior to the expiration of their existing contract will not be issued a new user ID and password, but can continue to use the ones previously provided.
- New Software Advantage customers receive their user ID and password within 4-6 weeks of their UPO purchase (processing and mail lead times required by IBM and business partners involved). If a new customer has not received their user ID and password within 4-6 weeks, they should contact IBM or their Business Partner for resolution.
- Customers who know their user ID and password and need to change them for their own internal password controls requirements can do so online from the IBM Software Choice Website.
- Customers who have lost or forgotten their user ID or password can contact IBM (at the phone number referenced in the "Help" section of the IBM Software Choice Website) to have it reset. IBM will ship the customer a new user ID and password to the contact identified in their Software Advantage contract.
- After the first periodic CD-ROM has been shipped, new customers who sign Software Advantage contracts, and purchase an eligible UPO, will receive the most recently released periodic CD-ROM within 4-6 weeks of their UPO purchase.

2.8 Software Choice Scenarios and Integration

The following sections describe how Software Choice might be used by different types of users and also how to integrate Software Choice features

into an existing software distribution environment. We assume that the reader is familiar with the concepts and usage of some software distribution mechanisms, such as NetFinity Server, NetView Distribution Manager/2 and TME 10 Software Distribution.

An end user here is defined as anyone who downloads from the Software Choice home page for use on their own system. This person could be:

- A connected end-user at home
- A connected end-user in a company
- An administrator of a workgroup without any software distribution mechanism

A *Software Choice Administrator* is usually a person who downloads features to provide them to others as attended or unattended software modules which are distributed with some software distribution mechanism. Some examples are:

- Users who can install features by themselves using a shared drive
- Users who are asked about an installation during a LAN logon
- Attended or unattended installation using the LAN CID Utility
- Attended or unattended installation using NetView Distribution Manager for OS/2
- Unattended installation using NetFinity Server 4.0
- Unattended installation using TME 10 Software Distribution for OS/2

We assume that a valid user ID and password are supplied by the user if required for downloading from Software Choice. See section 2.7, "Subscribing to Software Choice" on page 37, for more information about this prerequisite.

Obtaining the software to download is described in section 2.6, "Accessing the Software Choice Home Page" on page 29. We assume that the user will supply a valid user ID and password if the Software Choice feature is a subscription-based item. Refer to section 2.7, "Subscribing to Software Choice" on page 37, for additional information on the prerequisites for obtaining a subscription.

The feature download steps are repeated here:

1. Open Netscape Navigator and go to www.software.ibm.com/os/warp/swchoice by entering this address in the location entry field.
2. Click on the Software Choice graphic to reach the catalog listing.

3. Click on **IBM Software Choice Catalog**.
4. Choose the language you will interact with in the Software Choice catalog and click on **GO**. This is independent from the available language versions of the particular feature you may be interested in.
5. Select the feature to download.
6. Carefully read all product information, such as the overview, installation requirements, and README files for special tips and instructions on where to unpack or how to install the feature.
7. Click on **Download** on the bottom of the information page.
8. Read through the license agreement.
9. When you have finished reading the license agreement, click on **Yes, I agree with the license. Download this product**.
10. Select the language for the feature to download and click **GO**.
11. Select the server download type (for example, FTP) from which you want to download the feature.
12. If required, enter the user ID and password, in the case of a protected feature.

2.9 Introducing Feature Installer

In the past, installation programs have been specifically designed to install only the components they were written for. Often, each time a new application or component is created, a new, customized installation program must be written, which can be inflexible and difficult to code. Each program may also need to handle the possibility of using response files and supporting an unattended installation process. All this leads to unnecessary complexity when developing installation programs.

Many of the Software Choice features use a common, flexible installation program called Feature Installer. In fact, the OS/2 Warp 4 product shipped the Feature Installer Runtime Version 1.0. Feature Installer is used by IBM developers to develop installation routines quickly and easily, with a common look and feel as well as support for unattended installation, response file support, and the capability to install a feature to a RIPL server. As an IBM customer, you don't need to be concerned with the technical details of implementing Feature Installer, but you will be happy to see a familiar interface when you install a Software Choice feature that incorporates it. The interface for Feature Installer is the Netscape Navigator Browser. For example, the Java for OS/2 installation shown in Figure 15 on

page 43 is a Feature-Installer-developed installation program that uses the Netscape Navigator interface.

2.9.1 Hardware Prerequisites

Hardware requirements are the same as those needed to run OS/2 Warp Version 3.0 or higher and the Netscape Navigator for OS/2 Version 2.02 browser.

A mouse is recommended to interact with Netscape Navigator plug-ins. Refer to the appropriate documentation for hardware requirements.

2.9.2 Software

Feature Installer 1.0 (Runtime only) is included in OS/2 Warp Version 4. The latest version (1.11 as of 3Q 97) is available on the Software Choice Website. This latest version replaces the shipped version and also runs on OS/2 Warp Version 3. To install some of the Software Choice features, the following components are required:

- OS/2 3.0 or higher
- Netscape Navigator for OS/2 2.02 or higher
- Feature Installer Runtime (latest version)
- Feature Installer plug-in Runtime Dynamic Link Library (DLL) and support files
- Package file for installation

For more detailed information on using Feature Installer, refer to the IBM redbook titled *Remote Installation of OS/2 Warp 4 using CID*, SG24-2010.

2.10 Software Choice Feature Installation - Java for OS/2

In section 2.6, "Accessing the Software Choice Home Page" on page 29, we described how to access Software Choice and download features, using Java for OS/2 as an example. This section continues the example by describing the process for a graphical, attended installation of Java on an OS/2 system. As mentioned before, this feature uses the Feature Installer mechanism for its installation.

Once the feature has been downloaded, it can be stored on the local hard drive or on a server's hard drive where it can be accessed by the user. The following steps describe the actual installation:

1. Open an OS/2 Window.

2. Change to the subdirectory where the Java ZIP file, JAVA111.ZIP, is located. In our example, the ZIP file is in the C:\TEMP directory.
3. Unpack the ZIP file using any OS/2 utility that supports ZIP files. PKUNZIP2 is usually available from the \IBMCOM directory. Use the -D option to properly unpack any subdirectories that are included in the ZIP file. Type the following:

```
[c:\temp]PKUNZIP2 -d JAVA111.ZIP
```
4. Be sure to peruse the README file that is included in the package.
5. Run the installation program described in the README file (for example, INSTALL.EXE).

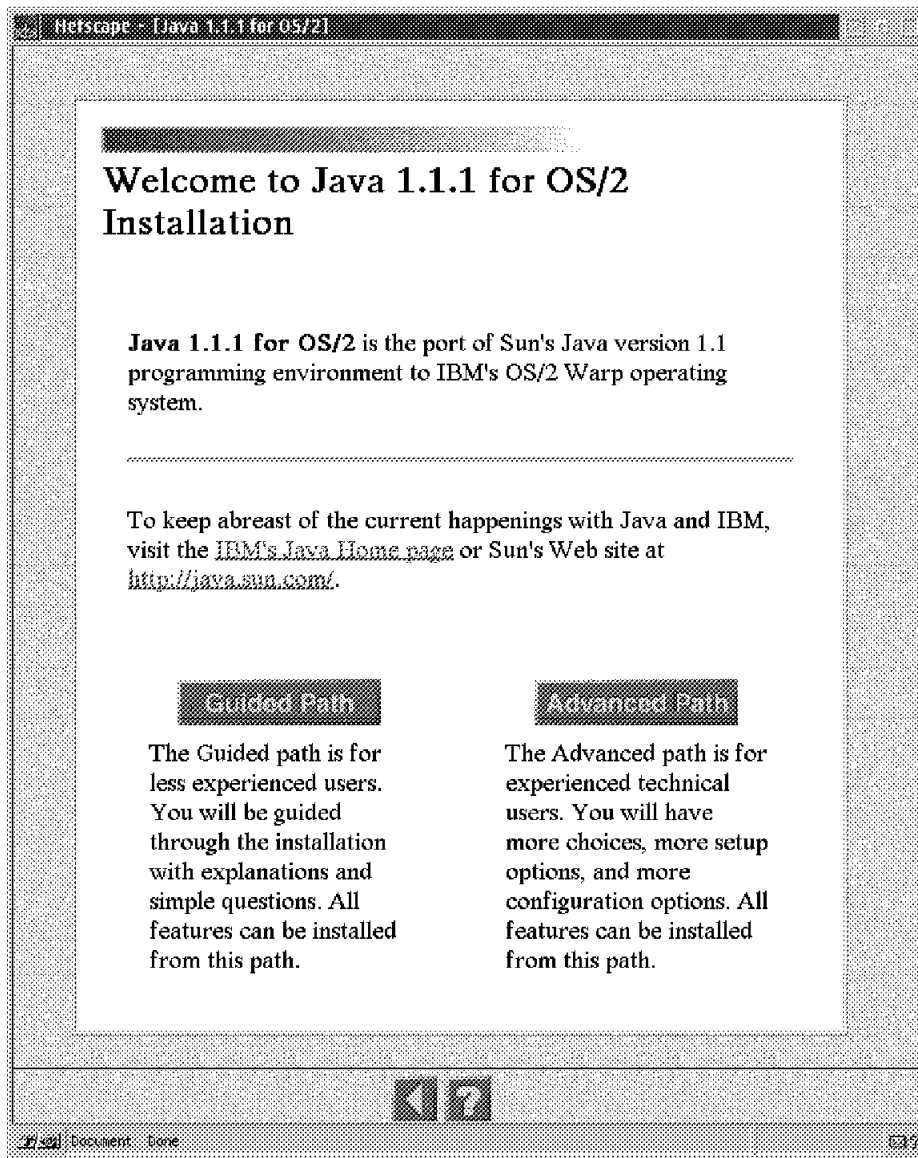


Figure 15. Java for OS/2 Browser-based Installation

The INSTALL.EXE program, shown in Figure 15, begins the installation process for the Java for OS/2 feature. This program was developed using the Feature Installer and uses the familiar Netscape browser interface for the graphical, attended installation. There are options for a Guided Path for less experienced users and an Advanced Path for technical or experienced users.

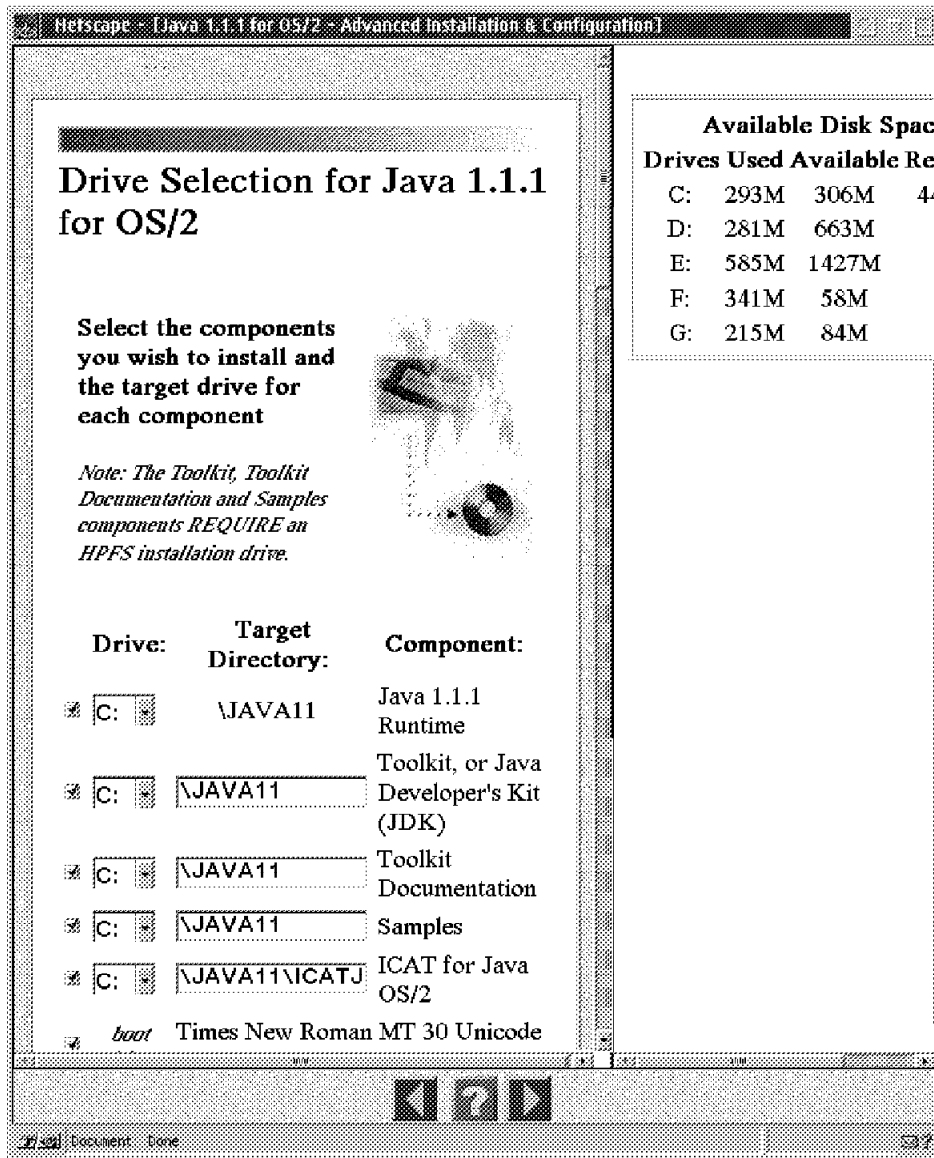


Figure 16. Java for OS/2 Advanced Path Installation

Figure 16 shows the Advanced Path installation panel that allows the user to specify many of the parameters to be used for the Java installation, such as the default installation directory, C:\JAVA11. The remainder of the installation process is straightforward and is not described here. After the installation completes, you are prompted to stop your applications and shut down the system to reboot it.

2.11 Integration with TME 10 NetFinity Server for OS/2 4.0

The following sections describe how to integrate Software Choice software components with the TME 10 NetFinity Server for OS/2.

2.11.1 Introduction

TME 10 NetFinity Server 4.0 is a component of the OS/2 Warp Server SMP Feature, released in late 1996. IBM offered a special promotion for customers who purchased OS/2 Warp Server Advanced, making a copy of OS/2 Warp Server SMP available to them at no charge. Ask your IBM Sales Representative if this program is still applicable.

The software distribution function of TME 10 NetFinity Server 4.0 is based on IBM SystemView for OS/2, and other parts of the server are based on NetFinity, which was developed by the IBM PC Company. After the acquisition of Tivoli, all SystemView products have been merged into TME 10 products, and responsibility was transferred to the Tivoli group. Tivoli's TME 10 software distribution framework is the strategic software distribution platform that IBM customers should consider for the future.

Many OS/2 Warp Server customers chose to implement the TME 10 NetFinity Server because of its power and connectivity. Many functions are integrated, such as:

- Remote Workstation Control
- Hardware and Software Inventory
- Software Distribution
- License Management
- AntiVirus Protection
- Alert Processing
- Event Scheduling
- Controlling a wide variety of vital product data

2.11.2 Prerequisites

Both the Software Distribution Server and the Software Distribution Client must be installed as a minimum.

Note: TME 10 NetFinity Server for OS/2 4.0 does not support the installation of a client without an existing operating environment (also known as a pristine client). This function is expected to be in a future version of Tivoli Software Distribution for OS/2.

The following examples utilize the TME 10 NetFinity Server at the service level shown in Figure 17 on page 46:

```
C:\SYSVIEW2\BIN\SYSLEVEL.SAC
TME 10 NetFinity Server Administrator Console
Version 4.00      Component ID 569728801
Type OS/2
Current CSD level: XR00003
Prior   CSD level: XR00000

C:\SYSVIEW2\BIN\SYSLEVEL.SDO
Software Distribution Object Preparation
Version 4.00      Component ID 569728801
Type OS/2
Current CSD level: XR00003
Prior   CSD level: XR00000

C:\SYSVIEW2\BIN\SYSLEVEL.SDS
Software Distribution Server
Version 4.00      Component ID 569728801
Type OS/2
Current CSD level: XR00003
Prior   CSD level: XR00000
```

Figure 17. TME 10 NetFinity Server SYSLEVEL Information

2.11.3 Integration

Each Software Choice downloadable feature should have a set of files specific to each software distribution platform.

For the TME 10 NetFinity Server software distribution mechanism, the only file required is the Application Definition File. The ADF file specifies:

- How to set up the install image in the code server directory structure (usually)
- How to install the program
- How to remove the program

Note: The TME 10 NetFinity Server searches only the \SYSVIEW2\SWLIB directory for existing ADF files.

To integrate, for example, Java for OS/2 into your current TME 10 NetFinity Server software distribution environment, follow these steps:

1. Unpack **JAVAOS2.EXE** by executing it.

2. Copy **JAVA.ADF** from the download directory to the TME 10 NetFinity Server directory, \SYSVIEW2\SWLIB\.
3. Copy **JAVARESP.RSP** from the download directory to your Response file directory, \CID\RSP\JAVA102\.
4. Copy all other files from the download directory to your CID install image \CID\IMG\JAVA102\.
5. In the Response file directory, make a copy of the default Response file, and edit it for your specific needs. For example, a Response file for a full installation (FULL.RSP) or a Response file for just runtime installation (RUNTIME.RSP).

An example Response file called FULL.RSP is shown in Figure 18.

```
*-----
* Define the target directories.
*-----
FILE=C:
*-----
* Include a COMP keyword for every component in the package file.
* JAVATLKT and JAVASMPPL require HPFS logical drives to install properly.
* If you install them on a FAT drive no files will be copied to the
drive for those components.
*-----
COMP=OS/2 Java Runtime
COMP=OS/2 Java Toolkit
COMP=OS/2 Java Samples
*COMP=OS/2 Java DBCS Support
*-----
* The following 4 keywords are required. See the Software Installer
* Reference for possible values.
*-----
CFGUPDATE=AUTO
OVERWRITE=YES
SAVEBACKUP=NO
DELETEBACKUP=NO
```

Figure 18. Java for OS/2 Response File

6. In the TME 10 NetFinity Server Service Manager, double-click on CID Software Preparation (shown in Figure 2 on page 10).
7. Double-click on **Software Library**.
8. Create a new Software Library entry by selecting the **Software** menu pull-down and selecting **New**, as shown in Figure 19 on page 48.

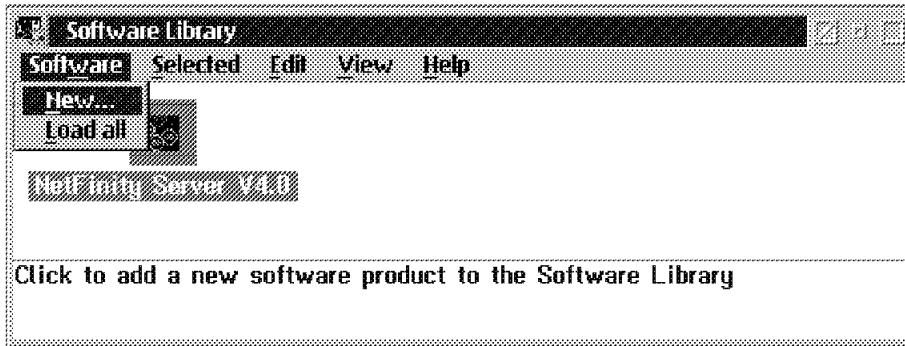


Figure 19. TME 10 Netfinity Server New Software Library Entry

9. The next panel, shown in Figure 20, asks for the name of the software entry, such as Java for OS/2 1.02. The Definition file can be found by using the Find button, which automatically jumps to \SYSVIEW2\SWLIB\.
- To add the new library entry, click on **Add**. A short message tells you that the software was successfully defined.

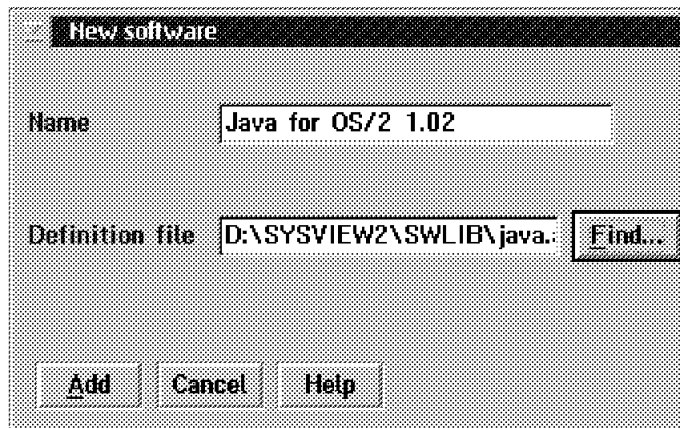


Figure 20. Software Library Entry Name and Definition File

10. Open the new Software Library entry, **Java for OS/2 1.02**, by double-clicking on it.
11. Create a new configuration. Some possible options are:
 - Full installation, including runtime, samples and toolkit
 - Only runtime
 - Runtime and samples

To do so, click on the **Configuration** pull-down menu item and then select **New**, as shown in Figure 21 on page 49.

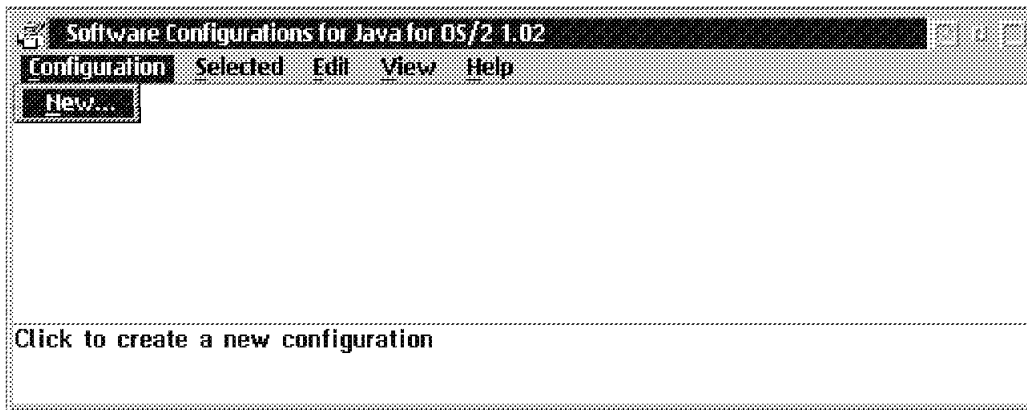


Figure 21. Software Library New Configuration

12. In the configuration panel shown in Figure 22 on page 50, enter the following:

| | |
|----------------------------|--|
| <i>Configuration name</i> | Java Full Installation |
| <i>Configure for</i> | Base Product (Refresh) |
| <i>Configure as</i> | Using Code Server stored Response file |
| <i>Catalog information</i> | Check the button |

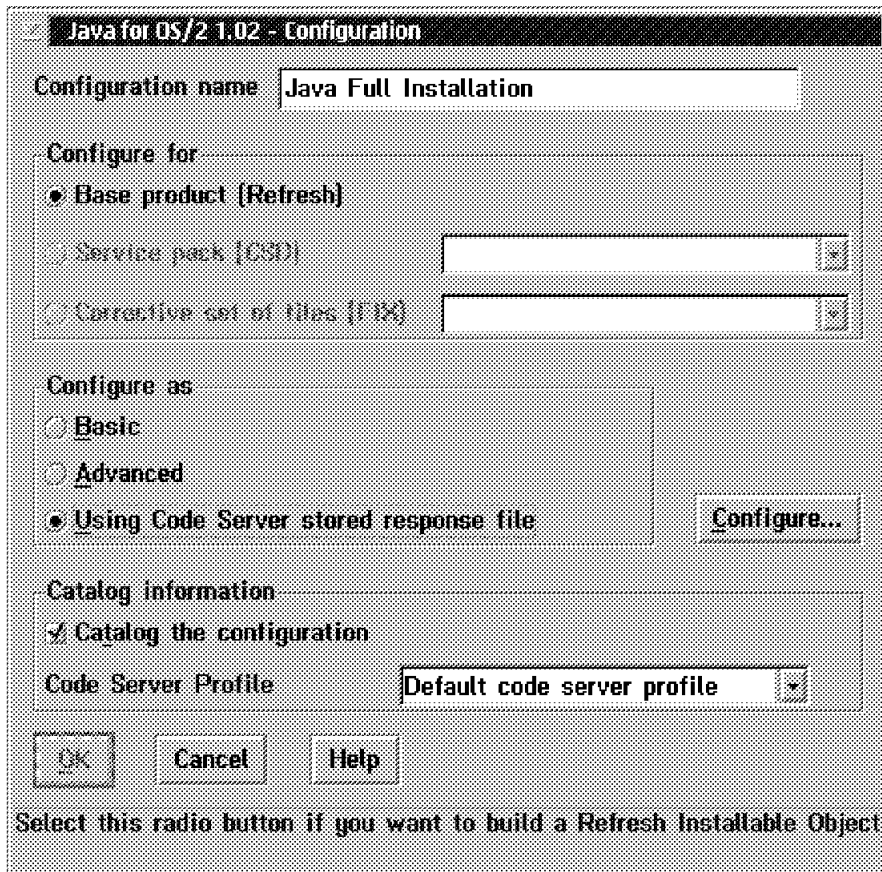


Figure 22. Java for OS/2 Configuration Panel

13. Click on **Configure...** to define installation subdirectories and the matching Response file for this configuration.

The predefined subdirectories are the name of the product in the ADF file. Change it if you have other names, or leave it to accept the default. The Response file name (shown in Figure 23 on page 51) can be entered with or without the extension, but it must be, if entered, RSP. Leaving the entry field empty forces TME 10 NetFinity Server to look for a Response file with the same name as the target workstation, for example CLIENT32.RSP for the target, CLIENT32. This can be helpful if you have a product that is workstation-dependent, such as TCPIP (without DHCP and DDNS of course). To always distribute the same configuration, you would define a default Response file, such as FULL.RSP.

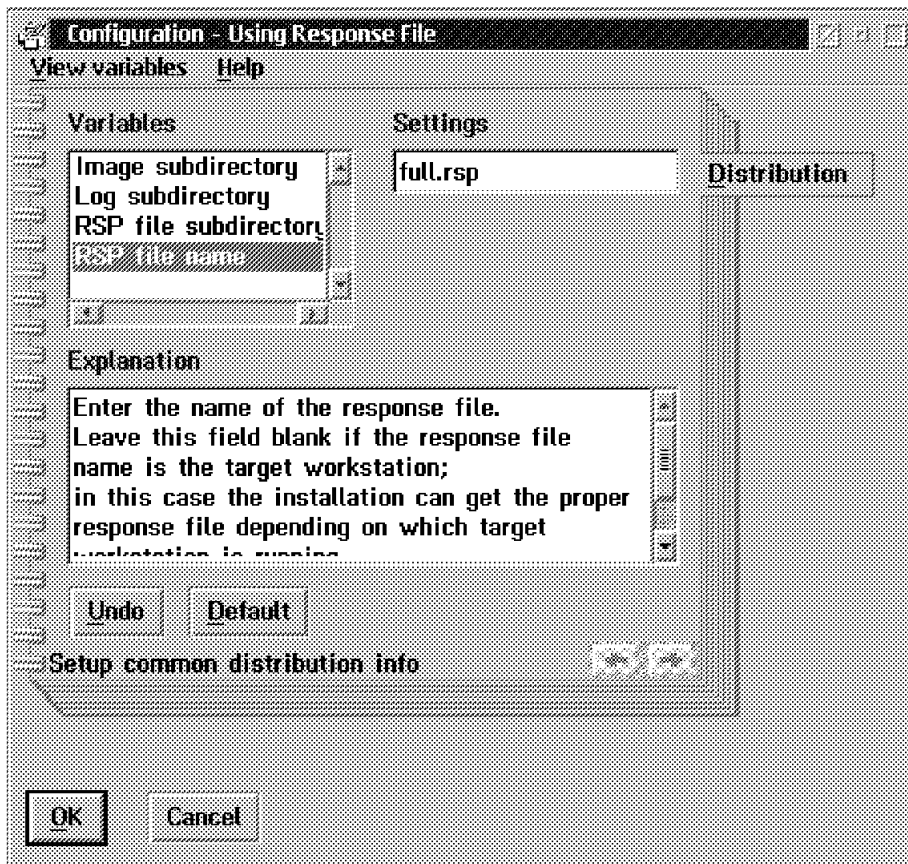


Figure 23. Configuration with Code Server Response File

14. Click on **OK** to close the Code Server Response file window.
15. Click on **OK** to catalog this configuration. A progress indicator will appear.
16. Close all CID Software Preparation windows. Your configuration is now ready to be distributed.

2.11.4 Distribution

To distribute this new Java package, follow these steps:

1. Select the Event Scheduler from TME 10 NetFinity Server Services Manager. The panel shown in Figure 24 on page 52 will appear.
2. Click on **New**.
3. Enter a name for the event, for example Java Full Install.

4. Select **Software Distribution** from the list of tasks.

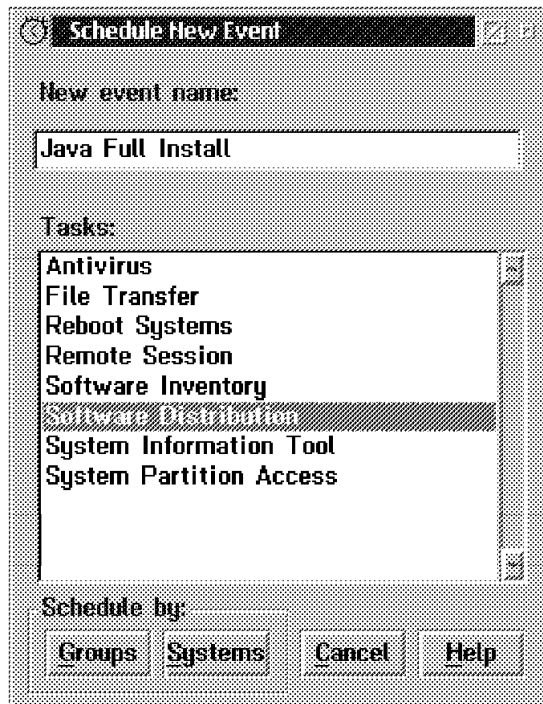


Figure 24. Schedule New Event

5. Now you must decide if you will install to individual systems or to predefined groups of systems. Click on either **Groups** or **Systems** to select to target workstations for the installation.

Using the Systems button, you are able to select individual systems according to the addresses found in a Remote Systems Manager group that was created before this installation. *Group* selection is valid only to all the members of a predefined group of systems. Individual members of a group can't be deselected.

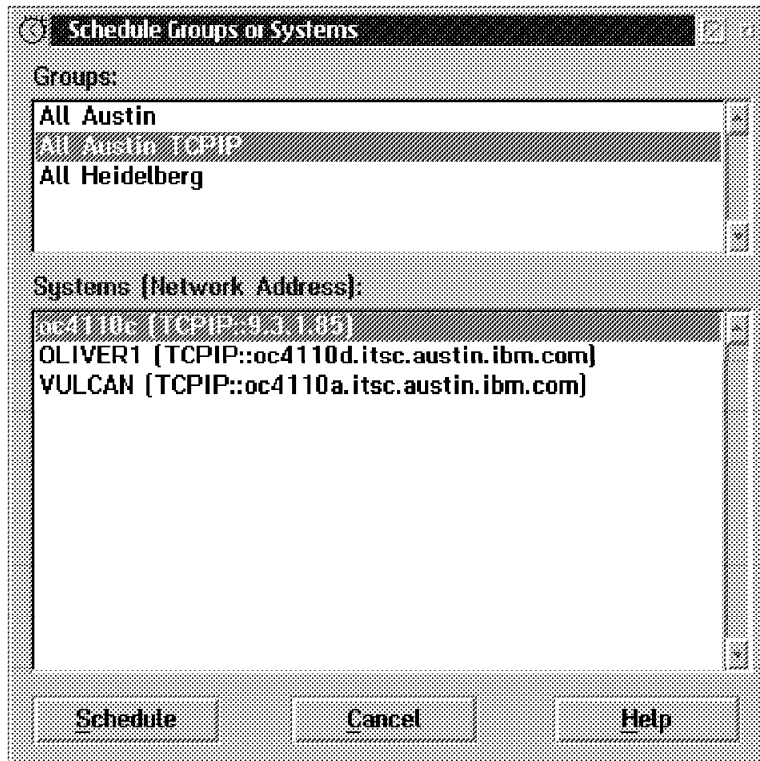


Figure 25. Schedule Targets

6. Click on **Schedule**. The Software Distribution Catalog is loaded.

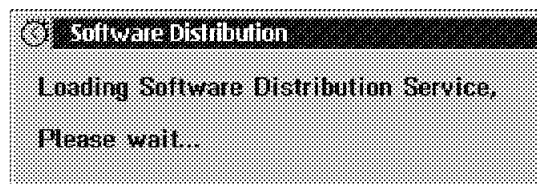


Figure 26. Schedule - Software Distribution Catalog

7. Select **Software Products** from the Scheduler - Software Distribution Groups.
8. Select **Full installation** and click on **Selected** and then choose **Install**.

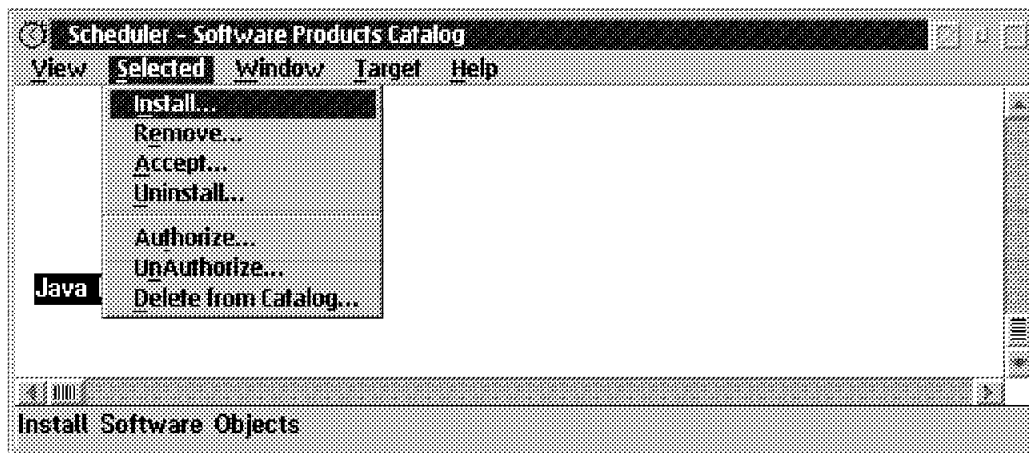


Figure 27. Schedule Install

9. Click on **Save** on the next panel to save and activate.
10. Select your desired method of distribution in the Schedule Date and Time field, or just click on **Save** to accept the default for an immediate, one time distribution.

Schedule Time and Date

Schedule Frequency

☒ One-Time
 ☐ Weekly
☐ Hourly
 ☐ Monthly
☐ Daily
 ☐ Yearly

Schedule Date and Time

Day of Week: Tuesday
 Week of Month: 3rd week
 Day of Month: *
 Month: May
 Year: 1997
 Time: Hrs Mins
 * *

Time

| | | |
|----------|------------|----------|
| Current: | 20.05.1997 | 22.53.28 |
| Next: | 20.05.1997 | 22.54.00 |

Figure 28. Schedule Date and Time

The complete installation process is logged in the file \SYSVIEW2\FNDLOG, in Figure 5 on page 25.

```

1997/05/09 08:51:37 NFSSRV99                    56 FNDCM030I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 :
Received an Install request for file IBM.JAVA10.JAVA1000.REF.010002.US_EN.
1997/05/09 08:51:38 NFSSRV99                    56 FNDCM022I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : The Alter-Active-Component option is Yes
- processing request in the Active Area.
1997/05/09 08:51:38 NFSSRV99                    56 FNDCM052I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : The Removability option is No
- no backups will be made.
1997/05/09 08:51:39 NFSSRV99                    56 FNDCM032I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : Installing change file
IBM.JAVA10.JAVA1000.REF.010002.US_EN.
1997/05/09 08:51:52 NFSSRV99                    56 FNDC0028I:
Program cidmount SRVIFS F: G: IFSSRV99 CODESRV LOG executed successfully
exit status 0.
1997/05/09 08:51:52 NFSSRV99                    56 FNDCM015I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : Calling CM Driver:
FNDCIDI C:\SYSVIEW2\WORK\rrstatus.
1997/05/09 08:51:57 NFSSRV99                    66 FNDC0015I:
Task fndcidi has pid 66.
1997/05/09 09:08:32 NFSSRV99                    56 FNDC0028I:
Program FNDCIDI C:\SYSVIEW2\WORK\rrstatus executed successfully
exit status 0.
1997/05/09 09:08:32 NFSSRV99                    56 FNDCM351I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : Program 'F:\IMG\JAVA102\INSTALL.EXE
/X /NMSG /O:DRIVE /R:F:\RSP\JAVA102\FULL.RSP
/L1:G:\LOG\JAVA102\NFSSRV99.L1
/L2:G:\LOG\JAVA102\NFSSRV99.L2
/S:F:\IMG\JAVA102 /A:I'
terminated successfully with return code '0000'.
1997/05/09 09:08:32 NFSSRV99                    56 FNDC0016I:
Task fndcidi has returned with return code 0.
1997/05/09 09:08:34 NFSSRV99                    56 FNDC0028I:
Program cidunmnt SRVIFS F: G: executed successfully
exit status 0.
1997/05/09 09:08:34 NFSSRV99                    56 FNDCM033I:
fndadmn NFSSRV99 8 0 N/A NFSSRV99 : Installed change file
IBM.JAVA10.JAVA1000.REF.010002.US_EN successfully.
1997/05/09 09:08:34 NFSSRV99                    56 FNDCM034I:
fndadmn NFSSRV99 8 0 N/A NFSSRV99 : IBM.JAVA10.JAVA1000.REF.010002.US_EN
and any corequisites were Installed successfully.

```

Figure 29 (Part 1 of 2). TME 10 NetFinity Server Logfile

```

1997/05/09 09:08:35 NFSSRV99          56 FNDDB001I:
Added or changed Target Parameters record.
1997/05/09 09:08:35 NFSSRV99          56 FNDRB053I:
Configuration for target NFSSRV99 has been updated.
1997/05/09 09:08:36 NFSSRV99          54 FNDSH010I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 : Install succeeded on
IBM.JAVA10.JAVA1000.REF.010002.US_EN.
1997/05/09 09:08:38 NFSSRV99          54 FNDDB001I:
Added or changed Change Management Status record.
1997/05/09 09:08:39 NFSSRV99          54 FNDRS015I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 :
Completed database updates for Install report.
1997/05/09 09:08:41 NFSSRV99          57 FNDRQ108I:
@fndadmn NFSSRV99 8 0 N/A NFSSRV99 :
Received successful Install report.
1997/05/09 09:08:42 NFSSRV99          57 FNDDB001I:
Added or changed Target Subrequest record.
1997/05/09 09:08:43 NFSSRV99          57 FNDDB001I:
Added or changed Server Subrequest record.
1997/05/09 09:08:45 NFSSRV99          57 FNDDB001I:
Added or changed Subrequest record.
1997/05/09 09:08:45 NFSSRV99          57 FNDRQ147I:
fndadmn NFSSRV99 8 0 N/A NFSSRV99 :
Install request completed successfully.

```

Figure 29 (Part 2 of 2). TME 10 NetFinity Server Logfile

2.12 Integration with NetView Distribution Manager for OS/2 2.11

The following sections describe how to integrate Software Choice software components with NetView Distribution Manager for OS/2 2.11.

2.12.1 Introduction

NetView Distribution Manager for OS/2 is one platform-specific implementation of software distribution. Others include NetView Distribution Manager for AIX and NetView Distribution Manager for MVS.

NetView DM/2 is used by many companies around the world, and its evolution over 10 years gave NetView DM/2 a solid install base. Eventually, full NetView DM/2 functionality will be part of the TME software distribution products.

Just like the TME 10 NetFinity Server, NetView DM/2 is a GUI-driven product, but with several important features:

- Ability to do pristine installations

- Install history per product or workstation
- Command-line interface available for all tasks
- Use of DB2/2 for an exhaustive history and logging database

2.12.2 Prerequisites

NetView Distribution Manager for OS/2 requires Database 2 for OS/2 (DB2/2) Version 1.2 or greater. Older versions of NetView DM/2 (SYSLEVEL XR20466 and below) require a fix installed on top of DB2/2 2.1.

The following example uses NDVM/2 at the following SYSLEVEL:

```
C:\IBMNDVM2\SYSLEVEL.NDM
IBM NetView DM/2 Change Distribution Manager
Version 2.10.1      Component ID 562143900
Current CSD level: XR00005
Prior   CSD level: XR00002

C:\SQLLIB\SYSLEVEL.CE2
IBM DB2 Client Application Enabler for OS/2
Version 2.10      Component ID 562212900
Type 32-bit
Current CSD level: WR08000
Prior   CSD level: WR08000

C:\SQLLIB\SYSLEVEL.SQC
IBM DB2 for OS/2 Single-User
Version 2.10      Component ID 562204401
Type 32-bit
Current CSD level: WR08000
Prior   CSD level: WR08000
```

Figure 30. NetView DM/2 SYSLEVEL Information

2.12.3 Integration

As discussed earlier, each Software Choice feature includes its own set of files for different software distribution mechanisms.

To distribute software with NetView DM/2, you need to build a change file using the GUI. This requires a profile that you easily build.

These steps integrate our example, Java for OS/2, into the NetView DM/2 environment:

1. Unpack **JAVAOS2.EXE** by executing it.
2. Create a NetView DM/2 profile by using the information provided by the ADF file. For more information about NetView DM/2 Profiles, refer to the NetView DM/2 documentation or to the redbook titled *The CID Guide*, SG24-4295.

A profile for our Java example, JAVA.PRO, is shown in Figure 31.

```

TargetDir=C:\JAVAOS2

Section Catalog
Begin
    ObjectType=Software
    GlobalName=IBM.JAVAFULL.INST.REF.1.02
    Description="Install Procedure for Java for OS/2 (Full Package)"
End

Section Install
Begin
    Program = SA:\IMG\JAVA102\INSTALL.EXE
    Parms= /X /NMSG /O:DRIVE /A:I /S:${SourceDir}
/R:${ResponseFile} /L1:${logfile1} /L2:${logfile2}
    SourceDir= SA:\IMG\JAVA102
    ResponseFile = SA:\RSP\JAVA102\FULL.RSP
    Logfile1=SB:\LOG\JAVA102\$(WorkStatName).L1
    Logfile2=SB:\LOG\JAVA102\$(WorkStatName).L2
End

```

Figure 31. Java for OS/2 Profile

3. Copy JAVA.PRO from the download directory to your Profile directory, \CID\PRO\JAVA102\.
4. Copy JAVARESP.RSP from the download directory to your Response file directory, \CID\RSP\JAVA102\.
5. Copy all other files from the download directory to your CID install image, \CID\IMG\JAVA102\.
6. In the Response file directory, copy the default Response file to your site-specific Response file and edit it. For example, a Response file for a complete installation (FULL.RSP) or a Response file for just a runtime installation (RUNTIME.RSP).

An example of FULL.RSP is shown in Figure 18 on page 47.

7. Open the NetView DM/2 Change Manager Catalog window.

8. Select **File** and then **Build from profile**.
9. As shown in Figure 32, enter the full path and filename for your profile, JAVAFULL.PRO in the Change file profile entry field, and enter a change file name, for example JAVAFULL.CHG, in the Target file entry field.
10. Press the **Build** button to start the catalog process. Press **OK** after reading the information message that the profile contains only an install section and also for the message that the build process is complete. You will find a new catalog entry in the NetView DM/2 CDM Catalog window.

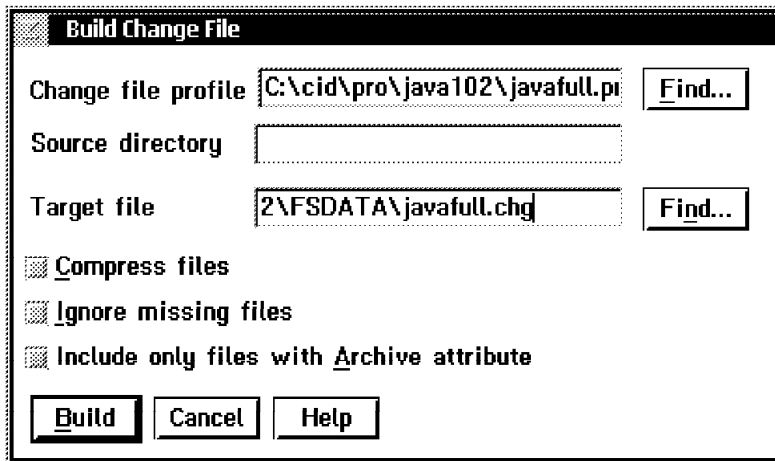


Figure 32. Catalog a Profile

2.12.4 Distribution

To distribute this newly-created package, follow these steps:

1. Highlight the catalog entry **IBM JAVAFULL.INST.REF.1.02** in the NetView DM/2 CDM Catalog window.
2. Click on **Selected** and then on **Install** and select one of the following:
 - **No Force** for a first time installation
 - **Force** for a reinstallation

No Force looks to the install history first to point out all possible workstations, which do not have this product installed. *Force* ignores the current installation status and shows you all NetView DM/2 workstations. Having a large catalog can cause several minutes of scanning using *No Force*, but it can save you from installing a product twice or from a failed installation because of a running product.

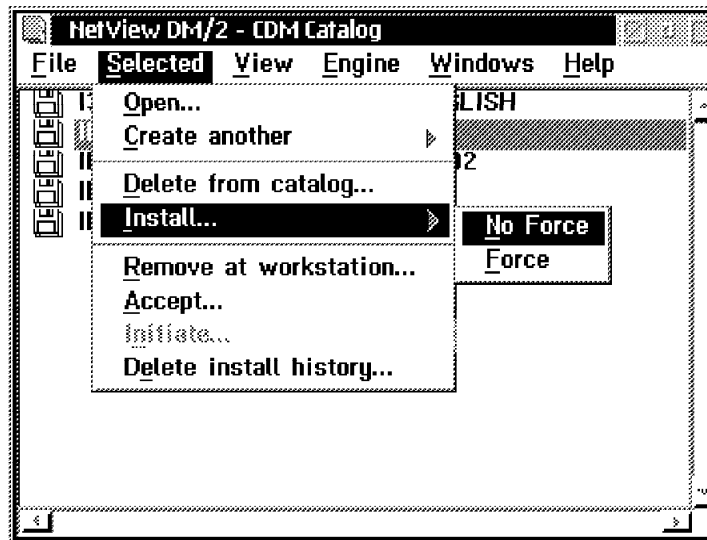


Figure 33. Install a Change File

3. Select the target workstations, reorder the products if necessary, and if you desire, you can install more than one product.
4. Click on **Install** to install the change file immediately, or click on **Schedule** to select a specific future date and time for installation. You can click on **Options** to change the install options, such as:
 - Disk Area to install to
 - Removable or not
 - Check target disk space before installation
 - Corequisite group if more than one change file
5. Open the NetView DM/2 Requests status window to see the installation process being executed.
6. Open the NetView DM/2 Local Message Log to see installation results.

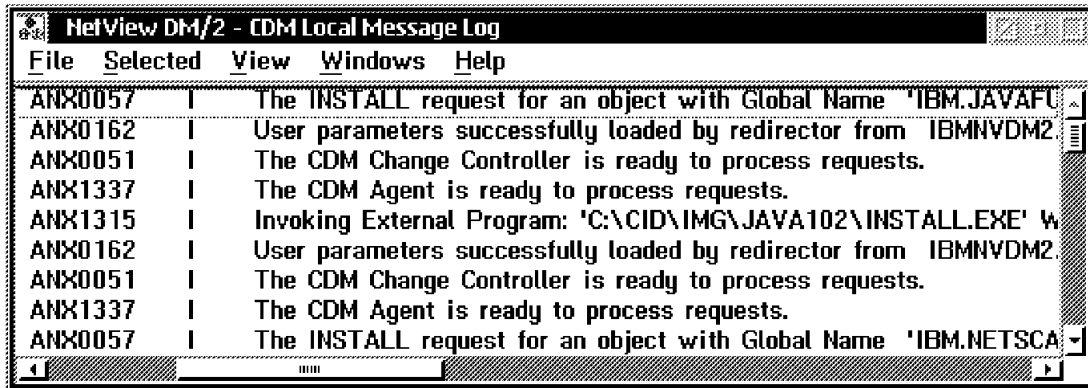


Figure 34. NetView DM/2 Local Message Log

2.13 Integration with Tivoli Software Distribution for OS/2

The following sections describe how to integrate Software Choice software components with the TME 10 Software Distribution for OS/2.

2.13.1 Introduction

TME 10 Software Distribution for OS/2 is the follow-on product for NetView DM/2, and it is integrated with the TME strategy. In fact, looking at SD/2, you can see many similarities with TME 10 NetFinity Server.

2.13.2 Prerequisites

In contrast to NetView DM/2, DB2/2 is not necessary for the installation of Software Distribution for OS/2. You can install Software Distribution for OS/2 3.1.3 with no prerequisites. For our example, we installed the following components:

- Software Distribution Server
- Software Distribution Server GUI
- Software Preparation GUI
- Software Distribution Documentation

To determine which version of Software Distribution for OS/2 you are running, you can:

- Look at the Software Distribution Workstation Discovery to find out the version of your Installation, or look at the file \SOFTDIST\FNDSWINV:

```
#IBM Software Distribution for OS/2 inventory discovery file
GLOBAL NAME:  TIVOLI.TME10.SWDS.313.OS2SERVER.REF.1.0.US
DESCRIPTION:  Tivoli TME 10 Software Distribution for OS/2
```

- See the SYSLEVEL information by using the SYSLEVEL command. Our example uses Drop 3 of May 1997.

```
C:\SOFTDIST\bin\SYSLEVEL.FND
Tivoli TME 10 Software Distribution for OS/2
Version 3.01.3      Component ID 5639B0600
Current CSD level: XR21382
Prior   CSD level: XR21052
```

Figure 35. Software Distribution for OS/2 SYSLEVEL Information

2.13.3 Integration

As discussed earlier, each Software Choice feature includes its own set of files for different software distribution mechanisms.

Software Distribution for OS/2 requires an ADF file to build a change file using the Software Preparation GUI.

The following steps integrate our example, Java for OS/2, into the Software Distribution for OS/2 environment:

1. Unpack **JAVAOS2.EXE** by executing it.
2. Copy **JAVA.ADF** from the download directory to the Software Distribution Server directory, \SYSVIEW2\SWLIB\.
3. Copy **JAVARESP.RSP** from the download directory to your Response file directory, \CID\RSP\JAVA102\.
4. Copy all other files from the download directory to your CID install image, \CID\IMG\JAVA102\.
5. In the Response file directory, copy the default Response file to your site-specific Response file and edit it, for example a Response file for a full installation (FULL.RSP) or a Response file for just a runtime installation (RUNTIME.RSP).

For an example of FULL.RSP, see Figure 18 on page 47.

6. Open the Software Preparation folder, and then open the CID Software folder.
7. Log on as Administrator or Builder if necessary.
8. Open the Software Library Folder.
9. Click on **Software** and then on **New**.

10. The next panel asks you for a description, for example Java for OS/2 1.02. The definition file can be found by using the Find button, which automatically searches the \SYSVIEW2\SWLIB directory.
11. Click on **Add** to register the software.
12. Open the new Software Library entry, Java for OS/2 1.02, by double-clicking on it.
13. To create a new configuration, click on the **Configuration** menu item and select **New**, as shown in Figure 36.

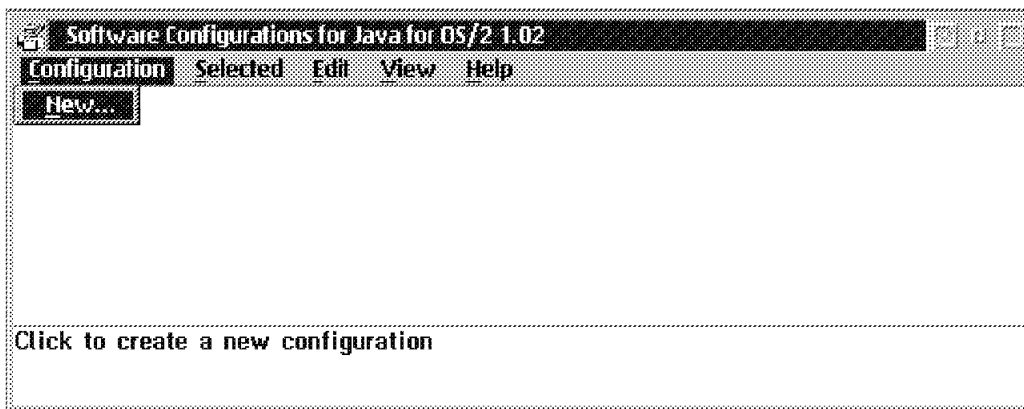


Figure 36. Software Library New Configuration

14. In the panel that appears, enter:

| | |
|----------------------------|--|
| <i>Configuration name</i> | Java Full Installation |
| <i>Configure for</i> | Base Product (Refresh) |
| <i>Configure as</i> | Using Code Server stored Response file |
| <i>Catalog information</i> | Check Catalog the configuration |
15. Click on **Configure** to define installation subdirectories and the matching Response file for this configuration.
 The predefined subdirectories are the name of the product in the ADF file. Change it if you have other names, or leave it to accept the default. The Response file name can be entered with or without the extension, but it must be, if entered, RSP. Leaving the entry field empty forces the Software Distribution Server to look for a Response file with the same name as the target workstation, for example CLIENT32.RSP for the target, CLIENT32. This can be helpful if you have a product that is workstation-dependent, such as TCP/IP (without DHCP and DDNS of

course). To always distribute the same configuration, you need to define a default Response file, such as FULL.RSP.

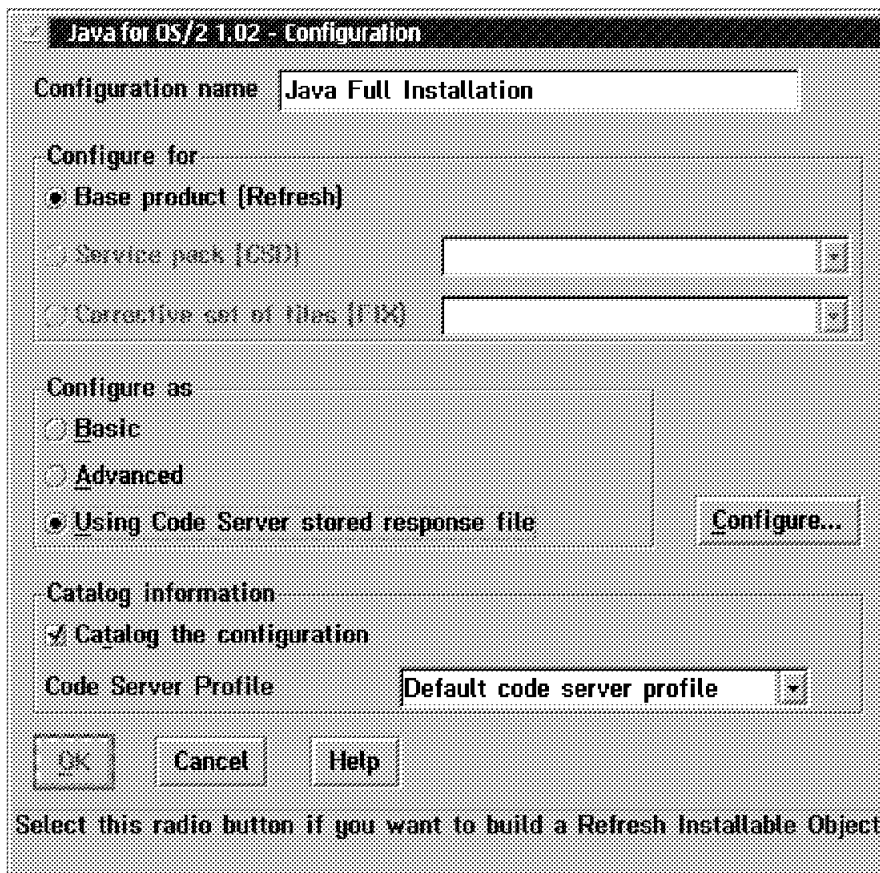


Figure 37. Configuration with Code Server Response File

16. Click on **OK** to close the Code Server Response file window.
17. Click on **OK** to catalog this configuration. A progress indicator is shown.
18. Close all CID Software Preparation windows. Your configuration is now ready to be distributed.

2.13.4 Distribution

To distribute our Java example, follow these steps:

1. Open TME 10 Software Distribution.
2. Log on as Administrator.
3. Select **IBM.JAVA10.JAVA1000.REF.010002.US_EN** from the main panel.

Note: You may double-click the entry to see more details.

4. Select **Selected** and then **Install**, similar to the example shown in Figure 33 on page 61.
5. Select your target system(s), as shown in Figure 38.

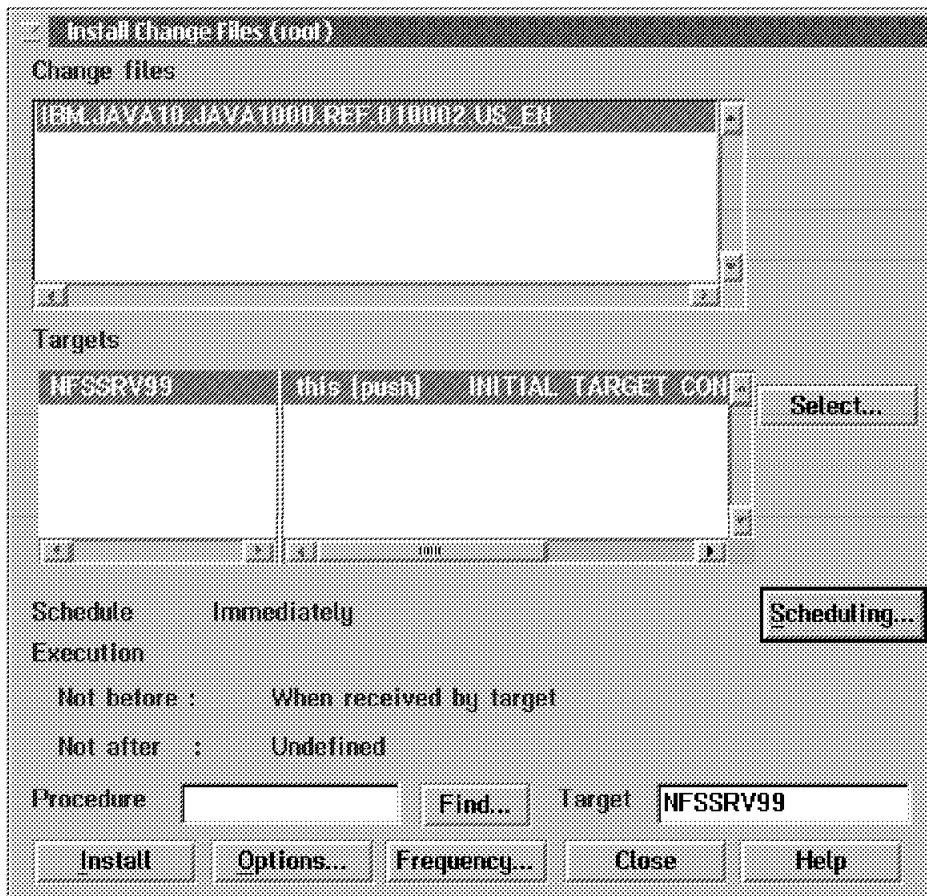


Figure 38. SD/2 Install Change File

6. Click on the **Schedule** button (as shown in Figure 39 on page 67) to specify scheduling details:
 - Date and Time for transmission
 - Date and Time for execution - not before
 - Date and Time for execution - not after
 - Time format: either server time or target time
 - High priority execution
 - Set execution on hold until a release event is transferred

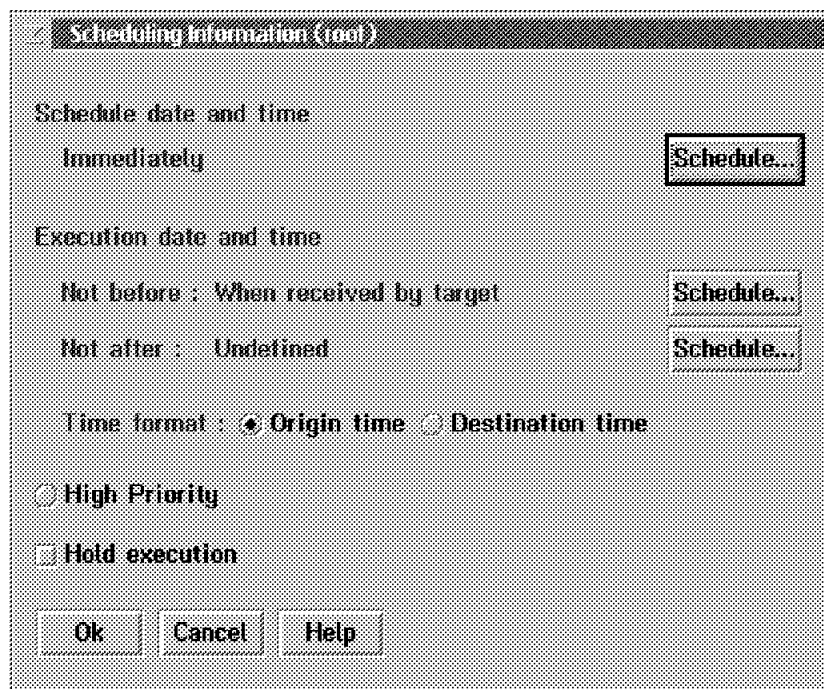


Figure 39. SD/2 Schedule Install Change File

7. Click on **OK** to close Schedule window. You will return to the panel shown in Figure 38 on page 66.
8. Click on the **Options** button at the bottom for additional installation options:
 - Install requiring activation (Reboot after installation)
 - Install removable (Keep a prior version)
 - Automatically accept install
 - Install as corequisite (if multiple files packages selected)
 - Ignore current status of change file (reinstalled even if package is already installed on target)
 - Force installation (do not look in SD/2 catalog)
 - Extend File System
 - Perform disconnected at Mobile Client
 - Hold on server until execution time for mobile client
 - Conditions
9. Click on **OK** to close the Schedule window.
10. Click on **Install** to release the installation request.
11. Click on **OK** in the message window.

12. Close the Install Change File window.

2.14 Installing Features to RIPL Clients

In the new era of Network Computing, an existing function, Remote Initial Program Load (RIPL), has received renewed importance. The RIPL process is essential for thin clients—that is, those clients who receive their operating system and applications directly from a server. The RIPL function in OS/2 Warp Server is described in great detail in the IBM redbook titled *Inside OS/2 LAN Server 4.0*, SG24-4428.

Many of the features listed in the Software Choice Catalog can also be used by OS/2 RIPL clients. There is a special procedure to install a feature that was created with the Feature Installer (and thus installs with the Netscape interface) to the RIPL client.

The following steps describe the procedure of installing a feature to a RIPL client:

1. On the server, type GENFIRPL at a OS/2 command prompt. The following parameters are required:

Parameter Description

| | |
|------------|--|
| /M: | Media path name where the feature is installed from |
| /R: | Path name of the RPL directory (C:\IBMLAN\RPL) |
| /U: | Path name of the RPLUSER directory (C:\IBMLAN\RPLUSER) |
| /F: | Name of the feature response file to be converted |
| /C: | Name of the client to create feature updates for |
| /B: | Client boot drive |

Notes:

- a. The client system must not be running when GENFIRPL is executed on the server.
- b. Only one GENFIRPL command can be run per client.
- c. Do not install the feature on the server if you want to use the server to install the same feature on a RIPL client.

The following example demonstrates how to use GENFIRPL:

```
genfirpl /m:c:\fismppkg\feature1 /r:c:\ibmlan\rpl /u:c:\ibmlan\rpluser  
/f:c:\fismppkg\feature1\feature1.rsp /c:ccc /b:z:
```

The GENFIRPL command creates a server Response file and a client Response file. The tasks that can only be performed by the server, such

as CONFIG.SYS updates and file creation, are added to the server Response file, FILES.RSP. The tasks that are performed on the client, such as object creation and class registration, are included in the client response file.

2. After running GENFIRPL, you must update the .FIT file on the server, which maps the directory access for the client system. Add the following line to the .FIT file:

```
Z:\OS2\INSTALL\INSTALL.INV \\SSS\WRKFILES\CCC\OS2\INSTALL\INSTALL.INV
```

where SSS represents the name of the RIPL server, and CCC represents the name of the RIPL client.

3. Log on as the administrator of the server, and type the following at an OS/2 command prompt:

```
CLIFI /A:I /R:C:\FILES.RSP
```

Be sure to specify the correct path name for FILES.RSP. The CLIFI command updates the .FIT file entry by adding the access that is necessary for the client to execute the application being installed and the appropriate .INI file entry to the client's .INI file.

4. On the client system, type the following at an OS/2 command prompt:

```
CLIFI /A:I /R:Z:\FEATURE1.RSP
```

where Z: is the boot drive and FEATURE1.RSP is the name of the client Response file. The CLIFI command creates the inventory object for the feature on the client system. The CLIFI command is described in more detail in the IBM redbook titled *Remote Installation of OS/2 Warp 4 using CID*, SG24-2010.

5. On the client system, type the INSTALL command. Complete the installation by following the instructions provided with the Netscape Navigator installation interface.

2.14.1 Removing Features from RIPL Clients

Software Choice features that have been installed onto RIPL clients directly using an install object can also be uninstalled. Feature Installer, the installation program for most Software Choice features, can also uninstall software packages that have been installed using the Feature Install plug-ins and the Netscape Navigator interface. The uninstallation removes all configuration changes and deletes the files and objects that were installed with the software package.

Software is uninstalled by selecting **Uninstall** from the inventory object's pop-up menu. To uninstall specific features only, open the inventory object

in tree view and select the features to uninstall by placing a check mark in the feature's checkbox.

Note: When removing a feature, it should first be removed from the client and then from the server.

Chapter 3. IBM Enhanced Remote Access for OS/2 Warp Server

This chapter describes the IBM Enhanced Remote Access Connection Server for OS/2 Warp Server Version 5.1. This is an enhancement to the Remote Access Services Connection Server—an optionally installable networking component of OS/2 Warp Server. However, unlike previous releases of OS/2 LAN Distance and Remote Access Services, there is no Remote Client version, but existing PPP clients can be used.

This chapter describes how this component may be installed, configured, used, and supported. We also describe some of the functions by using a simple scenario.

We also discuss configuration and use of various client machines, such as Windows 95 and OS/2.

It is assumed that you have an understanding of basic LAN concepts and terminology. For more detailed information about IBM Enhanced Remote Access for OS/2 Warp Server, refer to the online documentation that was supplied with OS/2 Warp Server, or refer to section 3.8, “IBM Enhanced Remote Access PPP Internal Architecture” on page 139.

3.1 Enhancements

For those users who are already familiar with the IBM Remote Access Services component supplied with OS/2 Warp Server, the major enhancement in IBM Enhanced Remote Access for OS/2 Warp Server is the addition of Point-to-Point Protocol (PPP) support. See section 3.2, “Overview and Concepts” on page 72, for more information about PPP support.

The following components are either new or modified to support PPP clients:

| | |
|------------------------|--|
| PPP component | A new component, responsible for processing PPP frames. |
| CHAP support | Challenge Handshake Authentication Protocol is defined by the PPP extension RFC 1334. This is used to verify the identity of the client at connect time. |
| MACFH component | The lowest level VLAN subcomponent, which during the connection phase gives the incoming PPP frame to the new PPP component for processing. When in runtime phase, MACFH |

| | |
|---------------------|---|
| | handles PPP encapsulation, PPP decapsulation, and adds a MAC header to the frame. |
| IP Router | This router allows PPP clients to have TCP/IP protocol stacks on a IBM Enhanced Remote Access virtual adapter. TCPBEUI is also supported over the IP connection. |
| WCLLOCAL.INI | The local configuration information for the IBM Enhanced Remote Access Connection Server workstation now includes a PPP section. These parameters are read when the Connection Server starts and they determine how PPP clients will get operating parameters for TCP/IP when they connect. |
| WCLIPADR.INI | A new configuration file on the IBM Enhanced Remote Access Connection Server, which contains the IP addresses to be allocated to PPP clients when the parameter ObtainIPAddr=LIST is configured in WCLLOCAL.INI. |

There are no new modem configuration (.PIF) files included with this release.

The above enhancements have been made to IBM Enhanced Remote Access Connection Server for OS/2 Warp Server; however, there have been no changes to the existing Remote Access Services client code. LAN Distance, Remote Access Services, and PPP Remote Clients can now establish connections to the IBM Enhanced Remote Access Connection Server for OS/2 Warp Server workstation.

The SYSLEVEL of the IBM Enhanced Remote Access is IPx8605 (in the U.S., it is IP08605), and the version is 5.1.

3.2 Overview and Concepts

This section discusses the various environments in which IBM Enhanced Remote Access Connection Server for OS/2 Warp Server can be configured. We also discuss client support, including new support for PPP Clients.

3.2.1 IBM Enhanced Remote Access Environments

The IBM Enhanced Remote Access Connection Server for OS/2 Warp Server product supports four different types of remote LAN access:

1. **Remote-to-remote:** Two remote systems can establish a WAN connection. A typical application of this method is where a traveling

employee needs to access their office workstation from a remote location. A remote client can have up to two simultaneous incoming remote connections.

2. **LAN-to-LAN:** You can establish a connection between two Connection Servers. In this situation, the two servers form a bridge between the two LANs.
3. **LAN-to-remote:** LAN-attached workstations can request the Connection Server to establish a connection with a remote workstation.
4. **Remote-to-LAN:** This scenario is probably the most common use of IBM Enhanced Remote Access. This solution allows users to access LAN resources from remote locations, such as their home, while visiting customers or while traveling.

This method also allows the IBM Enhanced Remote Access Connection Server for OS/2 Warp Server to be installed as a stand-alone server, supporting up to 128 remote workstations (a maximum of 64 PPP connections). No LAN hardware is necessary on the Connection Server, only WAN adapters. The remote workstations can access all the resources at the server. This may be suitable to allow file sharing for a small, remote workgroup.

Note: Callback is not supported on PPP clients. For more information about client restrictions, see section 3.3, "System Requirements" on page 76.

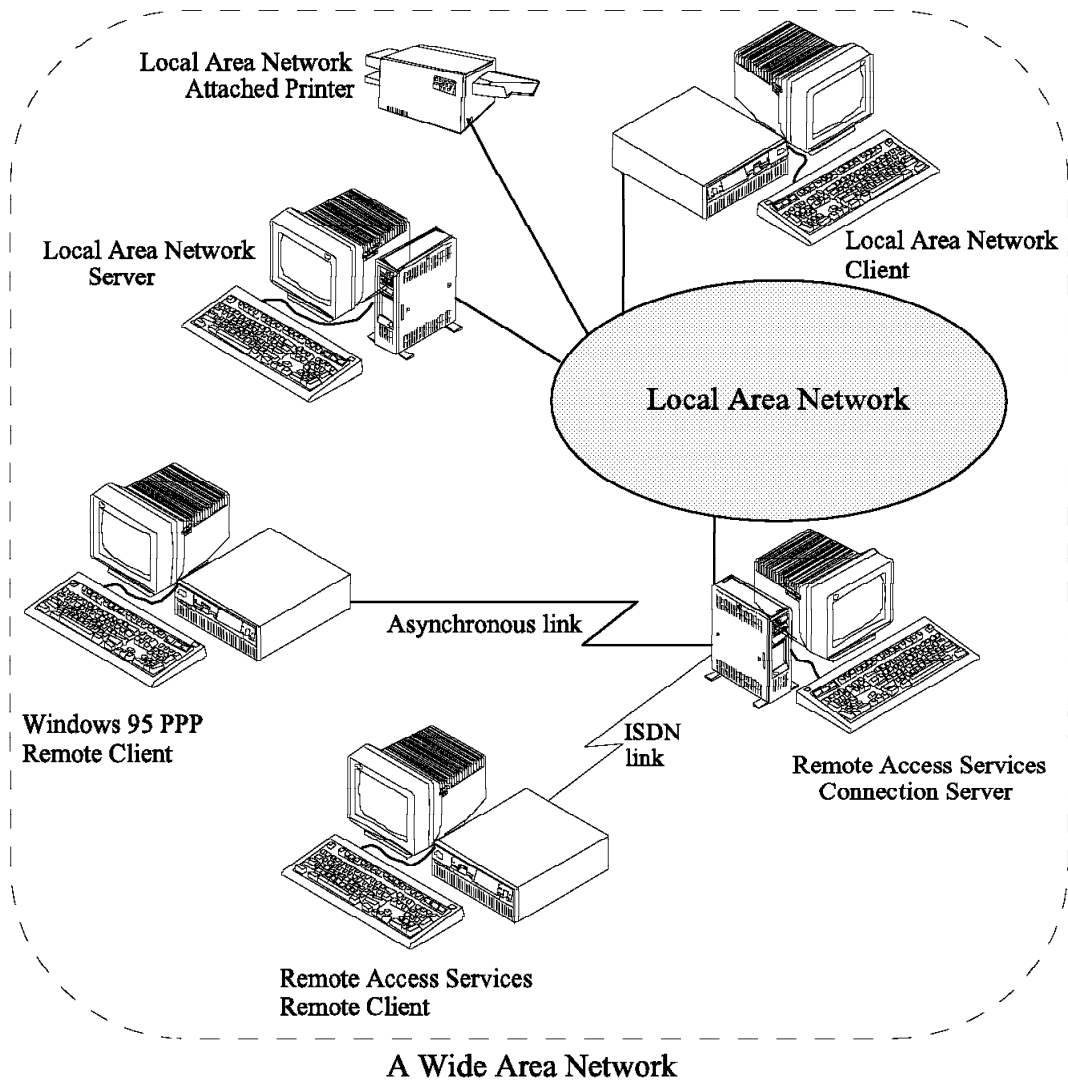


Figure 40. Common IBM Enhanced Remote Access Environments

Figure 40 shows a typical Remote-to-LAN scenarios. The Connection Server provides an interface for the OS/2 Remote Client and Windows 95 (or Windows NT) Remote Client to the LAN. Both clients can access printers and other devices on the LAN.

Notice that a Wide Area Network (WAN) is formed by the connection of the LAN-connected Connection Server and Remote Client. The LAN can either

be token-ring or Ethernet. Windows 3.1 or 3.11 Remote Access Services Remote Clients cannot use synchronous or ISDN links.

3.2.2 PPP Support

IBM Enhanced Remote Access Connection Server for OS/2 Warp Server adds Point-to-Point Protocol (PPP) support. PPP is recognized throughout the networking industry as a standard method for connecting a variety of hosts, bridges, and routers from one or more vendors.

Note: PPP is defined by the Internet Engineering Task Force (IETF) in Request For Comments (RFC) 1661.

IBM Enhanced Remote Access Connection Server for OS/2 Warp Server dynamically accepts calls from PPP clients whose LAN applications use the TCP/IP protocol. This is in addition to accepting calls from LAN Distance and Remote Access Services remote clients.

Support for Challenge Handshake Authentication Protocol (CHAP), as defined by PPP extension RFC 1334, has been added. CHAP is used to authenticate all PPP clients using an integrated database. Previous releases of LAN Distance and Remote Access Services only supported the Two Party Authentication Protocol (TPAP). TPAP will continue to be used to authenticate existing LAN Distance and Remote Access Services clients.

IBM Enhanced Remote Access Connection Server for OS/2 Warp Server now supports the TCP/IP protocol over PPP connections as well as IEEE 802.2, TCP/IP, IPX and NETBIOS over LAN Distance and Remote Access Services client connections.

This provides the capability for an IBM Enhanced Remote Access Connection Server to accept calls from, connect to and interoperate with any workstation that supports Point-to-Point Protocol and requires the TCP/IP protocol.

3.2.3 Client Support

The IBM Enhanced Remote Access Connection Server for OS/2 Warp Server supports multiple concurrent sessions of up to 128 clients, in any combination of:

- Up to 64 concurrent PPP connections
- Up to 128 concurrent Remote Access Services or LAN Distance Remote Clients.

The following clients have been officially tested with IBM Enhanced Remote Access for OS/2 Warp Server:

- Microsoft Windows 95 Version 4
- Microsoft Windows NT Version 4
- IBM 8235 DIALs Connect for Windows Version 4.1
- IBM LAN Distance Remote for Windows Version 5.0 (from OS/2 Warp Server)
- IBM Dial-Up for TCP/IP Version 2.0
- IBM 8235 DIALs for OS/2 Version 4.5.2
- IBM 8235 DIALs for OS/2 Version 4.0.3 and patch (see Note)
- IBM LAN Distance Remote for OS/2 Version 5.0 (from OS/2 Warp Server)

Note: The 8235 DIALs patch can be obtained from the World Wide Web (WWW) at the following URL:

<http://www.networking.ibm.com/nes/nes8235.htm>

The PPP connection support included with IBM Enhanced Remote Access for OS/2 Warp Server ensures long-term compatibility with other Internet-based products on a variety of computer platforms. The following clients have not been formally tested by IBM, but should work:

- LAN Distance Remote Client for OS/2 Version 1.11
- LAN Distance Remote Client for Windows Version 1.11
- Shiva PPP Client

3.3 System Requirements

The following sections describe:

- Hardware and Software requirements for IBM Enhanced Remote Access Connection Server for OS/2 Warp Server
- Hardware and Software requirements for Remote Clients
- Support restrictions for Remote Clients

3.3.1 IBM Enhanced Remote Access for OS/2 Warp Server System Requirements

The following prerequisite software and the WAN hardware should be installed before you install IBM Enhanced Remote Access:

- IBM OS/2 Warp Server Version 4.0 or later.
- Remote Access Services Connection Server component of OS/2 Warp Server.

- File and Print Services and any LAN applications to be run on the Connection Server.
- MPTS Requirement:
 - For OS/2 Warp Server: MPTS Version 5.11 or later.
 - For OS/2 Warp Server SMP: MPTS Version 5.2 with SMP MPTS APAR IC15968 or FixPak WRx8502.
- To support PPP clients, TCP/IP Version 3.1 or later is required.
- The minimum amount of memory recommended for OS/2, the IBM Enhanced Remote Access Connection Server component and one LAN application is 12 MB. The actual requirements of your Connection Server will depend on your LAN applications, data and response time requirements, and your workstation's processor speed.
- IBM Enhanced Remote Access requires 5.0 MB of fixed-disk storage space. Additional disk space is required to install FFST/2 (700 KB) and MPTS requires 2.2 MB, if these products are not already installed. If you are upgrading to IBM Enhanced Remote Access Connection Server for OS/2 Warp Server from a previous version, or reinstalling, you will require 2.4 MB of additional temporary disk space.
- A supported LAN adapter - see <http://www.austin.ibm.com/pspinfo/ldlan.htm> for a list of supported adapters.
- A supported WAN adapter - see <http://www.austin.ibm.com/pspinfo/ldwan.htm> for a list of supported adapters.

Note: This adapter will not be available for use by other applications simultaneously. For example, if you are using an ISDN adapter and you have installed Communications Manager/2 (CM/2) on your workstation, you must set up CM/2 so that it is *not* configured for ISDN.

- A modem to connect to the WAN adapter(s). To see a list of supported modems, refer to the online documentation:
 1. Type VIEW \BOOKS\A3T12MST.INF from an OS/2 window.
 2. Expand **Supported Hardware** and then double-click on **Modems**.

Note: The minimum baud rate of a modem used by IBM Enhanced Remote Access Connection Server for OS/2 Warp Server is 9600. The modem must also be certified in the country of attempted use.

- Non-switched (leased) or switched telephone lines to establish an asynchronous, synchronous or ISDN connection.

3.3.2 Remote Client System Requirements

All Remote Clients will require the following, plus additional requirements depending on the platform:

- A modem and/or adapter to connect to the server.

Note: WAN adapters will not be available for use by other applications simultaneously. For example, if you are using an ISDN adapter and you have installed Communications Manager/2 (CM/2) on your workstation, you must set up CM/2 so that it is *not* configured for ISDN.

- For asynchronous communications, it is recommended that the COM port of the Remote Client workstation be FIFO-buffered. This function is provided by a 16550 or 16550A UART chip in the workstation. This ensures you will be able to run your COM ports at up to 115200 baud without buffer over-run problems. However, some non-FIFO workstations with a processor faster than 25 MHz can support a reliable COM port speed of 38400 baud with a 14400 bps modem (or better).

To verify that your workstation has FIFO buffering, type `MODE COM1` at an OS/2 command prompt. Figure 41 shows our output of the the `MODE COM1` command:

| | | | |
|----------|----------|----------|--------|
| baud | = 115200 | parity | = NONE |
| databits | = 8 | stopbits | = 1 |
| TO | = OFF | XON | = OFF |
| IDSR | = OFF | ODSR | = OFF |
| OCTS | = OFF | DTR | = ON |
| RTS | = ON | BUFFER | = ON |

Figure 41. Output from `MODE COM1` Command

Note: If the response includes `BUFFER = N/A`, then your workstation does not have FIFO buffering.

- Non-switched (leased) or switched telephone lines to establish an asynchronous, synchronous or ISDN connection.

3.3.2.1 OS/2 and Windows 3.1 Remote Access Services Remote Client System Requirements

- One of the following operating systems:
 - IBM OS/2 Version 2.0 or later
 - Windows 3.1 or later, running on PC- or MS-DOS Version 5.0 or later
- The minimum amount of memory recommended for OS/2, the Remote Access Services Remote Client and one LAN application is 12 MB. The actual requirements of your Connection Server will depend on your LAN

applications, data and response time requirements, and your workstation's processor speed.

- The OS/2 Remote Access Services Remote Client requires 5.0 MB of fixed-disk storage space. Additional disk space is required to install FFST/2 (700 KB) and MPTS requires 2.2 MB, if these products are not already installed. If you are upgrading to Remote Access Services from LAN Distance Version 1.x, or reinstalling, you will require 2.4 MB of additional temporary disk space.
- The Windows 3.1 Remote Client requires 2.3 MB of fixed-disk storage space.

3.3.2.2 PPP Client System Requirements

One of the following operating systems:

1. IBM OS/2 Warp 3.0 or later and one of the following:
 - IBM OS/2 Internet Dialer supplied with the OS/2 Warp BonusPak or IBM TCP/IP Version 3.0 or later
 - IBM 8235 DIALs for OS/2 Version 4.5.2 or Version 4.03 and patch 4
2. Windows Version 3.1 or later, running on DOS Version 5.0 or later, and:
 - IBM 8235 DIALs for Windows Version 4.1
3. Windows 95 Version 4.0 PPP client—the Dial-Up network component of Network Neighborhood
4. Windows NT Version 4.0 Client

3.3.2.3 Remote Client Support Restrictions

The Remote Client supports a passphrase, which is case-sensitive, can include spaces, and can be up to 32 characters in length. If you are dialing in with a non-IBM PPP client, be aware of any password length or case-sensitivity restrictions with that client.

The following restrictions apply to IBM Enhanced Remote Access Remote Client:

- An OS/2 Remote Client can have up to two concurrent connections.
- A Windows 3.1 or 3.11 Remote Client can have only one asynchronous connection, using either a switched or non-switched line.
- Native X.25 support is provided by third parties, such as WAN Services for OS/2, announced by Eicon Technology.
- We recommend that you run LAN applications on the Remote Client that do not transfer large amounts of code or data over the WAN connection. For example, if an application loads 5 MB of code during start up, it may

take 5 to 10 seconds to load on a high-speed LAN. However, over a WAN connection using an asynchronous modem running at 14400 bps, this may take from 5 to 10 minutes. This is clearly not an acceptable response time.

The following restrictions apply to PPP:

- Callback is not supported for PPP clients.
- An IBM Enhanced Remote Access Connection Server does not support the ability to use LAN Distance logical adapter network addresses with a PPP user account.
- You cannot change passphrases from the client or perform security administration functions.
- Maximum passphrase age and maximum logon attempt policy options are not enforced for PPP clients.
- PPP clients cannot TCP/IP ping LAN Distance and Remote Access Services clients. LAN Distance and Remote Access Services clients cannot TCP/IP ping PPP clients.
- PPP clients can run only LAN applications and networking software that use TCP/IP (or TCPBEUI).
- PPP clients do not require LAN hardware to use a LAN Distance connection in order to access LAN resources. WAN communications hardware, such as a modem and COM port or an adapter, is required for the type of communications connection you want to support.

3.4 Installing IBM Enhanced Remote Access

There are a large number of installation options available due to the versatility of IBM Enhanced Remote Access. Using the most commonly used scenario as shown in Figure 40 on page 74, where Remote-to-LAN connectivity is provided by the Connection Server, we will describe the following installation and upgrade options:

1. Connection Server
 - a. Install IBM Enhanced Remote Access Connection Server for OS/2 Warp Server on a new server workstation. We will assume the LAN workstation to be used as the Connection Server has already been selected and had the prerequisite hardware installed.
 - b. Upgrade LAN Distance and Remote Access Services Connection Server workstations to IBM Enhanced Remote Access.
 - c. Configure the Connection Server—both for IBM Enhanced Remote Access and Point-to-Point Protocol support.

2. Remote Client

There is no upgrade for Remote Clients. Existing LAN Distance and Remote Access Services Remote Clients are still supported. Existing PPP clients are now also supported.

- a. Configure (as an example) a Windows 95 Version 4.0 PPP client.

3.4.1 Installing Remote Access Services in OS/2 Warp Server

IBM Enhanced Remote Access Connection Server for OS/2 Warp Server is an enhancement to Remote Access Services that was provided with OS/2 Warp Server. Therefore, you must install Remote Access Services during the OS/2 Warp Server installation, which we discuss briefly. After this task has been completed, you can upgrade the workstation to IBM Enhanced Remote Access Connection Server. If Remote Access Services is already installed, you can skip to section 3.4.2, "Upgrading to IBM Enhanced Remote Access" on page 87.

In the following example of installing Remote Access Services, we will assume that the OS/2 Warp Server installation has already been started and is currently at the networking selection stage.

1. Select Remote Access Services as well as other services you require from the OS/2 Warp Server Setup and Installation screen, as seen in Figure 42 on page 82.

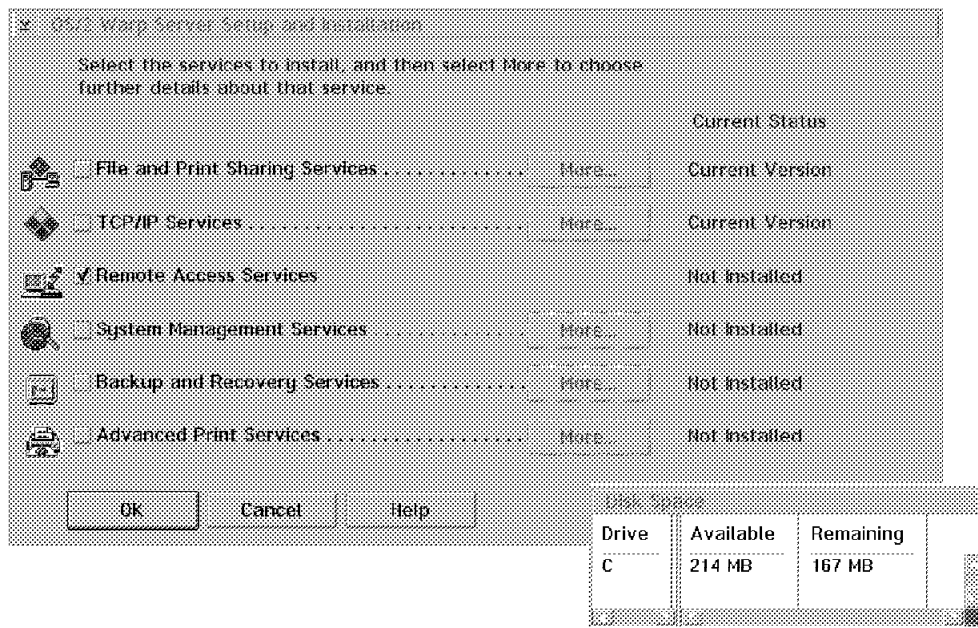


Figure 42. OS/2 Warp Server Setup and Installation Window

2. You will be asked to configure Remote Access Services and User ID and Password, as shown in Figure 43 on page 83:

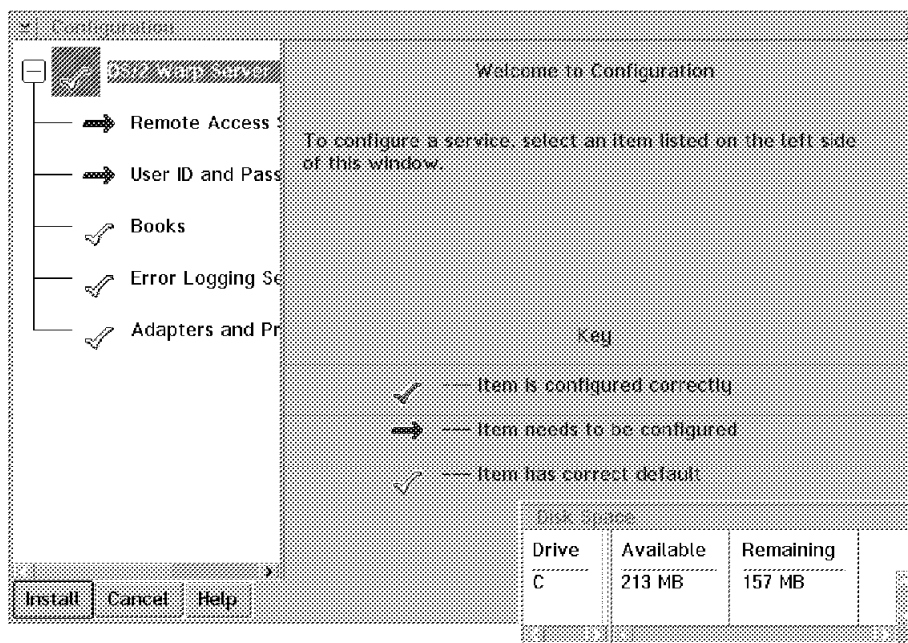


Figure 43. Remote Access Services Configuration Window

3. Select Remote Access Services by clicking on the **red arrow** shown in Figure 43.
4. In Figure 44 on page 84, we configured the Connection Server for one communications port (COM1) and a USRobotics Sportster 14400 modem.

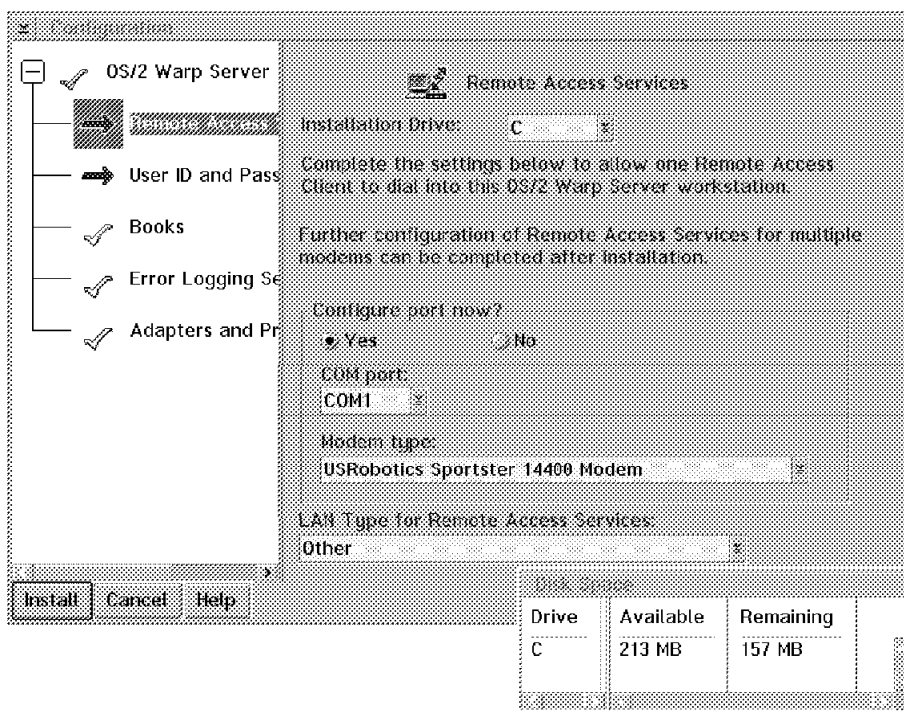


Figure 44. Remote Access Services Configuration Options Window

Notes:

- a. If you are installing a WAN adapter, select **No** in the Configure port now? field.
 - b. If your modem is not listed in the Modem type field, leave this set to none. You must run the CFMODEM utility after installation has completed.
 - c. The two options for LAN type are Ethernet and Other. If you have a token-ring LAN, select **Other**.
5. Select **User ID and Password** from the left-hand side of the Configuration window in Figure 44. You must enter the administrator's User ID and password. Take note of the User ID and password that you enter, as they will be required later when you logon to Remote Access Services.

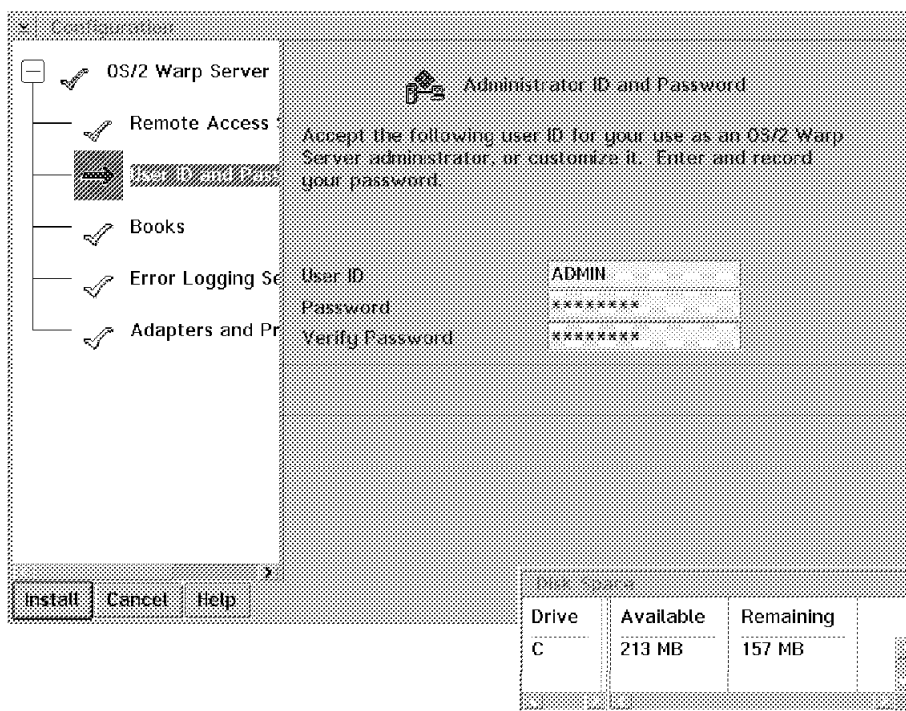


Figure 45. Remote Access Services Administrator Configuration Window

Note: In previous releases of LAN Distance, a default administrator user ID called SECADMIN with a default passphrase of SECADMIN was created automatically. This user ID is no longer created automatically. Instead, the default user ID and passphrase are those that you entered during installation. If you have forgotten the user ID or passphrase, see section 3.6.2, “Recovering the Administrator Passphrase” on page 135 , for recovery information.

- Now complete the installation by selecting **Install**. After the installation has completed, you must proceed to the next task—upgrading the workstation to IBM Enhanced Remote Access.

Table 3 on page 86 lists the changes that are made to the CONFIG.SYS and PROTOCOL.INI configuration files during installation of IBM Enhanced Remote Access. Backups of these system configuration files are saved before the files are changed.

Table 3 (Page 1 of 2). CONFIG.SYS Modifications During Connection Server Installation

| FILE | BACKUP | CHANGES |
|-------------|-------------|---|
| \CONFIG.SYS | \CONFIG.WAL | <ul style="list-style-type: none"> • The WAL directory is added to your path specifications for: <ul style="list-style-type: none"> – LIBPATH – DPATH – PATH • The LAN Distance helps are added to the HELP specification. • The specifications for the LAN Distance device drivers are added. • The device drivers for LAPS and NetBIOS are added. • If FFST/2 is installed during LAN Distance installation, appropriate statements for it are added. • Statements for the locked file device driver are added temporarily to the top of your CONFIG.SYS file. The statements are removed the next time you start your workstation. |

Table 3 (Page 2 of 2). CONFIG.SYS Modifications During Connection Server Installation

| FILE | BACKUP | CHANGES |
|------------------------|---------------------|--|
| \\IBMCOM\\PROTOCOL.INI | \\WAL\\PROTOCOL.WAL | <ul style="list-style-type: none"> • If NetBIOS is installed during LAN Distance installation, a section for NETBEUI_NIF is added. • Your NetBIOS timers are adjusted to minimize remote-access timeouts. • The number of NetBIOS NCBs, names, and sessions are increased, if not already done by the OS/2 Warp Server Tuning Assistant. • A section is added for VLAN_kernel. • A section for PDFH_NIF is added. |

Note: The drive letter for the paths listed is the drive where OS/2 Warp Server is installed.

3.4.2 Upgrading to IBM Enhanced Remote Access

1. You must first download the IBM Enhanced Remote Access installation code, which is available from the IBM Software Choice Website:

<http://www.software.ibm.com/os/warp/swchoice/>

Note that this code is available through subscription only. See section 2.7, "Subscribing to Software Choice" on page 37. for more information about IBM Software Choice subscriptions.

Download the ZIP file, which is about 10 MB in size, to a temporary directory, for example, \\TEMP.

2. Unzip the file, which contains the IBM Enhanced Remote Access diskette images, latest MPTS diskette images, online documentation and README files, with the following command:

```
PKUNZIP2 LD5051DK
```

In addition to the images and documentation, there are two command (.CMD) files created. The INSTALL.CMD is used to create the IBM Enhanced Remote Access diskettes, and the MAKEMPTS.CMD is used to

create the MPTS diskettes. Don't use INSTALL yet! Make sure your MPTS is at the proper level first. We also recommend that you read the README.PKG file.

3. As described in section 3.3.1, "IBM Enhanced Remote Access for OS/2 Warp Server System Requirements" on page 76, the level of MPTS must be upgraded to at least Version 5.11 before installing the IBM Enhanced Remote Access. You can use the MPTS Version 5.11 diskette images included in the ZIP file, or you can use the OS/2 Warp Server Advanced SMP MPTS code. If using the diskette images, use the MAKEMPTS command to create the four MPTS diskettes. Once the proper version of MPTS is installed and the machine is rebooted, proceed to the next step.
4. You will need four blank high-density diskettes for IBM Enhanced Remote Access: three diskettes for the code, and one diskette for the online documentation. Type INSTALL to begin the diskette creation process. Once the diskettes are created, you are ready to continue.
5. Back up the files listed in Table 4. These backups are required if you wish to uninstall IBM Enhanced Remote Access Connection Server for OS/2 Warp Server.

Table 4 (Page 1 of 2). IBM Enhanced Remote Access Configuration Files

| FILE NAME | FILE DESCRIPTION |
|----------------------|--|
| \CONFIG.SYS | OS/2 configuration |
| \IBMCOM\PROTOCOL.INI | LAN adapter protocol configuration |
| \WAL\WCLLOCAL.INI | Local configuration information for the IBM Enhanced Remote Access workstation |
| \MPTN\BIN\SETUP.CMD | TCP/IP configuration information |
| \BOOKS\A3T12MST.INF | IBM Enhanced Remote Access online manual |
| \WAL\WCBUSRF.ISF | Security information from the user account database |
| \WAL\WCLDIAL.CXD | Telephone numbers and connection information for phone book entries |
| \WAL\WCLNET.INI | Modem configuration information |

Table 4 (Page 2 of 2). IBM Enhanced Remote Access Configuration Files

| FILE NAME | FILE DESCRIPTION |
|---------------------|--|
| \\WAL\\WCLIPADR.INI | Configuration file containing a list of available IP addresses for Point-to-Point protocol (PPP). The administrator creates the file using an ASCII editor after installation is complete. |

Note: The driver letter for the paths listed is the drive containing the above directories.

6. Insert the IBM Enhanced Remote Access Connection Server diskette 1 in drive A: and open an OS/2 window or OS/2 full-screen. Type A:INSTALL and press **Enter**.

You will see the installation window shown in Figure 46.

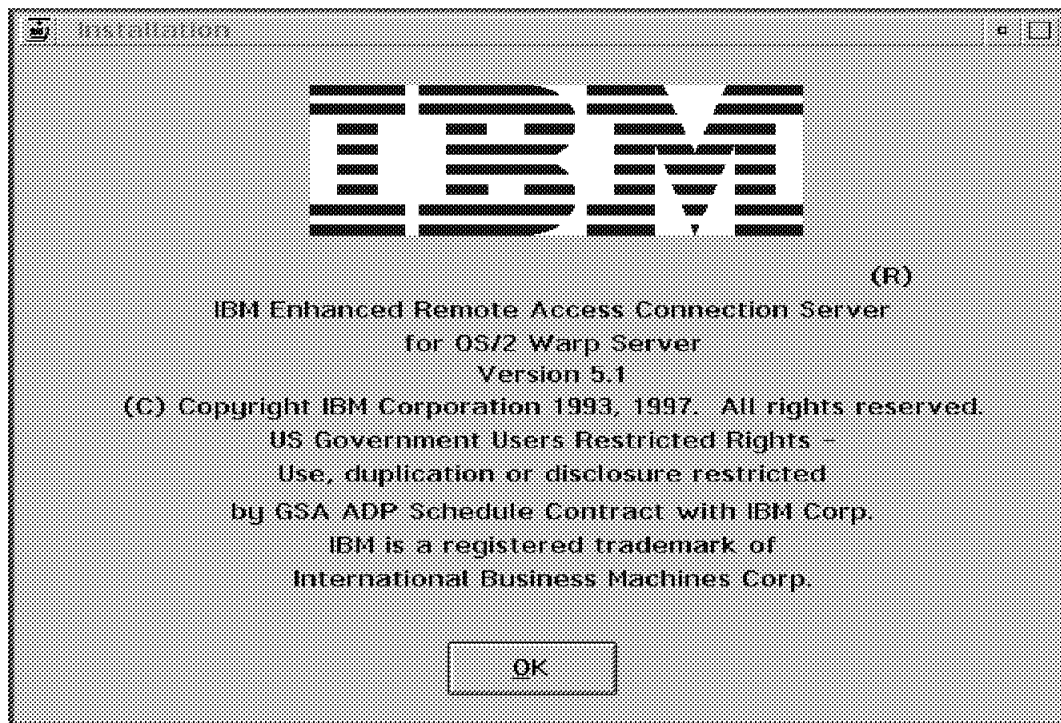


Figure 46. Installation Window

7. Select **OK** to begin the installation. The window shown in Figure 47 on page 90 appears:

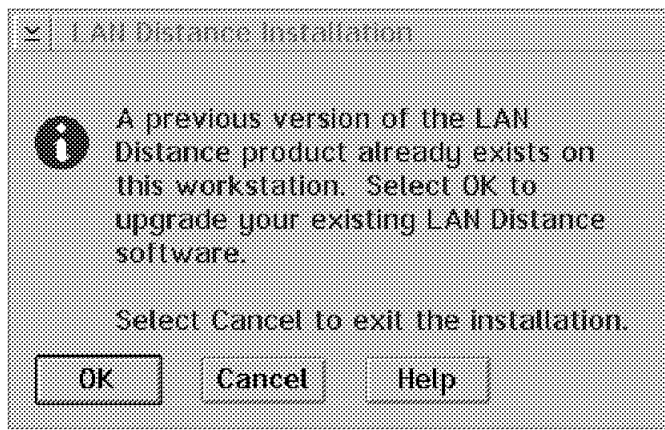


Figure 47. Upgrade Warning Window

8. Select **OK** to upgrade the workstation to IBM Enhanced Remote Access Connection Server for OS/2 Warp Server.
9. Follow the instructions to remove and insert diskettes. When the installation has completed, the installation program requests that you shut down and restart your machine, as shown in Figure 48 on page 91:

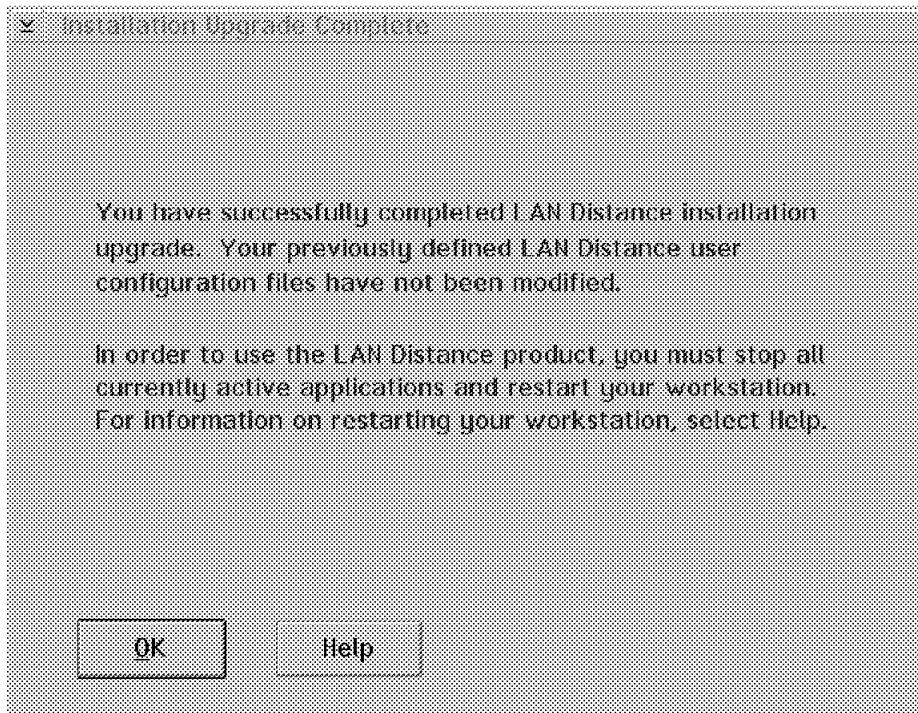


Figure 48. Installation Upgrade Complete Window

3.5 Configuring IBM Enhanced Remote Access

After you have installed IBM Enhanced Remote Access and restarted your workstation, a LAN Distance Remote Access folder appears on your desktop. Within this folder, you will find an IBM Remote Access Services icon. Double-click this icon to start the IBM Enhanced Remote Access.

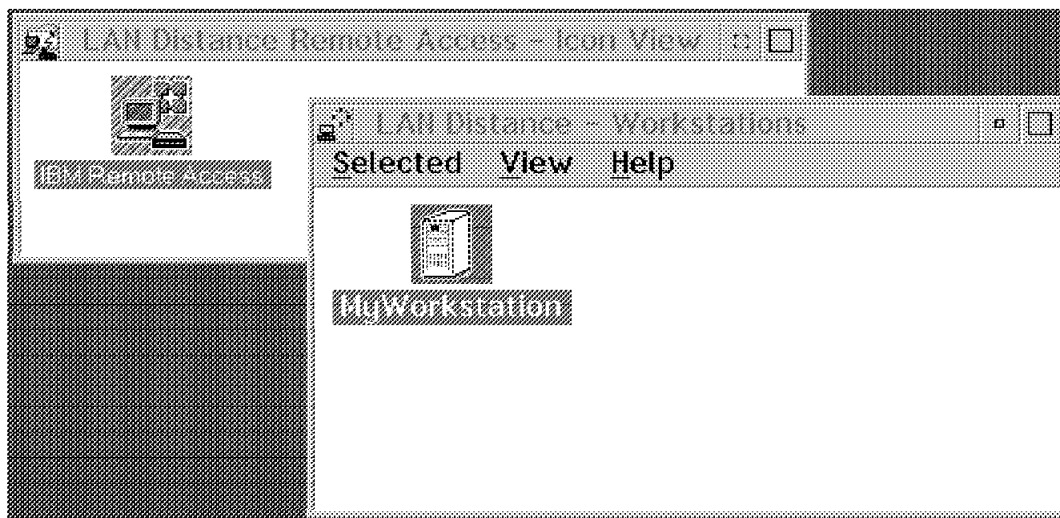


Figure 49. IBM Enhanced Remote Access Logon Option

After IBM Enhanced Remote Access has started, as shown in Figure 49, select the **Selected** pull-down menu; then **Open As** and then **Settings**. Alternatively, you can right-mouse-button select **MyWorkstation** and select **Settings**.

The configuration of IBM Enhanced Remote Access Connection Server for OS/2 Warp Server, IBM Enhanced Remote Access Remote Client for OS/2, and IBM Enhanced Remote Access Remote Client for Windows is the same as that in previous releases of Remote Access Services and LAN Distance products, except for configuring support for PPP clients on the Connection Server.

In the following sections, we discuss configuring the Connection Server for PPP support and configuring PPP clients on different platforms.

For information on configuring other parts of IBM Enhanced Remote Access, see the online documentation by issuing `VIEW x:\BOOKS\A3T12MST.INF` at an OS/2 command line. Also, refer to Chapter 7.4 of the IBM redbook *Inside Warp Server, Volume 1: Exploring the Core Components*, SG24-4602.

3.5.1 Configuring PPP Support on the Connection Server

There are several tasks required to configure the Connection Server to support PPP clients. These include:

- Reviewing IP address considerations for PPP clients

- Configuring a TCP/IP protocol router, which includes:
 - Bind the IBM TCP/IP protocol to certain adapters
 - Set TCP/IP configuration information
- Updating the \WAL\WCLLOCAL.INI file and adding the appropriate PPP operating parameters
- Administering IP addresses for PPP connections. There are three ways of accomplishing this:
 1. Local IP address list
 2. DHCP server services
 3. Client IP address configuration
- Creating user IDs for PPP clients

3.5.1.1 Reviewing IP Address Considerations for PPP Clients

IBM Enhanced Remote Access Connection Server supports two ways of routing frames between the LAN and the WAN for PPP clients:

1. LAN and WAN are different networks - the Connection Server workstation has two interfaces configured, each with an IP address from a different subnet. PPP clients must be assigned an IP address from the same subnet as the WAN interface.
2. LAN and WAN are on the same network - the IBM TCP/IP proxy Address Resolution Protocol (ARP) feature allows two interfaces to be configured with IP addresses from the same network. For example, the LAN interface is using a Class B network number of 172.16.x.x, which does not understand subnets. The IP address 172.16.1.26 is assigned to the LAN interface, and 172.16.2.8 is assigned to the WAN interface. Using a router subnet mask of 255.255.255.0 caused frames to be routed between the LAN and the WAN.

When a PPP client connects and is assigned an IP address of 172.16.2.x, the Connection Server adds ARP and route entries, as required, for the proxy ARP configuration. The TCP/IP router responds to ARP requests from the LAN to a PPP client with its own hardware address. When the Connection Server receives a frame that is intended for the PPP client, the TCP/IP router forwards the frame to the correct client, based on the ARP and Route table entries.

Note: An alternative way to configure the two TCP/IP interfaces on the Connection Server is to use two different subnet masks. For example, all LAN workstations use a subnet mask of 255.255.255.0. Use 255.255.255.0 for the LAN interface and 255.255.255.128 for the WAN interface. The MPTS FixPak which is a prerequisite for IBM Enhanced

Remote Access Connection Server for OS/2 Warp Server, enables this feature.

3.5.1.2 Configuring a TCP/IP Protocol Router

The IBM Enhanced Remote Access Connection Server bridges all data frames from IBM Enhanced Remote Access Remote Client between the LAN and the WAN. However, for PPP clients, data frames are sent to the TCP/IP stack that is bound to the LAN Distance logical adapter. Therefore, you must configure TCP/IP as a router between the LAN and the WAN.

To configure TCP/IP for routing, you must bind the IBM TCP/IP protocol to the:

- LAN adapter
- LAN Distance logical adapter

Note: When the IBM Enhanced Remote Access Connection Server is configured for transparent bridging and the TCP/IP router is configured, IBM Enhanced Remote Access clients will not be able to TCP/IP ping the LAN or WAN TCP/IP interfaces on the Connection Server.

3.5.1.3 Binding the IBM TCP/IP Protocol to the LAN and WAN Adapters

1. To bind the IBM TCP/IP protocol to the adapters, use the Adapters and Protocol Support application. Enter MPTS from an OS/2 command prompt.
2. When the Configure window is displayed, select the **LAN adapters and protocols** radio button. Click on the **Configure** pushbutton.
3. Use the Adapter and Protocol Configuration window to bind the IBM TCP/IP protocol to the adapters.

Note: IBM Enhanced Remote Access assumes the LAN adapter that is used for routing is the first adapter that is the same LAN type as the connection server (Ethernet or token-ring) and is configured for TCP/IP.

In the Current Configuration list box, highlight the LAN adapter you will use for routing. Highlight the **IBM TCP/IP protocol** in the Protocols list box. Click on the **Add** pushbutton directly under the Protocols list box, as shown in Figure 50 on page 95.

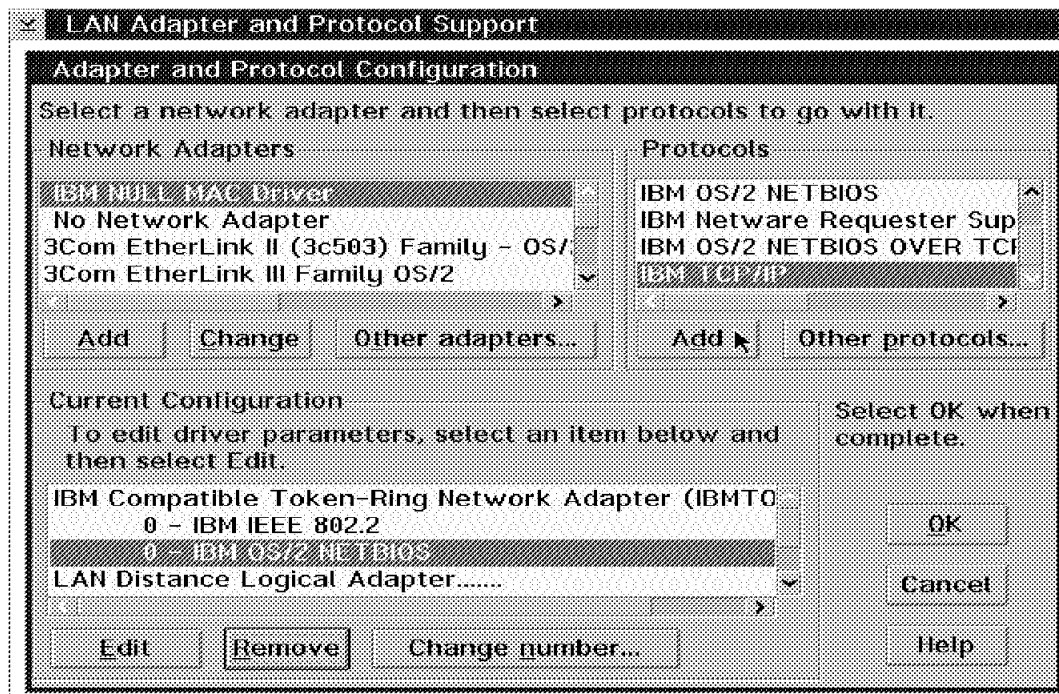


Figure 50. MPTS Configuration Window - Binding TCP/IP to LAN Adapter

The window refreshes and shows IBM TCP/IP below the LAN adapter you selected.

4. In the Current Configuration list box, highlight the **LAN Distance logical adapter**. Highlight the **IBM TCP/IP protocol** in the Protocols list box. Click on the **Add** pushbutton directly under the Protocols list box.

The window refreshes and shows IBM TCP/IP below the LAN Distance logical adapter you selected.

The following is a token-ring example of how the Current Configuration list box might look after you bind the TCP/IP protocol to the two adapters.

```

IBM Compatible Token-Ring Network Adapter (IBMTOK.OS2).....
    0 - IBM IEEE 802.2
    0 - IBM TCP/IP
LAN Distance Logical Adapter.....
    0 - IBM OS/2 NETBIOS
    1 - IBM TCP/IP

```

Figure 51. Configuration for a Token-Ring Adapter

The following is an Ethernet example of how the Current Configuration list box might look after you bind the TCP/IP protocol to the two adapters.

```

LAN Distance Logical Adapter.....
    0 - IBM OS/2 NETBIOS
    1 - IBM TCP/IP
SMC Ethernet MCA Adapter Family (SMC8000.OS2).....
    0 - SR_BRIDGE
    0 - IBM TCP/IP
BRIDGEFH.....
    1 - SR_BRIDGE

```

Figure 52. Configuration for an Ethernet Adapter

5. Select the appropriate pushbuttons to close the Adapters and Protocol Support application.
6. The application updates the CONFIG.SYS file. You are asked to select the appropriate drives for the file and the Update CONFIG.SYS checkbox.
7. Select the appropriate pushbuttons to close the application.
8. After you close the application, you must restart OS/2 Warp Server for the changes to be installed.

3.5.1.4 Setting TCP/IP Configuration for PPP

After you have bound the IBM TCP/IP protocol to the adapters, you must set TCP/IP configuration information for PPP. You must configure a TCP/IP LAN interface for the LAN adapter and also for the LAN Distance logical adapter.

1. Start TCP/IP configuration—follow the procedure that best describes your configuration:
 - If TCP/IP is not installed, use Multiprotocol Transport Services (MPTS). Type MPTS at an OS/2 command prompt or double-click on the **MPTS Adapters and Protocols** icon in the System Setup folder.
 - If TCP/IP is installed, use the **TCP/IP Configuration** application, which can be starting by entering TCPCFG from an OS/2 command

prompt or by selecting on the TCP/IP Configuration icon in the TCP/IP folder.

2. With either of the above configurations, you must configure an interface for the LAN adapter. Then, configure an interface for the LAN Distance logical adapter.

Note: Do not use DHCP to obtain the LAN and WAN interface IP addresses for the IBM Enhanced Remote Access Connection Server. Servers should use preassigned addresses.

3. Next, create a default route.
4. Some networks require dynamic routing. If your network requires dynamic routing, then start ROUTED. TCP/IP must be installed in order to start ROUTED.
5. After you have completed these steps, close the application.
6. You must shut down your workstation and then restart it for the changes to become effective.

3.5.1.5 Specifying PPP Parameters in \WAL\WCLLOCAL.INI

The WCLLOCAL.INI file contains new parameters that indicate if the Connection Server should configure an IP address for the Remote Client, where to get the IP address, and if a host name should also be configured.

When the LAN Distance connection server starts, it gets specific operating information from the \WAL\WCLLOCAL.INI file. You need to include operating parameters for point-to-point protocol (PPP) in this file.

To configure the \WAL\WCLLOCAL.INI file, edit it using an ASCII editor. Update a PPP section to the file as follows. Additional information about the parameters follows the example.

```
[PPP]
ObtainIPAddr={LIST, DHCP, USERSPEC}
pppSecurity={PAP, CHAP}
DDNS={YES, NO}
ClientsDomainNm=domain name
DHCPMaxWait=seconds
```

Figure 53. PPP Section of the \WAL\WCLLOCAL.INI Configuration File

| Parameter | Value |
|-------------------------|--|
| ObtainIPAddr= | <p>Indicates where PPP gets the IP addresses for a PPP session. Select one or more of the following:</p> <ul style="list-style-type: none"> • <i>LIST</i>—Get IP addresses from a list in the \WAL\WCLIPADR.INI file. • <i>DHCP</i>—Get IP addresses from a DHCP server that is available on the LAN. • <i>USERSPEC</i>—The client workstation or workstations have configured their own IP addresses. <p>Note: LIST, DHCP and USERSPEC can be used together. The server tries the options in the order specified.</p> |
| DDNS= | <p>Indicates whether PPP will enable DDNS for PPP sessions.</p> <ul style="list-style-type: none"> • <i>YES</i>—PPP will enable DDNS. • <i>NO</i>—PPP will not enable DDNS. <p>Note: Either YES or NO must be selected, but not both. The DHCP server uses the LAN Distance user ID to update the DNS server when using this method if no name is defined on the Remote Client.</p> |
| pppSecurity= | <p>Indicates whether PPP uses PAP security or CHAP security for user authentication.</p> <ul style="list-style-type: none"> • <i>PAP</i>—Use PAP security for user authentication. • <i>CHAP</i>—Use CHAP security for user authentication. <p>Note: PAP and CHAP can be used together. The server tries the authentication options in the order specified. We recommend that you specify CHAP before PAP.</p> |
| ClientsDomainNm= | <p>Indicates the domain name of the client. If you do not specify a value, the domain name is obtained from \MPTN\ETC\RESOLV2 on the IBM Enhanced Remote Access system.</p> |
| DHCPMaxWait= | <p>Indicates the interval, in seconds, that IBM Enhanced Remote Access waits for a response from any DHCP server. You can specify a value from 2 to 40 seconds. The default timeout value is 3 seconds. The IBM Enhanced Remote Access Connection Server will retry one time.</p> |

Note: Since the server will always retry one time, the client must be able to wait for the number of seconds specified by the parameter, times two. For example, if the DHCPMaxWait parameter is set to 5, the client must be able to wait for a connection response for at least 10 seconds. Some PPP clients will time out in as little as 8 seconds.

3.5.1.6 IP Addresses in WCLIPADR.INI

The WCLIPADR.INI file contains the list of IP addresses maintained by the IBM Enhanced Remote Access Connection Server.

```
[IPADDRESSES]
x.x.x.x
y.y.y.y-z.z.z.z
```

Figure 54. \WAL\WCLIPADR.INI IBM Enhanced Remote Access Configuration File

Where:

- x.x.x.x represents a single IP address that can be assigned for a PPP connection.
- y.y.y.y-z.z.z.z represents a range of IP addresses that can be assigned for a PPP connection.

3.5.1.7 Using DHCP Servers

If you will be using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to your PPP clients and have the client's LAN Distance user ID associated with the IP address on the DDNS server, your DHCP server must have a version of DHCP that contains the "DNS proxy A record." This feature is available through the following APARS:

- OS/2 Warp Server APAR IC15366
- OS/2 Warp Server SMP APAR IC16980

DHCP servers provide the IP addresses and configuration information to DHCP and Bootstrap Protocol (BootP) clients on the network. DHCP servers contain information about the host operational parameters, as specified by the network administrator.

By using a DHCP server, it is possible to assign an IP address to a client for a limited amount of time, and it also offers a way to supply all necessary configuration parameters with no end-user configuration required.

A PPP client that uses TCP/IP may or may not have a configured IP address. Clients that have not configured an IP address must be provided with one during PPP negotiation. This is provided by one of the following:

1. DHCP server on the LAN
2. IBM Enhanced Remote Access Connection Server with IP addresses contained in the WCLIPADR.INI

3.5.2 Remote Client

The LAN Distance Remote Client is unchanged from previous versions. See the redbook titled *Inside Warp Server, Volume 1: Exploring the Core Components*, SG24-4602, for information on configuring a Remote Client.

3.5.3 Windows 95 PPP Clients

PPP support is included with Windows 95 Version 4.0 through the Dial-Up Networking service. There are three components of Windows 95 that must be configured before this will work. They are:

1. Modem installation and configuration, which enables Windows 95 to operate your hardware
2. Network configuration, which makes Dial-Up Networking and TCP/IP available
3. Dial-Up Networking configuration, which allows configuration of the phone number, and modem settings

The following sections show an example of configuring Windows 95 PPP on an IBM ThinkPad 760ED with an IBM International 28.8 Kbps data/fax PCMCIA modem.

3.5.3.1 Modem Installation and Configuration

You must install and configure your modem in Windows 95 by following the instructions provided by the manufacturer. If you are using a desktop machine, the COM ports and modems will be configured when you are installing Windows 95 or after you have purchased a new modem.

In this example, an IBM International 28.8 Kbps data/fax PCMCIA modem is installed after Windows 95 is installed and running. The Hardware Manager detected that the card was installed in the PCMCIA slot of the ThinkPad and prompted installation of the device drivers by selecting the **Have Disk** option.

After installation of the modem device drivers, Windows 95 prompts you to restart Windows 95. When this has been completed, Windows 95 will be able to operate your modem.

Note: Depending on your COM port configuration, you may have to disable a COM port on the notebook so that it is available for the PCMCIA modem.

3.5.3.2 Network Configuration

If you have not already installed any networking components for Windows 95, there will be no Network Neighborhood icon on the desktop.

The following method of configuring network components will work whether or not you have a Network Neighborhood icon:

1. Select **Start** from the Task Bar.
2. Select **Settings**.
3. Select **Control Panel**.

This is shown in Figure 55.

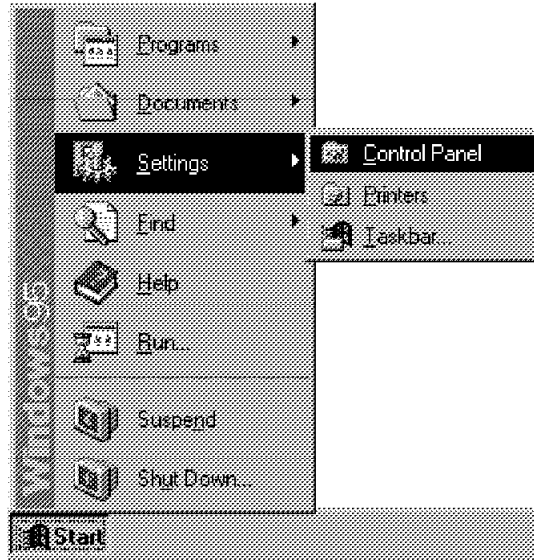


Figure 55. Opening the Windows 95 Control Panel

4. You must select the **Network** icon, as shown in Figure 56 on page 102.



Figure 56. Windows 95 Control Panel

5. You must select **Add** from the Configuration panel, as shown in Figure 57 on page 103.

Note: If you already have a Dial-Up Networking component installed, it will be displayed on this panel. If this is the case, you must highlight **Dial-Up Networking**, select **Properties**, then continue configuring by going to Figure 60 on page 106.

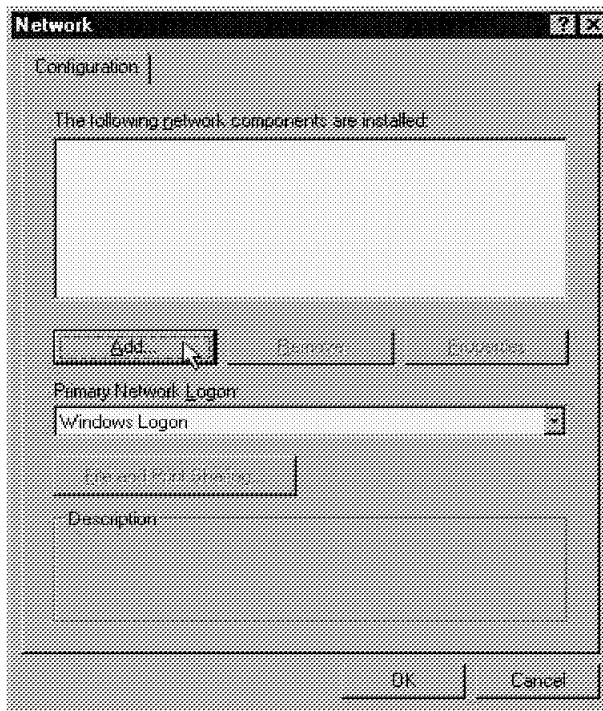


Figure 57. Windows 95 Network Configuration Window

6. You must highlight **Adapter** and push the **Add** button, as shown in Figure 58 on page 104.

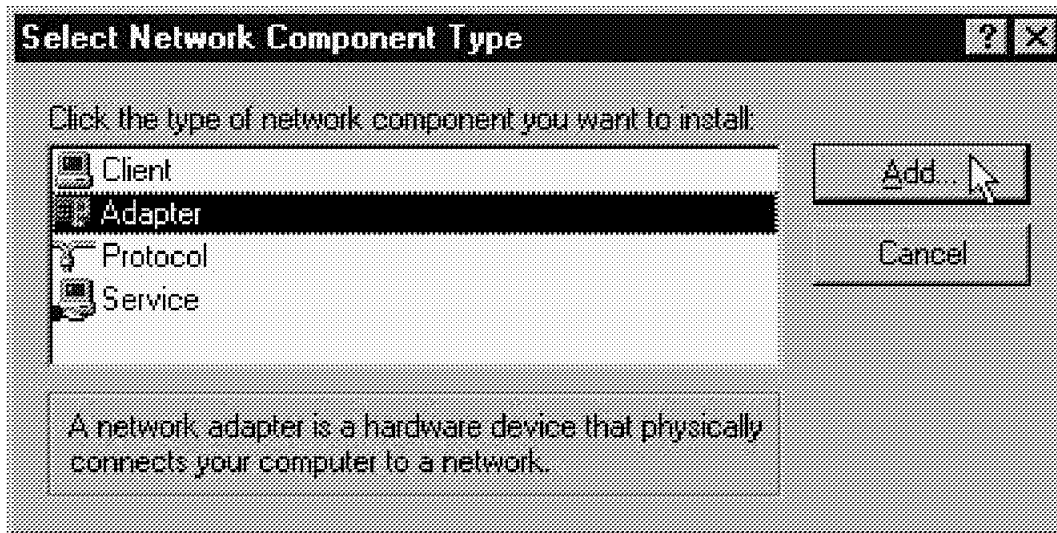


Figure 58. Adding a Network Adapter

7. Highlight **Microsoft** from the Manufacturers field and the Dial-Up Adapter will appear in the Network Adapters field. Now select **OK**, as shown in Figure 59 on page 105.

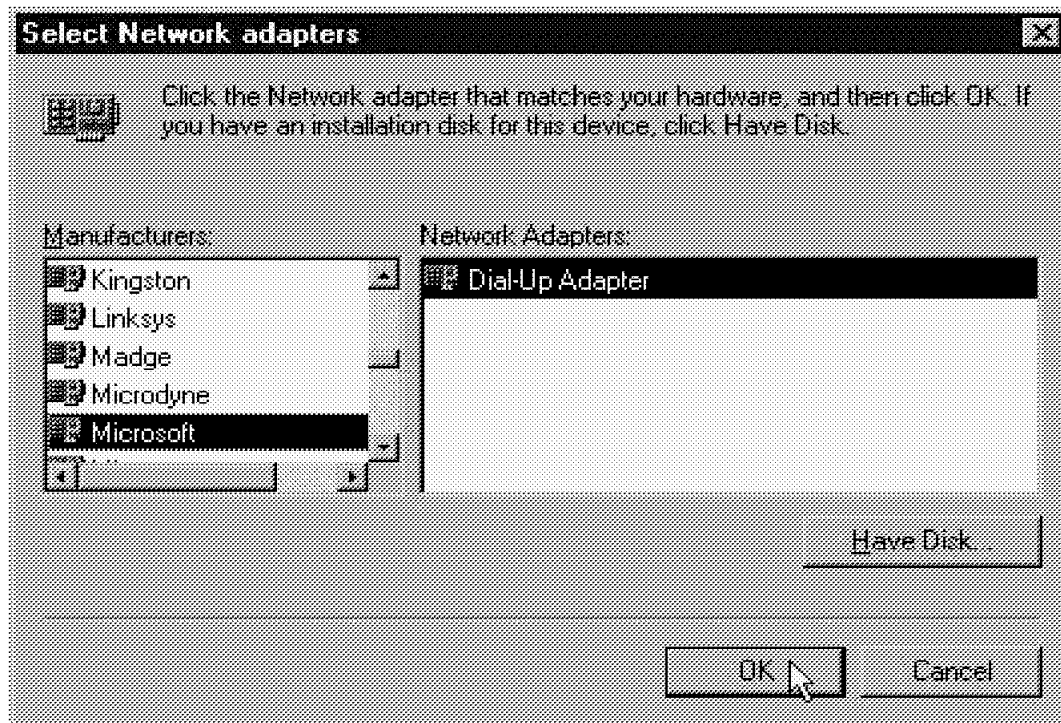


Figure 59. Adding the Dial-Up Adapter

8. Notice that the TCP/IP protocol is not included in the default configuration of the Dial-Up Adapter, as shown in Figure 60 on page 106. You must add TCP/IP by selecting **Add**.

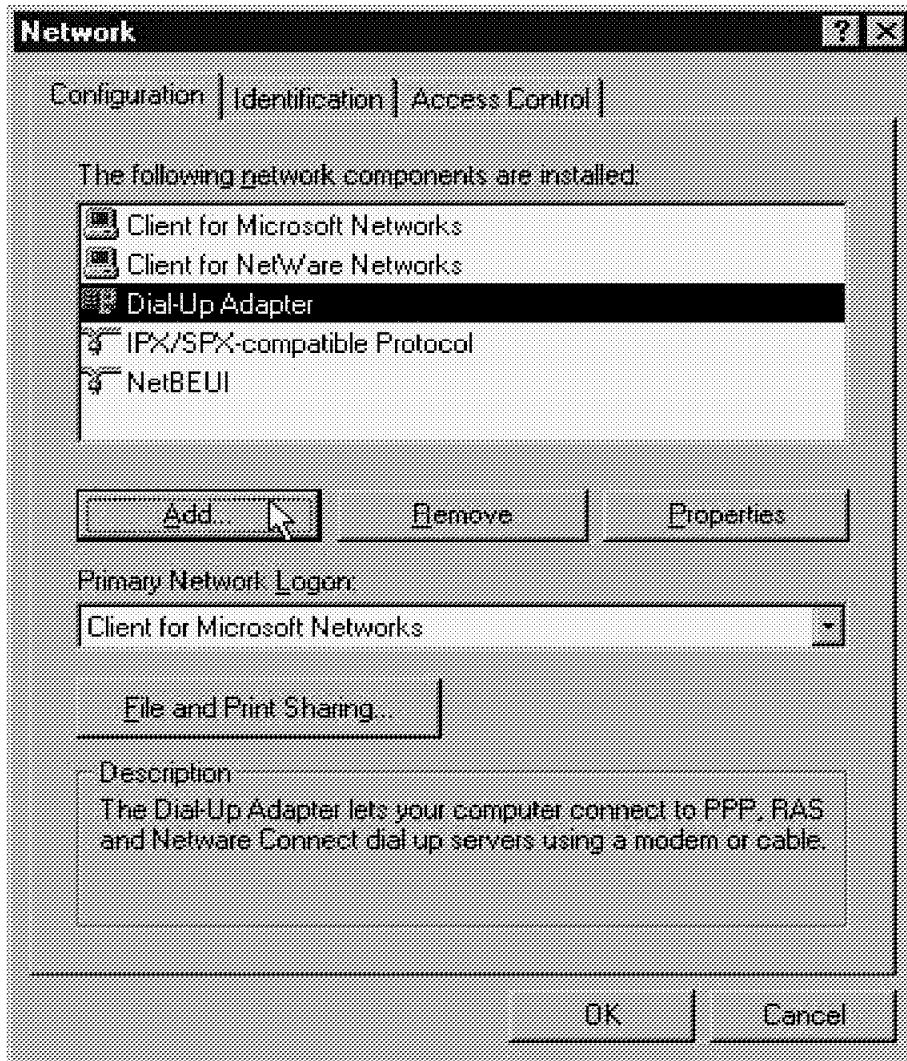


Figure 60. Default Protocols for Dial-Up Adapter

Notice that IPX/SPX-compatible and NetBEUI protocols were added by default. You can remove the IPX protocol from the Dial-Up Adapter if you are not accessing NetWare servers from this workstation. This protocol can be removed by highlighting **IPX/SPX-compatible Protocol** and selecting **Remove**.

Note: By leaving NetBEUI enabled on the Dial-Up Adapter, you will receive an error message when a connection to the IBM Enhanced Remote Access Connection Server, as only TCP/IP is passing over the

link between the Remote Client and the Connection Server. Just ignore the error message and continue with the connection, so TCPBEUI will be able to flow over the link.

9. Highlight **Protocol** and select **Add**, as shown in Figure 61.

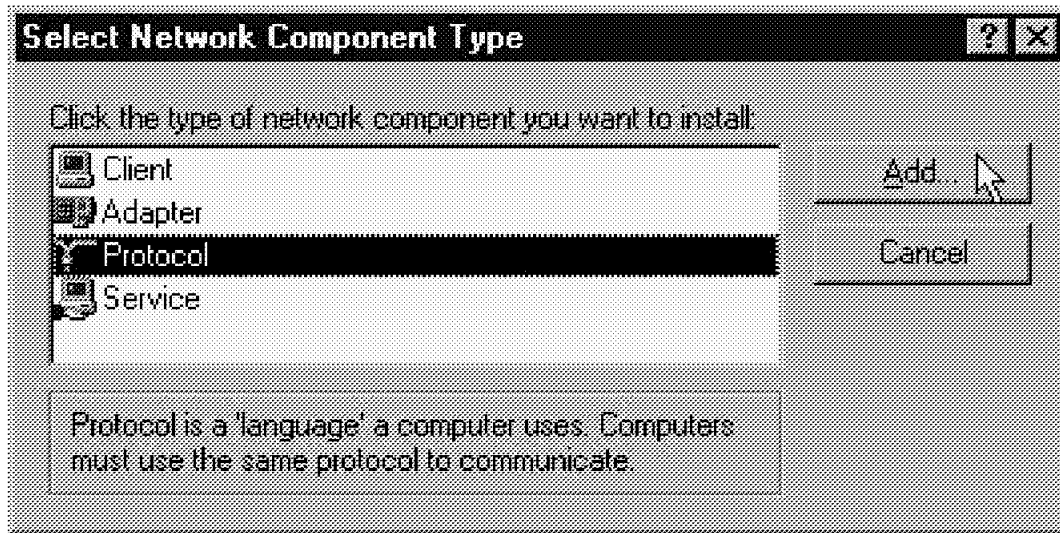


Figure 61. Adding a Protocol to Dial-Up Adapter

10. Highlight **Microsoft** from the Manufacturers field and highlight **TCP/IP** from the Network Protocols field, then select **OK**, as shown in Figure 62 on page 108.

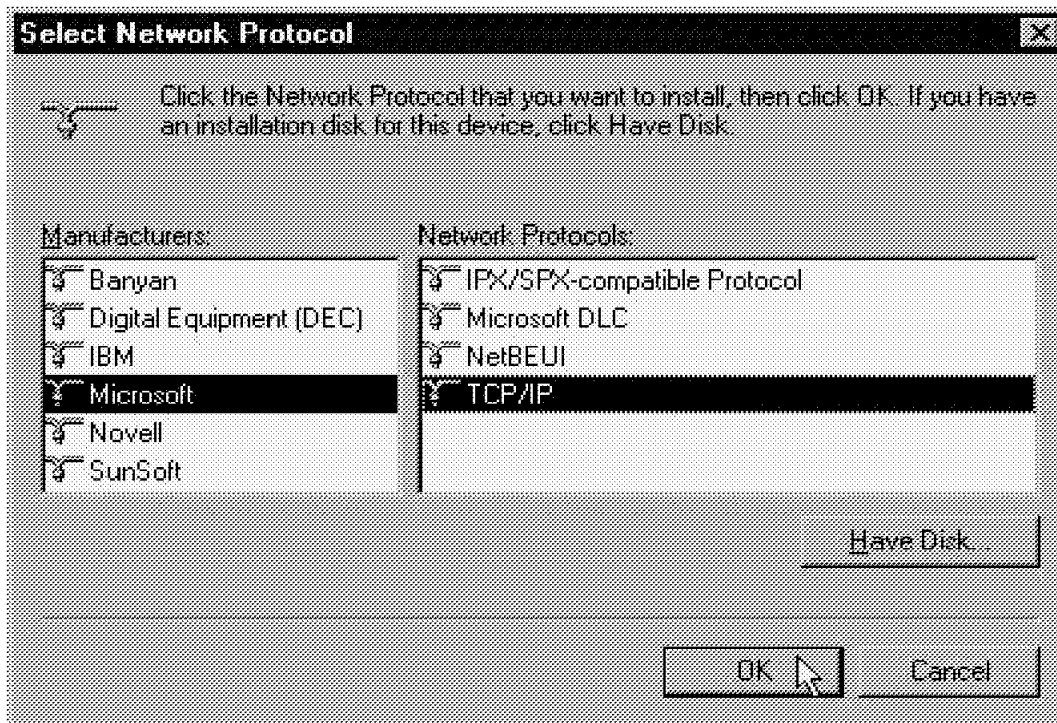


Figure 62. Adding TCP/IP Protocol to Dial-Up Adapter Configuration

11. Figure 63 on page 109 shows that TCP/IP is now installed.

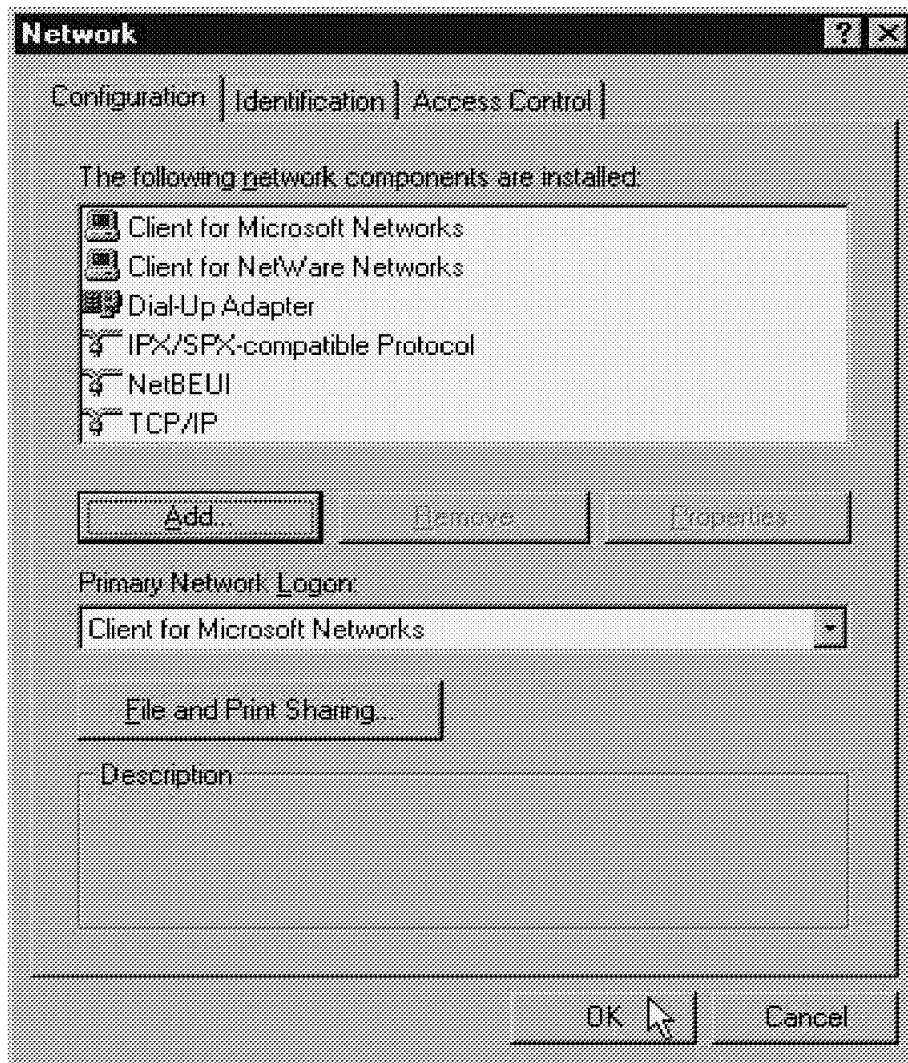


Figure 63. Dial-Up Adapter Configuration with TCP/IP Installed Protocol

Select **OK**, and you will be prompted to restart Windows 95 for the changes to take effect, as shown in Figure 64 on page 110.



Figure 64. Prompt to Restart Windows 95

12. Select **Yes** to shut down and restart Windows 95. The initial configuration now complete. The next step is to set up the actual usage of the Dial-Up Adapter.

3.5.3.3 Dial-Up Networking Configuration

1. After Windows 95 has restarted, you must configure the Dial-Up Adapter. Select **My Computer** and then select **Dial-Up Networking**. You will then see the window shown in Figure 65.

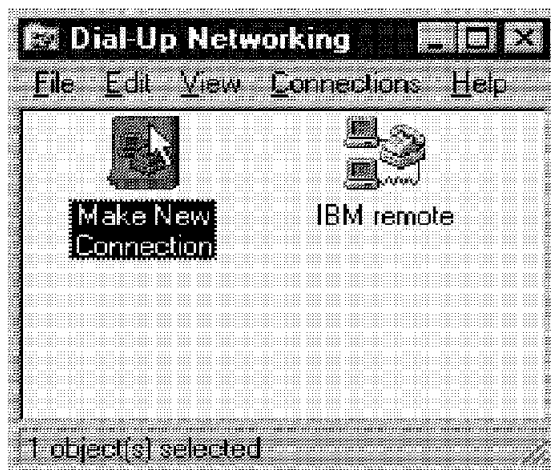


Figure 65. Dial-Up Networking New Connection

2. Double-click on the **Make New Connection** icon and enter a name for the computer you are dialing. This will become the name of the icon in the Dial-Up Networking folder you will select to make PPP connections. In Figure 66 on page 111, the name we chose is Remote Access PPP.

3. Select the type of modem you are using, as shown in Figure 66 on page 111.

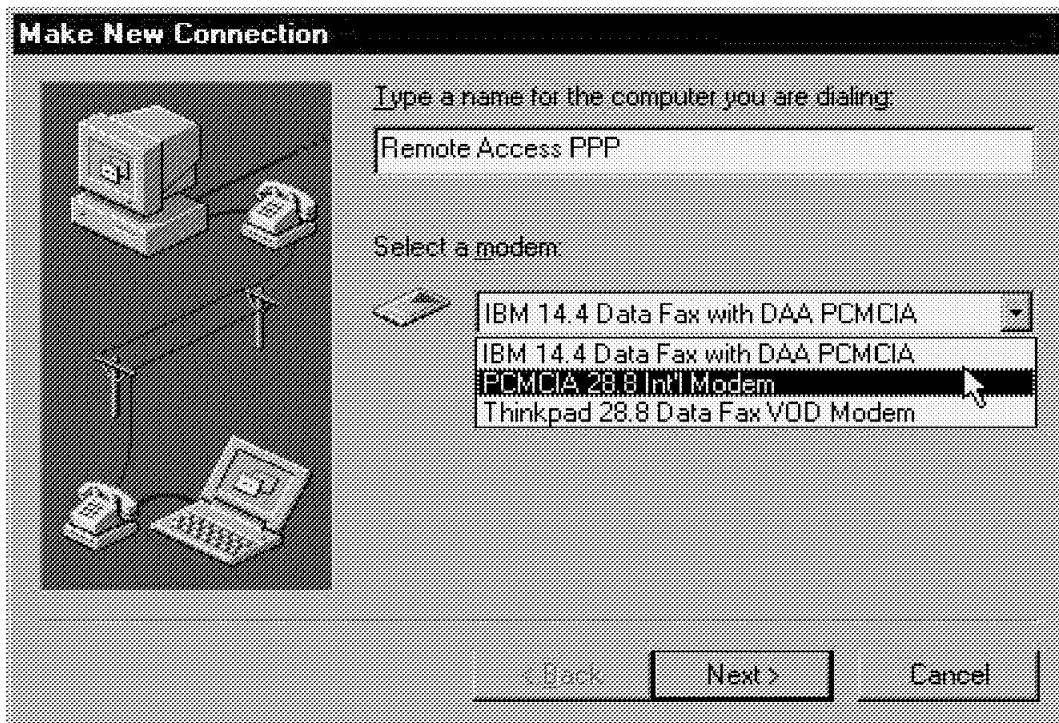


Figure 66. Make New Connection Configuration

4. Once the modem has been selected, you must configure it. Select **Configure** and you will see the window shown in Figure 67 on page 112.

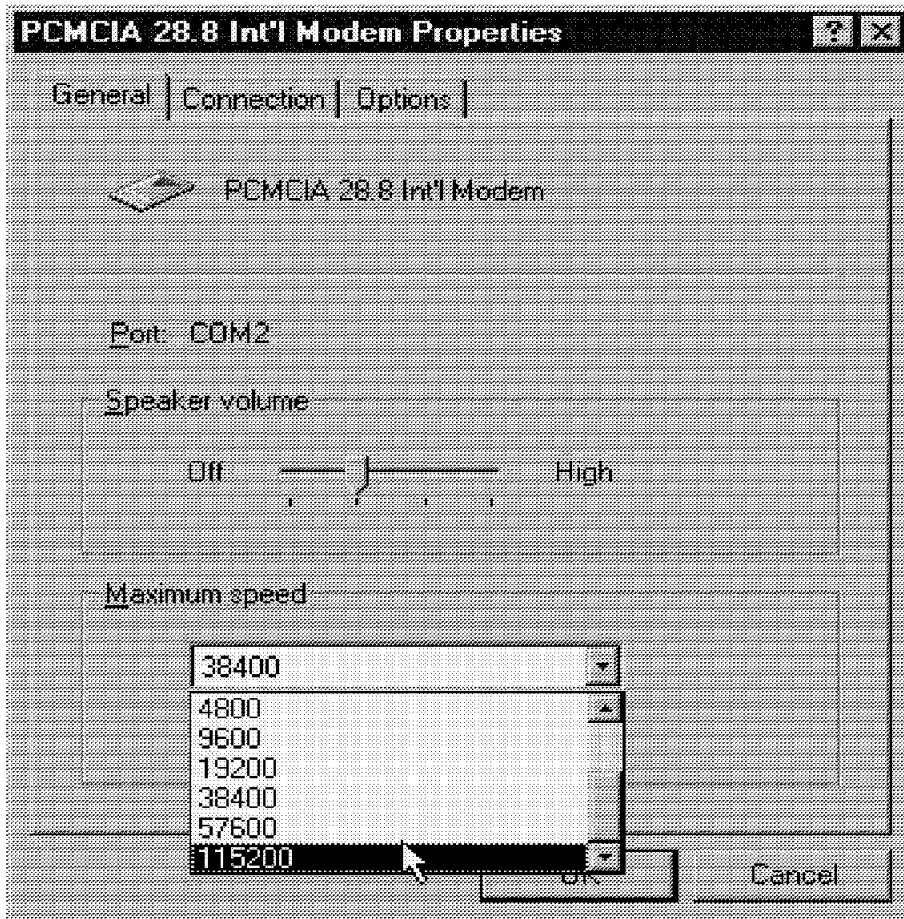


Figure 67. Selected Modem Properties

The Maximum speed parameter you select must match your modem's capabilities as well as the Connection Server modem capability. For example, if your modem is capable of 33600 baud, but the Connection Server modem is only capable of 14400 baud, the duration of handshaking at connection time will be longer than necessary due to negotiation of the modems over a compatible speed.

Once you have selected a suitable modem speed, select **OK**. You will return to the window shown in Figure 66 on page 111. Select **Next** to continue.

5. Enter the phone number of the Connection Server modem. This should be provided to you by the Remote Access Services administrator. You must also enter your country, as shown in Figure 68 on page 113.

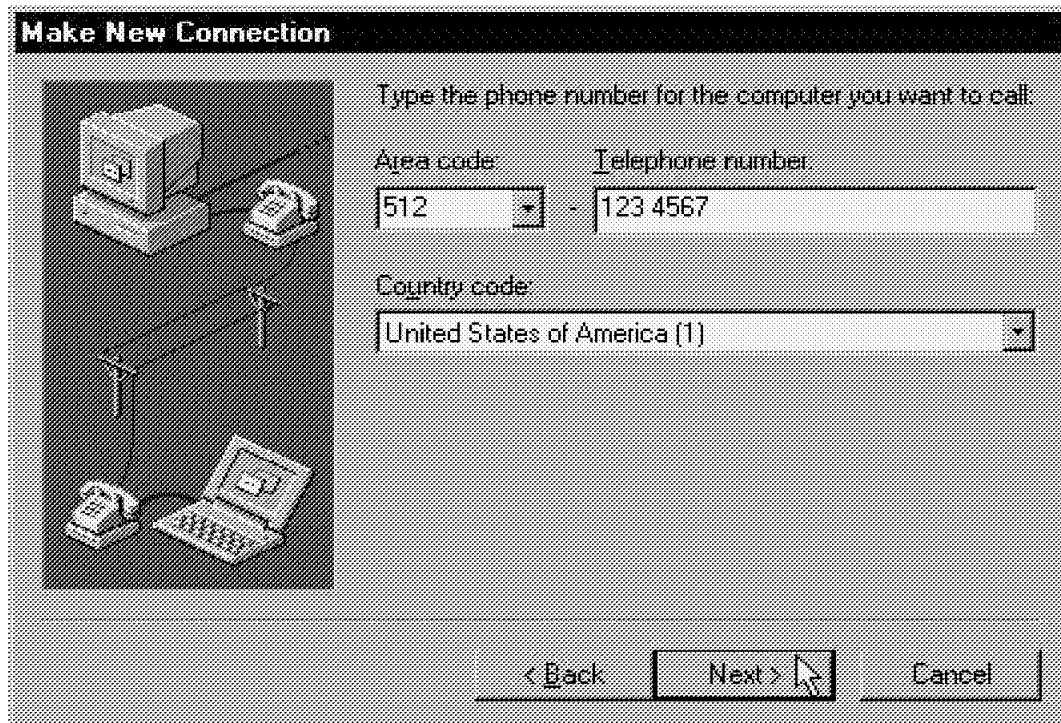


Figure 68. Connection Server Modem Number and Country Code Entry

6. After entering the Telephone number and Country code, select **Next**.
7. Complete the entry by selecting **Finish** when prompted. Once this is done, you will return to be back to the Dial-Up Networking window shown in Figure 65 on page 110. Your new configuration is represented by a new icon displayed in the window.

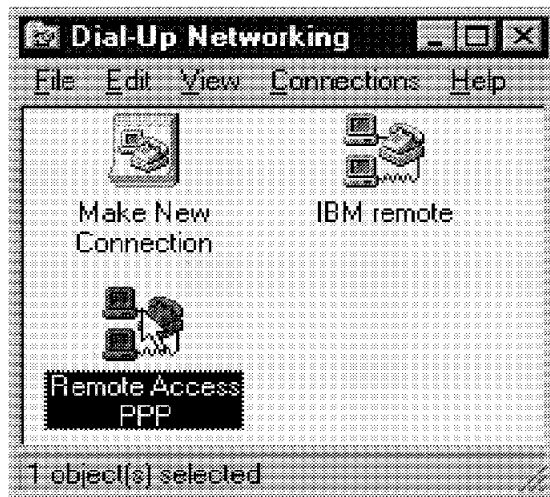


Figure 69. Dial-Up Networking with New Entry

8. Configure the server communications parameters in Dial-Up Networking. To do this, right-mouse-button click on the new icon and select **Properties**, as shown in Figure 70 on page 115.

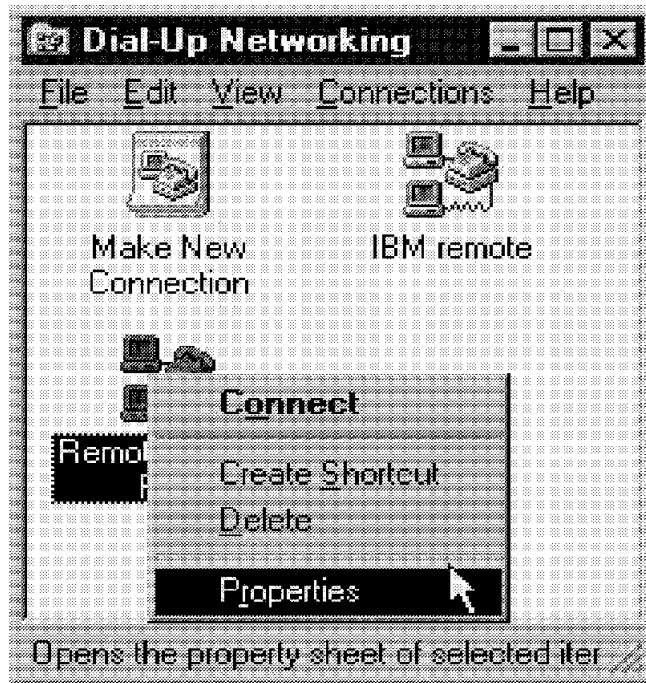


Figure 70. Selecting Dial-Up Networking Properties

9. Click on **Server Type**, as shown in Figure 71 on page 116.

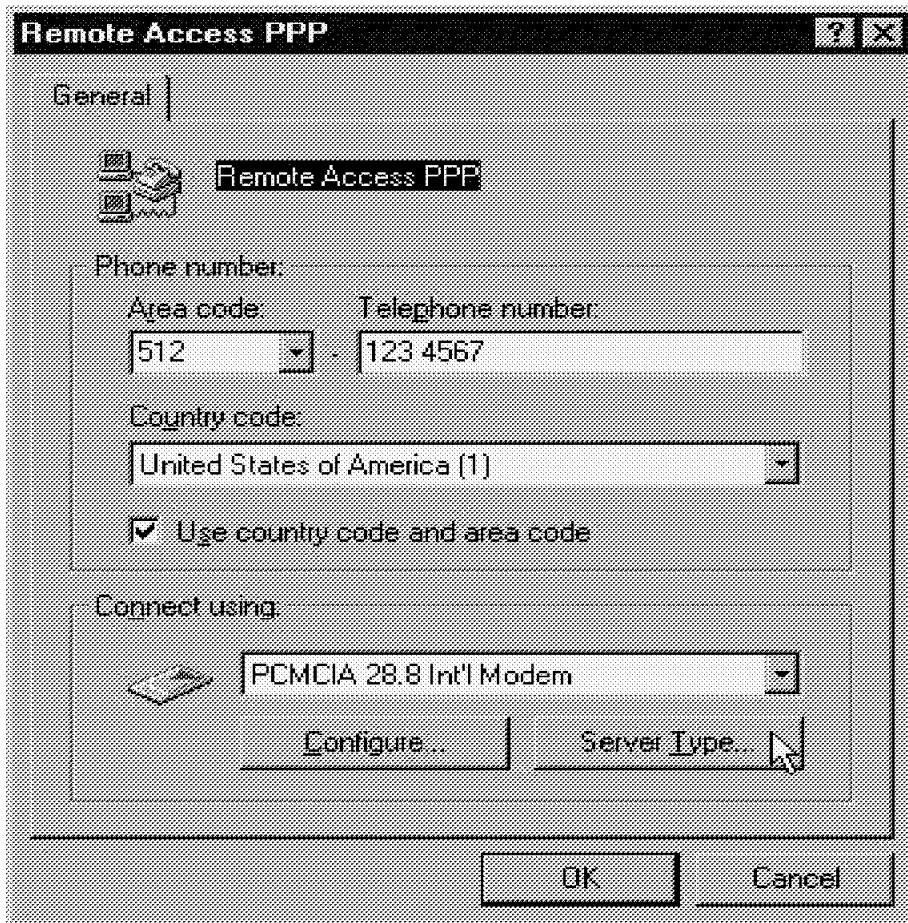


Figure 71. Configure Server Type Window

10. In the Type of Dial-Up Server field, select **PPP:Windows 95, Windows NT 3.5, Internet**.
11. Select **TCP/IP** in the Allowed network protocols field.
12. Select **TCP/IP Settings**, as shown in Figure 72 on page 117.

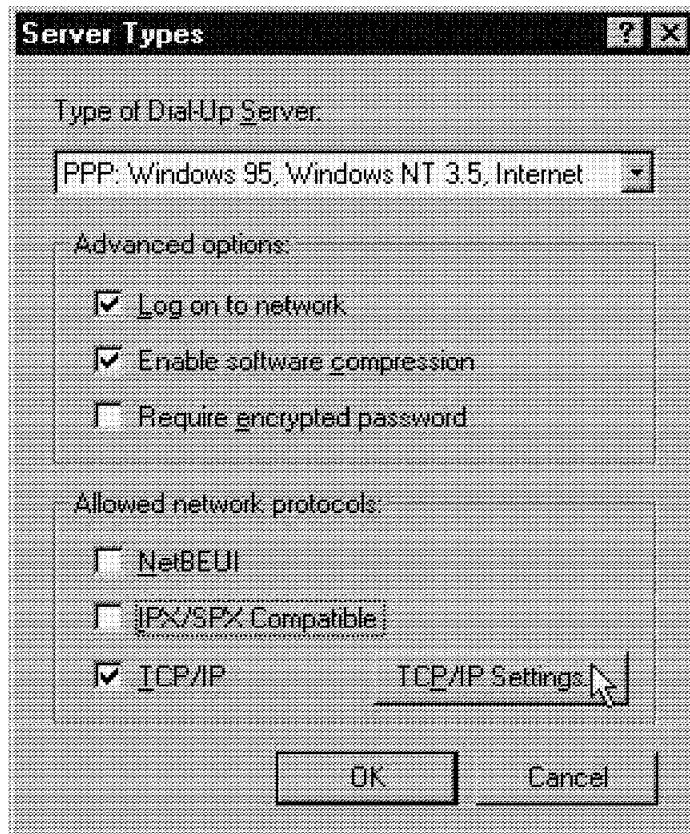


Figure 72. Dial-Up Server Settings

13. You must configure your IP address, as requested by your Remote Access Services Administrator. For example, if your Remote Access Services Administrator has configured the IBM Enhanced Remote Access workstation to issue IP addresses using the ObtainIPAddr=LIST or ObtainIPAddr=DHCP parameters in \WAL\WCLLOCAL.INI, you must select **Server assigned IP address**, as shown in Figure 73 on page 118. However, if you were advised by your Administrator to use your static IP address, select **Specify an IP address** and then enter the IP address in the IP address field.
14. Configure the domain name server to be used. If the parameter DDNS=YES is specified in \WAL\WCLLOCAL.INI, you should select **Server assigned name server addresses**. However, if DDNS=NO in \WAL\WCLLOCAL.INI, you should select Specify name server addresses and enter the Primary and Secondary DNS IP addresses, as specified by your TCP/IP administrator.

Leave the Primary WINS and Secondary WINS fields set to 0.0.0.0, as these are not required.

15. Select **OK** to return to the previous window.

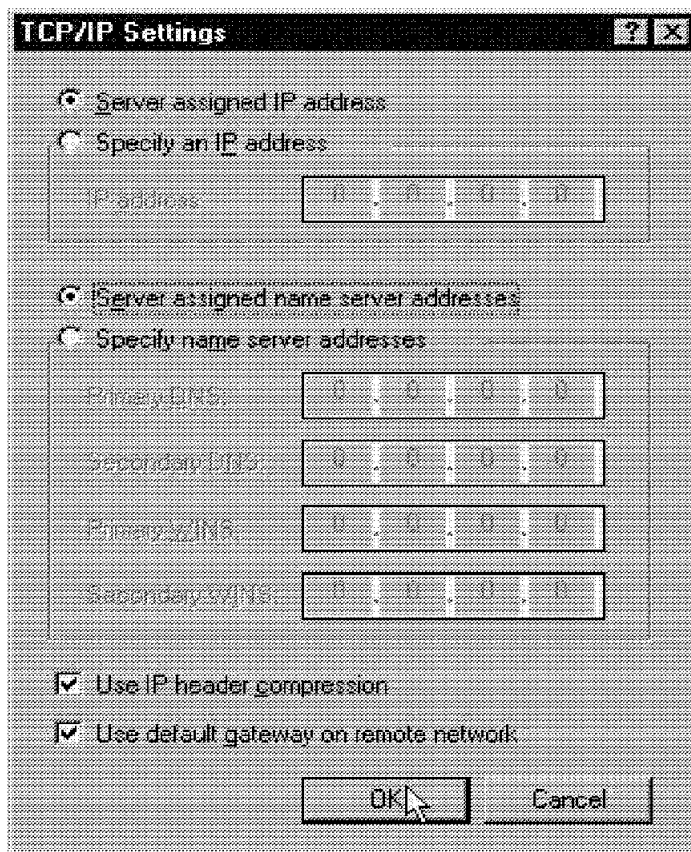


Figure 73. Dial-Up Networking TCP/IP Configuration

16. Select **OK** in the Server Types window to complete the TCP/IP configuration of Dial-Up Networking, as shown in Figure 74 on page 119.

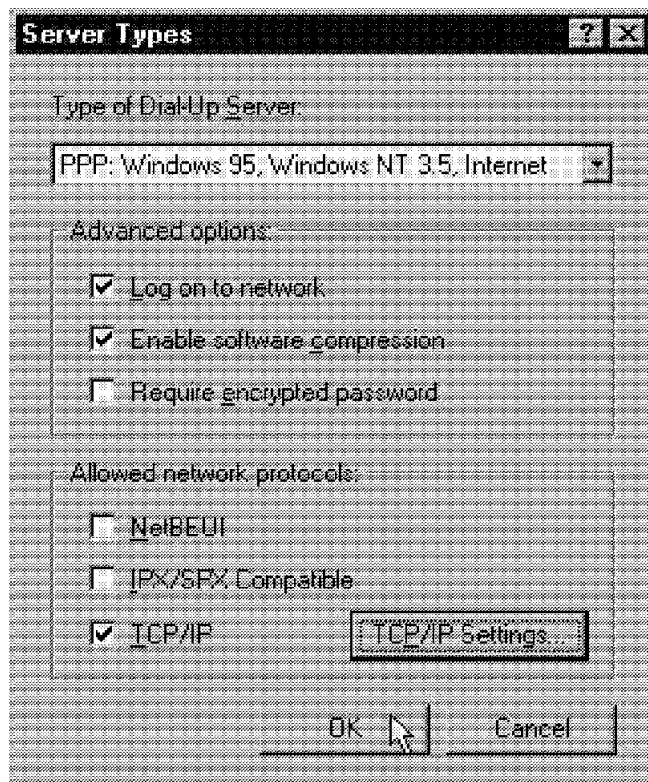


Figure 74. Server Types Configuration Window

17. Try to connect to the IBM Enhanced Remote Access Connection Server. Select the icon you just modified in the Dial-Up Networking window (shown in Figure 69 on page 114).
18. The Connect To window is displayed, as shown in Figure 75 on page 120. Enter your PPP user ID (allocated to you by your Remote Access Services Administrator) in the User name field.

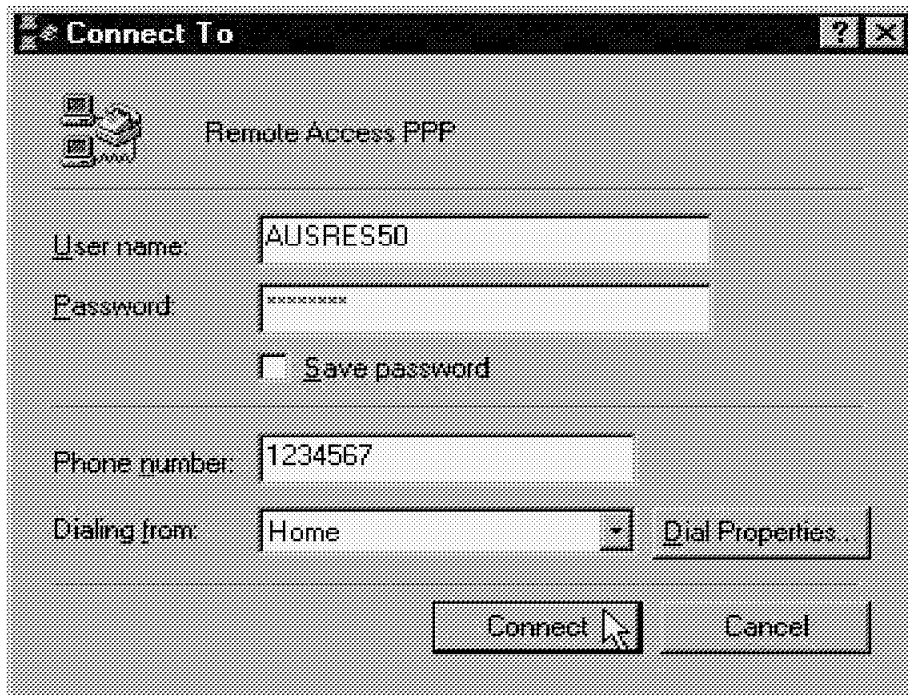


Figure 75. Connect To Window

19. Enter your password and select **Connect**. The modem will dial the configured number and start a PPP connection. After the modems have completed the negotiation process, the Windows 95 PPP client will be authenticated by the Connection Server, as shown in Figure 76.



Figure 76. Connecting to Enhanced Remote Access Services

20. After the authentication has completed, the Connected to window will be displayed, using the name of the current remote workstation configuration (Remote Access PPP, in this case). You can check that

TCP/IP protocol is active by selecting **Details**, which shows the information seen in Figure 77 on page 121.

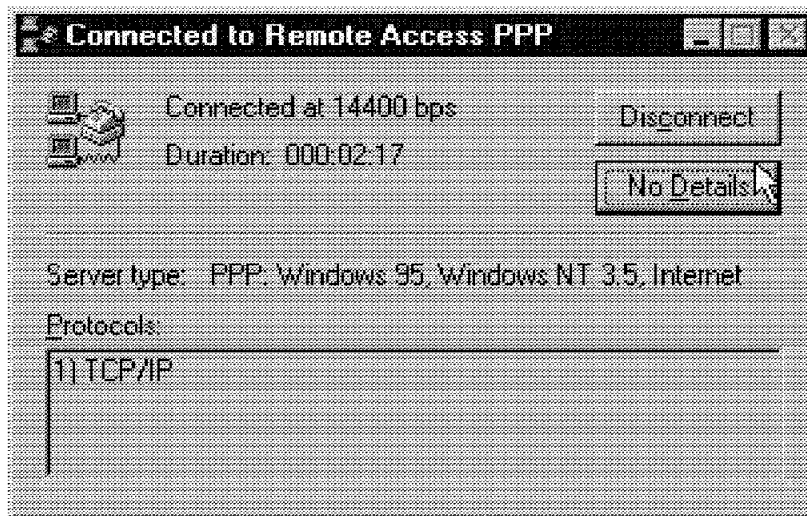


Figure 77. Connected to Window

You can now use TCP/IP services, such as FTP, Web browsing and so on.

If you have the NetBEUI protocol loaded on your Dial-Up Adapter, you can also logon to LANs, using the IBM Networks Client for Windows 95 (a free item available from the IBM Software Choice Website; refer to section 2.6, "Accessing the Software Choice Home Page" on page 29, for directions on accessing IBM Software Choice). You must first select the **Logoff** button and after logoff has completed, select the **Logon** button and enter your LAN user ID, password and domain in the Logon panel.

When you have finished working, you can terminate the connection by selecting **Disconnect** on the Connected to window shown in Figure 77.

3.5.4 Windows NT Version 4 PPP Clients

Install and configure Dial-Up Networking. The process used is the same as for Windows 95.

For a full description of installation and configuration of a Windows NT PPP client, refer to the IBM redbook titled *Network Clients for OS/2 Warp Server: OS/2 Warp 4, DOS/Windows, Windows 95/NT, and Apple Macintosh*, SG24-2009 (in press).

3.5.5 OS/2 Warp PPP Clients

Two types of OS/2 Warp PPP clients will be installed and configured on OS/2 Warp Version 4 in the following sections:

1. IBM Dial-Up for TCP/IP Version 2.0
2. IBM 8235 DIALs Client Version 4.52

3.5.5.1 IBM Dial-Up for TCP/IP Configuration

1. From the Desktop, open the Programs folder, and you will see window shown in Figure 78.

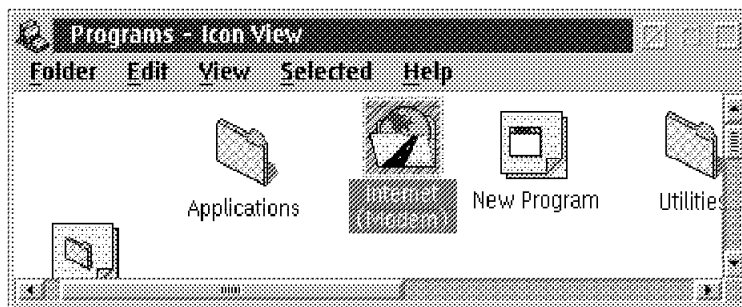


Figure 78. Programs Folder Contents

2. Double-click the **Internet (Modem)** folder to see the window shown in Figure 79.

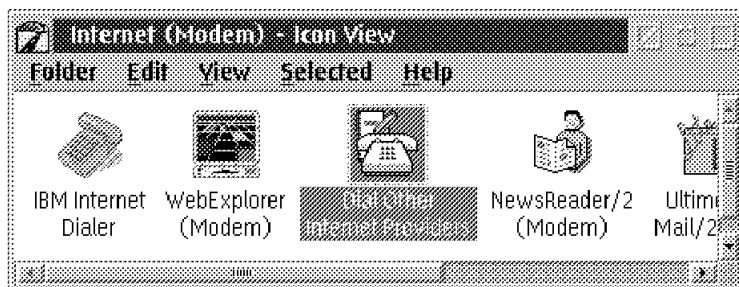


Figure 79. Internet (Modem) Folder Contents

3. Select the **Dial Other Internet Providers** object. Our program example is Revision 1.19, which can be found on the main panel by selecting the **Help** menu option and **Product Information**. You may have Revision 1.16.

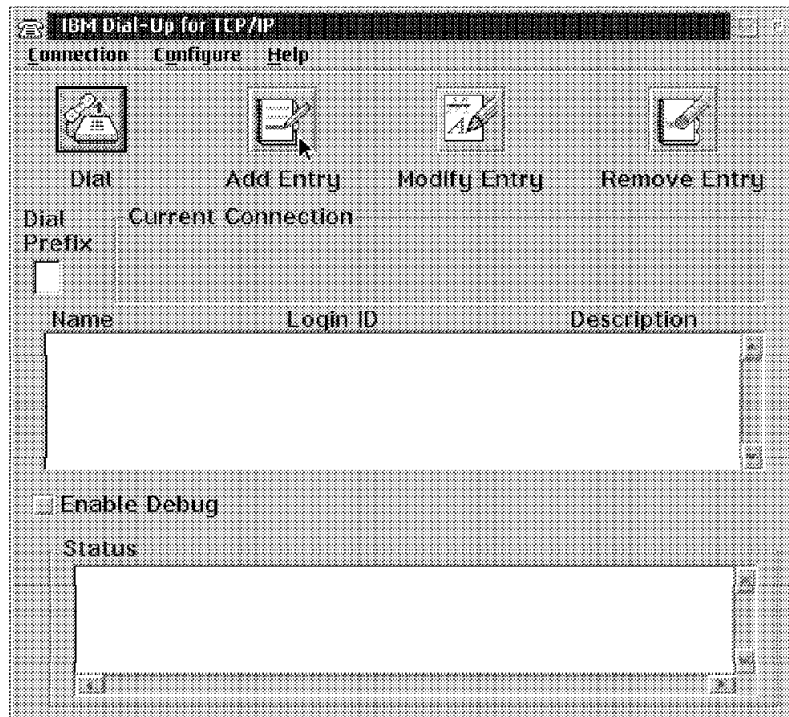


Figure 80. Internet Dialer New Entry

4. Select **Add Entry** so you can define the call and TCP/IP details.

Add Entries

*Name:

Description:

Login ID:

Password: ☒ Required

Phone Number:

Login Sequence:

Connection Type: ☐ SLIP ☒ PPP

Inactivity Timeout Option:

Minutes to Wait Before Automatic Hangup:

(* = required field)

Page 1 of 4

Login Info
Connect Info
Server Info
Modem Info

Figure 81. Login Info Tab of the Add Entry Dialog

5. Enter details as follows:
 - a. Name is the name of the call entry, such as PPP.
 - b. Description is a short description of the call entry, such as PPP ITS0.
 - c. Login ID is the PPP user ID assigned to you by the Connection Server administrator.
 - d. Password is the PPP password assigned to you by the Connection Server administrator.
 - e. Phone Number is the phone number to dial to reach the IBM Enhanced Remote Access Connection Server.
 - f. Login Sequence is a series of send-expect verbs, which are case sensitive. Leave the field as it is.

g. Connection Type should be set to PPP.

Note: Required fields are highlighted with an asterisk (*).

6. Select the **Connect Info** tab, and you will see the window shown in Figure 82:

The screenshot shows the 'Add Entries' dialog box with the 'Connect Info' tab selected. The dialog contains the following fields and controls:

- Fields:**
 - Your IP Address: []
 - Destination IP Address: []
 - Netmask: 255.255.255.0
 - *MRU Size: 1500
 - *Domain Nameserver: 9.3.1.74
 - Your Host Name: []
 - *Your Domain Name: itsc.austin.ibm.com
- Checkboxes:**
 - ☒ VJ Compression
 - ☐ Primary Interface
- Buttons and Text:**
 - Help button
 - (* = required field)
 - Page 2 of 4

Figure 82. Connect Info Tab of the Add Entry Dialog

7. Fill in details on this panel as provided by your Connection Server administrator. In this example, the IP address field is left blank, as it is being allocated by the DHCP function of the Connection Server. The application automatically enters 1500, the maximum size for the Maximum Response Unit (MRU, largest data size for PPP transmission), and also enables Van Jacobsen (VJ) header compression, used on TCP packets.

The other two fields that are required to be entered are:

- a. Domain Nameserver—the 32-bit dotted decimal notation IP address of the server that resolves host names to IP addresses, in our case, 9.3.1.74.
 - b. Your Domain Name—the name of the TCP/IP domain in which your computer resides, in our case, itsc.austin.ibm.com.
8. Select the **Server Info** tab to see the window shown in Figure 83.

The screenshot shows a window titled "Add Entries" with a tabbed interface. The "Server Info" tab is selected and highlighted. On the right side of the window, there are four tabs: "Login Info", "Connect Info", "Server Info" (which is active), and "Modem Info". A mouse cursor is pointing at the "Server Info" tab. The main area of the window contains two sections of input fields. The first section, titled "Default Servers/Hosts", includes three labels with corresponding text boxes: "News Server:", "Gopher Server:", and "WWW Server:". The second section, titled "Mail Server Information", includes six labels with corresponding text boxes: "Mail Gateway:", "POP Mail Server:", "Reply Domain:", "Reply (Mail) ID:", "POP Login ID:", and "POP Password:". At the bottom center of the window is a "Help" button. In the bottom right corner, it says "Page 3 of 4" with a double arrow icon.

Figure 83. Server Info Tab of the Add Entry Dialog

9. Enter the names of optional servers here, such as News Server, Gopher Server, and so on. It is not necessary to enter anything in these fields, unless you want to run IBM Web Explorer.
10. Select the **Modem Info** tab to see the next window, shown in Figure 84 on page 127.

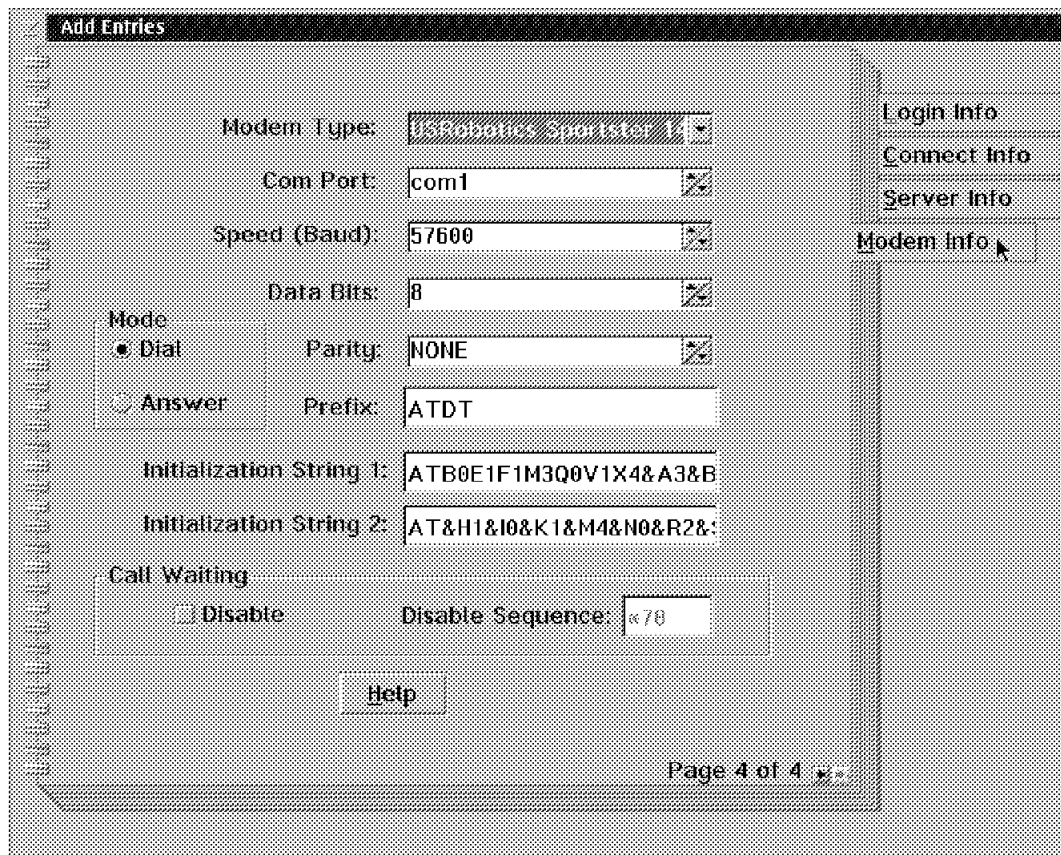


Figure 84. Modem Info Tab of the Add Entry Dialog

11. Select your modem from the list in the Modem Type field.
12. Adjust the speed to the maximum your hardware will support.
13. Close the Add Entries dialog by double-clicking on the title-bar icon, and the following window (shown in Figure 85 on page 128) appears:



Figure 85. Closing Dial Configuration Confirmation Window

14. Select **Save** to save the dial entry.
15. The IBM Dial-Up for TCP/IP window (shown in Figure 86 on page 129) appears again, but now your new entry (PPP) appears.

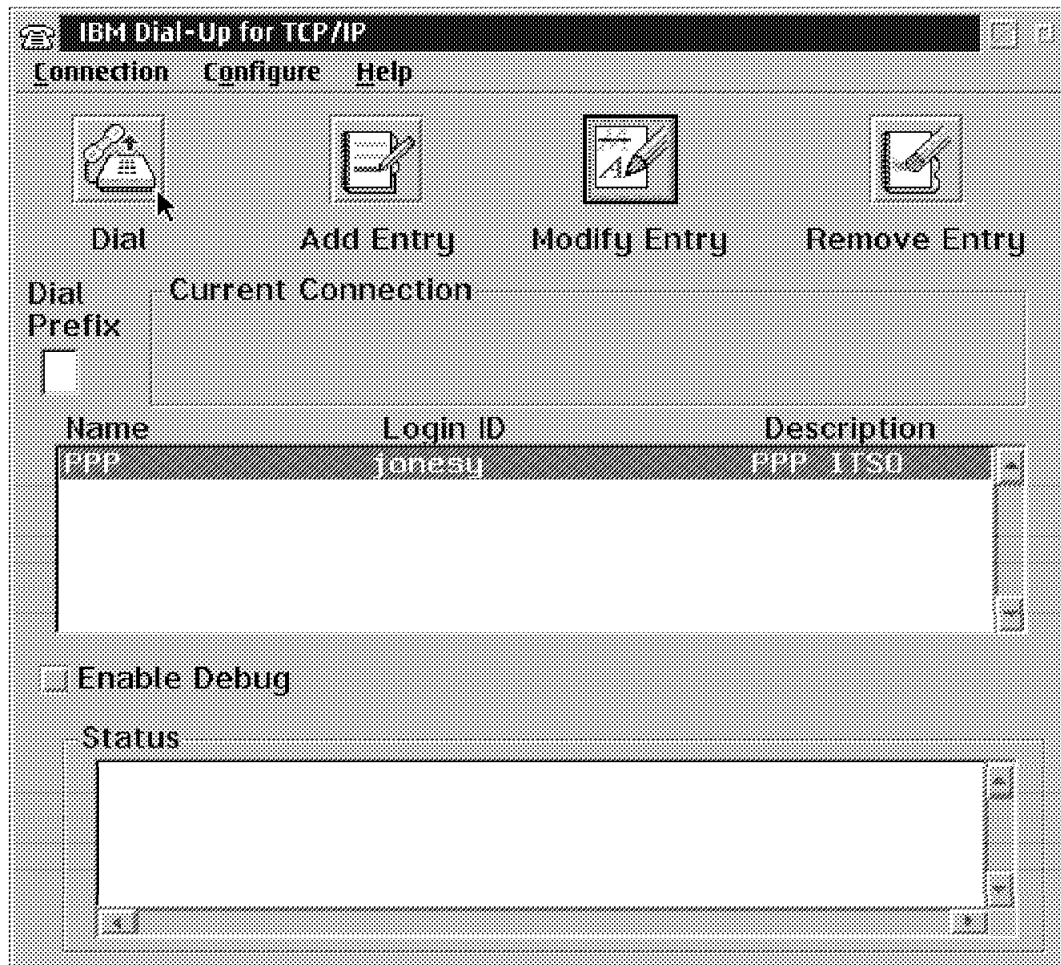


Figure 86. IBM Dial-Up for TCP/IP Window with New Entry

16. You can dial and connect to the IBM Enhanced Remote Access Connection Server by clicking the **Dial** icon. The connection is made, and the connection messages appear in the Status window, as shown in Figure 87 on page 130. It shows an example of a PPP connection with a DHCP-assigned IP address allocated.

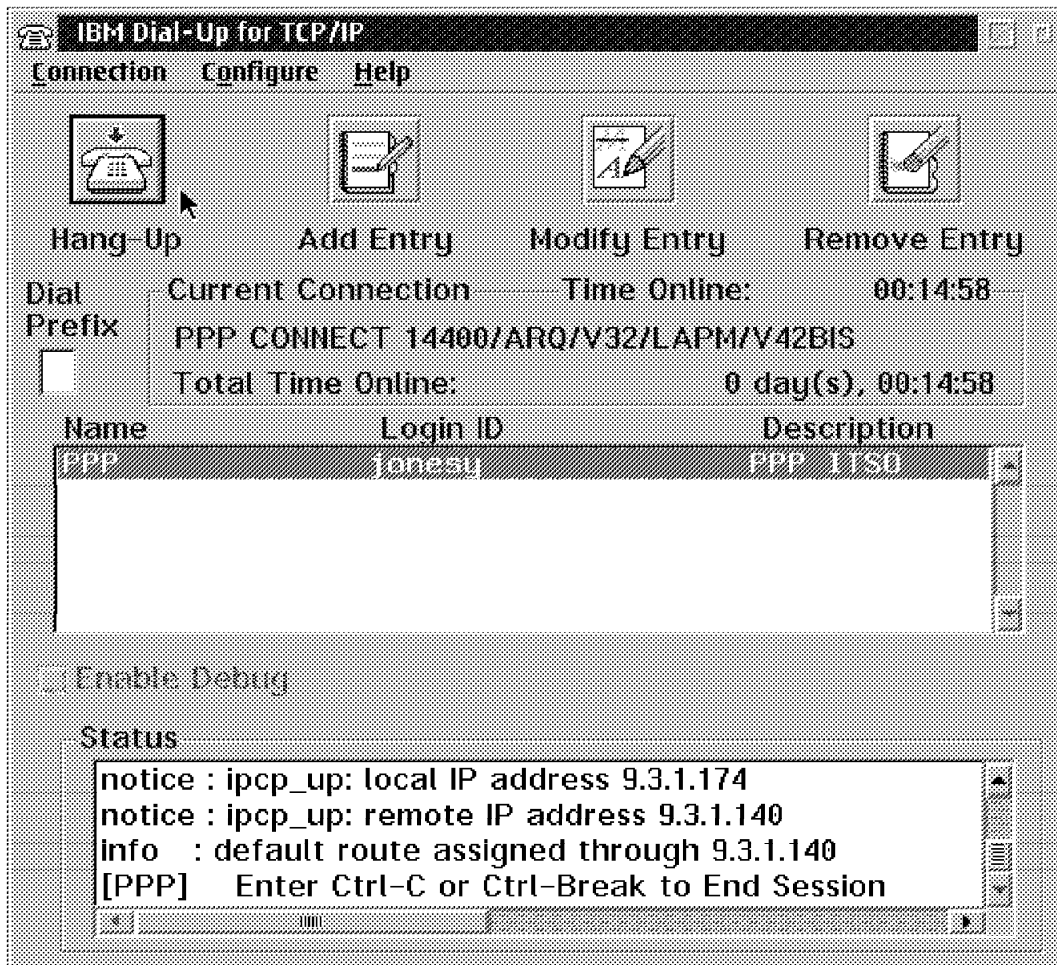


Figure 87. Connecting to an IBM Enhanced Remote Access Connection Server

17. You may begin using TCP/IP services. When you have finished working, you may end the connection by clicking the **Hang-Up** icon.

3.5.5.2 Configuring the IBM 8235 DIALs Client for OS/2 Version 4.52

1. Install IBM 8235 DIALs for OS/2 Version 4.52 by inserting the diskette in drive A:, typing the command A:\SETUP2, and replying to prompts, such as which directory to install the software, as shown in Figure 88 on page 131 .

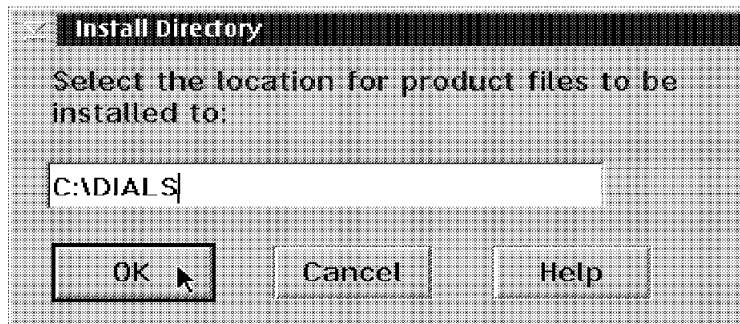


Figure 88. Installation Directory for DIALs Client

2. Select the proper communications port and also select your Modem Name from the drop-down menu list.

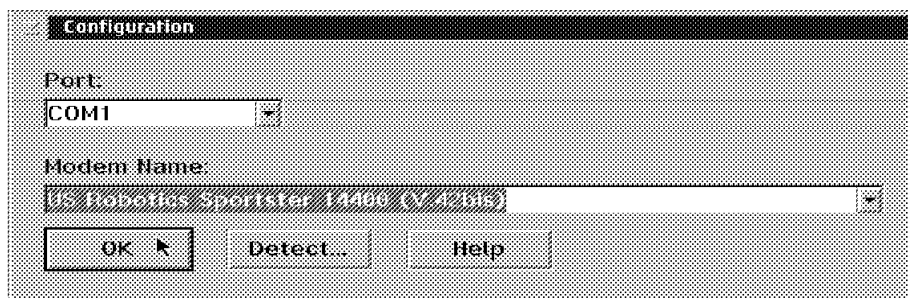


Figure 89. Modem and Port Selection for DIALs Client

3. After the installation program has completed, you will receive the following prompt, shown in Figure 90 on page 132.

Note: Do not run Shuttle to REMOTE yet—you must install the patches for the DIALs client first.



Figure 90. IBM 8235 DIALs Installation Complete Window

4. You must install the patch for IBM DIALs Client/2 Version 4.5.2. You can get the patch from the World Wide Web (WWW) at the URL:
<http://www.networking.ibm.com/nes/nes8235.htm>
 Follow the instructions included with the patch in the 452P1.TXT file.
5. Shut down and restart your system.
6. Open an OS/2 window and back up the CONFIG.SYS, IBMLAN.INI and PROTOCOL.INI files. Exit the OS/2 window.
7. Open the DIALs/2 folder and select **Shuttle to REMOTE**, as shown in Figure 91 .

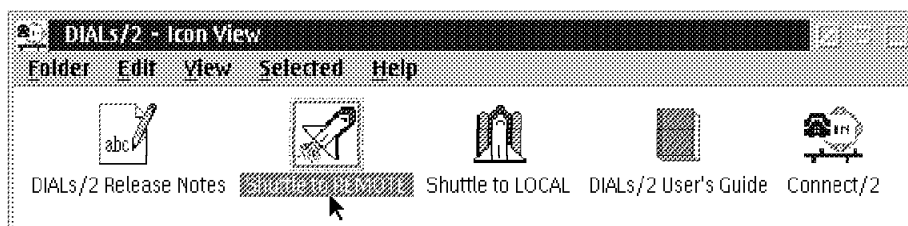


Figure 91. DIALs/2 Folder Contents

The first time Shuttle to REMOTE is run, a number of configuration files are created. A separate configuration for LAN connections are created with the files CONFIG.LAN and PROTOCOL.LAN in a new directory called \SHUTTLE2. There is also a separate configuration for remote connections in the SHUTTLE2 directory, with files CONFIG.DIA and PROTOCOL.DIA.

Each time you select Shuttle to REMOTE, you are in fact copying \SHUTTLE2\CONFIG.DIA to \CONFIG.SYS and \SHUTTLE2\PROTOCOL.DIA to \IBMC\PROTOCOL.INI. Similarly, when you select Shuttle to LOCAL, you are copying \SHUTTLE2\CONFIG.LAN to \CONFIG.SYS and \SHUTTLE2\PROTOCOL.LAN to \IBMC\PROTOCOL.INI.

Since these configuration files are read at system startup, you must reboot your workstation for the changes to take effect.

8. After the Shuttle to REMOTE has completed, you must shut down and restart OS/2 Warp so that the DIALs Client NDIS driver can load.
9. When the OS/2 Desktop has completed loading, open the DIALs/2 folder and select **Connect/2** (shown in Figure 91 on page 132).
10. Enter a description for the connection in the Description field, such as DIALs to Enhanced Remote Access. Enter your PPP user ID in the Dial-in Name field. Also, enter the phone number to dial in the Phone Number field. This is shown in Figure 92.

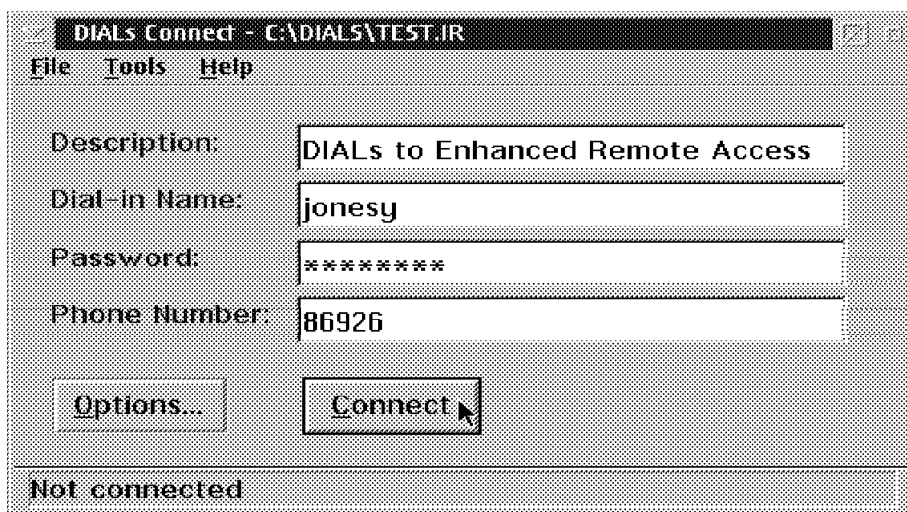


Figure 92. DIALs/2 Connection Information

11. Now select the **Options** button and enable the IP protocol. Also enable NetBEUI/LLC if you are going to log on to servers using the TCPBEUI protocol.

Note: You will receive a warning after connecting with NetBEUI/LLC enabled. Ignore this error message because NetBEUI frames are actually sent over the link in IP frames, according to RFC 1001/1002.
12. If you must use a static IP address, enter it in the IP Address field. If you wish to be allocated an IP address by either the DHCP server on your LAN, or by the IBM Enhanced Remote Access Connection Server, leave the IP Address to the default value - 0.0.0.0.
13. Select **OK** to accept the changes.
14. You can save this configuration by selecting **File** and **Save As**. Enter a suitable file name, with an extension of .IR, such as LDPPP.IR. You may also create an icon in the DIALS/2 folder, by selecting **File**, then **Make Icon** and finally enter an appropriate name for the icon in the Icon Name field. Select **OK** to create the icon.
15. You may establish a connection to the IBM Enhanced Remote Access Connection Server by entering your passphrase in the Password field and clicking on the **Connect** button.
16. After the connection has been established and your user ID has been authenticated, you may begin using IP services.
17. When you have finished work, you may select **Disconnect** to hang up.

3.6 Administration

The following sections discuss various required administration tasks, including:

- Changing passphrases after migration
- Security:
 - Recovering the administrator passphrase
 - Setting PPP user passphrases
- IP address administration

3.6.1 Changing Passphrases after Migration

When an existing Connection Server is migrated to IBM Enhanced Remote Access, PPP support is added. The algorithms used to store passphrases for PPP clients are different than for the existing LAN Distance clients. Because of this, each user ID in the LAN Distance Database (WCBUSRF.ISF) must now store the passphrase in two formats:

- LAN Distance client passphrase (using one-way Data Encryption Standard (DES) encryption)
- PPP Client passphrase (using MD5 encryption)

This is done when new IDs are created after the migration. For existing user IDs, the administrator must change the password in order for both passphrase types to be stored with the user ID. This will enable any ID to be used by a PPP client or a LAN Distance client.

3.6.2 Recovering the Administrator Passphrase

During the installation of IBM Enhanced Remote Access Connection Server, the security administrator user ID and passphrase were entered, as shown in Figure 45 on page 85.

If the user ID or passphrase for the administrator is lost or forgotten, you can use the following procedure to recover it:

1. Shut down the IBM Enhanced Remote Access Connection Server by double-clicking on the title-bar icon.
2. Open an OS/2 window and type `CD \WAL`.
3. Copy the security database file `\WAL\WCBUSRF.ISF` to another name. For example, `COPY WCBUSRF.ISF *.BAK`.
4. Make a temporary directory (with the command `MD TEMP`) and then change into that directory with `CD TEMP`.
5. Get the default security database file from the first IBM Enhanced Remote Access Connection Server diskette. Use `PKUNZIP2.EXE` to unzip the `INITRS.ZIP` file into the temporary directory. Copy the `WCBUSRF.ISF` file into the `\WAL` directory. Delete the files in the temporary directory and then remove temporary directory.
6. Start the IBM Enhanced Remote Access Connection Server.
7. Log on to the Connection Server using the user ID `SECADMIN` with a passphrase of `SECADMIN`. When prompted, change the passphrase to whatever you choose.

Note: The passphrase is case sensitive; however, user IDs are not.

At this time, there is only one user ID in the security database, the `SECADMIN` ID.

8. Open an OS/2 window and use the merge function of the `CMPROCESS` security database utility to recover the old security database. For example, if the `WCBUSRF.ISF` file was copied to `WCBUSRF.BAK`, issue the following command to merge the old database into the new one:
`CMPROCESS /CT:ME /FI:WCBUSRF.BAK /FO:MERGE.TXT`

Where MERGE.TXT is the merge output report. You should review this file to ensure the user IDs from the old security database were merged successfully. Figure 93 on page 136 shows an example of output from the CMPROCES utility:

```
The file to be merged is: WCBUSRF.BAK

The result of the merge
-----

  User ID      Return Code
-----
    ADMIN          0
    JONESY         0
    MARKO          0
    FHINNER        0

The number of user ID have been process:  4
```

Figure 93. CMPROCES Utility Database Merge

Note: A Return Code of 0 means merge of this user ID completed successfully. A Return Code of 17 means that this user ID was in the original security database as well as in the merged security database. In this situation, the original user ID is kept.

9. Change the passphrases of the old security administrator user IDs. Once this is complete, you have successfully recovered administrator control over the security database.

Note: The above process allows anyone with physical access to the IBM Enhanced Remote Access Connection Server workstation to grant themselves administrator access. It is therefore recommended that physical access to the IBM Enhanced Remote Access Connection Server be restricted to prevent unauthorized access.

3.6.3 PPP Security

Since PPP clients authenticate with a PPP server using CHAP or PAP, the MAC address—either Universal Adapter Address (UAA) or Locally Administered Address (LAA)—is not required. This means that a person connecting using PPP can do so from any machine that is correctly configured.

This is different from LAN Distance and Remote Access Services clients, which can be restricted to (up to eight) workstations by including the UAA or LAA of the workstations they use to connect to the Connection Server.

PPP client passphrases cannot be changed by the client. This means when the Connection Server administrator is requested to reset a passphrase, or entering a new user ID, the administrator must:

1. Log on as an administrator and right-mouse-button select **User Administration**.
2. Select the user ID which required a passphrase change (or select **Add** to enter a new user ID).
3. Select the **Passphrase** tab.
4. Enter a passphrase in the Passphrase field and Verify Passphrase field.
5. Save the changes by double-clicking on the title-bar icon.
6. Log off the administrator user ID.
7. Log on locally with the new user ID and use the initial passphrase.
8. After being prompted, enter a new passphrase and verify the new passphrase. This is the passphrase to be communicated to the user.

3.6.4 IP Address Configuration

PPP IP addresses can be administered in any of three ways:

1. Client-specified: If your site uses static IP addressing where a fixed IP address is allocated to a user, the Connection Server does not need to be configured to issue IP addresses.
2. Listed on the LAN Distance connection server.
3. Allocated by Dynamic Host Configuration Protocol (DHCP) services on the LAN.

The WCLIPADR.INI and WCLLOCAL.INI files must be customized to suit your site requirements. This means the IBM Enhanced Remote Access Connection Server administrator will need to communicate with the IP administrator to decide the most suitable method for your site.

3.7 Problem Determination

With the addition of PPP support in IBM Enhanced Remote Access, the problem determination process is essentially the same as in previous versions. When analyzing problems, it is helpful to view the logon process as a sequence of phases:

1. Establish physical connection

Did the remote client send commands to its modem successfully? Did the modem dial out using the interface provided? Was the Connection Server reached successfully?

2. Link Control Protocol (LCP) negotiation

The Connection Server determines if the client is using PPP (by sending a PPP frame) or the existing LAN Distance protocol (by sending an XID frame). For PPP establishment, each end of the data link must send LCP packets to configure and test the link before negotiation can continue. This layer also terminates the link.

If the failure occurs at this layer, take a PPP trace to obtain more information on the reason for the failure. Make sure a new ID was added for PPP or an existing ID had its password changed by the administrator.

3. Authentication

The client and server must agree on the type of authentication to be used, either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP), based on the type specified in the `pppSecurity` parameter of the `\WAL\WCLLOCAL.INI` file on the Connection Server.

If the remote client is not capable of PAP and/or CHAP authentication, errors will occur in this phase. This can be determined by a PPP trace.

4. IPCP Negotiation

The remote client must obtain an IP address from either its own configuration, from a list on the Connection Server, or from a DHCP server on the LAN, as specified by the `ObtainIPAddr` parameter in the `WCLLOCAL.INI` file on the Connection Server.

Make sure that the client's IP address was obtained in a manner that the Connection Server is configured for. For example, if the client has a hard-coded address, then the `ObtainIPAddr` parameter should include `USERSPEC`. On heavily-utilized networks, the remote client might time out waiting for a DHCP server to respond.

After these steps are completed, the remote client is fully connected and can attempt to access resources on the LAN. If a resource cannot be accessed, try to PING from the Connection Server to the resource to ensure that there are no problems on the LAN.

Other utilities for problem determination include the trace functions in the Tracking notebook and any programs provided by the client. For example, the 8235 DIALs for OS/2 client includes a `PPPLOG.EXE` program that can be used to trace the client connection, which includes the configuration negotiation exchange and IP address assignment.

3.8 IBM Enhanced Remote Access PPP Internal Architecture

This section describes the architecture of IBM Enhanced Remote Access Connection Server for OS/2 Warp Server, which allows IBM Enhanced Remote Access to support PPP, LAN Distance and Remote Access Services Remote Client workstations. The IBM Enhanced Remote Access PPP implementation is based on the current IBM TCP/IP implementation of the protocol.

Figure 94 shows the various components of IBM Enhanced Remote Access Connection Server for OS/2 Warp Server.

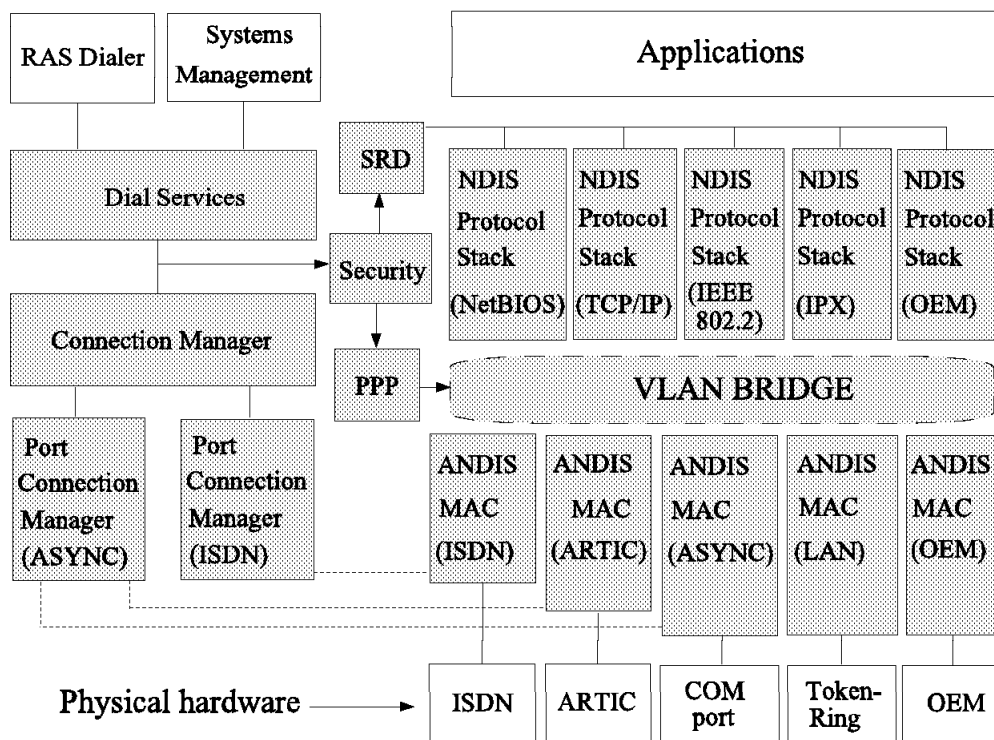


Figure 94. IBM Enhanced Remote Access Protocol Architecture

When the Connection Server is configured for "flows" mode and an answer to a call is accepted, the server always waits for the client to respond in order to determine the type of client that has just connected. A LAN Distance or Remote Access Services client always sends an XID frame, and

a PPP client always sends a PPP frame. The server will respond with the appropriate response, based on the client type.

The security component authenticates the client, based on the client response at connection time. PPP clients use CHAP or PAP authentication, while LAN Distance and Remote Access Services clients continue to use TPAP authentication. The differences between PAP and CHAP are described:

- PAP** Password Authentication Protocol is a simple, two-way mechanism which is done when the link between the remote client and server is initially established. Although RFC 1334 specifies that the default is to have passwords sent in clear text format, vendor implementations can encrypt this password before sending it over the link to be processed by the server.
- CHAP** Challenge Handshake Authentication Protocol (CHAP) is a stronger authentication mechanism. The server sends a CHAP Challenge packet to the remote client, which must calculate the proper value using a one-way hash function (MD5) and return it to the server. This is done at link establishment and can be repeated with a new Challenge value anytime after the link establishment. This protects against intruders using a "record and playback" scheme to gain access to servers.

A LAN Distance or Remote Access Services client uses bridgeable LAN frames as the frame type to transport data between the client and the server and for asynchronous links uses ISO 3309 to encapsulate the LAN frame.

All PPP clients send raw protocol frames encapsulated in a PPP frame. Raw protocol frames can only be processed by the appropriate protocol stack. This requirement mandates that a routing function exist in the IBM Enhanced Remote Access Connection Server workstation. The Network Device Interface Specification (NDIS) IP router must be configured on the Connection Server to support PPP clients. The IP router function is provided by the MPTS component of OS/2 Warp Server.

A router requires that each side of the route be a separate IP subnet. IBM Enhanced Remote Access uses the Proxy ARP function provided by MPTS Version 5.11 which allows the LAN and WAN to be the same subnet.

PPP clients may or may not have an IP address configured. Clients that have not configured an IP address must be provided with one as part of PPP negotiation. The IBM Enhanced Remote Access Connection Server provides the PPP client with an IP address if the \WAL\WCLLOCAL.INI file has the ObtainIPAddr=LIST parameter. The first IP address allocated is the first IP

address in the file \WAL\WCLIPADR.INI, and subsequent IP addresses allocated are the next number from this file.

If the \WAL\WCLLOCAL.INI file parameter is ObtainIPAddr=DHCP, the IP address is assigned by a DHCP server on the LAN.

When an IP address is allocated by a DHCP server or the IBM Enhanced Remote Access Connection Server, the PPP user ID is used as the TCP/IP host name.

The major new component of IBM Enhanced Remote Access Connection Server for OS/2 Warp Server is a component called PPP, which is contained in a DLL module. By necessity (for performance reasons), PPP is tightly coupled with the Virtual LAN (VLAN) component.

The VLAN has been modified to implement PPP framing and to interoperate with the PPP component. This design structure allows additional non-LAN Distance clients to be added in future, with minimal changes.

The VLAN tasks are divided into two major states:

1. Logical connection phase, which includes authentication
2. Runtime phase

The objective of this design is to minimize the changes to the VLAN component and the tasks it performs, especially while in runtime phase. To accomplish this, most of VLAN's PPP frame handling is placed in the lowest layer VLAN subcomponent, called MACFH.

During the connection phase, MACFH gives the incoming PPP frame to the new PPP component for processing. When in the runtime phase, MACFH handles PPP encapsulation, PPP decapsulation, and adding a MAC header to the frame. The intent of this design is to limit the changes to the rest of the VLAN subcomponents by making the frame look like a bridgeable LAN frame that is destined for the protocol stack in the server.

The flows between the Connection Server and the LAN Distance or Remote Access Services client remain unchanged from previous releases.

When the Connection Server is configured for "no flows" mode, all frames pass through the VLAN unmodified, as they do for previous releases of Connection Server code.

The following table displays the various methods of security authentication used by IBM Enhanced Remote Access Connection Server for OS/2 Warp Server.

| <i>Table 5. Security Authentication</i> | |
|---|--|
| Client Type | IBM Enhanced Remote Access Authentication |
| Non-LAN Distance or non-Remote Access Services client, without PPP | No flows mode ¹ |
| Non-LAN Distance or non-Remote Access Services client, with PPP | CHAP, PAP or none |
| LAN Distance or Remote Access Services client, with no flows configured | No flows mode ¹ |
| LAN Distance or Remote Access Services client, with flows configured | TPAP or none |
| Note: ¹ No flows mode implies no user identification or authentication. | |

Table 6 shows communications compatibility between the various versions of LAN Distance, Remote Access Services Connection Server, and Remote Client as well as IBM Enhanced Remote Access Connection Server for OS/2 Warp Server.

| <i>Table 6 (Page 1 of 2). Compatibility Among Components</i> | | | |
|--|---|---|---|
| | IBM Enhanced Remote Access Connection Server | LAN Distance or Remote Access Services Connection Server | LAN Distance or Remote Access Services Remote Client |
| OS/2 LAN Distance or Remote Access Services Connection Server | Yes | Yes | Yes |
| OS/2 LAN Distance or Remote Access Services Remote Client | Yes | Yes | Yes |
| Windows LAN Distance or Remote Access Services Remote Client | Yes | Yes | Yes |
| Non-LAN Distance or non-Remote Access Services client without PPP • | Yes | Yes | Yes |

| <i>Table 6 (Page 2 of 2). Compatibility Among Components</i> | | | |
|---|---|---|---|
| | IBM Enhanced Remote Access Connection Server | LAN Distance or Remote Access Services Connection Server | LAN Distance or Remote Access Services Remote Client |
| Non-LAN Distance or non-Remote Access Services client with PPP | Yes | No | No |
| Note: ¹ No flows mode implies no user identification or authentication. | | | |

3.8.1 Reference Information

The following InterNIC Standard and Request for Comments (RFCs) are useful for those who want greater detail in the these areas:

- STD0051 The Point-to-Point Protocol Protocol (obsoletes RFC1549, RFC1661 and RFC1662)
- RFC1332 PPP IP Control Protocol (IPCP)
- RFC1334 PPP Authentication Protocols (PAP and CHAP)
- RFC1541 Dynamic Host Configuration Protocol (DHCP)
- RFC1570 PPP Link Control Protocol (LCP) extensions

Chapter 4. IBM Neighborhood Browser Enabler

The ability to share resources is one of the biggest advantages of networked computer systems. To provide a way to determine what resources are available for Microsoft Windows Clients, the IBM Neighborhood Browser Enabler was developed. The IBM Neighborhood Browser Enabler helps you to maintain a centralized list of available resources and servers in your domain. The IBM Neighborhood Browser Enabler eliminates the need for every Microsoft Windows Client to maintain a list of shared network resources. This lowers the network traffic required to build and maintain the list and also frees the CPU time each Microsoft Windows Client will need to create a network resource list.

To enable an OS/2 Warp Server to function as a master browser for Microsoft Windows Client, the IBM Neighborhood Browser Enabler for OS/2 Warp Server was developed. We refer to it as IBM Neighborhood Browser Enabler. The Master Network Browser functionality allows Microsoft Windows NT and Microsoft Windows 95 clients to view the domain's OS/2 Warp Server machines and their resources. This is done by the Network Neighborhood object.

4.1 Prerequisites

The IBM Neighborhood Browser Enabler is based on OS/2 Warp Server and thus requires OS/2 Warp Server as the minimum software level. However, if a Master Network Browser is installed on a OS/2 Warp Server machine in a domain which includes OS/2 LAN Server, you will see the resources and OS/2 LAN Servers that are down level.

IBM Neighborhood Browser Enabler supports the following protocols that are used by OS/2 Warp Server:

- NetBIOS/NetBEUI
- TCPBEUI (NetBIOS over TCP/IP)

Note: If you are using the IBM Neighborhood Browser Enabler in a TCPBEUI environment, the IBM Neighborhood Browser Enabler supports Microsoft Windows Client within a single subnet. Microsoft Windows Client can browse only OS/2 Warp Server domains in the clients' subnet.

Use the SYSLEVEL command to determine what your system's OS/2 Warp Server service level is. One of the following service levels is required before installing the IBM Neighborhood Browser Enabler:

- OS/2 Warp Server Version 4.0 and FixPak IP_8260
- OS/2 Warp Server Version 4.0 Symmetric Multiprocessing (SMP) Feature

If you try to install the IBM Neighborhood Browser Enabler on OS/2 Warp Server and the service level is not at least CSD IP_8260, the installation program returns back to the command prompt and displays the words DOWN LEVEL.

Note: Check with an IBM support representative to determine the latest Corrective Service Fix available for your national language version of OS/2 Warp Server or OS/2 Warp Server SMP.

4.2 IBM Neighborhood Browser Enabler Architecture

The IBM Neighborhood Browser Enabler is architected as a server service that is added to the SRVSERVICES line in the [server] section of the main OS/2 Warp Server configuration file, \IBMLAN\IBMLAN.INI. As a server service, the IBM Neighborhood Browser Enabler also has its own SYSLEVEL. The current SYSLEVEL of the IBM Neighborhood Browser Enabler is shown in Figure 95.

```

.
.
.
C:\IBMLAN\SERVICES\SYSLEVEL.NBE
IBM Neighborhood Browser Enabler for OS/2 Warp Server
Version 1.00      Component ID 5639C1400
Current CSD level: IP08267
Prior   CSD level: IP08267
.
.
.

```

Figure 95. IBM Neighborhood Browser Enabler Service Level

Before installing the IBM Neighborhood Browser Enabler, you should consider how many clients and servers are in your network. To increase performance, you could install additional Backup Network Browsers in addition to the Master Network Browser.

Note: We recommend, for performance reasons, installing one additional Backup Network Browser for every 20 servers in a domain.

We recommend that you install the IBM Neighborhood Browser Enabler on the Domain Controller so that it will function as the Domain Master Browser.

4.2.1 Browser Types

The responsibility of providing a list of servers for Microsoft Windows Clients is distributed over multiple computers on the network. Systems running OS/2 Warp Server Version 4.0 Symmetric Multiprocessing (SMP) or OS/2 Warp Server Version 4.0 (with CSD IP_8260 or later) can perform any of the following browser service roles shown in Table 7.

| <i>Table 7. IBM Neighborhood Browser Types</i> | |
|--|--|
| Browser Type | Description |
| Domain Master Browser | The Domain Master Browser is used to maintain the master list of available network servers. This list is distributed to the Master Browser of each subnet in the domain. There is only one Domain Master Browser in a domain, and it must reside on a Domain Controller. |
| Backup Network Browser | A Backup Network Browser receives a copy of the browse list from the Master Browser. This list is distributed to the browser clients upon their request. |
| Potential Network Browser | The Potential Network Browser is a system that is capable of becoming a browser (either backup or master), if instructed to do so. A Potential Network Browser only announces itself to the network. |

4.2.2 IBM Neighborhood Browser Enabler NetBIOS Name Registration

The communication, as well as the update flow, is only able to work properly if the Master can identify the different browser types. This is done by adding names to the existing NetBIOS name table. The NetBIOS names are an important concept when working with the IBM Neighborhood Browser Enabler. A standard (not IBM Neighborhood Browser Enabler-enabled) Domain Controller with a server name of VULCAN and a domain name of STARTREK registers the following NetBIOS names shown in Figure 96 on page 148:

```

Permanent node name is 0x00000000000000000000d6d4c35a0010.
Jumper W2 off. Jumper W1 off. Software version 255, revision 64.
Duration of reporting period is 57 minutes.
0 CRC errors, 0 alignment errors.
0 collisions, 0 aborted transmissions.
2118 successful packets sent.
262882 successful packets received.
0 retransmissions, 5 times out of resources
248 NCB(s) free out of 254 NCB(s) configured (254 configurable).
2 sessions in use out of 254 configured (254 configurable).
The maximum data packet size is 4352
4 name(s) in local name table:
(2) VULCAN          (0) (Unique) (Registered)
(5) VULCAN          (3) (Unique) (Registered)
(6) STARTREK        (0) (Group)  (Registered)
(10) VULCAN         (Unique) (Registered)

```

Figure 96. Standard NetBIOS Name Table Entries

Once you install the IBM Neighborhood Browser Enabler and start the IBM Neighborhood Browser Enabler Browser service, you will find additional NetBIOS names registered in the NetBIOS name table. In our example, we installed the IBM Neighborhood Browser Enabler on our VULCAN server. The NetBIOS name table with new names registered by the IBM Neighborhood Browser Enabler is shown in Figure 97 on page 149:

```

Permanent node name is 0x000000000000000000000000d6d4c35a0010.
Jumper W2 off. Jumper W1 off. Software version 255, revision 64.
Duration of reporting period is 62 minutes.
0 CRC errors, 0 alignment errors.
0 collisions, 0 aborted transmissions.
2200 successful packets sent.
282689 successful packets received.
0 retransmissions, 5 times out of resources
243 NCB(s) free out of 254 NCB(s) configured (254 configurable).
2 sessions in use out of 254 configured (254 configurable).
The maximum data packet size is 4352
9 name(s) in local name table:
(2) VULCAN (0) (Unique (Registered)
(16) STARTREK ↑ (1e) (Group) (Registered)
(17) STARTREK (1c) (Group) (Registered)
(5) VULCAN (3) (Unique (Registered)
(6) STARTREK (0) (Group) (Registered)
(18) STARTREK ← (1b) (Unique) (Registered)
(19) STARTREK (1d) (Unique (Registered)
(20) ●●MSBROWSE●● (1) (Group) (Registered)
(10) VULCAN (Unique)(Registered)

```

Figure 97. IBM Neighborhood Browser Enabler NetBIOS Name Table Entries

In Figure 97, the NetBIOS Names added are based on the domain name, STARTREK. NetBIOS names are up to 16 bytes in length, and the 16th byte identifies the function. Note that you will find the domain name listed several times, each with a different last (16th) byte. This is described in Table 8.

| Table 8. NetBIOS Name Table Entries for Neighborhood Browser | |
|--|--|
| Value (HEX) | Browser function |
| STARTREK (1E) | Domain / Domain Name |
| STARTREK (1D) | Master |
| STARTREK (1B) | Domain Controller / Backup Domain Controller |
| ___MSBROWSE___ | Master; this name is preceded by x01x02 and terminated by x02x01 |
| STARTREK (1C) | Domain Controller / Backup Domain Controller |

4.2.3 Browser Communication Process

To locate resources on the network, the Browser client makes extensive use of the Browser server service. The steps shown in Figure 98 and the following description should help you understand the communication flow between the client and servers:

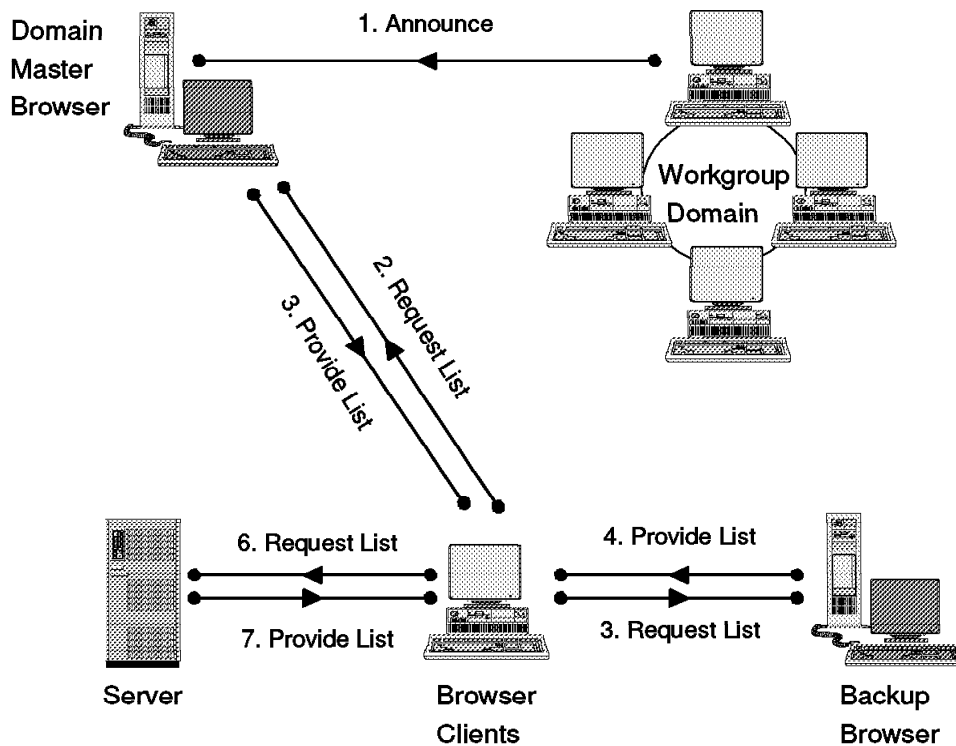


Figure 98. Browser Communication Process

The IBM Neighborhood Browser Enabler service operates in the following manner:

1. The server service of a workgroup or domain server announces its presence to the Domain Master Browser, regardless of whether it has shared resources to advertise or not.
2. When a client attempts to locate an available network server for the first time, the client contacts the Domain Master Browser of the subnet for a list of Backup Browsers.
3. The Domain Master Browser provides the client with a list of Backup Master Browsers.

4. The client requests the list of network servers from the Backup Master Browser. If no Backup Master Browser is installed, the list is distributed by the Domain Master Browser.
5. The Backup Master Browser responds to the requesting client with a list of servers in the domain.
6. The client selects a local server and requests its list of resources.
7. The selected server provides the client with a list of resources. If the proper access control rights are granted, the client can make use of the newly-found server resources.

4.2.4 Updating Browser Information

Because network resource availability changes often, the IBM Neighborhood Browser Enabler must update all browser information periodically. This is done at specific intervals, as shown in Figure 99:

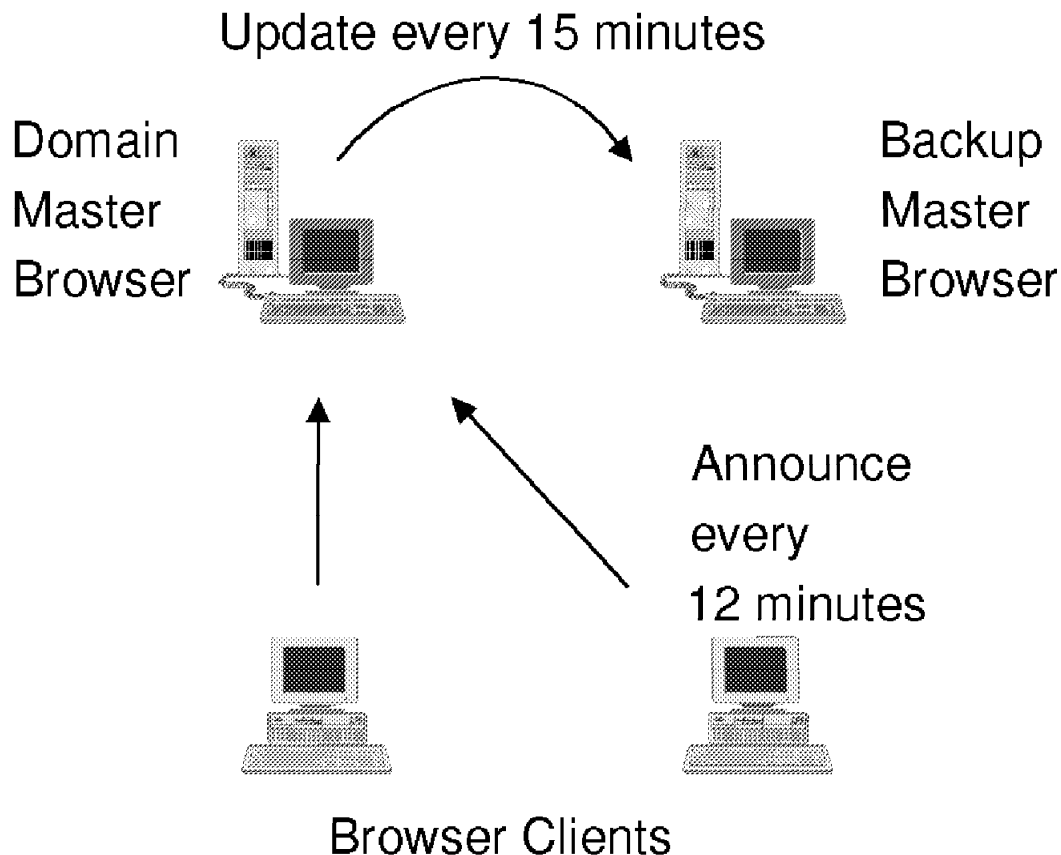


Figure 99. Updating the Browser Server List

4.2.5 Browser Election Process

If the Master Browser cannot be located by a client, or when a Backup Master Browser attempts to update its network resource list and cannot locate the Master Browser, a new Master Browser must be selected. The Browser election process is started to ensure that only one Master Browser exists per subnet.

Systems can initiate the election process by broadcasting an election packet containing the requesting computer's criteria value. This election packet is processed by all browsers.

When a browser receives an election packet, it examines the packet and compares the requesting computer's criteria value with its own election criteria. If the receiving browser has better election criteria than the issuer of the election packet, the browser issues its own election packet and enters what is called an *election-in-progress* state. This process continues until a Master Browser is elected, based on the highest ranking criteria value.

The ranking criteria is determined by the machine's role in the network and its machine type. This is shown in Figure 100.

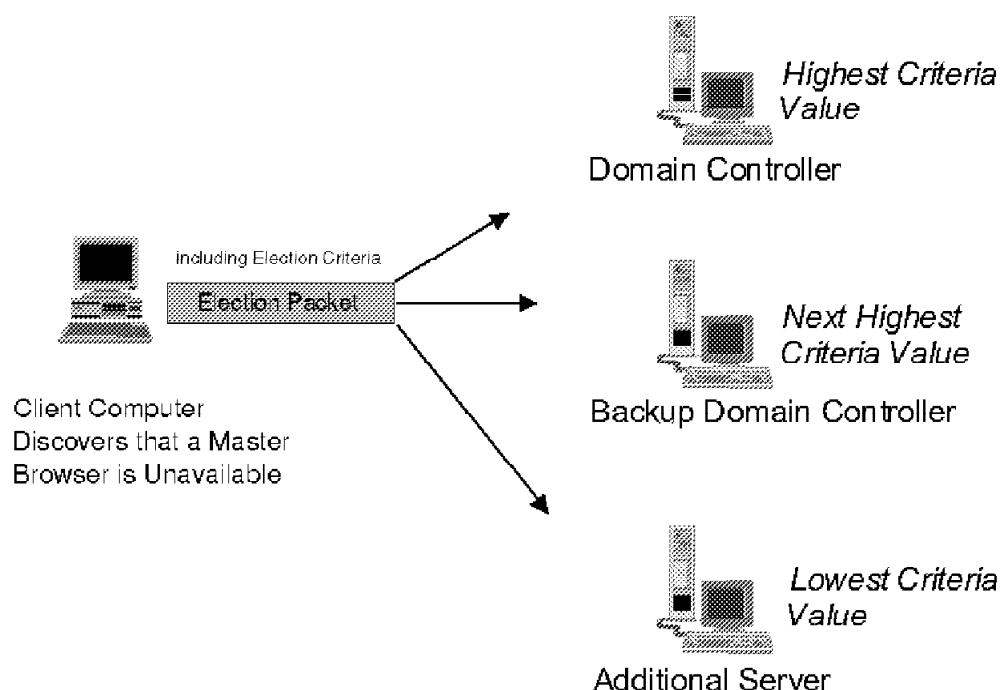


Figure 100. Master Browser Election Process

As shown in Figure 100, the election criteria have the following ranking:

1. Domain Controller
2. Backup Domain Controller
3. Additional Server

4.2.6 IBM Neighborhood Browser Enabler Installation

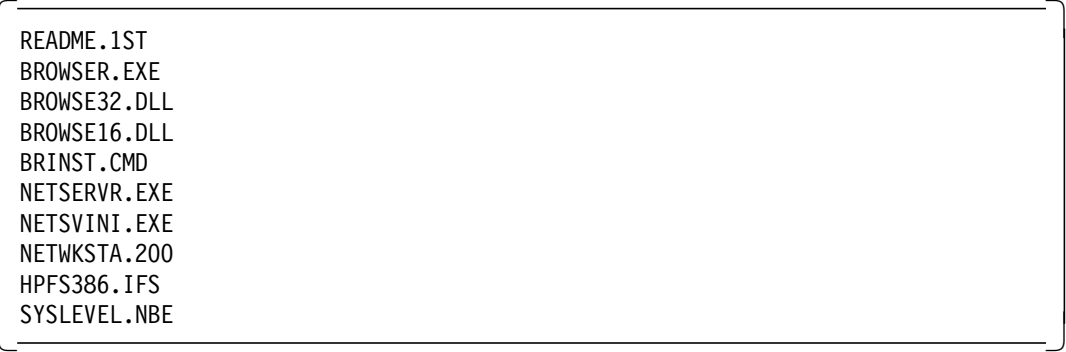
The IBM Neighborhood Browser Enabler installation process replaces some existing server modules and adds the new browser functions to the server. The installation source can be any media, including hard disk or diskette. A copy of the IBM Neighborhood Browser Enabler for OS/2 Warp Server can be downloaded from the IBM Software Choice Website at the following URL:

<http://www.software.ibm.com/os/warp/swchoice>

The BROWSE.ZIP file you will download is about 0.5 MB in size. To obtain the IBM Neighborhood Browser Enabler for OS/2 Warp Server SMP, download the BROWSERS.ZIP file (about 0.6 MB) from the following URL:

<http://www.software.ibm.com/os/warp-server/clients/clifnt.htm>.

The ZIP file should contain the following files listed in Figure 101.



```
README.1ST  
BROWSER.EXE  
BROWSE32.DLL  
BROWSE16.DLL  
BRINST.CMD  
NETSERVR.EXE  
NETSVINI.EXE  
NETWKSTA.200  
HPFS386.IFS  
SYSLEVEL.NBE
```

Figure 101. IBM Neighborhood Browser Enabler Files

Note: If you downloaded the IBM Neighborhood Browser Enabler for Warp Server SMP, you will have a NETAPI32.DLL in addition to the above files.

The installation program, BRINST.CMD, is a REXX command file and has no parameters. The IBM Neighborhood Browser Enabler can also be installed by an unattended CID procedure.

The following steps are performed during the installation of the IBM Neighborhood Browser Enabler:

1. Four modules, NETSERVER.EXE, NETSVINI.EXE, NETWKSTA.200, and HPFS386.IFS (and NETAPI32.DLL for OS/2 Warp Server SMP) are OS/2 LAN Server modules that are already installed on your server.
2. If your server has OS/2 Warp Server with CSD IPx8260 installed, these four modules will replace the existing modules on your server.
3. If your server has Warp Server SMP installed, all five modules will replace the existing modules on your server. The existing modules are backed up before the new modules are copied to your server.

To install the IBM Neighborhood Browser Enabler code, follow these steps:

1. If the server is running, stop it by typing the NET STOP SERVER command.
2. Switch to the drive and directory where the downloaded files reside.
3. Start the installation by typing BRINST.

When you start the BRINST program, the following occurs:

- a. It copies the browser files to the appropriate directories.
 - b. It backs up the existing IBMLAN.INI file as IBMLAN.IBR.
 - c. If you are installing on Warp Server 4.0 with CSD IPx8260 installed or on Warp Server SMP with no CSD installed, it backs up some existing LAN Server modules and replaces them with newer versions.
 - d. It modifies IBMLAN.INI so that the browser starts and stops automatically with the server service.
4. Do one of the following:
 - If you have Warp Server 4.0 with CSD IPx8260 installed, you must shut down and restart your computer before you can start the server. Then continue to the next step.
 - If your Warp Server SMP machine does not have any CSD installed, do the following:

In step 3, the NETAPI32.NEW file was copied to the \MUGLIB\DLL directory on the drive where OS/2 LAN Server is installed. This file replaces \MUGLIB\DLL\NETAPI32.DLL, but cannot be copied during the install process because NETAPI32.DLL is in use. You must install the new version of NETAPI32.DLL by doing the following:

a. Edit the CONFIG.SYS file.

b. Add the following line:

RUN=X:\OS2\XCOPY.EXE Y:\MUGLIB\DLL\NETAPI32.NEW Y:\MUGLIB\DLL\NETAPI32.DLL

Note: Where x: is the drive where OS/2 is installed and y: is the drive where OS/2 LAN Server is installed.

- c. Shut down and restart your computer.
 - d. Edit the CONFIG.SYS file and remove the line you added in step b.
5. Start the server by issuing the NET START SERVER command.

The IBM Neighborhood Browser Enabler is automatically started when starting the OS/2 Warp Server. If you want to disable the automatic start of this service, do the following steps:

1. Switch to the \IBMLAN directory.
2. Edit the IBMLAN.INI file with your favorite editor (like EDLIN).
3. Scroll down to the [server] section near the bottom of the file.
4. Go to the SRVSERVICES line and delete the word BROWSER.
5. Save the file. At the next server restart, the IBM Neighborhood Browser Enabler Browser service will not be started.

If you want to start the IBM Neighborhood Browser Enabler Browser service after disabling the automatic start, type:

```
NET START BROWSER
```

To stop the IBM Neighborhood Browser Enabler Browser Enabler manually, type:

```
NET STOP BROWSER
```

4.2.7 Uninstalling the IBM Neighborhood Browser Enabler

If you no longer require the IBM Neighborhood Browser Enabler function, you can easily uninstall the IBM Neighborhood Browser Enabler by doing the following:

1. Stop the server with the NET STOP SERVER command.
2. Once the server is stopped, execute the BRINST /R command.

Note: Using the BRINST command to uninstall IBM Neighborhood Browser Enabler causes the files to be removed from the fixed disk. In addition, references to the browser in the IBMLAN.INI file are removed. If server modules were replaced during the IBM Neighborhood Browser Enabler installation, the backed up modules are restored.

3. Restart the server with the NET START SERVER command.

Chapter 5. File Systems Overview and CHKDSK Enhancements

This chapter describes the long-awaited enhancements to the venerable CHKDSK program, which corrects file system errors on hard disks. It also describes in detail the structure and design of the High Performance File System (HPFS) as well as HPFS386, IBM's optimized file system for OS/2 LAN Server and OS/2 Warp Server.

5.1 CHKDSK Overview

The CHKDSK program has been in existence since the early days of DOS. Its purpose is to analyze the file system to determine if there are any errors and correct them. Until recently, CHKDSK on OS/2 was implemented as a 16-bit application. Because of this, the data structures that CHKDSK used were inefficient for examining large disk partitions (more than 10-12 GB), which could take several hours. Also, it occasionally displayed messages about insufficient memory, despite the fact that a large amount of RAM (128 MB, for example) was installed. In truth, the problem was with the 16-bit design, not the amount of RAM in the system.

The new version of CHKDSK is a 32-bit application and offers significant improvements over the existing version. This new version can analyze High Performance File System (HPFS) and HPFS386 partitions only. Since the File Allocation Table (FAT) file system is still a 12- or 16-bit implementation (depending on the version of DOS installed), the new 32-bit CHKDSK will not work for FAT; you should continue to use the original 16-bit CHKDSK program.

Unless otherwise specified, references to HPFS also apply to the HPFS386 file system.

5.1.1 32-bit CHKDSK System Requirements

The operating system requirements for running the new 32-bit CHKDSK code are one of the following:

- IBM OS/2 WARP 3.0
- IBM OS/2 Warp Server Version 4 (or Advanced)
- IBM OS/2 Warp Server Version 4 SMP

Notes

This enhanced 32-bit CHKDSK code has not been officially tested for the following operating systems and is therefore not supported:

- IBM OS/2 Version 2.x
- IBM OS/2 Version 2.11 for SMP

5.1.2 Benefits

The new version of 32-bit CHKDSK offers the following significant improvements for use with High Performance File System (HPFS) drives:

1. Single pass correction of errors, so you can run CHKDSK once to fix all errors on an HPFS drive.
2. Performance improvements—CHKDSK execution is up to two times faster on non-RAID drives and up to 11 times faster on large RAID drives.
3. Reduced memory requirement—CHKDSK now uses less memory to check drives larger than 4 GB.
4. Improved FOUND directory format—Files and directories recovered by CHKDSK are placed in the FOUND directory and now have their original names (or as much as can be recovered from the FNodes—see sections 5.3.2.5, “Fixing and Recovering Data using CHKDSK” on page 170) appended to the names assigned by the 32-bit CHKDSK.
5. More sophisticated error detection, which means this version of CHKDSK recognizes errors that previous versions could not detect.
6. More sophisticated error correction—The 32-bit CHKDSK will recover files and directories in cases where previous versions would have deleted them.
7. Better analysis—A binary log file is now created in the root directory for use by IBM Service. The log file name is CHKDSK.LOG and a backup file (CHKDSK.OLD) is also kept. IBM Service has a Log Formatter called PMCHKLOG that formats and analyzes the log file.

Note: A CHKDSK.LOG is created when the /F command-line parameter is used or when AUTOCHECK is run during CONFIG.SYS processing.

IBM Systems Engineers and technical experts who have detailed knowledge of HPFS can follow the OS2FISYS FORUM and also download the Log Formatter from the following URL inside the IBM firewall:

<http://logos.austin.ibm.com/chkdsk.html>

The new 32-bit CHKDSK allows AUTOCHECK (during CONFIG.SYS processing) of drives up to and including 64 GB in size. Checking a 64 GB drive requires at least 32 MB of physical memory.

5.2 Enhanced CHKDSK Design

The new CHKDSK enhancements are valid only on HPFS drives. However, to ensure that AUTOCHECK works properly in a mixed file system environment, the CHKDSK developers utilized the Installable File System (IFS) design mechanism.

When CHKDSK starts, it checks the partition table to determine the partition type. Based on the result, it either jumps to the IFS module (in the case of HPFS or HPFS386), or it runs the standard CHKDSK (in the case of a FAT partition). Figure 102 shows the program flow in a mixed file system environment. The CHKDSK32.EXE program's sole function is to load CHKDSK32.DLL during AUTOCHECK for enhanced processing. Do not try to invoke it from the command line.

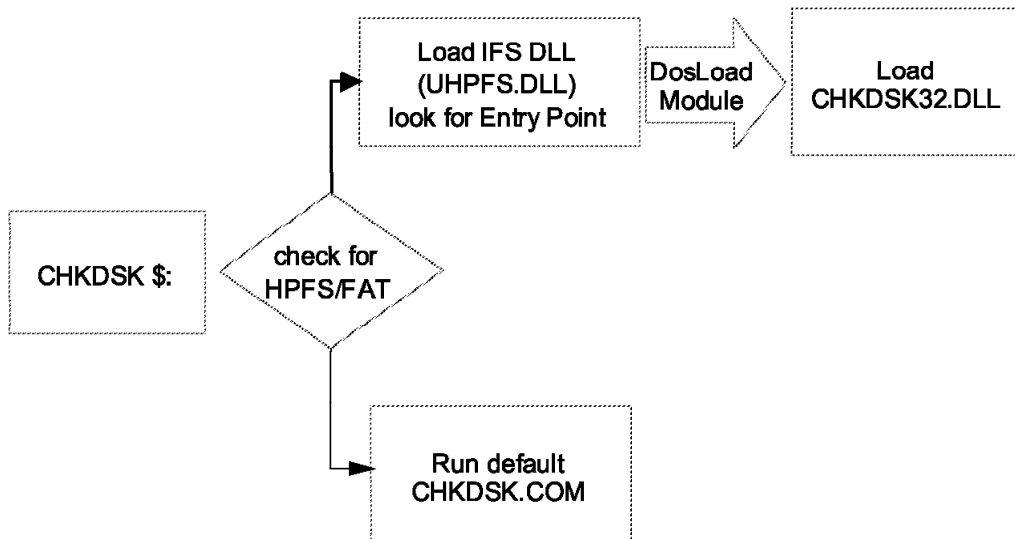


Figure 102. CHKDSK Flow during AUTOCHECK Processing

5.2.1 Installing the 32-bit CHKDSK

The new 32-bit CHKDSK is included in the 32-bit CHKDSK Service Fix and can be obtained through your local IBM Service contact. The 32-bit CHKDSK is included in OS/2 Warp Version 3 FixPak 30 and FixPak 2 for

OS/2 Warp Version 4. It is also available within the IBM firewall at the following URL:

<http://logos.austin.ibm.com/chkdsk.html>

To install the new 32-bit CHKDSK, follow these steps:

1. Back up your system and ensure that this backup works.
2. Open an OS/2 Window.
3. Switch to the drive and directory where the new CHKDSK files are located.
4. Type INSTALL and press **Enter**. The entire README file is displayed, after which you can press **Y** to continue the installation. If you are not ready to install, press any other key, and the installation will end at your request. Press **Y** to continue.
5. The target drive is displayed. If this is incorrect, type the drive letter (without the colon (:)) of the correct drive.
6. Five files are copied to your system, and the installation program completes successfully.

The 32-bit CHKDSK installation program adds and modifies the following files shown in Table 9.

| Table 9. CHKDSK Installation Changes | |
|--------------------------------------|----------|
| File | Action |
| \OS2\CHKDSK32.EXE | Added |
| \OS2\DLL\CHKDSK32.DLL | Added |
| \OS2\DLL\UHPFS.DLL | Replaced |
| \OS2\BOOT\CHKDSK.SYS | Added |

Note: The old UHPFS.DLL will be saved to OS2\DLL\UHPFS.SAV during the installation process.

The new 32-bit CHKDSK will now be invoked instead of the original CHKDSK. This also includes the AUTOCHECK operation.

5.2.2 AUTOCHECK Function

AUTOCHECK is a parameter on the HPFS IFS statement at the top of the CONFIG.SYS file. An example line is shown here:

```
IFS=C:\OS2\HPFS.IFS /CACHE:2048 /CRECL:4 /AUTOCHECK:CD+E
```

The AUTOCHECK parameter checks each drive letter listed during system startup to determine if it is in an inconsistent state, such as an improper shutdown or the result of a power outage. If such a state is found, the CHKDSK /F command is automatically run on the drive to repair any damage to the file system. If you add a plus (+) sign in front of the drive letter, the CHKDSK /F is automatically run on that particular drive (the E: drive in our example) at each system startup.

To enable AUTOCHECK on large drives, make sure that the CHKDSK.SYS file resides in the root or \OS2\BOOT directory. Add the following line to your CONFIG.SYS:

```
BASEDEV=CHKDSK.SYS
```

5.2.3 Using CHKDSK

To run the new CHKDSK, you still type the same command, CHKDSK, or the same PM interface, PMCHKDSK. Do not type CHKDSK32 because you will not get the result you wanted!

When you format an HPFS partition using OS/2 Warp Version 3 or Version 4, a quick format (which does not test the drive media, unlike a long format with the /L command) is usually run. When you run the 32-bit CHKDSK against that partition for the first time, you will see errors displayed. These errors are harmless and aren't shown if you use the /F option against the partition.

CHKDSK can rebuild an entire HPFS partition by scanning it methodically. The parameters used to invoke CHKDSK have different recovery levels. You specify the recovery level with the /F:x parameter, where the x is one of the options listed in Table 10.

| <i>Table 10 (Page 1 of 2). CHKDSK /F: Parameter Options</i> | |
|---|--|
| Parameter | Action |
| 0 | <ul style="list-style-type: none"> Analyzes file system Displays information about its state No repairs are performed |
| 1 | <ul style="list-style-type: none"> Analyzes file system Displays information about its state Resolves inconsistent file system structures |

| Table 10 (Page 2 of 2). CHKDSK /F: Parameter Options | |
|--|---|
| Parameter | Action |
| 2 | <ul style="list-style-type: none"> • Default when the /F parameter is specified • Analyzes the file system • Displays information about its state • Resolves inconsistent file system structures • Scans disk space that is not in use and not referred to by the file system. If recognizable file directory structures are found, it will recover them. |
| 3 | <ul style="list-style-type: none"> • Analyzes file system • Displays information about its state • Resolves inconsistent file system structure • Scans disk space that is not in use and not referred to by the file system. If recognizable file directory structures are found, it recovers them. • Scans the entire disk partition for recognizable file system structures. |
| C | <ul style="list-style-type: none"> • Checks disk with level 2, but only when the dirty flag is set. <p>Note: This could be used on a Domain Controller when only the main partition is checked to enable logon capability again. The STARTUP.CMD would start CHKDSK for the other partitions.</p> |

During the initial boot sequence, the file system inspects the HPFS volumes for the dirty flag settings. HPFS protects itself against an abrupt system switch-off by placing the Dirty File System flags into the Spareblock of every HPFS volume. This flag is cleared only during a shutdown, which notifies the file system to flush the disk cache, update directories and bring the disk back to a consistent state.

If the system is not shut down properly, the dirty flag is not cleared. CHKDSK must be run prior to resetting the system to a consistent state. This can be done manually, or it can be done automatically by setting the AUTOCHECK parameter in the HPFS IFS statement in CONFIG.SYS.

5.2.4 Uninstalling the 32-bit CHKDSK

To remove the 32-bit CHKDSK, follow these steps:

1. On the drive where the new CHKDSK is installed, go to the \OS2 subdirectory.
2. Erase the **CHKDSK32.EXE** file.
3. Go to the \OS2\DLL subdirectory on the same drive.

4. Verify that the **UHPFS.SAV** file still resides in the \OS2\DLL subdirectory.
5. Delete the **UHPFS.DLL** file.
6. Copy the saved **UHPFS.SAV** back to **UHPFS.DLL**.
7. Erase the **CHKDSK32.DLL** file.
8. If you have enabled AUTOCHECK, go to the \OS2\BOOT or the root directory on the same drive.
9. Erase the **CHKDSK.SYS** file.
10. Remove the **BASEDEV=CHKDSK.SYS** statement from your CONFIG.SYS.

After executing these steps, the original 16-bit CHKDSK is again your current version.

5.3 FAT and HPFS File System Design

The following sections provide a short overview of FAT and HPFS, their history, and some of their advantages and disadvantages. This should help you to better understand why CHKDSK is needed and exactly what it is does for you.

5.3.1 File Allocation Table (FAT)

The File Allocation Table (FAT) was designed and coded in February 1976. It was a version for the BASIC programming language that could store programs and data on floppy disks. The FAT design was incorporated by Tim Patterson in an early version of an operating system for the Intel 8086 chip. Bill Gates bought the rights to the system, then rewrote it to create the first version of DOS.

The FAT file system is simple and reliable. It does not lose data if the computer crashes in the middle of an update. It does not use a lot of memory. It does not require extra administrative I/O to different areas of the partition.

FAT was a good, quick method to access files on a diskette drive. At this time, diskette drives had a capacity of 128 KB, 360 KB and later 1.2 MB. To optimize I/O performance, the FAT was read into memory. This was a big advantage compared to the Control Program/Microprocessor (CP/M) operating system, where allocation information was scattered over the entire disk.

These advantages eventually turned into big disadvantages with the advent of the comparatively large hard disk. This shifted the placement of data and its relationship to memory. An IBM PC with 64 KB of RAM and a 360 KB

diskette drive had a memory-to-storage ratio of about 1:5. An IBM PC with 640 KB RAM and a 40 MB disk drive had a memory-to-storage ratio of about 1:63. The result was that the FAT, in the flow of this PC hardware evolution, could only be partly read into memory. This meant that the hard disk had to make several head movements to read a single file, which slowed down the whole system.

There was another hard disk size problem that DOS fixed in Version 4.0. This version was the first that supported partitions greater than 32 MB. Although theoretically it is possible to support partitions up to 2048 GB (32-bit pointer to 512 byte sectors), FAT's usefulness declines for partitions greater than 128 MB. This is because a file with a length of 1 byte reserves a 2 KB cluster of disk space. This value doubles at partition sizes of 256 MB, 512 MB, 1024 MB and so on. This is shown in Table 11.

| <i>Table 11. Relationship between Cluster Size and Partition Size</i> | | |
|---|---------------------|-------------------------------|
| Sectors per Cluster | Cluster Size | Maximum Partition Size |
| 1 | 0.5 KB | 32 MB |
| 2 | 1 KB | 64 MB |
| 4 | 2 KB | 128 MB |
| 8 | 4 KB | 256 MB |
| 16 | 8 KB | 512 MB |
| 32 | 16 KB | 1 GB |
| 64 | 32 KB | 2 GB |
| 128 | 64 KB | 4 GB |

This phenomenon is due to the use of 16-bit pointers to the clusters of a file. A 16-bit pointer can address up to 65536 different values ($2^{16}=65536$). This represents the number of clusters that could be given to different files. Because of this, a cluster can have different sector sizes.

Note: This means that larger clusters waste more space for small files. For example, a batch file that is 400 bytes long on a 512 MB disk occupies an 8 KB cluster—a 95% waste of space. This is in contrast to HPFS, where the same file would occupy a 512 byte sector—a 22% waste of space.

The beginning of the FAT partition holds the Boot sector. It contains a short load sequence (IBMDOS.COM) and the Basic Input Output System (IBMBIOS.COM), a set of basic system routines for operations on different parts of the hardware. Following the Boot sector is a representation of the

cluster for the partition. Each cluster has a 12- or 16-Bit entry, depending on the DOS version being used. This representation is the File Allocation Table. This is shown in Figure 103 on page 165.

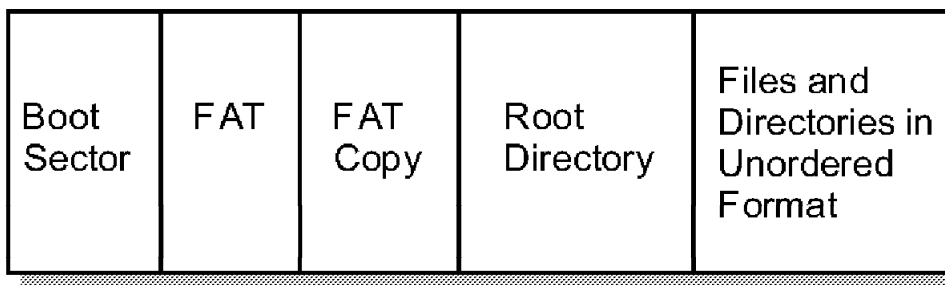


Figure 103. FAT Partition Data Structures

A copy of the FAT follows the initial FAT table. Following the FAT copy is the root directory, which is followed by the file and directory area.

The directory is allocated at the start of the partition, and it contains the table of free space for the partition. To write a new file, or to add data to an existing file, the disk arm must be constantly moved between the location of the directory and the place where the data is being written.

If the system crashes, no data is lost. A FAT system may have removed disk area from the chain of free space, but may not yet have assigned it to any permanent new file. The CHKDSK program (or on newer systems, SCANDISK) examines the FAT table to determine the status of every record on disk. The records which are not part of any file or directory structure are returned to the free space chain. After CHKDSK finds unallocated sectors, it asks you whether they should be turned into files.

By design, FAT supports a maximum of 65536 allocation units (clusters). As was shown in Table 11 on page 164, when the disk partition is 32 megabytes or less, an allocation unit is a 512 byte sector. As the disk gets larger, the units get larger. A 64 MB disk partition has a 1 KB allocation unit size. A 256 MB partition has a 4 KB allocation unit size.

Each file occupies one or more allocation unit. As the allocation units get large, any large number of small files wastes a lot of disk space. The classical FAT directory structure limits file names to eight characters with a three-character extension. This 8.3 naming convention was borrowed from earlier DEC minicomputers.

The FAT structure also maintains the following attributes for each file:

- System file or directory
- Hidden file or directory
- Archived next time the disk is backed up
- Read-only

There is also a data and time stamp when the file was last changed. OS/2 allows a FAT file to have additional Extended Attributes (EAs). Since there is no room for these attributes in the FAT directory, OS/2 creates a separate hidden file, EA DATA. SF, on the disk volume and stores the EA information in this file.

For directories, DOS stores 32 bytes in the FAT. Directories share the same space as the files. Only the root directory has a fixed position. This means the directories are stored unordered together and between the files. The effect is that the operating system must traverse many parts of the disk partition when traversing large subdirectory structures, thus repositioning the disk head each time. This slows down overall system performance. HPFS improves this by reorganizing the entire file system structure. Table 12 shows the advantages and disadvantages of the FAT system.

| <i>Table 12. FAT Advantages and Disadvantages</i> | |
|---|---|
| Advantages | Disadvantages |
| Supported by many operating systems | Limited to 8.3 file names |
| Minimal memory usage | Inefficient for partitions greater than 32 MB |
| Simple and reliable | Unsuitable for file servers |

5.3.2 High Performance File System (HPFS)

OS/2 Version 1.2 introduced a new file system called High Performance File System (HPFS). This file system was developed by IBM and Microsoft to overcome the limitations of the FAT file system design. HPFS is included in OS/2 Version 1.2, 1.3, 2.x, Warp Version 3 and Version 4. It is also included in OS/2 LAN Server Version 1.2 and later and all OS/2 Warp Server implementations.

With HPFS, IBM followed a new concept in file system implementation called the Installable File System (IFS). An IFS driver, which contains the code needed to manage media formatted other than the FAT format, can be loaded at system startup time.

Some people think that an HPFS partition can defragment itself. This is not correct. HPFS has, by design, a better structure that prevents data from

fragmentation. Technically, the tables that describe the location of files and freespace are positioned at regular intervals throughout the partition. New files and directories are written where there is a large amount of freespace. This reduces fragmentation and keeps the disk arm from excessive movement. In addition, the information for all directories is placed in the middle of the disk, which makes it possible to find directories more quickly and prevent the disk from excessive head movements during directory traversal.

5.3.2.1 HPFS Structure

Data management on an HPFS partition is much more effective because the disk is managed at sector level. HPFS maintains a 512-byte allocation unit (cluster size) no matter how large the partition becomes. This allows HPFS to minimize the disk space that is lost for small files. A 1-byte file occupies only a 512-byte sector regardless of the partition size. The HPFS directory allows file names to go beyond the 8.3 FAT construct by allowing multiple periods within the file or directory name and having mixed-case names.

The structure on the disk is enhanced to achieve efficient head movement, enabling much better performance as the partition size increases. HPFS splits file bands and bitmap bands over the partition. The file bands are surrounded by the bitmap bands. To write to a file, the system looks at the bitmap band and writes the file to the free space in the adjacent file band. The band structure is shown in Figure 104.

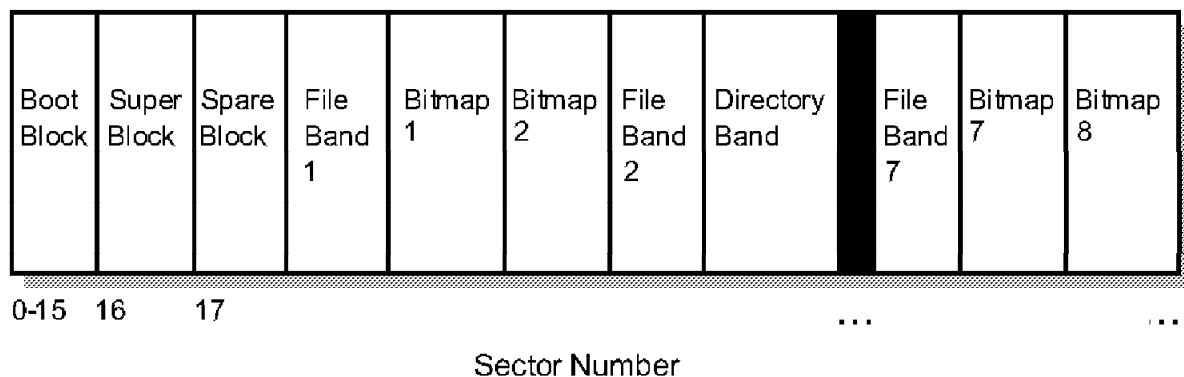


Figure 104. High Performance File System (HPFS) Data Structure

The first 16 sectors (sectors 0 to 15) of an HPFS partition represent the Boot block. Inside the Boot block is the partition name, a 32-bit partition ID, the BIOS Parameter Block (BPB), and a bootstrap program.

Sector 16 is the location of the Superblock. The Superblock consists of pointers to the bitmap band, a list of defective blocks, directory bands, and the root directory. The Superblock also records when the hard disk was checked last with CHKDSK /F to find inconsistencies.

5.3.2.2 Caching in HPFS

Critical for the high performance of HPFS is the technology HPFS uses to cache write accesses to the hard disk. The lazy-write design writes data to a memory cache before writing to disk; so the application sees faster performance because the file I/O operation returns more quickly. HPFS keeps information in the cache until it needs to be written to disk. It is also possible to switch off this feature.

Although caching can yield significant application I/O performance improvements, it can also be a problem. The system (using CHKDSK) can only find defective sectors when attempting an actual write to the disk. If a power failure occurs, data in the cache may not have been written to disk (maximum cache age can help minimize this). To be sure that all the information has been properly written to disk, a user should shut the system down properly (using the SHUTDOWN command or the Shutdown icon) rather than just turning the power off.

5.3.2.3 File and Directory Organization on HPFS Partitions

This section describes the layout of file and directory data structures on an HPFS partition.

The layout of files and directories on an HPFS disk is much more complex than the FAT file system. At specific sectors on an HPFS partition, there exist the Superblock and the Spareblock. Together, these data structures identify the partition as an HPFS partition and point to the root directory structures, the allocated-sector and bad-block bitmaps, and the space allocated for use when creating new directories and files.

There is an Fnode for every file and directory on an HPFS partition. As shown in Figure 105 on page 169, the Superblock points to the Fnode for the root directory. In addition to being the primary disk allocation structure for each directory entry, the Fnode contains additional information for the file or directory, such as the location of the file, extended attributes and data about the EAs.

Each Fnode corresponds to either a file or a directory and is located in the sector before the start of the file or directory sector. For file Fnodes, there are data structures in the Fnode that describe the disk allocation for the file's data. For directory Fnodes, the allocation portion points to the location of the topmost directory block (DIRBLK) that holds entries for each of the

files and subdirectories in that directory. The topmost directory block is the top node in a binary tree, or Btree. A Btree is a data structure that is sorted and organized in such a way that allows very quick searches for data within it.

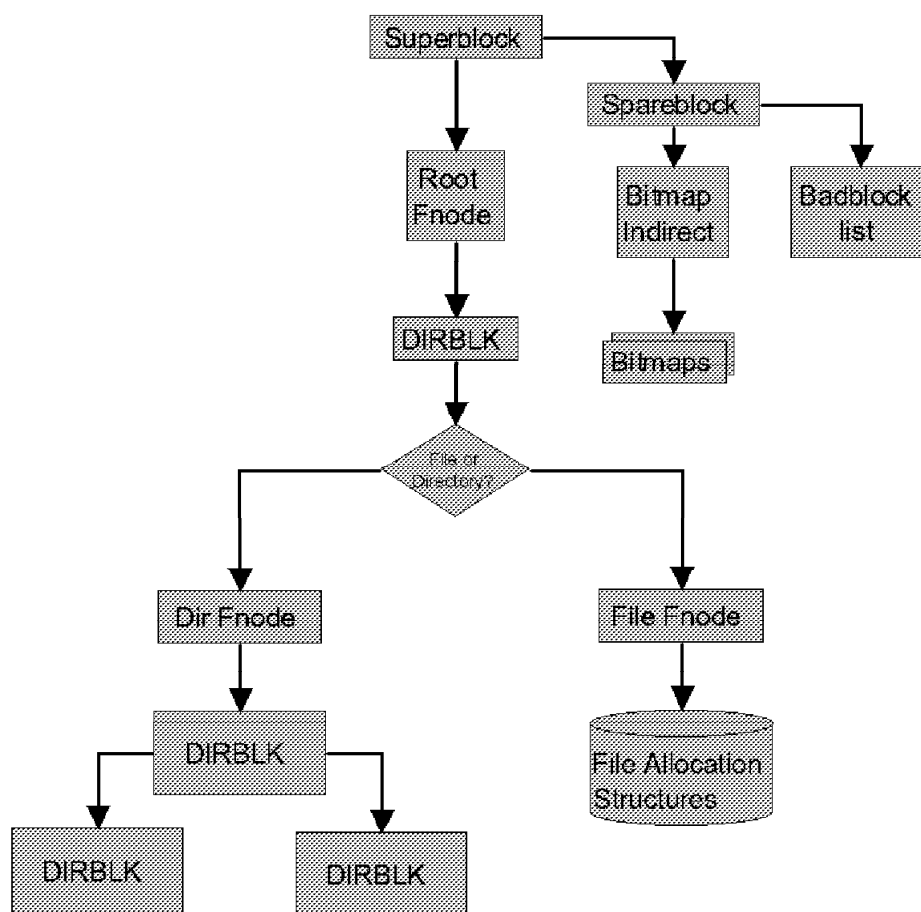


Figure 105. HPFS File and Directory Organization

5.3.2.4 HPFS Hotfix Sector

Because of caching and write delay, HPFS must be able to handle the discovery of defective sectors on the disk. Within the Spareblock, there are pointers to hotfix sectors.

When a write operation is attempted to a sector and the attempt fails, HPFS places that sector on the list of the defective sectors. The write operation is redirected to an available sector in the hotfix-sector list. All read and write

accesses will first check first the sector numbers to see if they have been remapped to the hotfix list. The hotfix takes approximately 2 KB of disk space.

In addition, the Dirty Flag inside the Spareblock will be set to indicate that not all physical write accesses were completed. The system recognizes this during system startup and therefore checks the hard disk automatically (using our friend, CHKDSK).

CACHE386.EXE reports the number of times it wrote to the hotfix area, thus indicating the number of bad disk sectors found since the last system restart.

5.3.2.5 Fixing and Recovering Data using CHKDSK

Systems will occasionally crash, leaving any HPFS partition marked dirty. Using the GammaTech Sector Editor, the Dirty Flag will appear as shown in Figure 106 .

```

Edit: SpareBlock (11)           Position: 00000000  0
Size: 00000200 (512)

00002200  49 18 91 F9 C5 29 52 FA-01 00 00 00 20 00 00 00 *I....)R.....*
00002210  00 00 00 00 64 00 00 00-14 00 00 00 14 00 00 00 *....d.....*
00002220  88 00 00 00 02 00 00 00-D6 F2 DB C8 18 45 CC 2F *.....E./.*
00002230  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 *.....*
00002240  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 *.....*
00002250  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 *.....*
00002260  00 00 00 00 00 00 00 00-00 00 00 00 AC 87 01 00 *.....*
00002270  B0 87 01 00 B4 87 01 00-B8 87 01 00 BC 87 01 00 *.....*
00002280  C0 87 01 00 C4 87 01 00-C8 87 01 00 CC 87 01 00 *.....*
00002290  D0 87 01 00 D4 87 01 00-D8 87 01 00 DC 87 01 00 *.....*

Sector 00000011 (Spare Block)
Signature.....: F9911849 FA5229C5
Flags.....: 01 Dirty

First HotFIX...: 00000020
# hotfix used...: 00000000
Max hotfix size: 00000064

# spare dblks...: 00000014
Max spare dblks: 00000014

```

Figure 106. HPFS Dirty Bit

Before the partition can be accessed properly, the next boot of the operating system should have AUTOCHECK run CHKDSK to examine the chains of free space and file locations to correct any problems. As disk volumes get larger, running CHKDSK after a crash can take time, even several hours. For example, the old CHKDSK took nine hours to complete on a 63 GB RAID partition, and the new CHKDSK completed in 54 minutes on the same partition. Your results, of course, may vary.

CHKDSK can recover serious problems in the file system because of the HPFS architecture. Every data object is doubly-connected, has a 32-bit signature, and the Fnodes are aware of the starting letters of the files and directories.

CHKDSK must not only recover inconsistent partitions. It must also rebuild files from the hotfix sector back into the normal part of the file system and make more room in the hotfix for the next emergency.

5.3.3 HPFS386 Architecture

The HPFS386 is highly optimized and designed for Pentium Pro, Pentium, 80486, 80386 and 80486SX and 80386SX-based platforms with large disk systems. The HPFS386 provides extremely fast access to large disk volumes and optimizes performance in the server environment, where many files are open simultaneously. HPFS386 is an enhancement of the regular HPFS. It represents the logical evolution of LAN Server technology. The server consists of an optimized ring 0 server tightly coupled with a bootable Installable File System (IFS) and customized device drivers to accelerate network I/O. The result is that clients receive their data (such as an application executable or a spreadsheet data file) much more quickly.

The 386-specific version of the HPFS is disk-format compatible with the OS/2 Standard Edition Version 1.2 and later. The existing HPFS partitions do not require reformatting when HPFS386 is installed.

HPFS386 includes the following enhancements:

- Cache addressing capability beyond 16 MB memory (HPFS has only a 2 MB cache)
- Increased maximum number of open files from 8192 to 65536
- Increased maximum number of file finds from 3072 to 8192
- Increased maximum number of file searches from 1024 to 6144
- Access Control Lists (ACLs) are contained within the directory and file structure
- Directory- and user-based disk space limitations

- Local Security
- Software RAID-1 (Fault Tolerance)
- Fault Tolerance support for mirroring and duplexing
- Configurable Heap size depending on cache
- Minimum cache size of 256 KB, maximum based on available memory (HPFS386 maximum is 320 MB)
- Efficient for large disks and concurrent I/O operations.

The only possible considerations using HPFS386 are the following:

- Special HPFS386-specific boot diskettes are required to access HPFS386 partitions.
- There is no support by other operating systems.

5.3.3.1 Access Control System

The user IDs, group IDs, and passwords for all users within a server's domain are stored in the user account accounts database (NET.ACC) on the server. On an OS/2 LAN Server Entry server with either the FAT or HPFS file system, the Access Control Profile information is stored in the NET.ACC file. On an OS/2 LAN Server Advanced (or OS/2 Warp Server) server with HPFS386 installed, the Access Control Profiles for the HPFS386 files and directories are stored within the file system.

The Access Control Profiles for all other resources (for example, FAT files, print spooler queues, and serial device queues) and drive-level Access Control Profiles for HPFS386 drives are stored in the NET.ACC file. Up to 8192 Access Control Profiles can be stored in the NET.ACC file. A HPFS386 server stores an unlimited number of Access Control Profiles for directories and files residing on the HPFS386 drives.

The Access Control List consists of different entries, called Access Control Entries (ACE). For every access restriction of an ID, you can find an entry. The entry consists of the user ID or the group and the permission. The entries are created when an access profile is created for a special file or directory. Each ACE is sometimes called an Access Control Profile (ACP).

5.3.3.2 Inherited Access Control

For file aliases, an Access Control Profile usually must be created before users can use this resource. However, an Access Control Profile is inherited automatically if the file resource is either created remotely or resides on an HPFS drive and HPFS386 is installed on the server.

When you create a directory either locally or remotely on a HPFS386 server, the newly-created directory inherits the Access Control Profile information of the parent directory. Because of the way the file allocation table (FAT) works, you can inherit only a remotely-created directory's Access Control Profile on a FAT file server. You must have access to the Access Control Profile on the server to be able to inherit it. You must be logged on with an ID that is allowed access to the parent Access Control Profile. If successful, a new profile is created with the same permissions as the parent of the new directory.

5.3.3.3 Renaming or Deleting Directories

If you rename a directory, you must manually delete and recreate any Access Control Profiles for subdirectories under the directory. Renaming a directory does not automatically update Access Control Profiles for the subdirectories. This only applies to HPFS or FAT file systems. The HPFS386 Access Control Profiles remain with the renamed directory.

If you delete a directory on a local drive, the associated Access Control Profile is not deleted. However, if you delete a directory on a local HPFS386 drive, the Access Control Profile is deleted. If you delete the directory of a redirected drive, the Access Control Profile is always deleted, whether it is on a local HPFS386 drive or not. Check the list of Access Control Profiles on each server periodically, and delete those that have no existing files resource.

5.3.3.4 Backing Up Access Control Information

Access control information is normally not copied when backing up files to tape because the ACL (Access Control List) is now in the Fnode, which is before the start of the file or directory. It is recommended that the BACKACC utility be used to back up the ACLs in HPFS386 into a file. Then back up the whole disk using the tape backup program.

5.3.3.5 Existing Drives or Other File Systems

When you install the HPFS386 option, it installs a device driver that automatically initiates the HPFS partition on which you are installing to HPFS386. The data integrity remains the same (a format is not required if the partition or drive is already formatted as HPFS).

With OS/2 Warp Server, HPFS drives (other than the install drive) do not become HPFS386 drives until the OS/2 Warp Server program accesses that drive. For example, the HPFS drive will remain simple HPFS until an alias, a NET SHARE, or an Access Control Profile is created on that drive.

Therefore, an HPFS partition may not be a HPFS386 drive unless you have used that drive in association with OS/2 Warp Server. To force an existing

HPFS drive to become a HPFS386 drive, try creating an alias for a resource on it. If this does not resolve the situation, try running CHKDSK with the /F parameter on that drive.

Note that if you need to keep certain partitions as FAT or HPFS, it is important to not have OS/2 Warp Server deal with that particular partition (which you may be using with a different operating system). If the OS/2 Warp Server system does use that partition, it will become HPFS386-formatted, and the other operating system may not be able to utilize that drive again.

5.3.4 Enhanced High Performance File System (HPFS) File Recovery

Because of the double signatures and the fact that the Fnodes hold the first 14 to 15 bytes of the filename, the new 32-bit CHKDSK is more effective in recovering found files.

The 32-bit CHKDSK has enhanced the format of recovering files by appending the FOUND.001 and FILE.001 statements with these 15 characters. If the filename is less than 15 characters, the full filename is recovered. Other files are much easier to identify if the first 15 characters of the filename are known.

Chapter 6. TCP/IP Enhanced New Functions

TCP/IP has become the protocol of choice within company networks as well as between them. Because of this, it is increasingly important to include the capability of using the TCP/IP network for communications with clients. OS/2 Warp Server includes the TCP/IP protocol stack for use by its various services, such as File and Print Services and System Management Services. There are two minor new functions included in the Version 3.5 TCP/IP stack:

- Aliasing
- Variable Subnet Routing

These functions give you additional flexibility in the setup and usage of your IP addressing environment.

Note: A major new release of TCP/IP is due in late 1997. It will be discussed more thoroughly in an upcoming redbook.

6.1 Obtaining TCP/IP Updates

With the increasing importance of TCP/IP, administrators must be aware of changes and enhancements that are developed. The latest TCP/IP corrective service fixes and updated code can be obtained from the following URL:

http://ps.boulder.ibm.com/pbin-usa-ps/getobj.pl?pdocs-usa/tcpip_stack_rsu.html

Many fixes are available, including those for TCP/IP Version 3.x and 4.0, DHCP, DDNS, and Winsock. Some fixes, such as TCP/IP Version 4 for OS/2 Warp 4, can be installed directly from the Web page.

6.2 TCP/IP Aliasing

The Aliasing function of TCP/IP allows you to have a single system assume multiple IP addresses. One benefit is that it allows you to easily migrate systems to a single machine without risking addressing problems because of hard-coded IP addresses.

Figure 107 on page 176 shows an example of this:

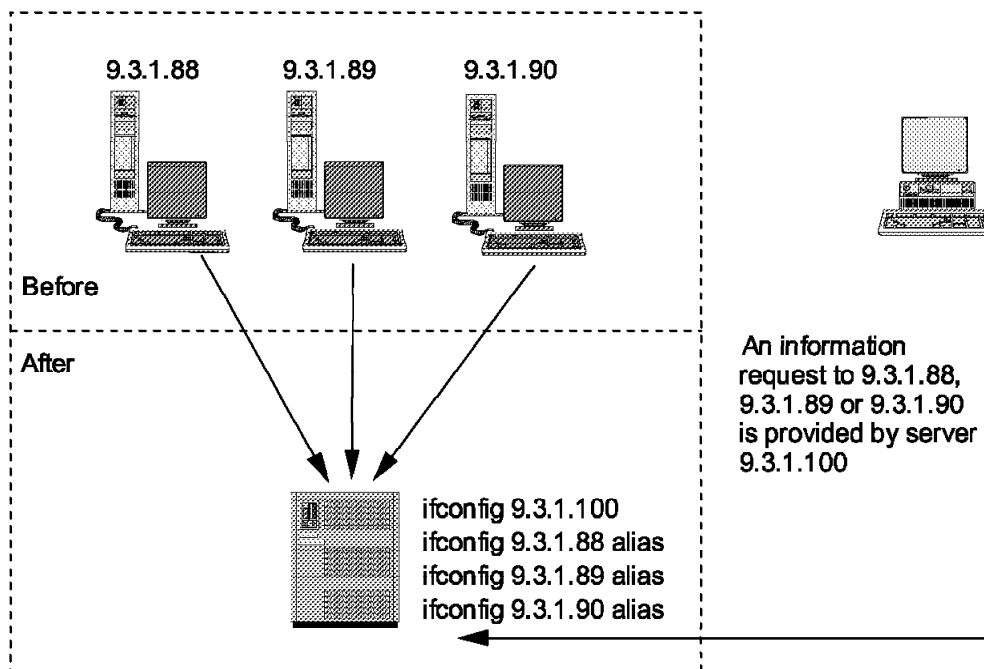


Figure 107. Using IP Aliasing during System Consolidation

In Figure 107, if the applications on 9.3.1.88 are also installed on 9.3.1.100, clients making requests (such as FTP) to 9.3.1.88 will receive responses from 9.3.1.100. Administrators can use this feature to maintain availability while the original system is down for maintenance or system service.

6.2.1 Configuring TCP/IP Aliasing

The IP addressing portion of the TCP/IP configuration is held in the \MPTN\BIN\SETUP.CMD file. In our example, we have an existing system with an IP address of 9.3.1.100 on the lan0 interface. We want the addresses 9.3.1.88, 9.3.1.89 and 9.3.1.90 to be aliased to this system. We would make the following changes, shown in bold in Figure 108 on page 177.

```
route -fh
arp -f
ifconfig lan0 9.3.1.100 netmask 255.255.255.0
ifconfig lan0 9.3.1.88 netmask 255.255.255.0 alias
ifconfig lan0 9.3.1.89 netmask 255.255.255.0 alias
ifconfig lan0 9.3.1.90 netmask 255.255.255.0 alias
REM ifconfig lan1
REM ifconfig lan2
REM ifconfig lan3
REM ifconfig lan4
REM ifconfig lan5
REM ifconfig lan6
REM ifconfig lan7
REM ifconfig sl0
route add default 9.3.1.74 1
route add net 9 9.3.1.74 1 netmask 255.0.0.0
ipgate off
```

Figure 108. *SETUP.CMD* for IP Address Aliasing

Our 9.3.1.100 system is now ready to receive IP requests as 9.3.1.88, 9.3.1.89 and 9.3.1.90.

6.3 Subnet Masking

The IP Address Mask (shown as the netmask parameter on the `ifconfig` line in Figure 108) is a configuration parameter used by a TCP/IP host and IP router to differentiate between that part of the IP address that represents the network and the part that represents the host.

A router uses the mask value to create a key value that is looked up in the router table to determine where to forward a frame. An end-node uses the mask value to create the same key value, but the value is used to compare the destination address with the end-node address to determine whether the destination is directly reachable (on the same network) or remote (in which case the frame must be sent to a router and cannot be sent directly to the destination).

The mask value can be assigned by default, or it can be specified by the installer of the end-node or router software. The destination IP address and the mask value are combined with a Boolean AND operation to produce the resultant key value. Consider the following example:

An end-node is assigned the IP address 140.6.15.3 and a mask value of 255.255.0.0. This end-node wants to send a frame to 140.7.9.2. If 140.7.9.2 is

on the same network as 140.6.15.3, the end-node will broadcast an ARP (Address Resolution Protocol) frame to determine the data link address of the destination, and it will then send the frame directly to the destination. If 140.7.9.2 is on a different network, the workstation must send the frame to a router for forwarding to the ultimate destination network.

All the dotted-decimal notation must be converted to the underlying 32-bit binary numbers to understand what is taking place.

| | | | | | |
|-----------------------|---|----------|----------|----------|----------|
| End-Node 140.6.15.3 | = | 10001100 | 00000110 | 00001111 | 00000011 |
| Mask 255.255.0.0 | = | 11111111 | 11111111 | 00000000 | 00000000 |
| Destination 140.7.9.2 | = | 10001100 | 00000111 | 00001001 | 00000010 |

When the end-node IP address is combined through the AND operation with the mask the result is:

| | | | | | |
|---------------------|---|----------|----------|----------|----------|
| End-Node 140.6.15.3 | = | 10001100 | 00000110 | 00001111 | 00000011 |
| Mask 255.255.0.0 | = | 11111111 | 11111111 | 00000000 | 00000000 |
| ----- | | | | | |
| RESULT OF "AND" | = | 10001100 | 00000110 | 00000000 | 00000000 |
| (In dotted-decimal) | = | 140. | 6. | 0. | 0 |

When the destination IP address is combined through the AND operation with the mask the result is:

| | | | | | |
|-----------------------|---|----------|----------|----------|----------|
| Destination 140.7.9.2 | = | 10001100 | 00000111 | 00001001 | 00000010 |
| Mask 255.255.0.0 | = | 11111111 | 11111111 | 00000000 | 00000000 |
| ----- | | | | | |
| RESULT OF "AND" | = | 10001100 | 00000111 | 00000000 | 00000000 |
| (In dotted-decimal) | = | 140. | 7. | 0. | 0 |

Since the results (140.6.0.0 and 140.7.0.0) are not equal, the end-node concludes that the destination must be on a different network, and the frame is sent to a router. This is the way an end-node uses the mask value. A router, on the other hand, masks the destination address in an incoming frame, and the result is used as a lookup key in the routing table.

6.4 Variable Length Subnet Masks

Consider the XYZ Corporation which has been assigned the network number 160.6.0.0 from the InterNIC. The world sees this company as 160.6.0.0. Within the XYZ Corporation, however, the division of the network is very different. They could use Variable Length Subnet Masks to divide their world into a multilevel hierarchy.

The term Variable Length Subnet Mask (VLSM) refers to a design practice of creating sub-subnets in a tree-structured network. XYZ Corp has an office in many states, 23 field offices in all. The designers of the XYZ Corp network decide to divide their network into 32 subnets using a mask of 255.255.252.0. In binary, the mask bits are 11111111 11111111 11111100 00000000. The six bits of "1" in the third octet are the subnet bits (since the first 16 bits represent the network). These six bits can differentiate between up to 64 different subnetworks. This is the same logic as would be applied to any subnet mask.

Now, however, it is realized that at each site there is a sales division, an accounting department, a marketing group, and a technical support group. The designers want to further subdivide each site with a router. This requires further division of the address field. No problem. The main, central routers are subnetted 255.255.252.0, and they differentiate between field offices. The field office routers, however, are subnetted with 255.255.255.128. Think about this in the binary representation.

```
Main Router:  11111111 11111111 11111100 00000000
Field Router: 11111111 11111111 11111111 10000000
```

Notice that the field router defines an additional three bits in the mask. These three bits can be used to differentiate between seven more subnets. These are going to be used to route between the sales, accounting, marketing, and tech support groups at each field site. Perhaps the assignment is like this:

```
Sales =      001
Accounting =  010
Marketing =   011
Tech Support = 100
```

So, at a particular location, we discover that the bit sequence "000011" has been used to represent the site, say the network at the field office in Palo Alto, California. Here are the four divisions:

```
Sales =      000011 001 XXXXXXXX
Accounting =  000011 010 XXXXXXXX
Marketing =   000011 011 XXXXXXXX
Tech Support = 000011 100 XXXXXXXX
```

The "X"s represent the bits that are available to differentiate between individual stations (hosts) in each department. When viewed in the binary sense, this scheme identifies FOUR fields. The NETWORK PORTION (in each case this is 160.6.0.0), the SUBNET (which is 000011), a "sub"-subnet (001,010,011, and 100) and the node portion (the "X"s). The routers understand how to divide the address based on the subnet mask. The world,

in our example, sees 255.255.0.0. The company sees 255.255.252.0. Each field office sees 255.255.255.128. The router masks the address and looks up the result in its table to determine how to forward the frame. Since the router "thinks" in binary, there is no confusion, no problem. We, however, don't think in binary. Consider these three stations shown with their dotted decimal and binary representations:

```
160.6.12.129    10100000 . 00000110 . 00001100 . 10000001
160.6.14.1      10100000 . 00000110 . 00001110 . 00000001
160.6.14.129    10100000 . 00000110 . 00001110 . 10000001
```

When looking at the dotted-decimal notation, there is nothing immediately obtuse. In fact, when looking at the binary, you don't necessarily see the conflict immediately. To understand any subnet masking, it is necessary to break the 32-bit address into the fields defined by the variable length masks.

First, mask the addresses with the 255.255.0.0 used by the world at large:

```
Mask =          11111111 . 11111111 . 00000000 . 00000000
160.6.12.129 =  10100000 . 00000110 . 00001100 . 10000001
-----
Result =        10100000 . 00000110 . 00000000 . 00000000
```

You can see that all three address mask back to 160.6.0.0; they are all on the same network as far as the world is concerned. Now let's just consider the last 16 bits of each address (since we know the first 16 are the same in all three cases).

The next router uses the mask 255.255.252.0; we are considering the 252.0 part. The masking now continues as follows:

```
Mask =          11111100 . 00000000
(160.6).12.129  00001100 . 10000001
(160.6).14.1    00001110 . 00000001
(160.6).14.129  00001110 . 10000001
```

Do you see that all three stations are identified with 000011 as the bit pattern included in the masked portion? This means that the next router in line (the one masked as 255.255.252.0) will direct frames intended for any of these three stations to the same destination router according to its routing table.

The last router in this hierarchy is using the mask 255.255.255.128. Here is the masking:

RESULT OF MASKING

| | | |
|----------------|---------------------|---------------------|
| Mask = | 11111111 . 10000000 | |
| (160.6).12.129 | 00001100 . 10000001 | 00001100 . 10000000 |
| (160.6).14.1 | 00001110 . 00000001 | 00001110 . 00000000 |
| (160.6).14.129 | 00001110 . 10000001 | 00001110 . 10000000 |

It is critical that you understand this last step. Do you see that the bits included by the mask have been included in the result? Do you see the three additional bits used as the mask went from 255.255.252.0 to 255.255.255.128? Now we can assess the validity of the addresses. We know that the design intent called for four "sub"-subnetworks (001, 010, 011, and 100). Don't be confused because these bits "span" the dot in the dotted-decimal notation. This is the confusing aspect of using anything other than "255"s in a subnet mask; the actual fields don't break at the dots. The fields break as defined by the mask bits.

In this example, we know that all three stations are on the subnet defined with the leading bits "000011". This leaves the "other" three bits to further differentiate between sub-subnets. (By the way, the term "sub"-subnet is being used only in the context of this document. The real world simply calls all of them "subnets" without regard for their level of hierarchical differentiation.) The remaining three bits may be broken out as follows (this is the table above, simply repeated and clarified):

RESULT OF MASKING

| | | |
|----------------|---------------------|---------------------------|
| Mask = | 11111111 . 10000000 | |
| (160.6).12.129 | 00001100 . 10000001 | 000011 [00 . 1] 0000000 |
| (160.6).14.1 | 00001110 . 00000001 | 000011 [10 . 0] 0000000 |
| (160.6).14.129 | 00001110 . 10000001 | 000011 [10 . 1] 0000000 |

Compare this to the design document which defined:

| | | | |
|----------------|--------|-----|---------|
| Sales = | 000011 | 001 | XXXXXXX |
| Accounting = | 000011 | 010 | XXXXXXX |
| Marketing = | 000011 | 011 | XXXXXXX |
| Tech Support = | 000011 | 100 | XXXXXXX |

What we now see is that the address 160.6.14.129 has the subnet bits 101 at the mask point 255.255.255.128. This is an address which is not defined by the design of the network. Herein lies the danger with variable length masking: it's awfully confusing to our decimal brains.

Appendix A. Sharing Microsoft Office 97 and Lotus SmartSuite 97 from OS/2 Warp Server

Two popular application suites, Microsoft Office 97 and Lotus SmartSuite 97, can be easily integrated into the OS/2 Warp Server environment to serve Windows 95 and Windows NT clients. This Appendix includes instructions for setting up these application suites onto the server.

These instructions were developed and provided by Harold Madere and Vince Munoz of the IBM Personal Systems Solutions Center in Dallas, Texas. We gratefully acknowledge their permission to include these helpful instructions in this redbook.

Both installation procedures follow a similar outline:

1. Configure the server
 - a. Define a group
 - b. Define an alias
2. Install software to the server from a workstation
3. Install to other workstations from the server

A.1 Sharing Microsoft Office 97

To install Microsoft Office 97 onto an OS/2 Warp Server domain, follow these steps:

1. Configure the server
 - a. Define a Group for users of Microsoft Office 97:
 - 1) From the OS/2 Warp Server desktop, double-click on the **LAN Server Administration** icon and log on as an Administrator.
 - 2) When the LAN Server Administration - Icon View appears, double-click on the **Domain** icon. Define a group for the application by double-clicking on the **Groups** icon and click mouse button 2 (usually the right mouse button) on the **Group Template** icon and drag it to an open space in the window.
 - 3) Fill in the Name and Description blocks. Click on the **Users** tab. Click the **Add** button and select all users for that group.
 - 4) Click the **Add** button. Click the **General** tab and fill in the Title for the group. Click the **Create** button and close the window.
 - b. Define an Alias for Microsoft Office 97:

- 1) In the Domain Icon View window, double-click on the **Resource Definitions** icon. In the Resource Definitions window, create a directory alias by clicking the right mouse button and dragging it to an open space within the window.
- 2) In the Directory Alias - Create screen, fill in all required information on the Identify tab. Change the entry fields based on your specific installation needs:

| | |
|--------------------|----------------------|
| Field | Description |
| Alias | WINAPPS |
| Description | MSOFFICE for Windows |
| Server Name | SERVER01 |
| Path | C:\WINAPPS |

- 3) Select the **General** tab and fill in the Title box to name the alias, then click on the **Create** button.
 - 4) When the Access Control Profile does not exist warning appears, select **OK** to create a new profile.
 - 5) In the Access Control Profile - Settings View window, select the **Permissions** tab, then click the **Add** button. Select the names and groups you want to have access to this resource and the permissions that you want each to have.

Note: The only permissions that users require for this resource are create, read and execute.
 - 6) After permissions have been given, click on the **Create** button. When the Propagate Access Profile to subdirectories window appears, click **OK**. When the Setting View window reappears, click the **Set** button. Close the Resource Definitions window.
2. Install Microsoft Office 97 onto the server from a workstation. These instructions use the IBM Networks Client for Windows 95 or Windows NT Version 4.0, with a CD-ROM drive. If you do not have this client, it can be obtained from the following URL:
- <http://www.software.ibm.com/os/warp-server/clients/clifnt.ht>
- a. From the Windows 95 or NT 4.0 desktop, start the IBM Networks Client from the desktop and log on as an Administrator. Then click on **Drives** and connect to the WINAPPS alias (or use the name you defined) and close the window when completed.
 - b. From the Windows 95 or NT 4.0 desktop, insert the Microsoft Office CD-ROM in the drive. Click the **Start** button, then the **Run** button. When the Run window appears, type in the drive letter of the

CD-ROM drive and type in the `x:\SETUP.EXE /A` command to install the program, where x is the CD-ROM drive letter. The /A switch indicates the program is to run in administrative mode, which is available only from the original media.

- c. Click the **OK** button to continue.
 - d. When the Microsoft Office Setup window appears, click **Continue** and read the information on the remaining setup screens carefully before continuing with each step.
 - e. Fill in the Organization Name box and click **OK**.
 - f. Confirm the Organization Name and click **OK**.
 - g. Type the CD KEY number and click **OK**.
 - h. Click **OK** to verify the information on the Product ID screen.
 - i. The next screen asks which folder the program will be installed into. Click on the **Change Folder** button and select the WINAPPS alias (or the name that you used) and click **OK**.
 - j. On the next screen, ensure that the alias drive is set as the default to install the MSAPPS folder. If it is not the default, then select the default and click **OK**.
 - k. Click **Yes** when prompted to create the MSAPPS folder.
 - l. Verify your information on the Network Server Confirmation screen and click **Continue**.
 - m. Select the location where you want the shared files to be located and click **OK**. We recommend installing the files in the user home directory.
 - n. Select the desired Paper Format & Language type and click **OK**.
 - o. The installation progress bar appears while the program installs. The installation takes approximately 45 minutes to complete.
 - p. Click **OK** on the Setup Completed Successfully screen to exit the installation program.
3. Installing the Microsoft Office client on a Windows 95 or NT 4.0 workstation:
- a. Verify that the IBM Networks Client is installed on the workstation. If not, it can be obtained from the URL specified in Step 2.
 - b. From the client desktop, click **Start** and then **Programs** and start the IBM Networks Client.

- c. When the IBM Networks Client screen appears, click on the **Drives** icon and click the **Find** button.
- d. Select the alias (WINAPPS) where the program is located and click **OK**.
- e. Click on the **Connect** button and click **Close**.
- f. Close the IBM Networks Client window.
- g. Double-click the **My Computer** icon, and then click on the Alias drive icon.
- h. The alias directory window will display two folders in the subdirectory, MSOFFICE and MSAPPS. Double-click on the **MSOFFICE** folder icon.
- i. Double-click on the **Setup** icon.
- j. Select **Continue** from the MSOFFICE Setup screen.
- k. Fill in the Name Information window and click **OK**.
- l. Click **OK** to confirm the information.
- m. Click **OK** when the Microsoft Office setup Product ID window appears.
- n. Select the product installation path. If desired, set to the user home directory or set to the local hard drive.
- o. Select **OK**.
- p. Select the location for shared files installation. We recommend putting them on the server.
- q. Click on the **Run from Network Server** button. The installation progress bar appears while the program installs.
- r. Click **OK** on the Setup Completed Successfully screen to exit the installation program.
- s. Close all open windows and restart the client system.

A.2 Sharing Lotus SmartSuite 97

To install Lotus SmartSuite 97 onto an OS/2 Warp Server domain, follow these steps:

1. Configure the server:
 - a. Define a Group for users of Lotus SmartSuite 97:
 - 1) From the OS/2 Warp Server desktop, double-click on the **LAN Server Administration** icon and log on as an Administrator.

- 2) When the LAN Server Administration - Icon View appears, double-click on the **Domain** icon. Define a group for the application by double-clicking on the **Groups** icon and click mouse button 2 (usually the right mouse button) on the **Group Template** icon and drag it to an open space in the window.
 - 3) Fill in the Name and Description blocks. Click on the **Users** tab. Click the **Add** button and select all users for that group.
 - 4) Click the **Add** button. Click the **General** tab and fill in the Title for the group. Click the **Create** button and close the window.
- b. Define an Alias for Lotus SmartSuite 97:

- 1) In the Domain Icon View window, double-click on the **Resource Definitions** icon. In the Resource Definitions window, create a directory alias by clicking the right mouse button and dragging it to an open space within the window.
- 2) In the Directory Alias - Create screen, fill in all required information on the Identify tab. Change the entry fields based on your specific installation needs:

| | |
|--------------------|------------------------|
| Field | Description |
| Alias | WINAPPS |
| Description | SmartSuite for Windows |
| Server Name | SERVER01 |
| Path | C:\WINAPPS |

- 3) Select the **General** tab and fill in the Title box to name the alias, then click on the **Create** button.
- 4) When the Access Control Profile does not exist warning appears, select **OK** to create a new profile.
- 5) In the Access Control Profile - Settings View window, select the **Permissions** tab, then click the **Add** button. Select the names and groups you want to have access to this resource and the permissions that you want each to have.

Note: The only permissions that users require for this resource are create, read and execute.
- 6) After permissions have been given, click on the Create button. When the "Propagate Access Profile to subdirectories" window appears, click OK. When the Setting View window reappears, click the Set button. Close the Resource Definitions window.

2. Install Lotus SmartSuite 97 onto the server from a workstation. These instructions use the IBM Networks Client for Windows 95 or Windows NT Version 4.0, with a CD-ROM drive. If you do not have this client, it can be obtained from the following URL:

<http://www.software.ibm.com/os/warp-server/clients/clifnt.ht>

- a. From the Windows 95 or NT 4.0 desktop, start the IBM Networks Client from the desktop and log on as an Administrator. Then click on **Drives** and connect to the WINAPPS alias (or use the name you defined) and close the window when completed.
 - b. Insert the Lotus SmartSuite CD-ROM in the client CD-ROM drive. Click the **Start** button, then the **Run** button. When the Run window appears, type in the drive letter of the CD-ROM drive and type in the `x:\INSTALL.EXE` command to install the program, where x is the CD-ROM drive letter.
 - c. Click the **OK** button to continue.
 - d. When the Welcome screen appears, click the **File Server or Multiple User Install** box and click on **Next**.
 - e. After confirming the names, click **Yes**.
 - f. Select **File Server Install**, and click **Next**.
 - g. When the Networks Administrators Guide screen appears, select **Open** and print the documentation if desired, otherwise click **Next**.
 - h. Select the target drive letter to install the program. This should be the alias (WINAPPS) that was created on the server in Step 1.
 - i. Click **OK** to accept the defaults or change to the folder you want to use. We recommend accepting the default folders for the program.
 - j. The Shared Tools folder appears, accept the default and click **Next**.
 - k. Select the applications that you want to install and click **Next**.
 - l. On the install options screen, select the options you want to install and click **Next**.
 - m. Select the **Program** folder, then select the folder where you want to install the program and click **Next**.
 - n. When prompted to begin copying files to the hard disk, click **Yes**. The installation takes approximately 35 minutes to complete.
 - o. When the Installation Complete screen appears, click **Done**.
 - p. Run the Node installation program.
3. Installing the Lotus SmartSuite client on a Windows 95 or NT 4.0 workstation:

- a. Verify that the IBM Networks Client is installed on the workstation. If not, it can be obtained from the URL specified in Step 2.
- b. From the client desktop, click **Start** and then **Programs** and start the IBM Networks Client.
- c. When the IBM Networks Client screen appears, click on the **Drives** icon and click on the **Find** button.
- d. Select the alias (WINAPPS) where the program is located and click **OK**.
- e. Click on the **Connect** button and click **Close**.
- f. Close the IBM Networks Client window.
- g. Double-click the **My Computer** icon, and then click on the Alias drive icon.
- h. The alias directory window will display all folders in the subdirectory. Select the **Lotus** folder and open it.
- i. Double-click on the **Install** icon.
- j. When the "Welcome to SmartSuite 97 Install" screen appears, type in your name and click **Next**. Click **Yes** to confirm the names you entered.
- k. In the "Specify Lotus SmartSuite folder" window, select the drive and folder where you want all of the SmartSuite 97 applications to be installed; click **Next**.
- l. It may be advantageous to install the program on the user's home directory.
- m. In the next screen, select the features to install, drive location and folder, then click **Next**.
- n. In the Local Node Features window, deselect all blocks, and click **Next**.
- o. In the Select Program Folder screen, accept the default or send to a new folder and click **Next**.
- p. Click **Yes** when the Begin Copying Files screen appears.
- q. Click **Done** when the Install Complete screen appears, and close all windows and restart the client system.

Appendix B. Special Notices

This publication is intended to help IBMers, Customers, Business Partners, and anyone else who is involved in the marketing, planning, implementation, and support of OS/2 Warp Server and related products. The information in this publication is not intended as the specification of any programming interfaces that are provided by OS/2 Warp Server. See the PUBLICATIONS section of the IBM Programming Announcement for OS/2 Warp Server Version 4 for more information about what publications are considered to be product documentation.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

| | |
|----------------------|----------------------------|
| ADSTAR | Advanced Function Printing |
| AFP | AIX |
| AnyNet | AS/400 |
| BESTeam | BookManager |
| DB2 | FFST/2 |
| IBM | ISSC |
| LAN Distance | NetFinity |
| NetView | OS/2 |
| Presentation Manager | PS/2 |
| RS/6000 | S/390 |
| SD/2 | SystemView |
| ThinkPad | |

The following terms are trademarks of other companies:

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

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

Pentium, MMX, ProShare, LANdesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

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

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How To Get ITSO Redbooks" on page 195.

- *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*, SG24-4602
- *Inside OS/2 Warp Server, Volume 2: System Management, Backup/Recovery and Advanced Print Services*, SG24-4702
- *OS/2 Installation Techniques: The CID Guide*, SG24-4295
- *OS/2 Warp Server, Windows NT, and NetWare: A Network Operating System Study*, SG24-4786
- *Network Clients for OS/2 Warp Server: OS/2 Warp 4, DOS/Windows, Windows 95/NT, and Apple Macintosh*, SG24-2009 (in press)
- *Remote Installation of OS/2 Warp 4 using CID*, SG24-2010 (in press)

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

| CD-ROM Title | Subscription Number | Collection Kit Number |
|---|---------------------|-----------------------|
| System/390 Redbooks Collection | SBOF-7201 | SK2T-2177 |
| Networking and Systems Management Redbooks Collection | SBOF-7370 | SK2T-6022 |
| Transaction Processing and Data Management Redbook | SBOF-7240 | SK2T-8038 |
| AS/400 Redbooks Collection | SBOF-7270 | SK2T-2849 |
| RISC System/6000 Redbooks Collection (HTML, BkMgr) | SBOF-7230 | SK2T-8040 |
| RISC System/6000 Redbooks Collection (PostScript) | SBOF-7205 | SK2T-8041 |
| Application Development Redbooks Collection | SBOF-7290 | SK2T-8037 |
| Personal Systems Redbooks Collection | SBOF-7250 | SK2T-8042 |

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL <http://www.redbooks.ibm.com>.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

To get LIST3820s of redbooks, type one of the following commands:

```
TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
```

To get lists of redbooks:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
```

To register for information on workshops, residencies, and redbooks:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
```

For a list of product area specialists in the ITSO:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
```

- **Redbooks Home Page on the World Wide Web**
<http://w3.itso.ibm.com/redbooks>
- **IBM Direct Publications Catalog on the World Wide Web**
<http://www.elink.ibm.link.ibm.com/pbl/pbl>
IBM employees may obtain LIST3820s of redbooks from this page.
- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

| | IBMMAIL | Internet |
|------------------------|---------------------|----------------------|
| In United States: | usib6fpl at ibmmail | usib6fpl@ibmmail.com |
| In Canada: | caibmbkz at ibmmail | lmannix@vnet.ibm.com |
| Outside North America: | dkibmbsh at ibmmail | bookshop@dk.ibm.com |

- **Telephone orders**

| | |
|---------------------------|-------------------------------|
| United States (toll free) | 1-800-879-2755 |
| Canada (toll free) | 1-800-IBM-4YOU |
| Outside North America | (long distance charges apply) |
| (+45) 4810-1320 - Danish | (+45) 4810-1020 - German |
| (+45) 4810-1420 - Dutch | (+45) 4810-1620 - Italian |
| (+45) 4810-1540 - English | (+45) 4810-1270 - Norwegian |
| (+45) 4810-1670 - Finnish | (+45) 4810-1120 - Spanish |
| (+45) 4810-1220 - French | (+45) 4810-1170 - Swedish |

- **Mail Orders** — send orders to:

| | | |
|--|--|--|
| IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA | IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada | IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark |
|--|--|--|

- **Fax** — send orders to:

| | |
|---------------------------|---|
| United States (toll free) | 1-800-445-9269 |
| Canada | 1-403-267-4455 |
| Outside North America | (+45) 48 14 2207 (long distance charge) |

- **1-800-IBM-4FAX (United States) or (+1) 415 855 43 29 (Outside USA)** — ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com

- **On the World Wide Web**

| | |
|---------------------------------|---|
| Redbooks Home Page | http://www.redbooks.ibm.com |
| IBM Direct Publications Catalog | http://www.elink.ibm.link.ibm.com/pbl/pbl |

- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

| Title | Order Number | Quantity |
|-------|--------------|----------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | |
|------------|-----------|
| First name | Last name |
|------------|-----------|

| |
|---------|
| Company |
|---------|

| |
|---------|
| Address |
|---------|

| | | |
|------|-------------|---------|
| City | Postal code | Country |
|------|-------------|---------|

| | | |
|------------------|----------------|------------|
| Telephone number | Telefax number | VAT number |
|------------------|----------------|------------|

- Invoice to customer number

- Credit card number

| | | |
|-----------------------------|----------------|-----------|
| Credit card expiration date | Card issued to | Signature |
|-----------------------------|----------------|-----------|

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

List of Abbreviations

| | | | |
|--------------|---|---------------|--|
| ACE | Access Control Entry | HTTP | HyperText Transfer Protocol |
| ACP | Access Control Profile | IBM | International Business Machines Corporation |
| ADF | Application Definition File | IETF | Internet Engineering Task Force |
| ADSM | ADSTAR Distributed Storage Manager | IFS | Installable File System |
| AFP | Advanced Function Printing | IP | Internet Protocol |
| ARP | Address Resolution Protocol | IPCP | IP Control Protocol |
| ASD | Alternate Software Delivery | ITSO | International Technical Support Organization |
| BOOTP | Bootstrap Protocol | LAA | Locally Administered Address |
| CHAP | Challenge Handshake Authentication Protocol | LAPS | LAN Adapter and Protocol Services |
| CID | Configuration, Installation, Distribution | LCP | Link Control Protocol |
| CSF | Corrective Service Facility | LDAP | Lightweight Directory Access Protocol |
| DB2/2 | DataBase 2 for OS/2 | MD5 | Message Digest 5 |
| DCAF | Distributed Console Access Facility | MPTS | Multiprotocol Transport Services |
| DDE | Dynamic Data Exchange | MRU | Maximum Response Unit |
| DES | Data Encryption Standard | NVDM/2 | NetView Distribution Manager/2 |
| DDNS | Dynamic Domain Name Server | OS/2 | Operating System /2 |
| DHCP | Dynamic Host Configuration Protocol | PAP | Password Authentication Protocol |
| EA | Extended Attribute | PPP | Point-to-Point Protocol |
| FAT | File Allocation Table | RAID | Redundant Array of Independent Disks |
| FTP | File Transfer Protocol | RFC | Request For Comment |
| GUI | Grafical User Interface | RIPL | Remote Initial Program Load |
| HPFS | High Performance File System | RSP | Response File |
| HTML | HyperText Markup Language | SD/2 | Software Distribution for OS/2 |

| | | | |
|--------------------|--|--------------------|-------------------------------|
| <i>SMP</i> | Symmetric Multiprocessing | <i>UBF</i> | Use Based Feature |
| <i>TME</i> | Tivoli Management Environment | <i>UPO</i> | Upgrade Protection Option |
| <i>TPAP</i> | Two Party Authentication Protocol | <i>URL</i> | Universal Resource Locator |
| <i>UAA</i> | Universal Adapter Address | <i>VLAN</i> | Virtual Local Area Network |
| <i>UART</i> | Universal Asynchronous Receiver/Transmitter | <i>WAN</i> | Wide Area Network |
| | | <i>WWW</i> | World Wide Web |

Index

Numerics

8235 DIALs client 75, 122, 130, 138

A

Abbreviations 199
Acronyms 199
Advanced Print function 16
Alert Manager 10
AUTOCHECK 159, 160

B

BACKACC 173
Backup and Recovery component 15
bibliography 193
Browser
 See Network Neighborhood Enabler
Btree 169

C

CHAP 71, 75, 98, 140
CHKDSK
 AUTOCHECK 171
 design 159
 enhancements 158
 files included 160
 IFS statement 160
 installing 160
 obtaining code within IBM 158
 parameters 161, 162
 removing 162
 requirements 157
 unsupported operating systems 158
 using 161
CHKDSK.LOG file 158
Client
 browser flow 151
 installing software on RIPL clients 68
 IP addressing with PPP 93
 licensing 3
 NT PPP support 121

Client (*continued*)

 OS/2 PPP setup 122
 PPP passphrases 135
 PPP restrictions 79
 PPP support 75
 pristine installation support 57
 removing software from RIPL clients 69
 requirements for PPP 78
 supported platforms 4
CLIFI command 69
CMPROCES command 135
Critical File Monitor 11

D

DDNS 98, 117
DHCP 117
Dirty flag 162
Disk Checking
 See CHKDSK
Downloading from Software Choice 36, 39
Dynamic IP 18, 93, 99

E

Enhancements overview 21, 27
Event Scheduler 11

F

FAT
 allocation 165
 boot sector 164
 cluster size 164
 compared to HPFS 166
 history 163
 OS/2 EAs 166
 overview 163
 partition structure 165
Fault Tolerance 7, 172
Feature Installer
 overview 40
 prerequisites 41
 references 41

File and Print Folder contents 6
File and Print overview 5
Future enhancements 21

G

GENFIRPL command 68

H

Hotfix sectors 169

HPFS

- allocation 167
- AUTOCHECK 171
- Btree 169
- caching 168
- compared to FAT 166
- compared to HPFS386 171
- data recovery 170
- dirty flag 162
- file recovery 174
- Fnode 168
- fragmentation 166
- hotfix sectors 169
- inheritance 172
- organization 168
- overview 166
- partition structure 167
- Spareblock 168
- Superblock 167

HPFS386

- access controls 172
 - backing up 173
 - effect of renaming directories 173
 - inheritance 172
 - maximum number 172
- benefits 171
- description 171
- startup diskette 6

I

IFS 166

L

LAN Distance

See Remote Access

Licensing 3

- chargeable server services 3
- example 4
- UBF 3
- Windows 95 and NT 3

Lotus SmartSuite 97

- installing clients 188
- installing to server 188
- preparing the server 186

M

Microsoft Office 97

- installing clients 185
- installing to server 184
- preparing server 183

MPTS architecture 19

N

NetView Distribution Manager

- creating profile 59
- description 57
- distributing 60
- pristine installation support 57
- SYSLEVEL 58

NetWare support 5, 17

Network Neighborhood Enabler

- browser communications flow 150
- browser hierarchy 153
- browser types 147
- changes to IBMLAN.INI 146
- election process 152
- included files 153
- installing 154
- NetBIOS names 148
 - IBM Neighborhood Browser Enabler
 - names 149
 - standard names 148
- obtaining code 153
- operation 150
- prerequisites 154
- protocol requirements 145

Network Neighborhood Enabler (*continued*)

- purpose 145
- removing 155
- starting and stopping 155
- SYSLEVEL 146

O

OS/2 Warp Server

- access controls 172
 - Backup and Recovery 15
 - client licensing 3
 - components 1
 - Dynamic IP description 18
 - File and Print overview 5
 - Folder contents 6
 - functions in OS/2 Warp Server Advanced 2
 - future enhancements 21
 - HPFS386 2
 - MPTS architecture 19
 - Network Neighborhood Enabler 145
 - overview 1
 - Pentium support 3
 - Remote Access 16, 71
 - sharing Lotus SmartSuite 97 183
 - sharing Microsoft Office 97 183
 - SystemView components 9
 - TCP/IP enhancements 175
 - TCP/IP summary 17
 - viewing resource usage 14
- OS/2 Warp Server FirstStep 2

P

- PAP 98, 140
- PMCHKLOG 158
- Point-to-Point Protocol
 - See PPP
- Power-On Error Detect 11
- PPP
 - See also Remote Access
 - changing passphrases 134
 - client requirements 79
 - client restrictions 79
 - components 71
 - configuring 92
 - configuring Win95 support 101

PPP (*continued*)

- installing 87
- internals 139
- NT client 121
- OS/2 client 122
- problem determination 137
- protocol description 140
- recovering Administrator passphrase 135
- RFCs 143
- WCLIPADR.INI 99
- WCLLOCAL.INI PPP parameters 97
- Process Manager 11
- Public applications 5

R

Remote Access

- adding TCP/IP support 94
- changing passphrases 135
- client requirements 78
- client restrictions 79
- configuring PPP 93
- configuring Win95 support 101
- connection types 72
- Ethernet setup 96
- files changed 87
- icon 91
- install from OS/2 Warp Server 81
- maximum clients 75
- MPTS requirement 88
- new components 71
- obtaining code 87
- OS/2 client 122
- other clients 76
- overview 16
- PPP internals 139
- PPP support overview 75
- problem determination 137
- protocol description 140
- recovering Administrator passphrase 135
- requirements 76
 - adapter 77
 - disk and memory 77
 - software 76
- RFCs 143
- SYSLEVEL 72
- typical scenarios 74

- Remote Access (*continued*)
 - upgrading 87
 - WCLIPADR.INI 99
 - WCLLOCAL.INI 97
- Remote System Manager 11
- RIPL
 - installing software 68
 - removing software 69

S

- Screen View 12
- SECADMIN 85, 135
- Security Manager 12
- Serial Control 12
- Shuttling 132
- Software Advantage customer information 38
- Software Choice
 - accessing 29
 - Announcement letter 25
 - background 23
 - benefits 26
 - download steps 39
 - IBM internal access URL 33
 - installation with Feature Installer 40
 - installing to RIPL clients 68
 - integration description 25
 - integration diagram 25
 - introduction 24
 - Java for OS/2 example 41, 47
 - language support 28
 - product details 34
 - subscriptions 37
 - URLs 32
 - user ID requirements 37
 - using NetView DM/2 58
 - using Tivoli Software Distribution 62
 - using TME 10 Software Distribution 46, 51
- Software Distribution
 - icon and description 10
 - installing on RIPL clients 68
 - references 59
- Software Installation 12
- Software Inventory 13
- Spareblock 168
- Subscriptions to Software Choice 37

- Superblock 167
- System Information Tool 13
- System Monitor 14
- System Partition Access 14
- System Profile 15
- SystemView components 9

T

- TCP/IP
 - aliasing 176
 - enhancements 175
 - subnet masking 177
 - binary representation 178
 - variable length masks 178
- TCPBEUI 18, 134, 145
- Tivoli Software Distribution
 - configuring 64
 - distributing Software Choice feature 65
 - Java for OS/2 example 63
 - prerequisites 62
 - SYSLEVEL 63
- TME 10 NetFinity Server
 - description 45
 - distributing features 51
 - installing Software Choice features 46
 - Java for OS/2 example 47
 - log file 56
 - positioning with SystemView 45
 - pristining client considerations 45
 - software library entry 48
 - SYSLEVEL 46
- TPAP 75
- Tuning Assistant 9

U

- Use-Based Feature 3

W

- WCLIPADR.INI 72, 89, 99, 141
- WCLLOCAL.INI 72, 97, 141
- Windows 95 and NT
 - browser flow 151
 - licensing with OS/2 Warp Server 4
 - PPP in NT 121

Windows 95 and NT *(continued)*

PPP support 75, 100

support in OS/2 Warp Server 4

using Lotus SmartSuite 97 from Warp

Server 188

using Microsoft Office from Warp Server 185

with Software Choice 26

X

X.25 support 79

ITSO Redbook Evaluation

OS/2 Warp Server Functional Enhancements, Part 1
SG24-2008-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)



Printed in U.S.A.

SG24-2008-00

