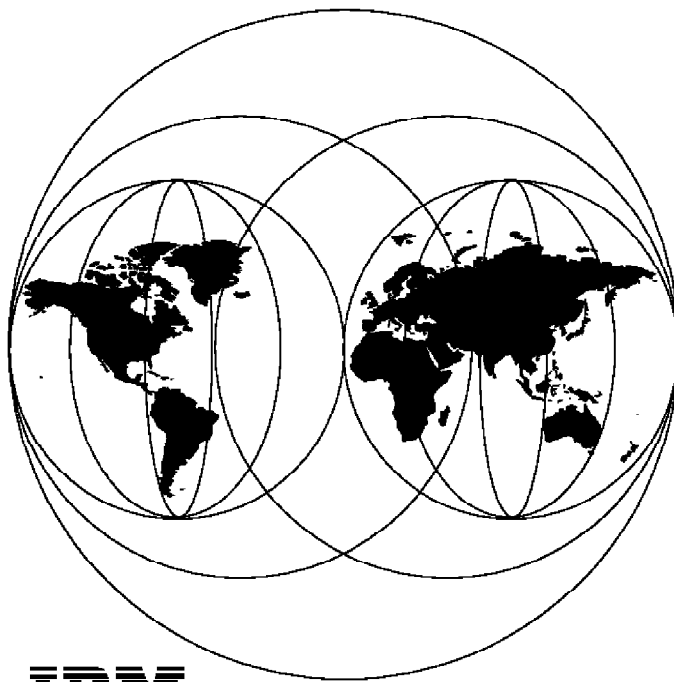# Network Clients for OS/2 Warp Server: OS/2 Warp 4 DOS/Windows, Windows 95/NT, and Apple Macintos

August 1997

IBM

International Technical Support Organization

Austin Center

International Technical Support Organization

Network Clients for OS/2 Warp Server: OS/2 Warp 4 DOS/Windows, Windows 95/NT, and Apple Macintos

August 1997

IBML

```
┌─ Take Note! ──────────────────────────────────────────────────────────────┐
│                                                                            │
│  Before using this information and the product it supports, be sure to read the general information │
│  in Appendix E, "Special Notices" on page 395.                             │
│                                                                            │
└────────────────────────────────────────────────────────────────────────────┘
```

First Edition (August 1997)

This edition applies to client-related enhancements made to OS/2 Warp Server 4.0 since its roll-out in October 1995.

Contents

Figures

Tables

Preface

Since the roll-out of OS/2 Warp Server in October 1995, IBM has continuously enhanced OS/2 Warp Server. IBM makes product enhancements available on the Internet to assure customers have the new products right away.

For example, the OS/2 Warp Family Web site can be found at:

```
http://www.software.ibm.com/os/warp/
```

This Web site provides information about the OS/2 Warp Family and provides links to pages of Downloads, Solutions, the Help Desk, News & Events, Partners, and Shop. If you select **Downloads**, then **Enhancements for Win95 and WinNT**, the Web site titled "OS/2 Warp Server Enhancements for Win95 and WinNT" is loaded as shown in Figure 1.

Figure 1. OS/2 Warp Server Download Web Site on the Internet.   The loaded Web Site is: http://www.software.ibm.com/os/warp-server/clients/clifnt.htm

This redbook details OS/2 Warp Server enhancements and emphasizes the integration of Windows 95 and Windows NT Workstation clients in an OS/2 Warp Server environment. We illustrate how to install and configure OS/2 Warp Server clients such as:

- OS/2 Warp 4
- DOS LAN Services for DOS and Windows
- IBM Networks Client for Windows 95
- IBM Networks Coordinated Logon Client for Windows NT 4.0
- IBM Networks Primary Logon Client for Windows NT 4.0
- Apple Macintosh

The disscussion of each platform focuses on file and print services configured for NetBIOS and TCP/IP environments, dynamic TCP/IP, where apropriate, and remote access through the Point-to-Point Protocol (PPP). In a dynamic TCP/IP environment, clients get their TCP/IP information from a Dynamic Host Configuration Protocol (DHCP) server and from a Dynamic Domain Name Server (DDNS). These two dynamic TCP/IP servers come with OS/2 Warp Server 4.0.

OS/2 Warp Server is now capable of supporting PPP; therefore, Microsoft clients with remote access services can remotely dial into an OS/2 Warp Server Remote Communication Server and into OS/2 Warp workstations that have the 8235 client installed. The Enhanced Remote Access Connection Server for OS/2 Warp Server is available through IBM Software Choice.
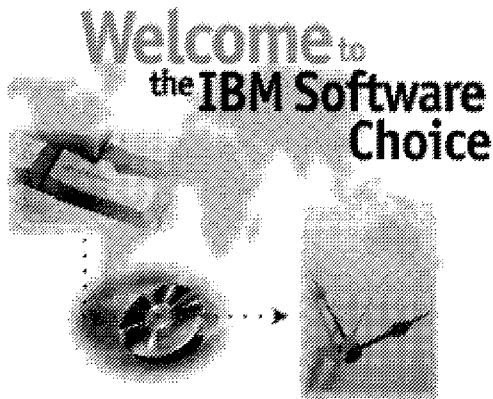
Figure 2. IBM Software Choice

You can navigate through the IBM Software Choice Web sites at the following Web site:

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

How This Redbook Is Organized

This redbook is divided into three parts:

- Part I, which provides common information applicable to all discussed clients.

- Part II, which starts with Chapter 10, "OS/2 Warp 4," provides platform-specific information. Each platform is discussed in its own chapter.

- Part III, Appendixes, provides information about network behaviours of Windows 95 clients and example files of DOS LAN Services configured with PCMCIA support.

This redbook is organized as follows:

1. Part 1, "Common Information"

  - Chapter 1, "OS/2 Warp Server Terms and Conditions" introduces OS/2 Warp Server briefly and clarifies the OS/2 Warp Server terms and conditions pertaining to charges.

  - Chapter 2, "Introducing IBM Networks Clients" contains an introduction to clients that can be attached to an OS/2 Warp Server environment. It also contains a summary of our conclusions and the tasks required for successfully setting up these machines. This will be especially useful for system integrators, to get an idea how complex a set up can be.

  - Chapter 3, "Concepts" discusses concepts such as when and why the idea of a workgroup and domain was defined. New administrators will value this kind of information.

  - Chapter 4, "The Truth about NetBEUI, NetBIOS, SMP, and NetBIOS over TCP/IP" discusses LAN protocols in detail. NetBIOS over TCP/IP implementation is illustrated here. For example, OS/2 Warp Server 4 fully supports IP on the wire through the TCPBEUI (NetBIOS over TCP/IP) implementation. The fact that a NetBIOS API is used as an internal API rather than sockets should not be a concern.

  - Chapter 5, "Installing and Configuring NTS Shadow" introduces Shadow, a NetBIOS Name Server developed by NTS, Network TeleSystems. We show how to install and configure the server as well as how to implement the server into your network, demonstrating its major features.

  - Chapter 6, "Dynamic TCP/IP" briefly defines the basic concepts of Dynamic TCP/IP, and explains how to configure the Dynamic Host

Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS) servers of OS/2 Warp Server.

- Chapter 7, "Remote Access through Point-to-Point Protocol" addresses remote access services through the Point-to-Point Protocol (PPP). In comparison to the former implementation of remote access services in OS/2 Warp Server, extending LAN Distance with PPP support greatly improves support for many remote access clients.

- Chapter 8, "IBM Neighborhood Browser Enabler for OS/2 Warp Server" briefly shows how to install and configure an OS/2 Warp Server enhancement called IBM Neighboorhood Browser Enabler for OS/2 Warp Server.

- Chapter 9, "IBM Networks Clients File and Print Graphical User Interface" discusses the File and Print Graphical User Interface (GUI) of IBM Networks Clients and DOS LAN Services. A major advantage of this interface is that it is used on DOS/Windows-based machines as well as Windows 95 and Windows NT-based machines. If an end user working with DOS LAN Services is upgraded to Windows 95 or Windows NT, they will not need additional education for the File and Print GUI.

2. Part 2, "Installing and Configuring IBM Networks Clients"

- Chapter 10, "OS/2 Warp 4" describes installing and configuring OS/2 Warp 4 for file and print, dynamic TCP/IP, and remote access by using the 8235 client which supports Point-to-Point protocol.

- Chapter 11, "DOS LAN Services for DOS with or without Windows" describes installing and configuring DOS LAN Services on DOS and Windows-based machines. It provides detailed information about memory management, which is crucial information for administrators that want to successfully run DOS and DOS/Windows machines connected to a LAN, with the maximum amount of base memory available. Enhancing DLS to support communication with a NetBIOS Name Server (Shadow) is also included in this chapter.

- Chapter 12, "IBM Networks Client for Windows 95" describes installing and configuring IBM Networks Client for Windows 95. It also shows how to successfully run IBM Dynamic IP Client for Windows 95, and shows how to do to make Windows 95 clients capable of dialing in remotely to an OS/2 Warp Server remote connection server.

- Chapter 13, "IBM Networks Client for Windows NT" describes how to install and configure IBM Networks Client for Windows NT. A detailed section is provided to show the differences between a

Coordinated Logon Client and Primary Logon Client, and shows administrators which of the two to choose in different environments. Dynamic TCP/IP and remote access are discussed here, along with configuration information for remote access through via PPP dialing in remotely to an OS/2 Warp Server remote connection server.

- Chapter 14, "Apple Macintosh Clients" introduces OS/2 LAN Server for Macintosh which, when installed on top of OS/2 Warp Server, supports Apple Macintosh through AppleTalk protocol. This chapter also provides information about a software vendor's product called DAVE, which enables Macintosh machines to log on to OS/2 Warp Server through NetBIOS over TCP/IP.

3. Appendixes

- Appendix A, "Windows 95 Logon Traces to Illustrate SMB Flows" shows traces that are taken to give a deeper view of the network traffic between the workstation and server during the logon process. It also shows that there is no native TCP/IP traffic but NetBIOS over TCP/IP traffic. Therefore, Windows 95 only mentions TCP/IP when dealing with requesters and LAN resources.

- Appendix B, "Windows 95 Logon Traces to Illustrate NetBIOS Flows in MS TCP/IP" shows a trace that was taken to illustrate that, although a Windows 95 client is configured to use TCP/IP for file and print, a NetBIOS session is established over TCP/IP. It also shows queries of Microsoft's proprietary use of NetBIOS names, such as NetBIOS names with the 16th-byte hex values 1Bh and 1Ch, which are not used in a typical OS/2 Warp Server environment unless the Neighborhood Browser Enabler for OS/2 Warp Server is installed.

- Appendix C, "Windows 95 Slow Network Performance" shows a symptom of slow network performance in Microsoft's redirector code that customers might experience when they log on to an OS/2 Warp Server. It gives a detailed description and resolution.

- Appendix D, "PCMCIA Configuration Files for DOS with Windows for Workgroups" shows example files how an IBM ThinkPad 750C was configured to work with PC DOS 7.0, Windows for Workgroups, and DOS LAN Services with TCPBEUI (Real-Mode) support.

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.

Uwe Zimmermann is an Advisory Systems Engineer at the International Technical Support Organization, Austin Center. He has ten years of experience in OS/2 networking and two years in Windows NT. Before joining the ITSO, he worked in an IBM Branch Office in Stuttgart, Germany, as a Networking Systems Engineer and was in charge of large account customers for more than five years. His areas of expertise include OS/2 LAN/Warp Server, Windows NT, NetWare, Software Distribution (CID), dynamic TCP/IP, and Network Computing (NC).

Veronika Moroian is a Software Services Specialist in IBM Argentina, with four years of experience in the personal computers software technical support field. She is an IBM Certified LAN Server Administrator and Engineer. Her areas of expertise include the OS/2 base operating system and OS/2 network environments. She has written several articles on OS/2 for computer magazines such as Byte and Compu Magazine. She was part of the team that wrote the book titled *Getting to Know OS/2 Warp 4*, an ITSO publication published by Prentice Hall in 1996. She has written extensively on the OS/2 Warp File and Print Client and TCPBEUI sections.

Anssi Nummi is a Services Specialist in IBM Finland. He has four years of experience in PC field, mainly in support and maintenance but in education and software developement as well. He has worked at IBM for more than two years, first in the OS/2 Support Group and later in the IBM Desktop Services/Global Services. His areas of expertise include workstation and server operating systems on the PC platform including Windows 95, Windows NT and OS/2 Warp. He has written extensively on the IBM Networks Client for Windows 95 and provided many TCP/IP and NetBIOS over TCP/IP traces.

Michael Persell is an Advisory I/T Specialist in IBM North America. He has ten years of experience in the technical marketing and public speaking fields. He has worked for IBM for more than two years, both as a Marketing Specialist and later as a Techline Sales Specialist. His areas of expertise include PC hardware configuration and deployment, the OS/2 family of products and PC based Lotus Notes. He has written on OS/2 Warp and DOS memory management.

Carl-Magnus Wiberg is a Software Specialist in IBM Sweden. He has six years of experience supporting the OS/2 base operating system, LAN Server 1.3 - 4.0 and OS/2 Warp Server. Being a certified World-Wide Professional

Server Expert, he provides local second-level support on both PC LAN software and PC Server Hardware. His areas of expertise include setting up Microsoft Office 4.x for use in an all-OS/2 LAN environment, CID, TME10 NetFinity, and Windows NT. He also has considerable experience in the areas of administration and translating IBM product code and documentation to Swedish. He has written extensively on the Windows NT and GUI sections.

Very special thanks to **Steve Tipton**, IBM Austin, Level 2.5 Team Lead for DOS and Windows-based Clients (DLS,95,NT) for all the hints and tips he contributed, allowing us to provide more detailed information in the DOS LAN Services, Networks Client for Windows 95, Networks Client for Windows NT, and Neighborhood Browser Enabler for OS/2 Warp Server chapters.

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

Mel Bryant, IBM Austin, OS/2 Warp Server Customer Focal Point
Peter Greulich, IBM Austin, Operations Systems
Bob Hanner, IBM Austin, Level 3 Technical Support
Franz-Stefan Hinner, IBM Stuttgart, Germany, Software Support
Gary Hunt, IBM Austin, Network Computing Team Lead
Steven King, IBM Austin, Product Manager OS/2 Warp Server
Doug Parnell, IBM Austin, Pre-Release Customer Program Development
Stan Smith, IBM Austin, PSP Development IBM Networks Clients
Randy Winkler, IBM Austin, PSP Pricing

International Technical Support Organization, Austin Center:

Marcus Brewer, Senior Editor
Oscar Cepeda, Staff Software Engineer
John Weiss, Associate Editor

Contributors at other IBM sites and at other companies:

Brice Bartek, Network TeleSystems, Sunnyvale, California
Steven Perricone, Network TeleSystems, Sunnyvale, California
Bill Thursby, Thursby Software Systems Inc., Arlington, Texas
Cyndi Yuchas, Thursby Software Systems Inc., Arlington, Texas

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!

Part 1. Common Information

Chapter 1. OS/2 Warp Server Terms and Conditions

The purpose of this chapter is to introduce OS/2 Warp Server and to clarify the OS/2 Warp Server terms and conditions pertaining to charges.

Figure 3. Terms and Conditions of OS/2 Warp Server

1.1 Overview

Whether you run a large enterprise or a small business, OS/2 Warp Server offers you a strategic network platform, for today and for the future. With OS/2 Warp Server, you gain a complete, fully-functional application server, a highly reliable network operating system, a systems management server, backup and recovery services and more. All in a single, cost-effective solution that's easy to install and manage.

OS/2 Warp Server supports clients running a variety of desktop operating systems, including OS/2 Warp, DOS (with OS/2 Warp Server's DOS LAN Services), Windows 3.x (with OS/2 Warp Server's DOS LAN Services), Windows 95 (with IBM Networks Client for Windows 95), Windows NT (with IBM Networks Client for Windows NT — Coordianted and Primary Logon Client), AIX (with NFS) and Apple Macintosh (with OS/2 LAN Server for Macintosh installed on OS/2 Warp Server). Plus, OS/2 Warp Server delivers the protocol independence you have asked for, concurrently supporting NetBIOS, IPX, TCP/IP, TCPBEUI, and 802.2.

As far as pricing is concerned, OS/2 Warp Server employs a Use-Based Pricing model. This means that the total price paid for OS/2 Warp Server

varies with the number of people who use the product. Use-based pricing is the industry standard for pricing server software.

1.2 Charges

When you buy OS/2 Warp Server, there are two separate charges:

1. A flat charge for the server license.

2. A charge for each authorized user of the server.

The total cost of a OS/2 Warp Server, then, is the cost of the server license added to the separate fees for each authorized user of the server. This user fee is a Use-Based Feature, or UBF.

1.3 Definition of a User

A user is defined as a person who is authorized to use the server. Authorization is determined by the number of users (not user IDs), so customers must pay a user fee for each person that is accessing OS/2 Warp Server.

It is important to note that the charge is for people, not PCs, and not PC operating systems. Therefore, a person who accesses the server from an IBM PC running OS/2 Warp 4 must buy a UBF. Similarly, a person accessing Warp Server from a non-IBM PC running Windows 95 must also buy a UBF.

1.3.1 When Do no Additional Charges Apply

No additional charges apply, when:

- A person has more than one user ID.

- A person accesses multiple OS/2 Warp Server services such as:

  - File and print services

  - Systems management services

  - Remote access services

- Local server IDs.

- Local user IDs.

- Guest IDs.

1.4 Rules

Purchase of a UBF allows access to all OS/2 LAN Servers and OS/2 Warp Servers in a customer's enterprise. Since we charge per person, there is no additional charge for access from your home or mobile PC once a UBF has been purchased. Each server includes one license for a UBF.

1.5 Upgrades

Customers may purchase OS/2 Warp Server at a reduced price when upgrading from previous versions of OS/2 LAN Server or competitive servers.

The requirement to purchase UBFs for OS/2 Warp Server does not change for upgrades. A UBF is still required for each user. Reduced prices are available for customers who previously purchased an OS/2 LAN Requester or competitive requesters.

It is a violation of the OS/2 Warp Server license agreement to access the server without purchasing a UBF. Many operating systems already contain the software code necessary to use the server. This does not override the requirement to purchase a UBF for each person authorized to use the server. IBM recently announced the IBM Networks Client for Windows 95, available as a Web download. Although there is no charge to download the code, authorized users using Windows 95 must purchase an OS/2 Warp Server UBF.

1.6 Exceptions

In two limited circumstances, it is not necessary to purchase a UBF:

1. A UBF is not required if access to Warp Server is solely to administer or configure the server.

2. A UBF is not required when Warp Server is being used solely as an application server for other applications, and the following Warp Server services are not used:

    • File system

    • Print functions

    • Remote access

    • Systems management

Announcement: UBF with OS/2 Warp 4

Announced 08/26/97 and effective on 01/01/98, OS/2 Warp 4 will come with one UBF.

1.7 Transition for OS/2 Warp Connect Customers

Customers who purchased OS/2 Warp Connect Version 3 were not required to buy an OS/2 LAN Requester to connect to OS/2 LAN Servers. To accomodate these customers, we allow customers to subtract the number of OS/2 Warp Connect licenses in use from the total UBFs required to be purchased. When these Warp Connect Version 3 licenses are upgraded to other operating systems, like OS/2 Warp Version 4, UBFs will need to be purchased at that time.

1.8 Questions and Answers

Following is a table that provides answers to questions regarding UBF.

Table 1 (Page 1 of 2). Questions and Answers to OS/2 Warp Server Terms and Conditions	
Question	**Answer**
I plan to upgrade all my OS/2 LAN Server 3.0 servers to OS/2 Warp Server. Many of our PCs run Windows 95, which contains code to enable connection to OS/2 Warp Server. Do I need to purchase a UBF for these workstations?	A UBF must be purchased for each person authorized to use the server. This requirement is totally independent of the PC Operating system used on that person's workstation. Each person who accesses an OS/2 Warp Server must purchase a UBF independent of amount of user IDs this person has.
I run Warp V4 on my workstation at work, but Windows 95 on my home PC. I access OS/2 Warp server from both PCs. How many UBFs do I need to purchase?	Only one. Each person who is authorized to use OS/2 Warp Server must purchase one UBF. This UBF allows access to all OS/2 Warp Servers in the enterprise, whether from work, at home, or on the road. The requirement to purchase a UBF is based on people, not PCs or PC operating systems.

Table 1 (Page 2 of 2). Questions and Answers to OS/2 Warp Server Terms and Conditions

Question	Answer
I currently have OS/2 LAN Server 4.0 Advanced servers, and all workstations run OS/2 Warp with OS/2 LAN Requester 4.0. Since the requester shipped with OS/2 Warp Server is the same requester that I already purchased, do I need to purchase OS/2 Warp Server UBFs?	Yes. Each Person authorized to access OS/2 Warp Server must purchase a UBF. Customers who purchased OS/2 LAN Requester 4.0 may purchase a UBF at a substantial discount. The requirement to purchase an OS/2 Warp Server UBF is unrelated to the software running on a user's PC. **Note:** OS/2 Warp Server 4.0 comes with LAN Requester 5.0.
One of the reasons I bought OS/2 Warp Connect was the free connection to OS/2 Lan Server 4.0. When I upgrade my OS/2 Lan Server 4.0s to OS/2 Warp Servers, do I have to buy UBFs for all my PCs?	Yes. Each person authorized to use OS/2 Warp Server must purchase a UBF. The requirement to purchase UBFs is based on people, not the software running on a person's PC. To help you transition to Warp Server, we allow you to subtract the total OS/2 Warp Connect V3 licenses in use from the total required UBFs. When OS/2 Warp Connect is upgraded, UBFs must be purchased to equal the total number of authorized users.
Why did you change your pricing model with OS/2 Warp Server?	Our pricing model for OS/2 Warp Server is consistent with current industry pricing models for server software. This model more closely aligns the value customers receive from the server software with the amount they pay for that software.
I am currently running Lotus Notes on an OS/2 Version 2.11 SMP. I would like to upgrade to OS/2 Warp Server Advanced SMP. Do I have to buy OS/2 Warp Server UBFs?	When Warp Server is being used solely as an application server, that is, you are not using the file & print, remote access, or systems management capabilities, then OS/2 Warp Server UBFs are not required. (Customers are allowed to upgrade from OS/2 Version 2.11 SMP to OS/2 Warp Server Advanced at a reduced upgrade price.)

Chapter 2. Introducing IBM Networks Clients

This chapter introduces file and print clients availale from IBM for OS/2 Warp Server, such as:

- OS/2 Warp 4

- DOS stand-alone or with

    - Windows 3.1

    - Windows 3.11

    - Windows for Workgroups (WfW)

- Windows 95

- Windows NT

Implemented in a plain NetBEUI and TCP/IP environment. If appropriate, dynamic TCP/IP, such as

- Dynamic Host Configuration Protocol (DHCP)

- Dynamic Domain Name Server (DDNS)

- NetBIOS Names Server (NBNS) / NTS Shadow / Windows Internet Name Server (WINS)

Is discussed as well. Remote Access Services using Point-to-Point (PPP) protocol dialing into an OS/2 Warp Server Remote Connection Server is also discussed.

2.1 Executive Overview IBM Networks Clients

IBM is introducing three products that significantly enhance the capabilities of Windows 95 clients and Windows NT workstations connecting to OS/2 Warp Servers:

1. IBM Networks Client for Windows 95

2. IBM Networks Client Coordinated Logon Client for Windows NT

3. IBM Networks Client Primary Logon Client for Windows NT

The IBM Networks Client for Windows 95 product as well as both IBM Networks Client for Windows NT improves the integration of network facilities in Windows 95 / Windows NT Workstation clients with OS/2 Warp Server. These new products allow companies using Windows 95 clients and Windows NT Workstation clients to effectively utilize OS/2 Warp and LAN Servers.

2.1.1 IBM Networks Client for Windows 95

This product features the following Windows 95 client enhancements when accessing OS/2 Warp Servers and LAN Servers:

- Single logon.

- Single user definition for authentication.

- Support of Windows client features for user profiles and system policies.

- Seamless client and server integration.

- Enabling OS/2 Warp Servers and LAN Servers to equal Microsoft Windows NT Servers for significant core functions — the functions most frequently cited by Microsoft as Windows client advantages.

Support for the OS/2 Warp Server functions (home directories, logon assignments, network applications, logon scripts) are now more readily available to Windows 95 clients. Both end users and system administrators benefit from this product.

The product removes limitations that existed in the previously released DOS LAN Services for Windows 95, delivered by IBM when Windows 95 was released.

2.1.2 IBM Networks Client for Windows NT (Coordinated and Primary)

These two products feature the following Windows NT client enhancements when accessing OS/2 Warp Servers and LAN Servers:

- Single logon.

- Single user definition for authentication and network connections in heterogeneous environments.

- Support of Windows client features for user profiles and system policies.

- Seamless client and server integration.

Support for the OS/2 Warp Server functions (home directories, logon assignments, network applications, and logon scripts) are now available to Windows NT Workstation clients. End users and system administrators benefit from these products.

Despite the Network Provider limitations that Microsoft has imposed with the Windows NT architecture, the IBM Networks Coordinated Logon Client for Windows NT product enables OS/2 Warp Servers and LAN Servers to equal Microsoft Windows NT Servers for significant core functions — the functions most frequently cited by Microsoft as Windows client advantages.

The IBM Networks Primary Logon Client for Windows NT product goes a step further and makes OS/2 Warp Servers and LAN Servers equal Microsoft Windows NT Servers on **all** functions.

2.2 What Worked before IBM Networks Clients

Before OS/2 Warp's updated client support, base Microsoft Windows 95/NT clients accessed a set of OS/2 Warp and LAN Server capabilities through common support of a significant subset of Server Message Block commands. See 4.3, "Server Message Block (SMB)" on page 33 for more details about this protocol.

2.2.1 Windows 95

Base Microsoft Windows 95 clients access a set of OS/2 Warp and LAN Server capabilities through common support of a significant subset of SMB (Server Message Block) commands, or through the IBM DOS LAN Services for Windows 95, delivered concurrently with the launch of Microsoft Windows 95. SMB is an XOpen specification that both Microsoft and IBM comply with. Therefore it is logical that we have a significant level of interoperability.

The IBM DOS LAN Services for Windows 95 product was created by porting the IBM DOS LAN Services for Windows 3.1 product and adding some screen enhancements. In general, end user support was the same as for IBM's Windows 3.1 client product. A unique GUI (Graphical User Interface) enabled the user to logon/logoff the OS/2 Warp Server or LAN Server domain, access the user's home directory, utilize logon assignments, and run shared applications. In addition, customers could issue NET USE commands from a command line.

The domain that defines valid users controlls access to the OS/2 Warp Server. A user at a Windows 95 client has to be defined in the OS/2 Warp Server domain to access its functions just like any other user of any other client wanting access to network resources of OS/2 Warp Server. A user at a Windows 95 workstation is confronted with two logons:

 • Local logon to the workstation enabling them to participate in sharing files and printers within a workgroup

 • Logon to a domain for accessing server resources

However, changing the default settings in Windows 95's SYSTEM.INI file can ease the logon process (see Table 17 on page 297) so that a user logon can be validated by the domain controller rather than locally enabling the user to participate in server and workgroup networking.

IBM utilizes some Microsoft LAN Manager functions that exist in Windows 95 to deliver IBM DOS LAN Services for Windows 95. However, subsequent changes by Microsoft to Windows 95, such as password handling, resulted in customer problems that IBM needed to resolve. The product also uses its own unique installation and configuration process rather than stay consistent with the Windows 95 installation and configuration process.

Workgroup capabilities provide additional support. If customers create a Workgroup environment (Peer to Peer Support), Windows 95 clients and OS/2 Warp Servers can share resources with each other using share level security for the Windows 95 machine and OS/2 Warp Server.

2.2.2 Windows NT

Base Microsoft Windows NT clients access a set of OS/2 Warp and LAN Server capabilities through common support of a significant subset of SMB (Server Message Block) commands. Customers can issue `NET USE` commands from a command line. This command allows clients to attach and use OS/2 Warp Server files and printers.

The domain defining valid users controls access to the OS/2 Warp Server. A user has to be defined in the OS/2 Warp Server domain to access functions from the Windows NT client. This required either synchronization of the user databases or inclusion of the User ID and password as part of the requested access to files or printers. Synchronization is a manual activity between the systems that either the user or server administrators must do that simply had to be eliminated.

Workgroup capabilities provide additional support. If customers create a Workgroup environment (Peer to Peer Support), Windows NT clients and OS/2 Warp Servers can share resources with each other using share level security for the Windows NT machine and OS/2 Warp Server.

2.3 What Was Needed for Windows 95

The IBM DOS LAN Services for Windows 95 product along with basic functions such as `NET USE` access to specific files and print resources on OS/2 Warp Servers satisfied a set of customer needs. Even with this support, end users encountered functional shortcomings and cumbersome workarounds. Neither IBM nor Microsoft have released code to enable critical functions that existing OS/2 Warp and LAN Server customers need. The following lists key customer requirements for OS/2 Warp Server support of Windows 95 clients:

- Single logon
  - Single step access to OS/2 Warp Server and LAN Server resources

- User access to OS/2 Warp Server functions through a common GUI (introduced with OS/2 Warp Server's DOS LAN Services for Windows 95)

- Single user definition for authentication

  - OS/2 Warp Server as the primary location for user account information and authentication.

- Windows client feature support

  - Storage and retrieval of Windows "user profiles", including desktop, to enable "roaming users"

  - Maintenance of Windows "system policies" from OS/2 Warp Servers

- Seamless client and server integration

  - Delivery of home directories, logon assignments, network applications, and logon scripts from OS/2 Warp Server to Windows 95 clients.

  - Standard Windows 95 installation and configuration methods.

These limitations lead people to believe that the Windows NT Server had better file and print support of Windows 95 clients than OS/2 Warp Server. With the IBM Networks Client for Windows 95 product, IBM has removed these limitations and delivered significant added value.

2.4 What Was Needed for Windows NT

The available base level functionality came from the LAN Manager code that Microsoft chose to support on Windows NT. However, Microsoft made a significant set of changes to the authentication (logon) flows required for Windows NT clients to access servers. By using a proprietary set of protocols and interfaces that they did not make publicly available, the only servers currently able to authenticate NT clients were NT Servers. The result was that neither IBM nor Microsoft released code to enable the critical set of functions existing OS/2 Warp and LAN Server customers need.

Although basic functions such as `NET USE` access to specific files and print resources on OS/2 Warp Servers do work between NT Clients and OS/2 Warp Servers, some customers are seeking more. The following highlights key customer requirements for OS/2 Warp Server support of Windows NT clients:

- Single logon

  - Single step access to OS/2 Warp Server and LAN Server resources

  - User access to OS/2 Warp Server functions through a common GUI

- Single user definition for authentication

  - OS/2 Warp Server as the primary location for user account information and authentication

- Network connections in heterogeneous environments

  - Establishment of resource connections for OS/2 Warp Servers and other Network Providers.

- Windows client feature support

  - Storage and retrieval of Windows "user profiles", including desktop, to enable "roaming users".

  - Maintenance of Windows "system policies" from OS/2 Warp Servers.

- Seamless client and server integration

  - Delivery of home directories, logon assignments, network applications, and logon scripts from OS/2 Warp Server to Windows NT clients.

  - Standard Windows NT installation and configuration methods.

To access other industry servers, Microsoft allows clients to call "additional Network Providers" following the successful authentication of a user against an NT user account. This NT authentication can be against an account held at a local NT workstation or at a NT Server domain.

Up to now, neither Microsoft nor IBM had provided a Network Provider that worked against a common SMB domain (which is used by Microsoft LAN Manager, OS/2 Warp Server, LAN Server, and many other servers in the industry). Therefore, servers other than Windows NT could not use account information located on SMB domains during the logon process to deliver functions.

These limitations lead people to believe that the Windows NT Server had better file and print support of Windows NT clients than OS/2 Warp Server. With the two IBM Networks Clients for Windows NT products, IBM has removed these limitations and delivered significant added value.

2.5 Introducing OS/2 Warp 4 as the Premier Client

OS/2 Warp 4 is the easiest way to a connected world. It incorporates features like Sun Microsystems' Java technology and IBM VoiceType speech recognition software, and promises to help transition customers into the era of network computing.

At its core is the fast, manageable and robust OS/2 operating system, to which IBM has added additional systems management features and networking and Internet functionality.

Using OS/2 Warp 4, customers will be able to access data on systems of many sizes, from peer networks to popular PC servers — like OS/2 Warp Server, Novell Netware and Windows NT — to mainframe systems. OS/2 Warp 4 also incorporates remote access capabilities, Mobile File Synchronization and Advanced Power Management, allowing users to take their offices on the road.

OS/2 Warp 4 is also the ideal Internet client. With Netscape Navigator Internet client software for OS/2 Warp, combined with object oriented technology and built-in VoiceType speech recognition software, Internet and intranet users visit a Web site as easy as clicking on a desktop icon.

But users do not need to be on the Internet to experience the power of OS/2 Warp 4, which is the first PC operating system allowing users to run Java applets and applications, independent of a Web browser on their desktops. OS/2 Warp 4 comes with the runtime code necessary for running Java applications, a Java developer toolkit and Java applet samples.

It also comes with runtime support for OpenDoc and support for Live Objects, providing an open framework for platform-independent reuse of OpenDoc components. OpenDoc creates component software that can be shared and customized across heterogeneous environments. Its component-based integrated structure allows developers and end-users to build higher quality applications faster, with reduced costs. With the ability to run OpenDoc components, Java applications, OS/2, DOS and most Windows 3.x programs, OS/2 Warp 4 provides users with incredible application support.

OS/2 Warp 4 also boasts a cleaner and more logical user interface with visual enhancements like 3-D shadowed icons, 256 color exploitation, an attractive new system font and the new WarpCenter — an icon ribbon on the desktop that combines the best of the Lotus SmartCenter and the OS/2 Warp LaunchPad to help users customize their desktops, group their applications and check on the status of their systems.

OS/2 Warp 4 is available in U.S. English and 28 national language versions. Find detailed information about this premier client in 10.1, "OS/2 Warp File and Print Client" on page 107.

2.6 Introducing DOS/Windows

There are over 100 million PCs that run DOS with or without Windows. DOS Clients need connectivity, such as printer sharing, file and application sharing, messaging, and Internet connectivity. DOS is not going away. IBM is commited to support customers who have DOS.

When Microsoft began to to design and develop "Chicago", the mainstream computer was a 33-MHz 386 with 4 MB of RAM, 100 MB of hard disk and a 9600 baud modem. CD-ROMs and game-quality sound cards were plentiful but bot preeminent. This configuration supported Windows 3.1 well, but Windows NT did not install or run well, if at all, on the machine.

The graphical user interfaces of Windows 3.1, Windows 3.11, and Windows for Workgroups are still the most popular ones. Microsoft is still licensing Windows for Workgroups to large accounts. However, within the Windows 3.x family networking functionality is only imbedded in Windows for Workgroups. Internet functionality is not included, however, Web browsers for the Windows environment are available from Netscape's Web site (Netscape Browser) or Microsoft's Web site for Windows support (Internet Explorer).

In order to run any of these Windows graphical user interfaces you need to install the DOS operating system. Without DOS, Windows will not run. Networking capabilities are added to the Windows environment with IBM's DOS LAN Services which is bundled with OS/2 Warp Server. DOS LAN Services offers a nice graphical user interface for DOS and Windows. Users do not have to install Windows to connect DOS-based machines to OS/2 LAN/Warp Server. Find detailed information about DOS-based and Windows-based clients in 11.1, "DOS LAN Services Overview" on page 207.

2.7 Introducing Windows 95

To bypass the problem of having DOS installed before you can install the Windows graphical user interface, Microsoft worked on a product that would succeed the Windows family: Windows 95, originally code-named "Chicago". In August 1995, Microsoft finally released Windows 95 following an extended period of media hype, user anticipation, and an extensive one-year-and-a-half beta program that involved tens of thousands of beta testers. Advertised as a 32 bit operating system, Windows 95 comes with a complete new graphical user interface which has dramatically enhanced compared to its predecessor products. This new interface is also embedded in Windows NT 4.0. However, sometimes you need to have DOS installed when you want to install Windows 95. That is when you have a CD-ROM

device where there are no CD-ROM drivers for Windows 95. In this case, you install DOS, the CD-ROM's DOS device driver, and then Windows 95.

Windows 95 comes with complete networking support as well as Internet browser. However, to take full advantage in a OS/2 Warp Server environment, such as file and print services and dynamic TCP/IP, IBM offers additional products that can be downloaded from the following Web site:

`http://www.software.ibm.com/os/warp/downloads/`

The new IBM Networks Client for Windows 95 makes it possible to gain the same OS/2 Warp Server domain services from a Windows 95 workstation as from an OS/2 workstation. The Windows 95 client supports logon assigments, time synchronization from a time source server, disk limits, shared applications and more. The new clients product lifts the integration of Windows and OS/2 worlds into new heights.

In order to enable a Windows 95 workstation to take part in OS/2 Warp Server's dynamic TCP/IP, that enables workstations to obtain a free IP address from a DHCP server while impounding a user's unique host name, you need to get the appropraite software from IBM. At the time this redbook was written, it was not decided where this software can be downloaded. We recommend checking IBM's Software Choice home page from time to time. The Web site is:

`http://www.software.ibm.com/os/warp/swchoice/`

The client product uses the same standard Windows 95 logon screen used when logging to a Windows NT domain; users do not have to learn anything new if changing from NT servers to OS/2 servers. If Windows NT or OS/2 Warp 4 look unattractive as a workstation operating system, Windows 95 now offers the same functionality when it comes to network services from a OS/2 Warp Server domain as its technically more sofisticated counterparts. Find detailed information about Windows 95 clients in 12.3, "Installing IBM Networks Client for Windows 95" on page 250.

2.8 Introducing Windows NT

Another 32 bit operating system by Microsoft is Windows NT 4.0. It comes in two versions:

 • Windows NT 4.0 Server

 • Windows NT 4.0 Workstation

It shares the same desktop as Windows 95 has but has a robust 32 bit environment. Just like Windows 95, Windows NT comes with networking support and an Internet browser. Windows NT was originally positioned for

large-scale corporate power users, while Windows 95 was positioned for the home user. Windows NT has been gaining a lot of popularity. However, Windows NT's proprietary logon flows focused customers to use Windows NT Server, because other servers such as OS/2 LAN/Warp Server and even Microsoft's own LAN Manager could not deal with these kind of logon flows.

The new OS/2 Warp Server network clients for Windows NT will provide the Windows NT user with the same set of functions and services that were previously exclusive to OS/2 and (to a large extent) DOS/Windows users. These network clients are the long-awaited IBM answer to the market requirements. With the strength and functionality of OS/2 Warp Server, corporate LAN support departments can incorporate Windows NT workstations in an OS/2 Warp Server LAN and really get the best out of both worlds.

There are two OS/2 Warp Server network clients for Windows NT 4.0:

- IBM Networks Coordinated Logon Client

  The IBM Networks Coordinated Logon Client for Windows NT is a Network Provider for Windows NT machines. Network providers require initial authentication against an NT user account before authenticating a user account in the OS/2 Warp Server domain. The coordinated logon requires synchronization of user account information between an NT client and the OS/2 Warp Server.

- IBM Networks Primary Logon Client

  The IBM Networks Primary Logon Client for Windows NT completely eliminates the requirement for initial authentication against a predefined Windows NT user account. Since a user is defined only in one location due to elimination of the NT user account, no synchronization is required. Following authentication, this product supports Windows client features and seamless client and server integration just as the Coordinated Logon Client.

The products can be downloaded from the following Web site:

`http://www.software.ibm.com/os/warp/downloads/`

The IBM Networks Primary Logon Client is the ideal network client in LAN environments consisting of OS/2 Warp Server domains only. The IBM Networks Coordinated Logon Client is optimized for use in mixed LAN environments, consisting of both OS/2 Warp Server and Windows NT domains. The main difference is how the respective client handles the logon process. The GUI is common to both network clients. Find detailed information about Windows NT clients in 13.1, "Client Overview" on page 321.

2.9 Introducing Apple Macintosh

Macintosh clients are supported when OS/2 Warp Server is enhanced with OS/2 LAN Server for Macintosh 1.01. This product provides AppleTalk file server function and print server function as well as AppleTalk Print Monitor to Macintosh clients.

Macintosh clients can access the directories and files on the OS/2 Warp Server and can send print jobs to a PostScript printer connected to an OS/2 Warp Server. On the other hand, OS/2 Warp 4 (and OS/2 Warp Connect) workstations can send PostScript print requests to an Apple LaserWriter on the AppleTalk network.

Alternatively, if you do not want to run the AppleTalk protocol on the server and simply want to have a NetBIOS interface to TCP/IP networking, you may want to use the DAVE client from Thursby Software Systems, Inc. whichs runs on any Macintosh with a 68020 or higher processor, MacOS 7.5.x or better with a minimum of 8 MB of RAM, Apple's MacTCP or Open Transport TCP/IP and any hardware required to run TCP/IP. Installing DAVE on a Macintosh will integrate the workstation into an OS/2 Warp Server environment. In comparison to OS/2 LAN Server for Macintosh, the client running DAVE is in charge of managing data forks and resource forks on the server. That requires DAVE to be installed on each client that wants to participate in an OS/2 Warp Server environment.

To get a trial copy of DAVE, point your Web browser to the following Web site:

```
http://www.thursby.com
```

Detailed information about integrating Apple Macintoshes into an OS/2 Warp Server environment is provided in 14.1, "File and Print Services with OS/2 LAN Server for Macintosh" on page 359 and 14.2, "File and Print Services for the Macintosh Using NetBIOS over TCP/IP" on page 365.

Chapter 3. Concepts

This chapter describes the aspects of workgroups, servers, and domains from a historical point of view as well as an implementation point of view. Pros and Cons are listed for all three concepts.

3.1 Historical View of Personal Computing and PC Networking

With the introduction of the fist personal computer in 1981 featuring a 180 KB diskette drive and CP/M, the predecessor of DOS, no one thought about integrating these intelligent machines into a network.

The personal computer and the home computers, or Apples, were introduced to give the user the ability to work on their own. This was supposed to make users independent from each other. The flexibility to run whatever program the user needed directly on their own machine gave the Personal Computer a big push.

Hardware with Intel's 80286/80386 processors and software that made that made use of the new 80286/80386 functions and features gave the Personal Computer business its next push. Users liked the comfort and flexibility of the /36 and /370 world. However, new operating systems had to be developed to make use of these new processors.

Flexibility was the greatest advantage of the personal computer. At this point, however, users could not exchange data like they could in their /36 or /370 environments. The only possibility was to exchange data by using diskettes.

Therefore PC-networking was introduced. At its onset no one talked about cabling systems or hub switches. The start was the connection between single PCs over parallel or serial port to exchange data. Most of the requirements like sharing drives, data stock and printers couldn't be met with these connections.

The next step was the introduction of mini networks, like Kirschbaum link, that enabled users to share drives with each other. This was the first step towards Peer-to-Peer Networking.

In the beginning of the 1980's the first networking concepts were introduced. The first step into the networking direction was made by ArcNet, which connected PCs over telephone lines. This was revolutionary at that time. In the middle of the 80s different bus-based technologies were introduced. One of those was the PC-Baseband Network from IBM. It only used different

21

frequencies in the wire to communicate. The Ethernet architecture has become more popular and has been around in different variantions. In 1987 IBM introduced the IBM Token-Ring topology based on a ring concept where workstations are connected to each other. Because of the Point-to-Point connections among all stations, this technology works differently than Ethernet. The greatest advantage of this technologie is that Token-Ring is not based on collision detaction as used in Ethernet networks.

3.2 Local Area Network Concepts

The biggest requirement for PC-based networks is to share resources, data and programs for common use. To meet this requirement there are different kinds of networks that can be distinguished by the following keywords:

- Workgroup and peer networks

- Server and domain networks

Because each networking concepts has it strengths and weaknesses, most enterprise networks use a combination of both concepts.

In the following sections we describe and explain which strenghts and weaknesses the different concepts have. It is needed as a basis to understand the concepts from the administrator perspectives and end user perspective.

Workgroup/Domain

Don't be confused when some software vendors use the names domain and workgroup interchangably. Usually they use either name to express a collection of computers connected to each other exchanging data.

Generally the difference between a domain/server and workgroup network is their behaviour. Domains and workgroups are both logical groups of workstations connected in a local area network (LAN). Workgroups are sometimes called peer network or peer domains.

A LAN can contain more than one domain, each operating independently from each other. Domain names must be unique across a LAN. As with OS/2 peer domains, mulitple OS/2 LAN Server domains can be defined on the network to simplify server managment. PCs defined in a workgroup can interact with PCs in a domain.

3.2.1 The Workgroup/Peer Network

A workgroup/peer network consists of a group of PCs that share resources using some form of peer LAN software, such as IBM Peer for OS/2 (part of OS/2 Warp Connect and OS/2 Warp 4), Windows for Workgroups, Windows 95 or Windows NT Workstation.

The group is not static and every machine is like a member of a community. All member's shares are controlled by their users. There is no regulation or master control over resources that are shared or not.

This also means that the users have to control the access rights to resources that are being shared from their workstation. Having your network designed as a workgroup/peer network allows all users to make use of hardware (CD-ROM drives, printers, etc.) and access data that is located on another user's PC.

Working together in a workgroup/peer network brings flexibility to all users. But it also brings a big responsibility as far as security is concerned. To make common use of all resources shared to the community all peer servers have to be up and running. As a conclusion you find the following advantages and disadvantages for workgroup/peer networking:

Advantages:

- Very flexible.

- Direct Data exchange with everyone.

- Fast and simple to implement.

- All resources in the community can be used by everyone.

Disadvantages:

- Complicated procedures of resource sharing and access rights definitions.

- Everyone needs a common knowledge in networking.

- Insufficient security for unallowed access.

- Irritation of clients that access resources on the sharing PC.

- Unreliable because PCs that are powered off limit the overall availability.

3.2.2 The Server/Domain Network

Looking at a server/domain network you will see that all resources shared over the network such as printers, directories, modems, data and programs, are controlled by a server. These servers are, depending on the network

design and network operating system (NOS) philosophy, dedicated servers. Server networks offer a lot more control over the resources shared and used.

Controlling the access to critical resources and data made cetral user access control necessary for Local Area Networks (LAN).

Therefore, typical server/domain networks have a user database which describes the user and their rights in the network. Resources are defined and controlled at domain controllers rather than workstations. The administration is centralized and provides remote administration from a remote workstation even via WAN (Wide Area Network) through Remote Access Services.

Advantages:

- High security against unauthorized access
- Offers good network structure
- Management of access control
- Data security centralized
- Data backup centralized
- Protocol and auditing

Disadvantages:

- Expenditure for planning, conception and documentation
- More expensive then a peer solution
- Skilled team of administrators necessary
- Dependence on the administrator

A server/domain network does not have the peer network's flexibility, and there are differences between server and domain networks. We clarify this in the following sections.

3.2.2.1 The Server Network

A server network is typically made-up of one or more single servers. These servers are visible as single servers to the user. Network resources are defined as share names or aliases in the network. In addition, share names or aliases can be accessed using Universal Naming Convention (UNC). For example, to execute an application from the server, you do not need to specify a drive letter. Instead of executing `P: LOTUSOS2 WORDPRO WORDPRO.EXE`, the user can type `[Server Name] LOTUSOS2 WORDPRO WORDPRO.EXE` to execute

Lotus Word Pro, assuming `LOTUSOS2` is a defined share name or alias at the server.

Each server in a server network appears as a single machine to the administrator so that each server must be administrated separately. This design is implemented in Netware 3.x.

In a server network, resources can be accessed across different servers if the client accessing them has the needed rights granted. These restrictions were acceptable with small networks. However, in a big network with 20 servers it is very difficult for administrators to administer every single server. To bypass this problem, the domain concept was introduced.

3.2.2.2 The Domain Network

A domain is a logical summary of servers to one group, which can be administered like one single machine. This is the Single-Server-Image concept.

With the Single-Sever-Image, users access their resources over the domain controller or backup domain controller and not over separate single servers or peer workstations. The resources are defined and controlled by an administrator within the domain. The users at workstations access resources located on servers of a domain. When a user connects to a network resource, they use that resource the same way they use resources on their workstation. Access to resources is controlled by a domain controller or backup domain controller.

One server in the domain is responsible for managing the primary copy of the user/group database, logon assignments, and application definitions. This primary server is called the domain controller. The domain controller or at least the backup domain controller must be up and running before users can log on to the domain and use its resources. Having backup domain controllers ensures not having a single point of failure in case the domain controller is not accessible. However, backup domain controllers do not allow alterations to databases due to read-only access to the domain controller database and user account database.

A physical network can consist of multiple domains. Workstations become part of the domain by logging on to the domain controller. After logon users can access the resources that are set up for them, assuming the resource's access cntrol rights have been properly granted.

There are several ways a user can have access to multiple domains. In an OS/2 LAN/Warp Server network, it is possible to access different domains by adding the same User ID on all domains. It is of advantage to apply the

same password to the User ID defined on each domain but this is not mandatory. Having identical User IDs defined on all domains enables users to access resources in all domains.

Microsofts Windows NT introduced a new concept called Trusted Domains allowing the use of resources of another domain by trust relationships. Find more detailed information about trusted domains and cross domain resources in the IBM Redbook SG24-4786, titled *OS/2 Warp Server, Windows NT, And NetWare: A Network Operating System Study*.

Chapter 4. The Truth about NetBEUI, NetBIOS, SMP, and NetBIOS over TCP/IP

In the following sections, information is provided about the two major protocols for file and print: NetBIOS and NetBIOS over TCP/IP. Both protocols are used with a so-called Server Message Block (SMB) server, such as OS/2 Warp Server. Another typical SMB server is Microsoft's Windows NT Server.

4.1 The NetBIOS Application Programming Interface

Originally developed by IBM as an Application Program Interface (API) for IBM PC programs to access LAN facilities, NetBIOS has become the basis of many other networking applications.

Strictly speaking, NetBIOS is an interface specification for access to network services, such as name-to-address resolution and sending and receiving data.

NetBIOS (Network Basic Input/Output System) is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. Originally designed as the network controller for IBM's PC Network LAN, NetBIOS has been extended to allow programs written using the NetBIOS interface to operate on the IBM Token Ring. NetBIOS has been adopted as an industry standard and it is common to refer to NetBIOS-compatible LANs.

NetBIOS offers LAN applications and a variety of "hooks" to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network.

The purpose of the NetBIOS is to isolate the application program from the actual type of hardware used in the LAN. It also spares the application programmer the details of network error recovery and low level message addressing or routing.

NetBIOS standardizes the interface between application programs and a LAN's operating capabilities. Applications can be written to access only the highest levels of the OSI model, making them transportable to other network environments. Any program can use the network while making the usual calls to DOS, but NetBIOS calls enable the user to instantly transmit information to an application on another network machine.

In a NetBIOS implementation of a LAN, the computers on the system are known by names. Each computer has a permanent name that is programmed onto the LAN card. Computers on the system can also be known by names designated by the programmer. The commands available in NetBIOS include commands to add and delete names.

Computers on a NetBIOS implementation of a LAN can communicate either by establishing a session or by using datagram or broadcast methods. Sessions allow a larger message to be sent and handle error detection and recovery, but they only allow computers to communicate on a one-to-one basis. Datagram and broadcast methods allow one computer to communicate with several other computers at the same time, but are limited in message size. Datagram and broadcast methods of communication do not handle error detection and recovery. NetBIOS session control commands and session data transfer commands allow communication through sessions. NetBIOS datagram commands allow communication without the use of sessions.

All commands are presented to the NetBIOS in a format called Network Control Blocks (NCB). These blocks are allocated in memory by the user program. The user program is also responsible for setting the neccessary input fields of the NCB and setting unused fields to zero. Several fields in the NCB are reserved for output from NetBIOS upon completion of a command.

NetBIOS is one of the commonly used protocols for the LAN environment today. It is supported on the Ethernet, token ring, and IBM PC Network environment. IBM introduced NetBIOS originally for use on the PC Network, an early LAN. It was actually defined as only an interface between the application programs and the network adapter LANs. However, some transport-like functions have been added. It is one of the de facto standards in the LAN environment, although several variations of NetBIOS are used.

NetBIOS was designed for a group of personal computers, all sharing a common broadcast medium. It provides both a connection-oriented (virtual circuit) and a connectionless (datagram) service. It supports both broadcast and multicast. Three types of services are provided by NetBIOS:

- **Name Service**

  Names are used to identify resources in NetBIOS. For example, for two processes to participate in a conversation, each must have a name. The names are dynamically assigned and checked. The client process identifies the specific server by the server's name, and the server can determine the name of the client. There are two types of names:

- Unique names

   A unique name must be unique across the network.

- Group names

   A group name does not have to be unique and all processes that
   have a given group name belong to the group.

Each NetBIOS node maintains a table of all names currently owned by
that node. These names continue to be owned by the NetBIOS node
until the names are specifically deleted or until the node is powered off
or reset.

- **Session Service**

   The NetBIOS session service provides a connection-oriented, reliable,
   full-duplex message service. NetBIOS does not provide any form of
   out-of-band data. NetBIOS requires one process to be the client and the
   other to be the server. NetBIOS session establishment requires a
   preordained cooperation between the two stations. One application
   must have issued a `LISTEN` command when another application issues a
   `CALL` command. The `LISTEN` command references a name in its NetBIOS
   name table, and also the remote name an application must use to
   qualify as a session partner. If the receiver (listener) is not already
   listening, the `CALL` will be unsuccessful. If the `CALL` is successful, each
   application receives notification of session establishment with the
   session-id. The `SEND` and `RECEIVE` commands then transfer data. At the
   end of a session, either application can issue a `HANG-UP` command.
   There is no real flow control for the session service because it is
   assumed a LAN is fast enough to carry the required traffic.

- **Datagram Service**

   Datagram Service Datagrams can be sent to a specific name, sent to all
   members of a group, or broadcast to the entire LAN. As with other
   datagram services, such as UPD/IP, the NetBIOS datagrams are
   connectionless and their delivery is not guaranteed yet fails reliable.
   The `SEND_DATAGRAM` command requires the caller to specify the name of
   the destination. If the destination is a group name, then every member
   of the group receives the datagram. The caller of the `RECEIVE_DATAGRAM`
   command must specify the local name for which it wants to receive
   datagrams. The `RECEIVE_DATAGRAM` command also returns the name of
   the sender, in addition to the actual datagram data. If NetBIOS receives
   a datagram, but there are no `RECEIVE_DATAGRAM` commands pending, then
   the datagram is discarded.

   The `SEND_BROADCAST_DATAGRAM` command sends the message to every
   NetBIOS system on the local network. When a broadcast datagram is

received by a NetBIOS node, every process that has issued a
RECEIVE_BROADCAST_DATAGRAM command receives the datagram. If none of
these commands are outstanding when the broadcast datagram is
received, the datagram is discarded.

NetBIOS is also a commonly-used network protocol for PC local area
networks. NetBIOS provides session and transport services (layers 4 and 5
of the OSI model). NetBIOS did not provide a standard frame format for
transmission over the network, causing different implementations of
NetBIOS to be created. For example, Artisoft's LANtastic uses a proprietary
version of NetBIOS for transmission between client and server. The frame
format was later formalized in NetBEUI. There are two NetBIOS modes.
The Datagram mode is the fastest mode, but does not guarantee delivery. It
uses a self-contained packet with send and receive name, usually limited to
512 bytes. If the recipient device is not listening for messages, the
datagram is lost. The session mode establishes a connection until broken.
It guarantees delivery of messages up to 64 KB long.

All nodes on the network can communicate with each other or with the
server on an equal basis (peer-to-peer communication).

NetBIOS' standardized set of function calls establishes and uses "sessions"
(logical connections between the server and a node), sends "datagrams"
(raw data transmitted in a general broadcast), and maintains a dynamic,
centralized list of names for devices attached to the network. These names
are hardware-independent.

This enables users to log into the network from any workstation, because
their names are not tied to a specific hardware address.

NetBIOS enables an application to establish a session with another device
and lets the network redirector and transaction protocols pass a request to
and from another machine. NetBIOS does not actually manipulate the data.
The NetBIOS specification defines an interface to the network protocol used
to reach those services, not the protocol itself. Historically, the NetBIOS
interface has been paired with a network protocol called NetBEUI (NetBIOS
Extended User Interface). The association of the interface and the protocol
has sometimes caused confusion, but the two are different.

Network protocols always provide at least one method for locating and
connecting to a particular service on a network. This is usually
accomplished by converting a node or service name to a network address
(name resolution). NetBIOS service names must be resolved to an IP
address before connections can be established with TCP/IP.

Most NetBIOS implementations for TCP/IP accomplish NetBIOS name-to-IP address resolution by using either:

- Broadcast

  A method where the PC node sends a broadcast to all network nodes seeking the IP address of the NetBIOS service name.

- RFCNAMES.LST(for OS/2 machines) or LMHOSTS (for Microsoft machines)

  A local PC file where each PC stores a file listing all network nodes (file server, authentication server, or peer PC) and their corresponding IP addresses.

Broadcasts are acceptable for small office-size LANS, but are not practical in larger networks with routers. Broadcasts have the potential of creating a "broadcast storm," where the capacity of the network is overwhelmed by the broadcast messages. Normal router configuration does not allow broadcast messages to travel beyond network segments. RFCNAMES.LST/LMHOSTS file NetBIOS name-to-IP address resolution also has drawbacks. Although services on different network segments can be reached using this method, it creates a new set of administrative problems. If a node's IP address changes, for instance, IS staff must update each individual PC's copy of the LMHOSTS file to reflect the change. In large, rapidly changing corporate networks this can be a problem.

Because both broadcast and RFCNAMES.LST/LMHOSTS files are not well-suited for large networks, people began to look for new ways to accomplish NetBIOS name-to-IP address resolution that offered more centralized control. Two alternatives are to use a TCP/IP name resolution technique known as:

- Domain Name Server (DNS)

- NetBIOS Name Server (NBNS)

DNS is similar to RFCNAMES.LST/LMHOSTS name service because it relies on a list of service names and corresponding IP addresses. However, DNS has one important advantage over RFCNAMES.LST/LMHOSTS: Its HOSTS file can be maintained on a single, centrally administered DNS server anywhere on the network.   However, DNS was not originally developped to do NetBIOS name-to-IP address resolution. Therefore, a service like this is not easy to set up using DNS. A dedicated NetBIOS Name Server is a far superior solution. See 4.4, "NetBIOS over TCP/IP" on page 35 and 4.4.3.1, "Introducing NetBIOS Name Server" on page 44 for more detailed information about names resolution.

4.2 The NetBEUI Protocol

Pronounced "net-booey," it is used by network operating systems such as Microsoft LAN Manager, OS/2 LAN Server, OS/2 Warp Server, Windows for Workgroups, Windows 95, and Windows NT. NetBEUI is a standardization of the NetBIOS transport frame, with additional functions and interoperability added by IBM. NetBEUI implements the OSI LLC2 protocol.

NetBEUI is the original PC networking protocol and interface designed by IBM for their OS/2 LAN Server/OS/2 Warp Server. This protocol was later adopted by Microsoft for their networking products. Many of the performance enhancements came from Microsoft. NetBEUI stands for NetBIOS Enhanced User Interface and specifies the way that higher level software sends and receives messages over the NetBIOS Frames Protocol. This protocol runs over the standard 802.2 data-link protocol layer and is specified in the IBM document titled *IBM Local Area Network Technical Reference Manual*.

NetBEUI is not routable because the 802.2 data-link protocol is not routable. Since this is a major limitation for a growing company, routable protocols such as TCP/IP are gaining more and more popularity. OS/2 Warp Server and Microsoft Windows NT implement the NetBIOS over TCP/IP protocol to bypass this limitation.

In the early 1990s Novell recognized that the WfW and LAN Manger/LAN Server networks needed to co-exist with NetWare and developed NetBIOS over IPX. This allowed NetBIOS-based software to run over routed networks and was a big improvement. NetBIOS over IPX was quickly adopted by IBM and Microsoft and put it into OS/2 LAN/Warp Server, WfW, Windows 95 and Windows NT.

When NetBEUI was developed in 1985, it was assumed that LANs would be segmented into workgroups of 20 to 200 computers and gateways would be used to connect that LAN segment to other LAN segments or a mainframe.

NetBEUI is optimized for very high performance when used in departmental LANs or LAN segments. For traffic within a LAN segment, NetBEUI is the fastest protocol shipped with OS/2 Warp Server and Windows NT.

NetBEUI addressing does not allow packet forwarding on routed networks, but the NetBIOS interface is adaptable to protocols that allow packet forwarding, such as IPX and TCP/IP. The specification for implementing the NetBIOS interface to TCP/IP is defined by RFC 1001 and 1002.

NetBEUI is very fast for LAN communications but does not have routability for WAN communications. One recommended method for setting up a network is to use both NetBEUI and another protocol, such as TCP/IP, on each computer that may need to access computers across a router or on a WAN. When you install both protocols on each computer OS/2 Warp Server and its clients and Windows NT use NetBEUI for the communication within each LAN segment and TCP/IP for communication across routers and to other parts of your WAN. Name-resolution algorithms handle communication within a network automatically even if TCP/IP is the first protocol on the LAN adapter.

The following are some of the most common network operating systems that use the NetBIOS interface:

Digital	Pathworks
Hewlett-Packard	HP LAN Manager and Resource Sharing
IBM	OS/2 LAN Server, OS/2 Warp Server, OS/2 Warp 3, OS/2 Warp Connect, OS/2 Warp 4, DOS LAN Services, and IBM Networks Client for Windows 95 and Windows NT in conjunction with Microsoft's networking software
Microsoft	LAN Manager, Windows for Workgroups, Windows 95, Windows NT

4.3 Server Message Block (SMB)

Server Message Block is the protocol that LAN Manger/LAN Server clients and servers use to communicate with each other. Client systems use this protocol to request file, print, and communications service from server systems over a network.

There are several different versions of this protocol. A particular version is referred to as a dialect. When two machines first come into network contact they negotiate the dialect to be used. For example, when an OS/2 Warp 4 client sends the NEGOTIATE SMB command, the domain controller or backup domain controller handling the logon will respond to the requester by selecting the SMB dialect which offers the highest security mode, such as LANMAN 2.1. In some cases the domain controller will respond with 0xFFFF if none of the client's listed protocol dialects was acceptable.

Once a protocol has been established the client can proceed to log on to the server, if required. They do this with a SESSSETUPx SMB command. The response indicates if they have supplied a valid user name password pair and if so, can provide additional information. One of the most important aspects of the response is the user ID of the logged on user. This user ID

must be submitted with all subsequent SMBs on that connection to the server. Once the client has logged on, the client can proceed to connect to a tree.

Different dialects can include new messages as well as changes to the fields and semantics of existing messages in other dialects.

The SMB protocol requires server authentication of users before file accesses are allowed, and each server authenticates its own users. A client system must send authentication information to the server before the server will allow access to its resources.

The SMB protocol defines two methods which can be selected by the server for security:

- Share level

  A share level server makes a directory on a disk device (or other resource) available. An optional password may be required to gain access. Therefore, any user on the network who knows the name of the server, the name of the resource and the password, has access to the resource. Share level security servers may use different passwords for the same shared resource with different passwords allowing different levels of access. For instance, Windows for Workgroups and Windows 95 peer servers implement the share level security model. OS/2 Warp Connect and OS/2 Warp 4 implement the share level and user level security model, leaving it up to the user what level of security they want to establish.

- User level

  A user level server makes a directory on a disk device (or other resource) available and requires the client to provide a user name and corresponding user password to gain access. OS/2 Warp Server and Windows NT servers implement the user level security model and do not support the share level model. User level servers are preferred over share level servers for any new server implementation, since corporations generally find user level servers easier to administer as employees come and go and also is a higher level of security.

When a user level server validates the account name and password presented by the client, an identifier representing that authenticated instance of the user is returned to the client in the user ID field of the response SMB.

4.4 NetBIOS over TCP/IP

Several components of OS/2 Warp Server can use NetBIOS for communications, but they can also use other protocols like TCP/IP or IPX. File and Print Services is the only OS/2 Warp Server and Windows 95/NT component that can only use NetBIOS as a programming interface.

The original NetBEUI protocol along with the NetBIOS API has some specific characteristics that limit its use in certain wide area network environments:

- NetBIOS uses a flat name space.

- NetBIOS relies on the broadcast technique to register and find a name.

- NetBIOS is not routable.

One solution to overcome these limitations is found in RFCs 1001 and 1002. They describe the standard way to implement the NetBIOS services on top of the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). RFC 1001/1002 is not an encapsulation technique; it builds special packets and sends them out by UDP/IP and TCP/IP. 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 4-byte session header that precedes the actual user data. Therefore, a NetBIOS chain send of 128 KB would have an overhead of only four bytes. Multi-Protocol and Transport Services provides a full TCP/IP protocol stack and a TCPBEUI API conversion layer, which is a ring 0 implementation of RFC 1001/1002.

Another solution of routing NetBIOS is to use the NetBIOS over the Internet Packet Exchange (IPX) protocol that is also supplied with Multi-Protocol and Transport Services.

The capability of running NetBIOS applications over routable protocols offers new flexibility when designing OS/2 Warp Server networks. In this way OS/2 Warp Server systems, Warp Connect Peer workstations, OS/2 Warp 4, LAN Servers, and LAN Requester workstations can be on remote LAN segments connected by IP routers. This also means that such systems can be introduced into existing TCP/IP networks without introducing an additional network protocol.

OS/2 TCPBEUI (TCP/IP NetBIOS extended user interface; IBM's implementation of NetBIOS over TCP/IP) is a high performance, ring 0 implementation of NetBIOS over TCP/IP. TCPBEUI provides the LM10 protocol driver interface. It is the same LM10 functionality that is also provided by NetBEUI.

NetBIOS over TCP/IP contains enhancements over the B-node standard that improve system performance by decreasing broadcast frames and by expanding communications over routers and bridges. These enhancements, as described in 4.4.2, "How to Enhance B-node Operations in OS/2 Warp 4" on page 37, are transparent to NetBIOS applications and do not interfere with other B-node implementations that lack similar functions.

TCPBEUI allows peer-to-peer communication over the TCP/IP network with other computers that have compatible services. RFCs 1001 and 1002 support applications using the NetBIOS API by using a TCP/IP network for transport. Essentially, NetBIOS is not a protocol but an application programming interface that knows very little about any underlying networking protocols. NetBIOS is used mostly in LAN environments and is implemented to use the IEEE 802.2 interface. That renders NetBIOS unusable for TCP/IP networks because it cannot be routed in that way.

RFC 1001/1002 implementations of NetBIOS over TCP/IP alleviate that problem and have become increasingly important with the presence of operating systems such as OS/2 Warp Server, Windows NT and Windows 95 which partly rely on NetBIOS for communications.

4.4.1.1 NetBIOS over TCP/IP Implementation in OS/2 Warp 4

IBM OS/2 NetBIOS over TCP/IP can be configured in a B-node, P-node or H-node implementation:

B-node   B-node defines the adapter as a Broadcast node. This is the implementation defined by default.

P-node   P-node specifies the adapter as a Point-to-point node.

H-node   H-node specifies the adapter as an Hybrid-mode node.

The B-node implementation uses broadcasting to resolve names. Information is exchanged between clients and servers using directed frames. This is the most widely used implementation and was available in previous releases of NetBIOS over TCP/IP.

OS/2 Warp 4 includes the new release of IBM NetBIOS over TCP/IP, which also provides P-node and H-node modes of operation. Both of these modes require two support servers: the NetBIOS Name Server (NBNS) and the NetBIOS Datagram Distributor Server (NBDD). The former is used for

NetBIOS-name-to-IP-address resolution, and the latter is used to deliver multicast or broadcast NetBIOS datagrams.

When both of these servers are available, NetBIOS over TCP/IP program operates as a P-node, as documented in RFC 1001/1002. Because a P-node relies on both of these servers being available, it does not operate if one or the other becomes unavailable.

An H-node is essentially a P-node as defined in the RFC, but with a degree of robustness added. If one of the servers becomes unavailable, the NetBIOS over TCP/IP application continues to operate in a hybrid mode as an H-node. What this means is that the NetBIOS over TCP/IP program exhibits both B-node and P-node characteristics. As just stated, when both servers are available to the NetBIOS over TCP/IP program, it operates as a P-node. If one of them fails, the program continues to operate in the manner described below.

When the NBNS is available, the NetBIOS over TCP/IP program uses the P-node transaction style for name resolution. A flag is kept that indicates if this server is available. If a problem occurs, such as a return code indicating some kind of internal error, the flag is changed to indicate that the server is unavailable and a polling loop is begun that periodically checks to see if the server is available again. While the server is unavailable, the NetBIOS over TCP/IP program switches to a B-node style transaction for name resolution, using IP broadcasts and the routing extensions described next in this section. The NetBIOS over TCP/IP program is always prepared to register and defend names in either mode of operation. If the server becomes available, the NetBIOS over TCP/IP program notices the change and switches back to a P-node style transaction, that is, begins using the NBNS again.

Similarly, the NetBIOS over TCP/IP program toggles a flag that indicates whether the NBDD server is available. The flag is set to an available state whenever the polling loop is able to contact the NBDD server. If the NBDD server is available, the NetBIOS over TCP/IP program operates as a P-node, using the NBDD server for datagram delivery. If the NBDD server becomes unavailable at any time, the NetBIOS over TCP/IP program switches to a B-node style of datagram delivery, resorting to IP broadcasts.

4.4.2 How to Enhance B-node Operations in OS/2 Warp 4

For B-node operations the NetBIOS over TCP/IP contains extensions that allow communication between networks over IP routers and bridges. The use of these extensions is optional, but if they are not active the NetBIOS over TCP/IP will operate only on the local LAN segment. The following are the three routing extensions for the IBM NetBIOS over TCP/IP:

- **Names File Routing Extension**

  This routing extension is implemented through the use of a names file, which contains NetBIOS name and IP address pairs. This implementation requires an entry in the names file for every workstation with which you want to communicate. This file is conceptually similar to the TCP/IP hosts file.

  The names file routing extension is enabled by setting the NAMESFILE parameter in the PROTOCOL.INI file equal to a nonzero integer value, which represents the maximum number of entries in the names file. For more information about updating this parameter, please refer to 10.3.1, "Important LAN System Files" on page 141 and 10.3.2, "Making Changes to the Networking Configuration" on page 144.

  The names file, called RFCNAMES.LST, is located in the \IBMCOM directory.
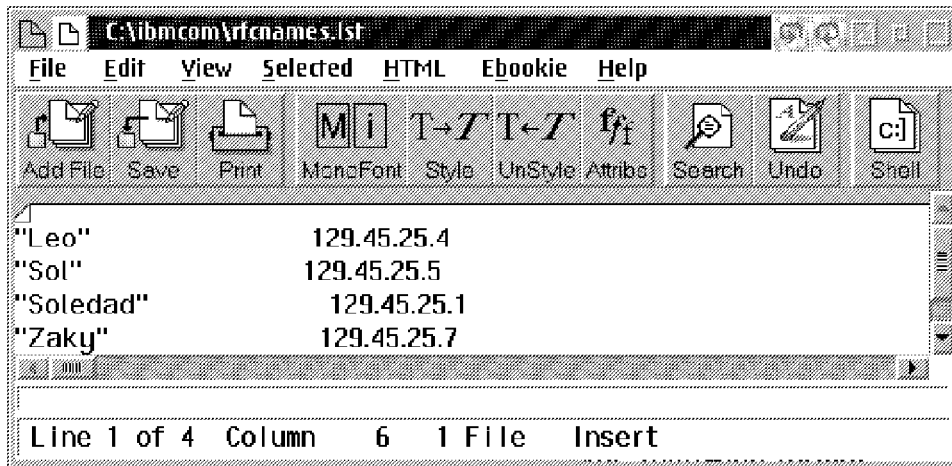
Figure 4. RFCNAMES.LST File

  The RFCNAMES.LST format consists of:

  String   String of characters used when searching for NetBIOS names in the file, delimited by double quotation marks.

  IP Address Either an IP address in dotted decimal form or a host name string that occurs in the local hosts file or on an Internet domain name server.

  The advantage of using a names file is in the reduction of name query broadcasts, because before the NetBIOS over TCP/IP program broadcasts to the network for NetBIOS name to IP address resolution, it searches this local file. The search is done by checking each names file entry up to the length of the entry. In our example, a requested name Soledad would match any of the following names file entries: S, So, Sol,

Sole and so on, but the first one encountered (Sol) is used. Therefore, due to this search technique, the order of entries in the names file is important.

If an address in the file is given as a host name string, it is translated to an IP address by the TCP/IP `GetHostByName()` function by looking it up in the local hosts file or by querying the Internet domain name server. The host name string must therefore be in the same form here as it is in the hosts file or on the domain name server.

For an OS/2 Warp Server environment, the requesters need a names file with computer name, IP address and domain name IP address of each server they contact. The servers need the computer name and IP address for each requester that contacts them. The computer name and domain names are found in the IBMLAN.INI files on these machines. For further information about the IBMLAN.INI file, refer to 10.3.1, "Important LAN System Files" on page 141.

- **Broadcast File Routing Extension**

  This routing extension is implemented through the use of a broadcast file which contains the IP addresses of other subnets. A TCP/IP broadcast is limited to one subnet unless other subnet addresses are included in the broadcast file.

  The broadcast file, named RFCBCST.LST is located in the \IBMCOM directory and has the following format:
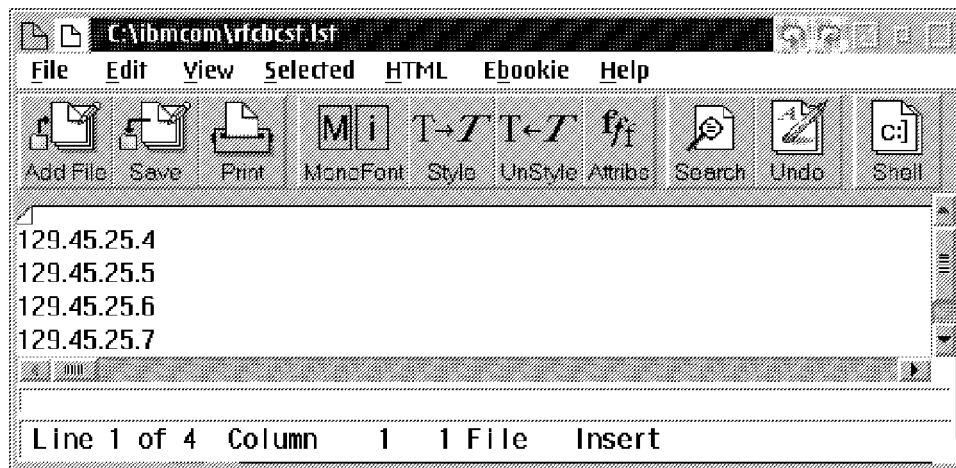
Figure 5. RFCBCST.LST File

The broadcast file contains a list of host names (such as `deptsrvr`), host IP addresses (such as `9.67.60.80`) or subnet broadcast addresses (such as `ausvm1.austin.ibm.com`). The file is read once at startup and each valid address is added to the set of destination addresses for broadcast

packets. Any host or network accessible by these addresses becomes part of the local NetBIOS broadcast domain; that is, they receive all name lookup and registration packets as well as all broadcast and group NetBIOS datagrams. These addresses can be on other networks and accessed through the appropriate router or bridge by the IBM TCP/IP program. The remote node is treated as if it were a node on the local network.

Each line of the broadcast file is either an IP address in dotted decimal notation (for example, `89.0.0.1`) or a host name string that occurs in either the local hosts file used by the IBM TCP/IP program or on an Internet domain name server. If an address is given as a host name string, it is translated to an IP address by the TCP/IP `GetHostByName()` function by looking it up in the local hosts file or by querying an Internet domain name server. The host name string must be in the same form here as it is in the hosts file or on the domain name server.

For OS/2 Warp Server and OS/2 Warp File and Print Clients, if the server and requester are on different networks, the broadcast file must be updated. At the clients, the broadcast file must include the IP address or TCP/IP host name for each server that this requester accesses using the NetBIOS over TCP/IP program. At the servers, the broadcast file must include the directed broadcast address for each subnet containing LAN requesters.

The fllowing list details broadcast file parameters:

- IP addresses, subnet broadcast addresses and host name strings are allowed.
- A maximum of 32 entries is allowed.
- Router documentation should be checked to ensure that it forwards directed broadcasts.
- Host name strings should match those in the hosts file and domain name server.

RFCADDR.EXE Program

When you make changes to the names/broadcast files while TCPBEUI is active, you can reinitialize TCPBEUI with the new files using the RFCADDR.EXE program. The cache will be updated with the new names.

- **Domain Name Server (DNS) Routing Extension**

This routing extension uses the TCP/IP Domain Name Server (DNS), which contains NetBIOS names and IP address pairs, so that the NetBIOS over TCP/IP clients can obtain the IP address of another workstation from it. This extension requires that the network

administrator enters the NetBIOS name and the IP address of every NetBIOS over TCP/IP workstation into the domain name server.

To enable the use of the Domain Name Server routing extension, you need to set the DOMAINSCOPE parameter in the PROTOCOL.INI file equal to your TCP/IP domain name. For example:

```
DOMAINSCOPE=austin.ibm.com
```

For more information about updating this parameter, please refer to 10.3.1, "Important LAN System Files" on page 141 and 10.3.2, "Making Changes to the Networking Configuration" on page 144.

If the names file search fails, the domain scope string, if specified, is appended to the encoded NetBIOS name. The new host name string is then used to resolve the NetBIOS name to an IP address by using the TCP/IP `GetHostByName()` function. This function tries to resolve the address by looking up the name in the local TCP/IP hosts file or by querying the Internet domain name server. If the domain server knows the name, it sends back the IP address to the NetBIOS over TCP/IP program.

The advantage of this implementation is that you have a central repository of all NetBIOS names. However, you have to update your Internet domain name server with NetBIOS names that are in an encoded format. An encoded format is necessary, because NetBIOS names are 16 bytes of any bit pattern and the domain name server accepts a limited character set. The NetBIOS over TCP/IP program encodes them into the 32-byte, reversible, half-ASCII format that is specified in the RFC 1001/1002. You can use the MAPNAME.EXE program, which is supplied as an applet, to encode and decode NetBIOS names.

However, a superior solution would be a dedicated server that maps NetBIOS names to IP addresses dynamically, whether or not TCP/IP host names are set equal to NetBIOS names. Such a solution is available by Network TeleSystems and is introduced in 4.4.3.1, "Introducing NetBIOS Name Server" on page 44 and described in 5.1, "The Shadow NetBIOS Name Server" on page 47. In contrast to WINS (Windows Internet Name Server), Microsoft's implementation of a NetBIOS Name Server, NTS' Shadow supports up to 16,000 names. This is a true enterprise solution, whereas WINS should only be used in workgroups since the number of names supported is very limited. In addition, WINS only supports Microsoft's proprietary world with its implementation of native NetBIOS and NetBIOS over TCP/IP. Shadow supports all standards, including Microsoft's.

4.4.2.1 OS/2 TCPBEUI NetBIOS Names Resolution Order B-Node

If B-node operation is set with routing extensions as illustrated in the previous chapter, an OS/2 client resolves NetBIOS names in the following order:

1. Local Name Cache

    • Edit \IBMCOM\PROTOCOL.INI file, section [tcpbeui_nif]

    ```
    SET PRELOADCACHE=YES   (Preload Remote Name Directory)
    NAMECACHE=1000         (Number of Names in Remote Name Directory
    NAMESFILE=100          (Maximum Number of Name-IP Address Pairs
    ```

2. Local Names File

    • \IBMCOM\RFCNAMES.LST File

    To enahnce performance, set the `NAMESFILE` parameter as described in previous item.

3. Search DNS (Domain Name Server)

    • by using the `GetHostByName()` call

    • `DOMAINSCOPE` is appended to encoded NetBIOS Name

    • Use `DOMAINSCOPE` parameter in `PROTOCOL.INI`

4. Check \MPTN\ETC\HOSTS file

5. Use broadcast file \IBMCOM\RFCBCST.LST

    • Maximal 32 entries

6. Broadcast to own subnet

4.4.2.2 OS/2 TCPBEUI NetBIOS Names Resolution w/NetBIOS Name Server

If a NetBIOS Name Server (NBNS) is present and OS/2 Warp 4 clients are configured to use a NBNS with H-node operation as illustrated in 4.4.3, "OS/2 Warp 4 Clients To Communicate with a NetBIOS Name Server," an OS/2 client resolves NetBIOS names in the following order:

1. Name Query to NBNS

2. If query fails after retries, then broadcast to own subnet

4.4.3 OS/2 Warp 4 Clients To Communicate with a NetBIOS Name Server

In order to have OS/2 Warp 4 clients communicate with a NetBIOS Name Server, you need to make changes to the default TCPBEUI settings. Using MPTS (Multi-Protocol and Transport Services) follow the steps below:

1. From System Setup (Warp Center pull-down menu) select **MPTS**.

2. Select **Configure** at the Multi-Protocol and Transport Services window.

3. Select the radio button for **LAN adapters and protocols** (which is usually set by default) and select **Configure**.

4. In the Adapter and Protocol window make sure the current configuration list contains the IBM OS/2 NetBIOS over TCP/IP protocol. If IBM OS/2 NetBIOS is listed, the number for IBM OS/2 NetBIOS over TCP/IP must be set to 1. Double-click on **IBM OS/2 NetBIOS over TCP/IP**.

5. At the following NetBIOS over TCP/IP window select the radio button for **Driver parameters** and click on **Configure**.

6. At the Parameters for IBM OS/2 NETBIOS OVER TCP/IP window, as shown in Figure 6, make the following changes:

Parameters for IBM OS/2 NETBIOS OVER TCP/IP

Edit the parameters as needed. Except for parameters preceded by "*", changes affect all instances of the driver.

Node Type	H-Node
Enable SLIP/PPP Interface	
NetBIOS Name Server address	9.3.1.81
Backup NetBIOS Name Server address	
NetBIOS Datagram Distributor address	9.3.1.81
Backup NetBIOS Datagram Distributor address	
NETBIOS trace level	0
Maximum sessions	225
Maximum commands	255
Maximum names	21
GDT selectors	15
Full buffer datagrams	NO
Query timeout	500
NETBIOS retries	2

OK   Range   Cancel   Help

Figure 6. IBM OS/2 NETBIOS OVER TCP/IP Window

- Change Node Type to H-Node.

- In the field for NetBIOS Name Server address type the TCP/IP address of the NetBIOS Name Server, for example, `9.3.1.81`.

- In the field for NetBIOS Datagram Distributor type the same TCP/IP address you used for the NetBIOS Name Server, for example, 9.3.1.81.

- Do accordingly with Backup server fields in case you have Backup NetBIOS Name Server installed on your LAN.

- Select **OK** and **Close** as many times necessary to exit MPTS and allow MPTS to update the CONFIG.SYS file if required.

- To make protocol changes active, you need to reboot your workstation. When the changes are made, your OS/2 Warp 4 workstation will ask the NetBIOS Name Server for a corresponding IP address to a NetBIOS name to communicate in P-node (Point-to-Point communication) rather that broadcasting into the network.

Alternatively you can use an ASCII editor, such as EPM or TEDIT, to make the changes mentioned above in the [tcpbeui_nif] section of the PROTOCOL.INI file which resides in the \IBMCOM directory where Multi-Protocol and Transport Services is installed.

4.4.3.1 Introducing NetBIOS Name Server

Clients and servers need to know how to find one another to share information. The NetBIOS conventions built into DOS, Windows (all sorts), and OS/2 are defined to let PCs and individual client/server applications refer to each other by name. NetBIOS names, like "Steve's PC" or "the printer in the lab" can be created by humans and built into programs with relative ease. It is advantageous that NetBIOS names can be used as unambiguous identifiers even if, for example, "th printer in the lab" station is moved and is no longer in the lab. However, to send each other packets of information, the TCP/IP protocol drivers of the respective PCs must refer to each other by an IP address. If there is a problem, then, of having to translate NetBIOS names into IP addresses to allow PC-to-PC communication on an IP network. To date, this translation has been handled in one of two ways:

- By use of static tables residing on each client and server

    - RFCNAMES.LST file on OS/2-based machines as described in 4.4.1.1, "NetBIOS over TCP/IP Implementation in OS/2 Warp 4" on page 36

    - LMHOSTS file on Windows-based machines as described in 12.7.5.4, "The LMHOSTS File" on page 287

- By use of dynamic broadcast queries (packets sent to every client and server in the broadcast subnet) asking in effect "Where is Steve's PC?"

The basic problem with static tables is that they must be continually updated and maintained, an activity far more troublesome than the maintenance of IP addresses alone. Every time any new station is added to the network, all of its applications' names must be added to the static table of each station that wants to send it data. Additionally, although names in static entries are always mappable, there is no telling whether the named application is active at the time interaction is desired by another station. The basic problem with broadcast queries is that IP networks cannot propagate broadcasts beyond a single (logical) cable segment. Therefore, resources located on the "other" side of a router from the broadcasting station will not receive the query, while every station on the "same" side of the router will be pestered with queries for which it doesn't know the answer.

A "NetBIOS-over-TCP/IP" protocol has been defined by the governing TCP standards body, the Internet Engineering Task Force (IETF), which deals with each of these problems. The IETF standard describes how NetBIOS stations may interact with a NetBIOS Name Server in order to dynamically register their own applications' names and to learn the name-to-address mappings of other applications. The authors are involved in the design of the NetBIOS-over-TCP/IP protocol and two different NetBIOS Name Server implementations. One is an application program written to run on top of IBM's OS/2 operating system, and the other runs stand-alone on a high performance PC platform without operating system involvement. 5.1, "The Shadow NetBIOS Name Server" on page 47 discusses the requirements and design considerations of a NetBIOS Name Server.

Chapter 5. Installing and Configuring NTS Shadow

This chapter details adapter and protocol-related information to provide a
common set of protocols used throughout this book.

5.1 The Shadow NetBIOS Name Server

Shadow is a software system for managing name and address assignments
and desktop configuration information within a TCP/IP (Transmission Control
Protocol/Internet Protocol) network. Shadow includes a robust set of
network services offered through standards-based protocol interactions,
such as:

  • DHCP (Dynamic Host Configuration Protocol) service

  • DNS (Domain Name Server) service

  • NBNS (NetBIOS Name Server) and NBDD (NetBIOS Datagram
    Distributor) services
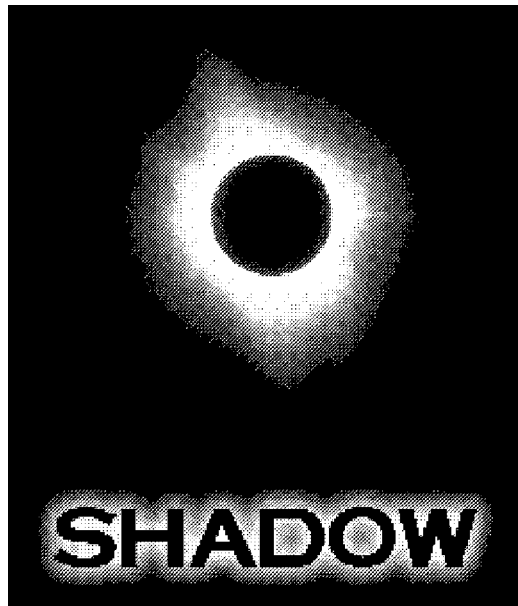
Figure 7. Network TeleSystems: Shadow Logo

The Shadow NBNS service is an integrated NetBIOS Name Server and
Datagram Distributor. The Shadow NBNS service fully implements RFCs
1001 and 1002. The NBNS service provides name resolution services similar
to those provided by Microsoft Windows NT WINS (Windows Internet Name
Server), another implementation of elements of RFCs 1001 and 1002.

However, the Shadow NBNS service also provides the datagram distributor as described in those RFCs.

Note: To use the datagram distributor, both the NBNS server and TCP/IP client stack must support datagram distribution, such as:

- OS/2 Warp Connect with latest MPTS ServicePak
- OS/2 Warp 4
- DOS LAN Services (part of OS/2 Warp Server)

If you plan to use the Shadow Datagram Distributor, you can use the Network TeleSystems TCP Pro protocol stack on the client. The TCP Pro protocol stack fully supports Datagram Distribution. The Microsoft Windows 95 and Windows NT protocol stacks do not support datagram distribution.

The Shadow NBNS server supports both IBM and Microsoft NetBIOS networks; the same NBNS server can be used with OS/2 Warp, DOS/Windows workstations with DOS LAN Services installed, Windows 95, and Windows NT workstations.

The idea of the NBNS is that instead of broadcasting the NetBIOS names to the whole IP subnet, the names to be registered are sent to a NBNS server. The NBNS server then checks if the name is already in use, and if not, the name is registered. All the future queries to that name will be resolved with one single query to the NBNS.

To get the full advantage of the Shadow NetBIOS name server, install the Neighborhood Browser Enabler software on the OS/2 Warp Server Domain Controller machine. This way the OS/2 Warp Server Domain Controller registeres the Microsoft network dependent NetBIOS names and acts as the domain master browser machine.

5.1.1 Prerequisites

The following table details hardware and software requirements for Shadow:

Table 2 (Page 1 of 2). Shadow Hardware and Software Requirements	
Type	**Details**
Processor	Intel processor (386 or higher).
Hard drive type	IDE only (SCSI is not supported).
Bus type	ISA bus for the NIU (Network Interface Unit), sometimes called the network card (PCI is not supported).

Table 2 (Page 2 of 2). Shadow Hardware and Software Requirements	
Type	**Details**
RAM	16MB.
Network cards	One of the following: • 3Com 3C509 (ISA). • Eagle Microdyne NE2000 (ISA). • UB NIUpc/EOTP (ISA). • UB pcNIU/ex 512K (ISA). • IBM Token Ring 16/4 card (ISA). **Note:** You can use the IBM Token Ring Turbo 16/4 if you use the LANAID software provided by IBM and place the card in 16/4 automode.
Operating System	IBM PC DOS 5.0 or later, or MS DOS 5.0 or later. **Note:** The server software uses its own 32-bit operating system and does not run on top of DOS. However, you need to use DOS to install the server files and start the server program.

The configuration used for this sample environment is:

- IBM ValuePoint 433DX
- Shadow NetBIOS Name Server Version 1.1
- 16 MB memory
- An IBM Auto 16/4 ISA Token-Ring Adapter, configured manually:
  - 16 MBit/sec data rate
  - ROM address DA00
  - RAM address DC00
  - RIPL disabled
  - Ring speed auto sense function disabled
- IBM PC DOS 7.0

5.1.2 Installation

The installation program (INSTALL.EXE) asks you for configuration information and makes entries in the NTS-SRVR.CFG file based on your input. To install the Shadow NetBIOS name server (NBNS) follow the steps below:

1. Make sure the following applies to the machine on which you will install Shadow:

   a. The whole hard disk must be configured as one primary partition.

   b. The hard disk must be formatted and installed with DOS.

c. No memory management statements in the CONFIG.SYS and AUTOEXEC.BAT files. If there are any, like `HIMEM.SYS` or `EMM386.EXE`, remove those lines.

d. Check the PC's time and date to verify that they are correct. If the time and date are not correct, set them using the DOS `TIME` and `DATE` commands.

   Note: Shadow uses the PC's time and date to time stamp system events. If the server is halted and then restarted during operation, the server uses the time stamps on server Configuration and Save files to determine which files to load. This can affect the data that is loaded into the server s database.

2. Place the Shadow Installation diskette into the PC's 3-1/2 floppy drive.

3. Start the installation program by issuing the following command:

   `<drive>:\INSTALL`

   where `<drive>` is the drive that contains the installation diskette.

4. When prompted, enter the required information such as the NBNS IP address, subnet mask and router address.

   Note: By default, the installation program guesses the gateway address by combining the network portion of the server's IP address with the host address 1.

5. When prompted, select the appropriate network adapter and adapter settings.

   Note: Your PC must contain one of the card types listed. If the PC does not contain one of the listed card types, you need to install one before using the server. Select the card type you plan to install and continue with the installation. If you do not know what card type you plan to install, select the **3COM 3C509**. If you need to, you can edit the NTS-SRVR.CFG file after you install the card. See the *Shadow Server Reference Manual* for more information.

6. After the installation is finished, use a DOS editor, like E (PC DOS) or EDIT (MS DOS), to edit the C: SHADOW NTS-SRVR.CFG file, where SHADOW is the NBNS server installation directory. Check that the network adapter I/O port address and RAM address are correct.

   The following is a sample NTS-SRVR.CFG file used with an IBM Auto ISA Token-Ring adapter:

```
#-------------------------------------------------------------------------------
#            Shadow Configuraton File
#
#            Network TeleSystems Inc.
#
# November 12,1996
#
# # = Comments
#-------------------------------------------------------------------------------
NOLOG                # Log files - Comment out to enable Logs
NOSAVE               # Save files - Comment out to enable Save Files
#HISTORY             # History file - Uncomment to enable History File
#AUTHORIZATION        # WEB Authorization - Uncomment to enable Authorization
#OUTAHERE            #
NODIAGS             #
NORESET             #
#RESOLVEPARENTS       #


#-------------------------------------------------------------------------------
#Hardware parameters
#-------------------------------------------------------------------------------

NIU IBMTR            # Adapter type
CONNECTOR TPI         # Twisted pair
#CONNECTOR THINNET    # Thin net
#CONNECTOR THICKNET   # Thick net
#CONNECTOR STARLAN    # Starlan
IO-PORT      0A20   # TR adapter I/O port
WINDOW       0DC00  # TR adapter RAM addres

#-------------------------------------------------------------------------------
#Server Configuration
#-------------------------------------------------------------------------------

NETSUBNETMASK  255.255.255.0
IPADDR        9.3.1.178
GATEWAYADDR    9.3.1.74
#BACKUPADDR    111.111.111.111,222.222.222.222
#COSERVER      111.111.111.111,222.222.222.222
#IPTIMETOLIVE  60     # IP time to live default = 60
#ARPTIMEOUT    120    # ARP timeout default = 120
SCOPE        NULL   #
TTL          10800  #(100000000=max) time to live (in seconds) for dynamic entri
#SYNCTTL       20    # Sync time to live - NBNS
#RELEASETTL    10    # Release time to live - NBNS
#AGENTTTL       1    # Agent time to live - AGENT
#NEGCACHETTL   360    # Negative response cache time to live - DNS
```

Figure 8. Shadow's NTS-SRVR.CFG Configuration File

The settings changed manually in the test environment were:

- The OUTAHERE parameter was remarked. This prevents Shadow from
  exiting when you accidentally hit the **Esc** key. To exit Shadow press
  Ctrl-Right Shift Key-Esc.
- The IO-PORT parameter was changed from A20 to 0A20

- The `WINDOW` parameter was set to `0DC00`. This is the Token-Ring adapter RAM address.
- The `TTL` (Time-To-Live) setting was set to `10800` seconds (3 hours) to give optimal support for Windows 95 clients.

  Note: If you do not have any Windows 95 clients in you network, you can set this value differently, for example, `100`.

7. Check if the statement `NTS-SRVR` was added to the AUTOEXEC.BAT file to autostart Shadow.

5.1.3 Global System Keywords

Table 3 lists the global system parameters and the keywords used to configure them. If the keyword is not commented out, then the parameter is in effect. If the keyword is commented out or is not present in the file, then the parameter is not in effect. To comment a keyword out, type # in front of the keyword.

Table 3 (Page 1 of 5). NTS-CFG Parameters	
Keyword	**Parameter**
OUTAHERE	Configures the key or key combination required to halt the server or enter the debug program.
	If the keyword is not commented out, the following keys are required to halt the server or enter the debug program:
	• ESC to halt the server (does not apply if you are exiting from on-line help on the server).
	• - (minus sign) to enter the debug program.
	If the keyword is commented out, the following keys are required to halt the server or enter the debug program:
	• Left Ctrl + right Shift + Esc to halt the server.
	• Left Ctrl + right Shift + - (minus sign on the numeric keypad) to enter the debug program.
NODIAGS	If the server uses the UB PCniu/EOTP Ethernet card, this keyword specifies whether the server runs diagnostics of the software on the card.
	• If the keyword is not commented out, the server does not run the diagnostics.
	• If the keyword is commented out, the server does run the diagnostics.
	Note: Diagnostics are run only if the software is reset on the card. Therefore, if the NTS-SRVR.CFG file contains the NORESET keyword and it is not commented out, diagnostics are not run even if the NODIAGS keyword is commented out.
	See also NORESET.

Table 3 (Page 2 of 5). NTS-CFG Parameters	
Keyword	**Parameter**
NORESET	If the server uses the UB PCniu/EOTP Ethernet card, this keyword specifies whether the server resets the card by reloading the NIU software each time the server is started. • If the keyword is not commented out, the server does not reload the software on the NIU. Instead, the server checks to see whether software is already running on the card and, if so, uses that. • If the keyword is commented out, the server does reload the NIU software each time you start the server. Reloading the software takes about 5 seconds. See also NODIAGS.
NOLOG	Controls whether the server saves archive files of the server log. The server can maintain four 64 KB logs in active memory at a time. Once the four logs are full, the server purges the first log so it can use it for new log entries. • If the keyword is not commented out, the server does not archive log files. Once the server purges a log file, the contents of the file are gone. • If the keyword is commented out, the server does archive log files. When the server is ready to purge a log file from active memory, it writes the contents of the log to a file. The log files are named as follows: `NTS-LOG-. <sequence>` where <sequence> is the numerical sequence of the file, starting at 000. **Note:** We recommend that you leave logging disabled unless you are attempting to track a particular problem or are advised to enable logging by Network TeleSystems technical support.

NOSAVE	Controls whether the server creates Save files when halted.
	
	• If the keyword is not commented out, the server does not create Save files. State information and dynamic entries are not saved.
	
	• If the keyword is commented out, the server creates Save files when halted:
	
	`NTS-CFG-.SAV`
	`NTS-DHC-.SAV`
	`NTS-NBN-.SAV`
	`NTS-DNS-.SAV`
	
	Note: Only the `NTS-NBN-.SAV` and `NTS-CFG-.SAV` are created with the Shadow NBNS-only product.
	
	When the server is restarted, it uses the Save files.

	Table 3 (Page 3 of 5). NTS-CFG Parameters	
Keyword	**Parameter**	
HISTORY	Controls whether the server creates History files. History files contain copies of the packets examined by the server and packets generated by the server itself.	
	• If the keyword is commented out, the server does not create History files.	
	• If the keyword is not commented out, the server does create History files. The log files are named as follows:	
	`NTS-HIS. <sequence>`	
	where `<sequence>` is the numerical sequence of the file, starting at 000.	
NIU	Specifies the type of NIU that connects the server to the network.	
	Note: NONE Prevents the server from connecting itself to the network. Use this keyword if you just want to observe the Console screens and options before placing the server in your network.	
IO-PORT	Specifies the I/O (Input/Output) port for the NIU. If you use the INSTALL.EXE program to configure the NTS-SRVR.CFG file, the program gives you a list of valid I/O ports for the NIU type you select. You also can refer to the manufacturer's instructions for the card for the appropriate I/O port.	
	Note: If the server uses a 3C509, you do not need to specify the I/O port.	
WINDOW	Specifies the memory window for the NIU. If you use the INSTALL.EXE program to configure the NTS-SRVR.CFG file, the program gives you a list of valid memory windows for the NIU type you select. You can also refer to the manufacturer's instructions for the card for the appropriate memory window.	
	Note: If the server uses a 3C509, you do not need to specify the memory window.	
CONNECTOR	Specifies the connector type for the 3Com 3C509 or Eagle Microdyne NE2000 Ethernet card. (If the server uses a different type of card, you do not need to specify the connector type. The software can obtain this information from the card.)	
	You can specify one of the following connection types:	
	``` STARLAN A connector type used on some NE2000 Ethernet cards THICKNET An AUI (Access Unit Interface) connector THINNET A BNC (Basenet Connection) coaxial connector TPI A twisted-pair connector. ```	
TOKENRING	Changes the default network type assumed by the server from Ethernet to token ring. Use this keyword only if the server is using the IBM Token Ring 16/4 card as the NIU type.	
	Note: You also can specify ETHERNET, but the ETHERNET keyword is unnecessary because the server assumes Ethernet by default.	

Table 3 (Page 4 of 5). NTS-CFG Parameters	
Keyword	**Parameter**
MACADDR	Specifies the hardware address (sometimes called the MAC address or NIU address) of the NIU. Type the address without using spaces or dashes to separate the numbers.

ARPTIMEOUT	Specifies the number of seconds the server will retain a cached ARP entry before discarding it.
	
	`Default:  300`
	`Range:    0 to 65535`

GATEWAYADDR	Specifies the IP address of the gateway (router) that connects the server to the rest of your intranet or the Internet.
IPADDR	Specifies the IP address of the server.
NETSUBNETMASK	Specifies the subnet mask of the network into which you plan to place the server.

IPTIMETOLIVE	Specifies the number of seconds that an IP packet can live in your intranet. (Most routers measure the IP TTL as the number of hops.)
	
	`Default:  60`
	`Range:    0 to 255`

BACKUPADDR	Specifies the IP address of this server's NBNS backup peer.
COSERVER	Specifies the IP addresses of up to 15 other Shadow servers as this server's NBNS Coservers.

BACKUPLIMIT	Specifies the NBNS backup limit. The backup limit is the number of changes to the NBNS database on this server that can be made before the NBNS service sends a backup packet to its NBNS backup peer.
	
	When the backup limit is reached, the server sends a backup packet immediately; the server does not wait for the backup time to expire. The backup limit and backup time together control the frequency of update transactions between backup peers, and thus influence the synchronization of the servers' databases.
	
	`Default: 10`
	`Value:    0 to 65535`

SYNCTTL	Specifies the Time-to-Live (in seconds) for cached entries obtained from an NBNS Coserver Peer. The TTL is measured in seconds. When the Sync TTL for a cached entry expires, the server removes it from its database.
	
	Note: The Sync TTL applies only to the cached entry that this server makes after receiving the NBNS data from a Coserver peer. The Sync TTL does not affect the entry in the Coserver peer's database. The Sync TTL is not reset when the Coserver peer receives a query for the cached entry.
	
	`Default: 10 (seconds)`
	`Range:    0 to 100000000 (100 million seconds)`

Keyword	Parameter
RELEASETTL	Specifies the Time-to-Live for NBNS release entries. The TTL is measured in seconds. When the TTL expires, the released entry is removed from the server.
	A release entry is an entry that has been marked for deletion but has not yet been removed from the database. During the Release TTL, the NBNS service will not acknowledge the entry if it receives a request for it from the network. However, if that entry s client renews itself before the Release TTL expires, the NBNS service will reactivate the entry with a new Time-to-Die.
	If the client does not reregister itself before the Release TTL expires, the entry is finally deleted from the database.
	`Default:  10 (seconds)` `Range:    0 to 100000000 (100 million seconds)`
TTL	Specifies the maximum Time-To-Live (TTL) for dynamic NetBIOS entries. The NetBIOS TTL is measured in seconds. Entries that exceed the maximum TTL are removed from the server. Usually, a static entry does not have a TTL and remains in the server database unless you or another network administrator deletes it.
	`Default:  10800 (3 hours)` `Value:    0 to 100000000 (100 million)`

Table 3 (Page 5 of 5). NTS-CFG Parameters

5.1.4 Setting Up and Using the Shadow Remote Manager

You can manage the Shadow NBNS from a remote workstation with the Shadow Remote Manager software. The remote manager software is a 16-bit Windows software and can be run in a Win-OS/2 session, in Windows with DLS (DOS LAN Services) configured with TCPBEUI, or in Windows 95. You have to configure the TCP/IP protocol in Windows 95, and both TCP/IP and NetBIOS over TCP/IP interfaces in OS/2 in order to run the software. Before installing the remote management software, you must define the NBNS NetBIOS name and IP address on the Shadow server. Set the address from the Shadow NBNS server console, as noted below:

1. Use the arrow keys to select the NBNS screen on the server.

2. Press **F2** to activate the edit window.

   The fields of the edit window appear above the list of NBNS entries. Each edit field corresponds to the NBNS field directly below it.

3. Define the NBNS server NetBIOS name, name type, node type, IP address and entry type. For example,

   `SHADOWSRV----- UH     009.003.001.178 S`

   where

SHADOWSRV is the NBNS server's NetBIOS name.

NetBIOS names must be 16 characters long and can contain any combination of 8-bit ASCII characters. All 256 8-bit ASCII characters are allowed.

If you specify a name that is shorter than 16 characters, the server displays the blank spaces at the end of the name as dashes. If the name actually contains dashes, the dashes are shown using their hexadecimal equivalent, `0x20`.

Characters that cannot be displayed are represented by pairs of hexadecimal digits (`0` through `F`) surrounded by square brackets (`[ ]`). The brackets can contain more than one hexadecimal pair.

U Indicates that the name is a unique name. The entry type can be one of the following:

`U` Unique
`G` Group

H Indicates that the node type is to be H-node. The node type can be one of the following:

`B` Broadcast
`P` Point-to-point
`H` Hybrid
`?` Unknown

9.3.1.178 Specifies the Shadow NetBIOS name server's IP address; the address must match one set in the NTS-SRVR.CFG file.

S Indicates that the entry is a static entry. Press the **Spacebar** to select whether the entry is static or dynamic:

`S` Static
`D` Dynamic

4. Press **F4** to add the completed entry to the list.

5. Press **F2** to close the edit window.

After configuring the NBNS server name, continue with the Shadow Remote Manager installation as follows:

1. Select [**Start — Run...**] in Windows 95 or [**File — Run...**] in WIN-OS/2 Full Screen, enter the command SETUP.EXE and click the **OK** button.

2. Read the license agreement and click the **Yes** button.

3. Select the installation directory and click the **Next** button.

Start the program by double-clicking the Shadow Manager icon. The first thing to do is to make the connection to the server. Select [**NBNS — Select NBNS Server...**] and enter the NBNS server NetBIOS name defined, for example `SHADOWSRV`. The names are case sensitive and have to be entered exactly the same way as on the server console.

When the connection is made, you get the server console NBNS screen as shown in Figure 9. You can do all the administration remotely, including deleting or adding NetBIOS names, changing IP addresses for names and changing the server configuration.

```
Manager [NBNS] SHADOWSRV                                        _ □ ×
File  Options  NBNS  DHCP  Help
[0102]__MSBROWSE__[0201]
                          gh  9.3.1.140          05Jun97-12:19:00
SHADOW----------          gh  155.155.155.155    Static
SHADOWSRV-------          up  9.3.1.178          Static
W95CLI01----[00]Mgr       u?  9.3.1.11           05Jun97-14:39:18
W95CLI01-------[00]       u?  9.3.1.11           05Jun97-14:39:18
W95CLI01-------[03]       u?  9.3.1.11           05Jun97-14:39:18
W95TEST2-------[03]       u?  9.3.1.11           05Jun97-14:39:18
WS_DOM01-------[00]       g?  9.3.1.11           05Jun97-14:39:18
                          gh  9.3.1.140          05Jun97-12:17:13
WS_DOM01-------[1B]       uh  9.3.1.140          05Jun97-12:17:55
WS_DOM01-------[1C]       gh  9.3.1.140          05Jun97-12:17:54
WS_DOM01-------[1D]       uh  9.3.1.140          05Jun97-12:18:59
WS_DOM01-------[1E]       gh  9.3.1.140          05Jun97-12:17:52
WS_SRV01-------[00]       uh  9.3.1.140          05Jun97-12:17:09
WS_SRV01-------[03]       uh  9.3.1.140          05Jun97-12:17:11
WS_SRV01--------          uh  9.3.1.140          05Jun97-12:17:23

                                         05Jun97-11 41 01    Idle
```

Figure 9. The Shadow NBNS Screen from the Remote Manager

For more information (for example a White Paper on NetBIOS Name Server) visit the NTS Web site at:

`http://www.nts.com`

or contact:

• Eastern US/Canada

Regional Sales Manager, Jim Cooney:

Phone: (617) 944-3220; Fax: (617) 944-8335; e-mail: jcooney@nts.com

- Central US

  Regional Sales Manager, Bill Moore:

  Phone: (972) 663-9383; Fax: (972) 773-1101; e-mail: bmoore@nts.com

- Western US/Can

  Regional Sales Manager, Hal Kroeger:

  Phone: (408) 523-6334; Fax: (408) 523-8118; e-mail: kroeger@nts.com

- International (All other countries):

  Contact NTS Corporate HQ in California, US for nearest distributor

  Phone: (408) 523-8100; Fax: (408) 523-8118; e-mail: sales@nts.com

5.1.5 Client Configuration for the Shadow NetBIOS Name Server

After installing the NBNS, configure all the servers and clients running NetBIOS over TCP/IP to use the NBNS service. Notice that servers and clients normally register their NetBIOS names when the requester services are started.

5.1.5.1 OS/2 Warp Server and OS/2 Warp Configuration

In order to have OS/2 Warp 4 clients communicate with a NetBIOS Name Server, you need to make changes to the default TCPBEUI settings. Using MPTS (Multi-Protocol and Transport Services) follow the steps below:

1. From System Setup (Warp Center pull-down menu) select **MPTS**.

2. Select **Configure** at the Multi-Protocol and Transport Services window.

3. Select the radio button for **LAN adapters and protocols** (which is usually set by default) and select **Configure**.

4. In the Adapter and Protocol window make sure the current configuration list contains the IBM OS/2 NetBIOS over TCP/IP protocol. If IBM OS/2 NetBIOS is listed, the number for IBM OS/2 NetBIOS over TCP/IP must be set to 1. Double-click on **IBM OS/2 NetBIOS over TCP/IP**.

5. At the following NetBIOS over TCP/IP window select the radio button for **Driver parameters** and click on **Configure**.

6. At the Parameters for IBM OS/2 NETBIOS OVER TCP/IP window, make the following changes:

   - Set the Node Type parameter to `H-node` or `P-node`, depending on the need. In most situations it is recommended to use `H-node`. If `P-node` is used, registrations cannot be done without NBNS server. If `H-node` is used, the registrations are broadcasted if the NBNS server is not available.

- Set the NetBIOS Name Server address parameter to the NBNS server IP address, for example `9.3.1.178`.
- Set the NetBIOS Datagram Distribution server parameter to the NBNS sever IP address, for example `9.3.1.178`.

7. Select **OK** and **Close** as many times necessary to exit MPTS and allow MPTS to update the CONFIG.SYS file if required.

8. To make protocol changes active, you need to reboot your workstation.

5.1.5.2 Windows 95 and Windows NT Configuration

In Windows NT and Windows 95 the NBNS server IP address has to be defined as a WINS server. The operating system takes care of the proper node-type selection. Set the WINS address the following way:

1. Go to the Control Panel and double-click the **Network** icon.

2. In Windows NT only, select the Protocols tab.

3. Select the TCP/IP protocol from the list and click the **Properties** button.

4. Select the WINS tab, and enter the NBNS server IP address, for example `9.3.1.178`.

5. Save the changes and reboot the machine to make the new settings effective.

Chapter 6. Dynamic TCP/IP

This chapter briefly defines the basic concepts of Dynamic TCP/IP, and explains how to configure the Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS) servers of OS/2 Warp Server

6.1 Dynamic TCP/IP in OS/2 Warp Server

Dynamic TCP/IP is the integration of the TCP/IP networking standards of Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Services (DDNS). DHCP and DDNS perform complementary functions in accomplishing the goal of automatic IP network access.

IBM's TCP/IP for OS/2 Warp Server provides support for Dynamic TCP/IP. This networking technology allows you to define network host configuration parameters at a central location and automate configuration of IP hosts. Therefore, it simplifies both IP network access and IP network administration and is well-suited for supporting mobile hosts.

DHCP enables you to centrally locate and dynamically distribute configuration information, including IP addresses. Clients can obtain IP network configuration, including an IP address, from a central DHCP server. DHCP servers control whether the addresses they provide to clients are allocated permanently or are "leased" for a specific time period. When a client is allocated a leased address, it must periodically check in with the server to revalidate the address and renew the lease. The processes of address allocation, leasing and lease renewal are all handled by the DHCP client and server programs and are transparent to endusers.

DDNS can be used to automatically register your host name and DHCP-assigned IP address mapping information in a Dynamic DNS server so that other hosts in the network may find your IP address through DNS name queries. That is, DDNS defines extensions to the domain name system to enable DNS servers to accept requests to update the DNS database dynamically and securely. These extensions define mechanisms for adding and deleting a set of names and associated resource records.

The OS/2 Warp 4's dynamic TCP/IP client software includes DHCP and DDNS client programs that work in conjunction with their server counterparts in the network. DHCP and DDNS client programs for Windows 95 clients can be downloaded from the following Web site:

```
http://www.software.ibm.com/os/warp/downloads/
```

If your network supports DHCP services, you can choose to use the OS/2 Warp 4 DHCP client to automatically configure TCP/IP network parameters from a DHCP server, rather than manually configure from parameter values provided by your network administrator.

If your network supports Dynamic DNS services, you may choose to complement DHCP client operation with integrated Dynamic DNS support to enable dynamic TCP/IP operation.

Advantage of Dynamic TCP/IP

One benefit of DHCP is the freedom it provides client hosts to move from one subnet to another without having to know ahead of time what IP configuration information it needs on the new subnet. As long as the subnets to which a host relocates have access to a DHCP server, DHCP clients will automatically configure themselves correctly to access those subnets.

6.1.1 Components of a Dynamic TCP/IP Network

The following four types of network components can comprise a Dynamic IP network:

Dynamic IP Hosts   Dynamic IP hosts run the DHCP and DDNS client programs. The DHCP and DDNS clients work together and with their server counterparts to obtain and implement configuration information to automatically access IP networks.

DHCP Servers   DHCP servers provide the IP address and configuration information to DHCP and BootP clients on the network. DHCP servers contain information about the network configuration and the host operational parameters as specified by the network administrator. Dynamic IP DHCP servers have the added capability of updating Dynamic DNS servers with IP address-to-host name mappings using host name information provided by the DHCP clients.

Dynamic DNS Servers Dynamic DNS servers are a superset of traditional DNS servers. The dynamic extensions of the DNS protocols implemented in a DDNS server enable your host to dynamically and securely register your name and address mapping in the DNS tables rather than requiring a network administrator to manually perform the updates.

BootP Relay Agents   BootP Relay agents, also called BootP helpers, can be used in IP router products to forward information between DHCP clients and servers on different subnets. BootP relays eliminate the need for having a DHCP server on each subnet to service the broadcast requests from DHCP clients. These BootP Relay Agents are widely available as features of commercial internetworking router products.

In the following section we demonstrate how easy it is to set up a dynamic TCP/IP environment under OS/2 Warp Server.

6.1.2 Configuring and Using DHCP Server

1. At the OS/2 Warp Server workstation, open the DHCP Server Services window that resides in the TCP/IP folder, as shown in Figure 10.
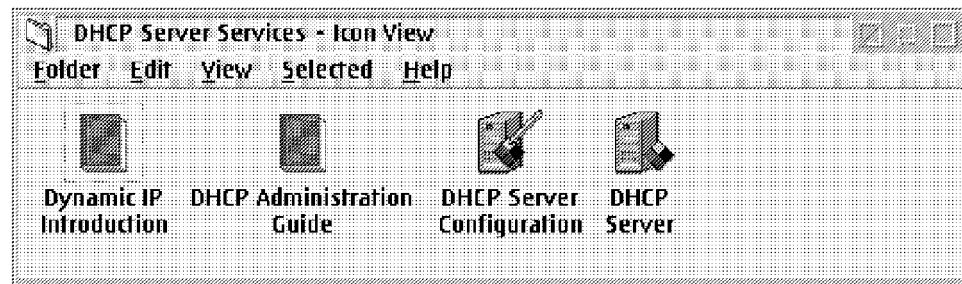
Figure 10. DHCP Server Services Window

2. To begin configuring the DHCP server, open DHCP Server Configuration. The DHCP configuration graphical interface is displayed as shown in Figure 11 on page 64.
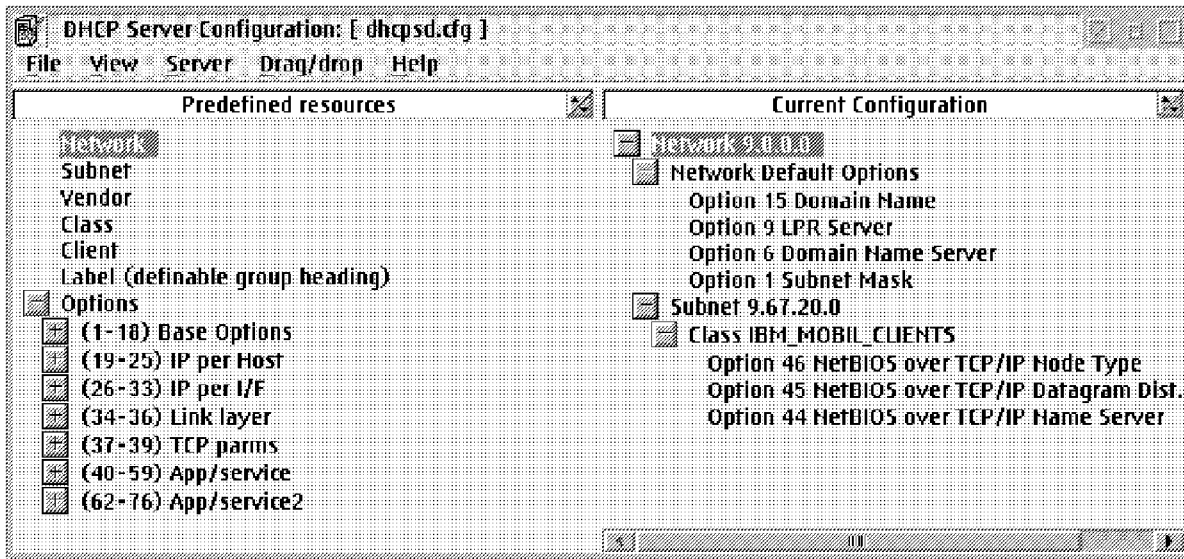
Figure 11. DHCP Server Configuration Window

Configuring is made very easy. Using the drag-and-drop technique, you select one item after another from the list of Predefined Resources and drag it to the list of Current Configuration. Therefore, if you need to delete an item from the list of Current Configuration, you need to drag and drop that item to the Shredder (which usually resides on the Workplace Shell).

This example gives instructions on how to set up a DHCP server for the subnet 9.67.20.0. You can extend the configuration for other subnets by doing the steps shown here for a single subnet.

a. First drag and drop the **Network** item to the list of Current Configuration and double-click on it. Use the spin-button arrows to define the subnet mask. In Figure 12 on page 65 you find an example for subnetting the 9.0.0.0 network.
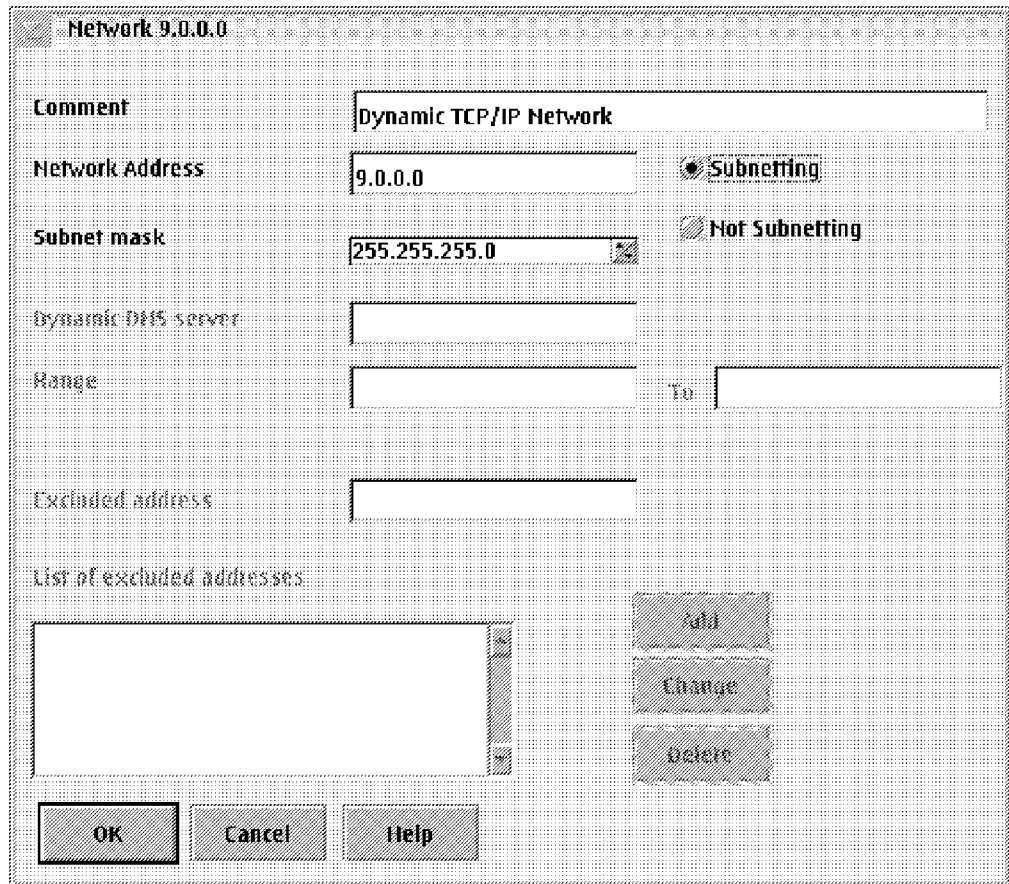
Figure 12. Network 9.0.0.0 Item Window

> **Note:** Since you are subnetting in this example, you cannot type in information for Dynamic DNS server and Range of IP addresses.

b. Drag and drop the Label item on top of the Network 9.0.0.0 item in the list of Current Configuration so that an Expand-Tree sign will appear just next to the Network 9.0.0.0 item. Expand the tree now and double-click on the **Label** item. Provide a name, for example Network Default Options.

> **Note:** You must see the Expand Tree sign left of the Network 9.0.0.0 item; otherwise you did not drop directly on top of the Network item. If this is the case, delete the item by dragging and dropping it to the Shredder, and redo this step.

c. Expand the Options tree and then (1-18) Base Options in the list of Predefined resources. Drag and drop **Option 15 Domain Name** on top of the Network Default Options item in the list of Current Configuration. Expand the tree and double-click on the new item. Provide information as shown in Figure 13 on page 66.
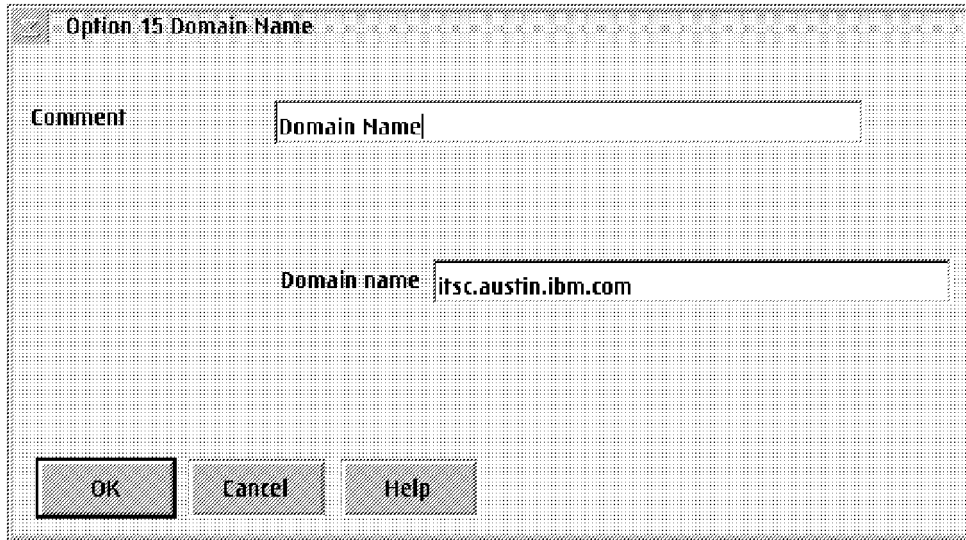
Figure 13. Option 15 Domain Name Item Window

    d. If you have an LPR (Line Printer) server in your TCP/IP network, drag and drop **Option 9 LPT Server** to the Network Default Options item and double-click on it. Type in the TCP/IP address of the LPR server (example shown in Figure 14).
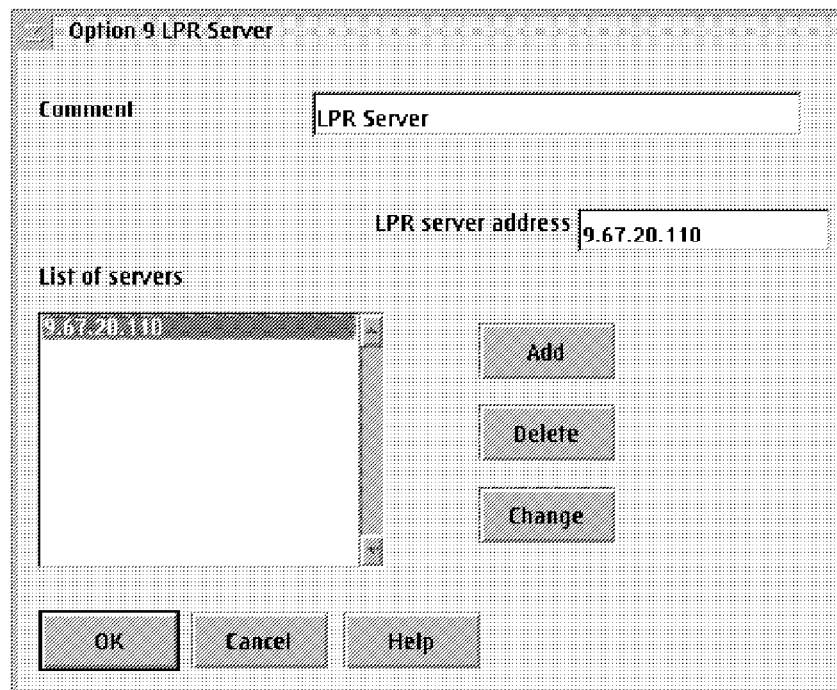
Figure 14. Option 9 LPR Server Item Window

e. Now we need to provide the TCP/IP address of the subnet's DNS server by dragging and dropping **Option 6 Domain Name Server** from the list of Predefined Resources on top of the Network Default Options item in the list of Current Configuration. Double-click on it, and provide information as shown in Figure 15.
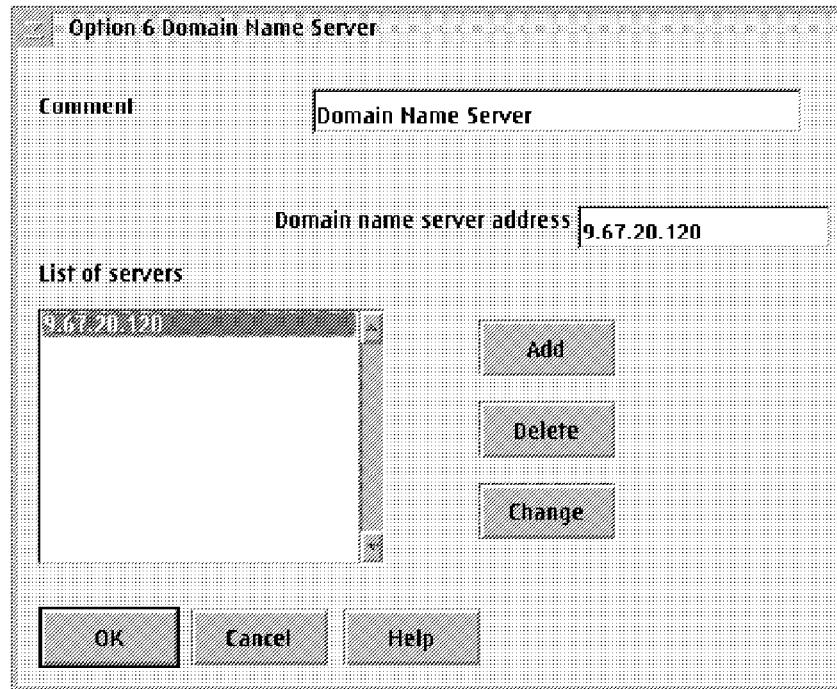
Figure 15. Option 6 Domain Name Server Item Window

f. To provide subnet mask information to the Dynamic IP client, drag and drop **Option 1 Subnet Mask** on top of Default Network Options and double-click on it. Find an example shown in Figure 16.
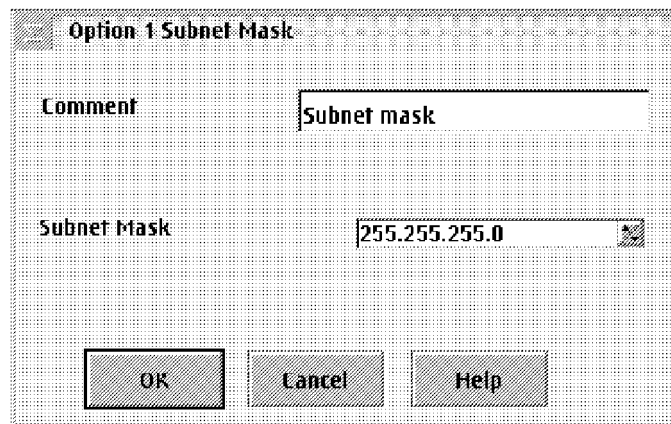
Figure 16. Option 1 Subnet Mask Item Window

g. Now the time has come to define a subnet. To do so, drag and drop the **Subnet** item (second item from the beginning) on top of the Network 9.0.0.0 item in the list of Current Configuration. Provide information as shown in the example of Figure 17 on page 68.

Figure 17. Subnet 9.67.20.0 Window

Specify the range of IP addresses and exclude the ones taken in this range. For example, 9.67.20.115 will be the static IP address for the NetBIOS Name Server, and 9.67.20.120 will be the address of the Dynamic DNS server. Excluded addresses will not be offered to requesting IP clients.

Note: You do not need to provide information about the Dynamic DNS server since this server has been defined already in the Network Default Options section.

The IBM DHCP Server also allows you to choose which configuration information is provided to the client based on who is using the client or what the client is being used for.

Using DHCP classing, you can provide unique configuration information to clients that identify themselves as belonging to a certain group. Further, you can administer parameters to a class either independent of or with respect to the location of the client, or a combination of both. For example, if you wanted all the users of IBM mobile clients to use the Shadow NetBIOS name server at 9.67.20.115, you would do the following steps:

Note: At the OS/2 Warp 4 client, you need to configure the client to identify itself as belonging to the Class "IBM_MOBIL_CLIENTS" which is described in 10.4.1.3, "Configuring the Dynamic IP Client for User Class Support" on page 183.

h. Now drag and drop the **Class** item on top of the Subnet 9.67.20.0 item; expand the tree and double-click on the new item. In this example, we defined a class containing dynamic IP configuration for mobile IBM clients (Figure 18).
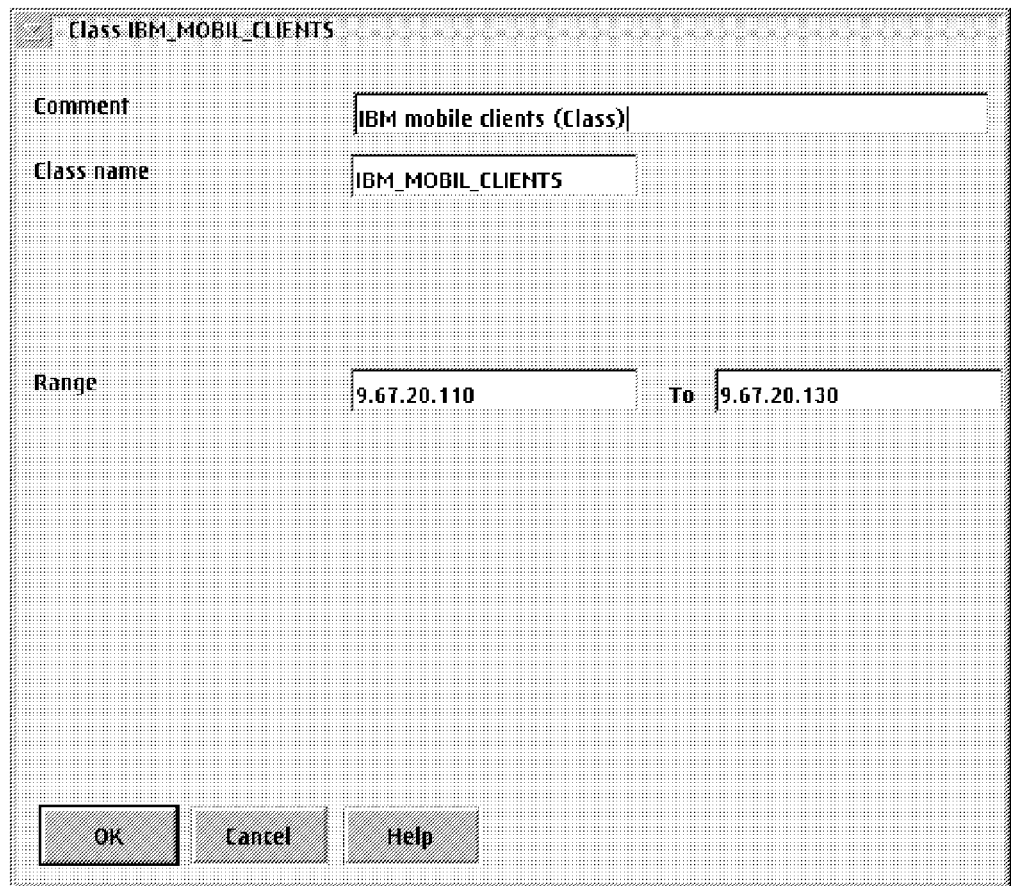
Figure 18. Class IBM_MOBIL_CLIENTS Item Window

For all IBM mobile clients defined in the step before that are configured with the TCPBEUI protocol, we will now provide information for a NetBIOS Name Server which supports datagram distribution (such as the Shadow product as described in 5.1, "The Shadow NetBIOS Name Server" on page 47 so that these clients get NetBIOS names to IP address resolution from that server.

i. Expand the (40-59) App/Service Options in the list of Predefined resources. Drag and drop **Option 46 NetBIOS over TCP/IP Node Type** on top of the IBM_MOBIL_CLIENTS item in the list of Current Configuration and double-click on it. Use the spin-button arrows to the right to provide information as shown in Figure 19.

```
Option 46 NetBIOS over TCP/IP Node Type

Comment                    NetBIOS over TCP/IP Node Type

NetBIOS node type          H

        OK          Cancel          Help
```
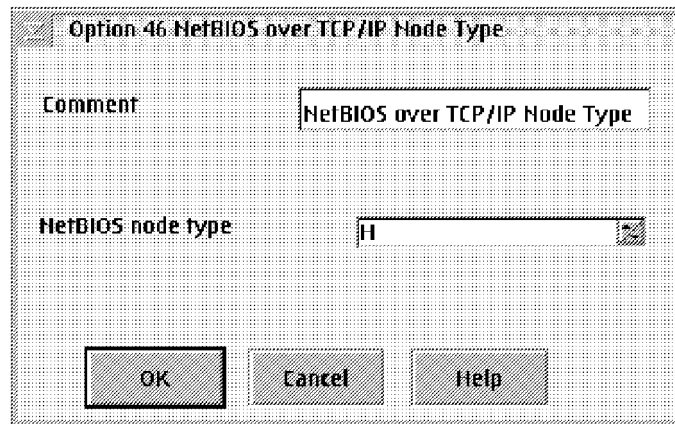
Figure 19. Option 46 NetBIOS over TCP/IP Node Type Item Window

Select **H** as the NetBIOS node type (Hybrid Mode).

j. Drag and drop **Option 45 NetBIOS over TCP/IP Datagram Distribution Server** on top of the IBM_MOBIL_CLIENTS item in the list of Current Configuration; double-click on it and provide the TCP/IP address of the NetBIOS Name Server (in our example it is 9.67.20.115).

Note: WINS as a NetBIOS Name Server does not support datagram distribution.

Figure 20 on page 71 demonstrates an example.
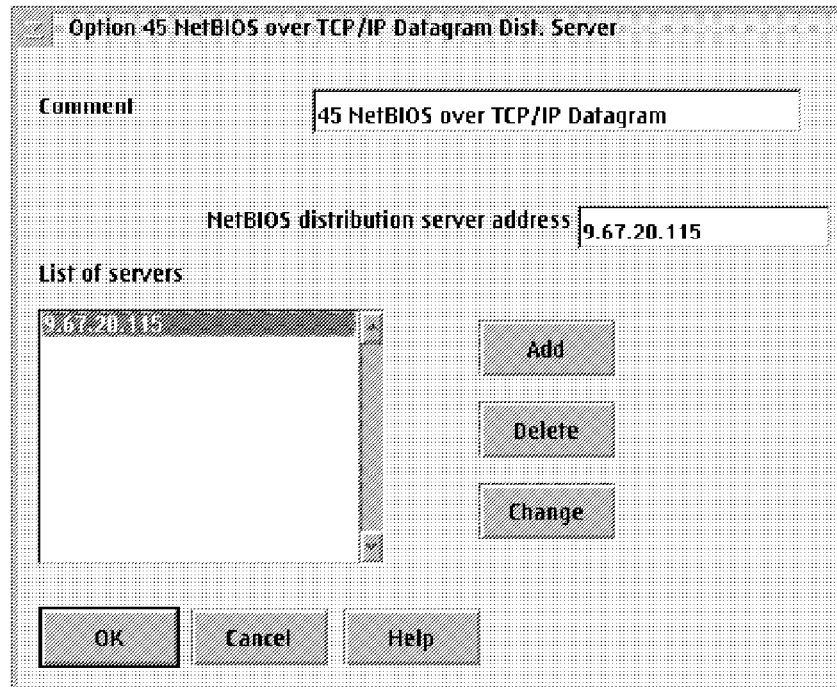
Figure 20. Option 45 NetBIOS over TCP/IP Datagram Distribution Server Item Window

    k. Last but not least, drag and drop **Option 44 NetBIOS over TCP/IP Name Server** on top of the IBM_MOBIL_CLIENTS item in the list of Current Configuration; double-click on it and provide the TCP/IP address of the NetBIOS Name Server (in our example it is 9.67.20.115) as shown in Figure 21 on page 72.
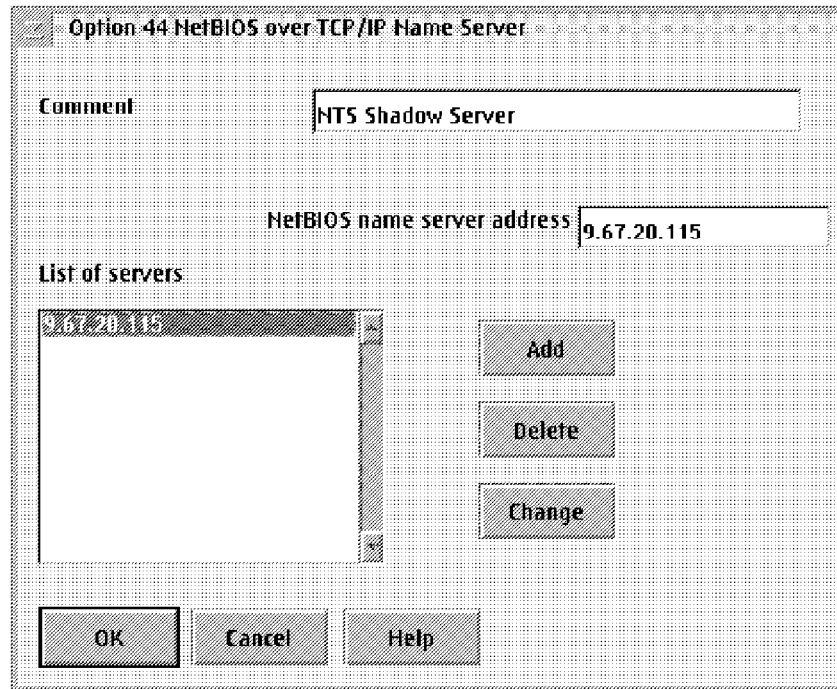
Figure 21. Option 44 NetBIOS over TCP/IP Name Server Item Window

l. Almost done, but you still need to provide server parameters. In the action bar, open the Server's pull-down menu, and select **View/change server parameters**, and provide information as shown in Figure 22 on page 73.
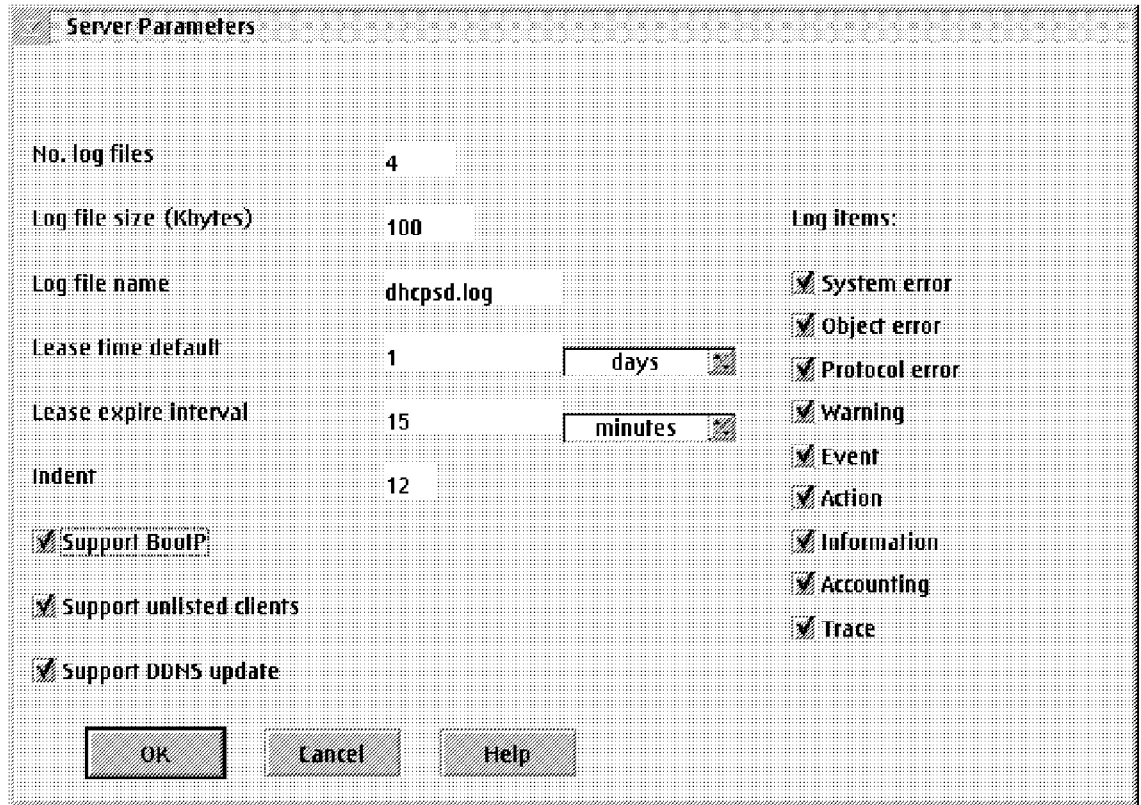
Figure 22. Server Parameters Window

You need to provide Lease time default as well as Lease expire interval information. The Leasing time will apply to all ranges of IP addresses defined in each subnet (in our case, the 9.67.20.0 subnet). Check the box for Support DDNS update so that the DHCP Server is allowed to communicate with the DDNS Server.

m. Save your configuration as DHCPSD.CFG.

n. To support DDNS updates, you have to select the respective option on the Server Parameters window. Click on the **Update DDNS data file** option on the File menu of the DHCP server configuration program. This will create the DHCPSD.DAT file where information about the primary nameserver and the encryption key to be used in DDNS updates are stored. To actually enable the DDNS update function, you must merge the information from the DHCPSD.DAT file into the DDNS.DAT file that will be created by the DDNSZONE command when you configure the DDNS server.

6.1.3 Running the DHCP Server

Within the TCP/IP folder, open the DHCP Server Services window.

Hint

We recommend you to change the properties (settings) of the DHCP
Server object. In the Parameters section, type in $-v$. This will give you
information about clients who are trying to obtain an IP address from the
DHCP Server once the server is up and running. You have a better
control over what is going on in your defined subnet(s).

Start DHCP Server by double-clicking on its object. The following
information will be presented to you, as shown in Figure 23, when the DHCP
Server is up and running, and a dynamic IP client tries to get dynamic IP
configuration information.

```
     IBM TCP/IP for WARP Server
  Dynamic Host Configuration Protocol
            Server


  Version:   3.1
  Released:  Nov 14 1995   16:31:23


Server Initialized at Mon Jun  9 12:05:05 1997
Request From:    1-0x08005a2161ae
      Type:     DISCOVER
      Status:   Offering address to the client - REPLY OFFER
      IP Addr:  9.67.20.111
      Options:  1 6 9 15 44 45 46 51 77
Request From:    1-0x08005a2161ae
      Type:     REQUEST
      Status:   Requesting a reserved address - REPLY ACK
      IP Addr:  9.67.20.111
      Options:  1 6 9 15 44 45 46 51 77
```

Figure 23. DHCP Server Window

The requesting dynamic IP client now sort of owns the offered and
acknowledged IP address. The next time the dynamic IP boots up, it will
request the same address and will get it if still available. The message that
would be displayed on your DHCP Server console, is shown in Figure 24 on
page 75.

```
Request From:     1-0x08005a2161ae
       Type:     REQUEST
       Status:   Requesting an existing lease - REPLY ACK
       IP Addr:  9.67.20.111
       Options:  1 6 9 15 44 45 46 51 77
```

Figure 24. DHCP Server Console Window

If the DHCP server returns a `No addresses available` message back to you as
shown in Figure 25, please refer to 10.4.1.3, "Configuring the Dynamic IP
Client for User Class Support" on page 183 for more information about how
to set up dynamic IP clients for certain classes. Remember, we set the
DHCP Server up for supporting classes.

```
Request From:     1-0x08005a2161ae
       Type:     DISCOVER
       Status:   No addresses available for the client - NO REPLY
```

Figure 25. DHCP Server No Address Available Message Console Window

To check what IP addresses are available, not available (N/A), or assigned
to IP clients, type the DSTAT command from an OS/2 command prompt. The
following information will be presented to you as shown in Figure 26 on
page 76.

```
Status of DHCP server maverick (9.67.20.120) as of Mon Jun  9 12:19:17 1997
IP Address      Status   Lease Time Start Time  Last Leased  ClientId
9.67.20.110     N/A
9.67.20.111     Leased     24:00:00  06/10 09:37  06/10 09:37  0x08005a2161a
9.67.20.112     Free
9.67.20.113     Free
9.67.20.114     Free
9.67.20.115     Free
9.67.20.116     Free
9.67.20.117     Free
9.67.20.118     Free
9.67.20.119     Free
9.67.20.120     N/A
9.67.20.121     Free
9.67.20.122     Free
9.67.20.123     Free
9.67.20.124     Free
9.67.20.125     Free
9.67.20.126     Free
9.67.20.127     Free
9.67.20.128     Free
9.67.20.129     Free
9.67.20.130     Free
```

Figure 26. Executed DSTAT Command Window

6.1.4 A Short Introduction to Cryptography

Since the IBM OS/2 DDNS server and client products implement not only
dynamic DNS but also DNS security functions, we briefly explain the terms
and usage of cryptographic processes.

6.1.4.1 Secret Key Cryptography

This method uses a secret key to encrypt a message. The same secret key
must be used again to decrypt the message. This means that the key must
be sent along with the message which exposes it to whoever may be
eavesdropping on the conversation. Secret keys are very fast in terms of
processing, and it is not easy to break them, even though they are exposed
through the communication process.

6.1.4.2 Public Key Cryptography

This method uses a combination of a modulus and a pair of exponents,
called the public key and the private key. Exponents and modulus must be
used together to encrypt or decrypt a message, but only the modulus and
the public exponent are communicated since they are important to everyone
who wants to send or receive encrypted messages using this method. The
private exponent will never be publicly exposed. This ensures that no one

else can decrypt messages that have been intended for a specified recipient, nor can anyone else disguise as that recipient in order to intercept a message.

6.1.4.3 Encryption and Authentication

Encryption means that a message will be scrambled before it can be sent over a communications link. The plain message itself will never be sent in order to ensure privacy. Authentication is used to ensure that a message has indeed originated from the source which is specified in the message, and that the message has not been altered in transit. It additionally serves the purpose of non-repudiation, which means that whoever has digitally signed a message cannot claim later that he or she has not done so. In this case, the plain message itself will be sent since there is no need for privacy. The message will also be used to generate a digital signature by using one of the aforementioned cryptographic methods, preferably public keys.

6.1.4.4 Hash Functions

A hash function is a computation that takes a variable-size input and returns a fixed-size string, which is called the hash value. If the hash function is one-way, that means hard to invert, it is also called a message-digest function, and the result is called a message digest. The idea is that a digest represents concisely the longer message or document from which it was computed; one can think of a message digest as a digital fingerprint of the larger document.

6.1.5 The RSA Encryption Standard

This standard public key encryption method, along with the MD5 hash function, is used with the IBM DDNS products in OS/2 Warp Server. The principle of the RSA algorithm is as follows:

1. Take two large primes, p and q.
2. Find their product n = p * q; n is called the modulus.
3. Choose a number, e, less than n and relatively prime to (p-1) * (q-1).
4. Find its inverse, d, mod (p-1) * (q-1), which means that e * d = 1 mod (p-1) * (q-1).

e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is d. The factors p and q must be kept secret or destroyed.

The following is an example of RSA privacy (encryption):

Suppose Alice wants to send a private message, m, to Bob. Alice creates the ciphertext c by exponentiating:

```
c = m^e mod n
```

where e and n are Bob's public key. To decrypt, Bob also exponentiates:

`m = c^d mod n`

and recovers the original message, m; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt.

The following is an example of RSA authentication:

Suppose Alice wants to send a signed document, m, to Bob. Alice creates a digital signature s by exponentiating:

`s = m^d mod n`

where d and n belong to Alice's key pair. She sends s and m to Bob. To verify the signature, Bob exponentiates and checks that the message, m, is recovered:

`m = s^e mod n`

where e and n belong to Alice's public key.

Thus encryption and authentication take place without any sharing of private keys: each person uses only other people's public keys and his or her own private key. Anyone can send an encrypted message or verify a signed message, using only public keys, but only someone in possession of the correct private key can decrypt or sign a message.

To make encryption methods secure, a fairly large modulus should be chosen since it becomes increasingly difficult to break a large number into factors to determine the original primes. RSA uses a minimum length of 512 bits for the modulus, which would convert to a number with approximately 155 digits.

Due to security concerns, public key systems that use a key length of more than 512 bits must not be exported from the US.

For encryption, in reality, RSA is combined with a secret-key crypto system, such as DES, to encrypt a message by means of an RSA digital envelope. Data Encryption Standard (DES) is one of the most widely used secret key algorithms and was originally developed by IBM.

Suppose Alice wishes to send an encrypted message to Bob. She first encrypts the message with DES, using a randomly chosen DES key. Then she looks up Bob's public key and uses it to encrypt the DES key. The DES-encrypted message and the RSA-encrypted DES key together form the RSA digital envelope and are sent to Bob. Upon receiving the digital

envelope, Bob decrypts the DES key with his private key, then uses the DES key to decrypt the message itself.

For authentication, in reality, RSA is combined with a hash function, such as MD5. Suppose Alice wishes to send a signed message to Bob. She uses a hash function on the message to create a message digest, which serves as a digital fingerprint of the message. She then encrypts the message digest with her RSA private key; this is the digital signature, which she sends to Bob along with the message itself. Bob, upon receiving the message and signature, decrypts the signature with Alice's public key to recover the message digest. He then hashes the message with the same hash function Alice used and compares the result to the message digest decrypted from the signature. If they are exactly equal, the signature has been successfully verified, and he can be confident that the message did indeed come from Alice. If, however, they are not equal, then the message either originated elsewhere or was altered after it was signed, and he rejects the message.

Note that for authentication, the roles of the public and private keys are converse to their roles in encryption, where the public key is used to encrypt and the private key to decrypt. In practice, the public exponent is usually much smaller than the private exponent; this means that the verification of a signature is faster than the signing. This is desirable because a message or document will only be signed by an individual once, but the signature may be verified many times.

6.1.6 Configuring and Using DDNS Server

There is no explicit configuration utility for the DDNS server as there is for the DHCP server. You can either create new DDNS server configuration files, or you can migrate an existing DNS configuration to dynamic DNS server configuration files. In this section, we show you how to configure and use a DDNS server.

Follow the steps below to create DDNS server configuration files. The files required for a minimum configuration are:

NAMED.BT   The nameserver boot file that contains the path and file names for any other configuration files. This file must be in the MPTN ETC NAMEDB directory (or wherever the ETC environment variable points to). It will be examined by the DDNS server at startup.

NAMED.DOM   The nameserver domain file that contains information about the zones for which this server will be authoritative, and all mappings from names to IP addresses (ordinary or forward name resolution).

NAMED.REV   The nameserver reverse file that contains information about the mappings from IP addresses to names (inverse or reverse name resolution).

1. Create the MPTN ETC NAMEDB directory, or create a NAMEDB directory under the directory where the ETC environment variable points to. Normally, this directory should have been created during OS/2 Warp Server installation.

2. Create the DDNS configuration files. Those files are plain ASCII files, so you can create them, for instance, with the OS/2 system editor. You can also modify the samples that are shipped with OS/2 Warp Server and contained in the TCPIP SAMPLES ETC NAMEDB directory. Normally, those sample files should also be found in the MPTN ETC NAMEDB directory.

   A nameserver boot file might look as follows:

```
;NAMED.BT file for name server configuration
;
;TYPE          DOMAIN                  SOURCE FILE of HOST
primary itsc.austin.ibm.com           c:\\mptn\\etc\\namedb\\named.dom dynam
primary 20.67.9.in-addr.arpa          c:\\mptn\\etc\\namedb\\named.rev dynam
```

Figure 27. NAMED.BT File

   On the `primary` statements, you can specify if you want to use the DDNS server in dynamic or in dynamic pre-secured mode by using either the `dynamic` or the `dynamic secure` keywords. A nameserver domain file might look as follows:

```
;
;*******************************
;*  Start of Authority Records  *
;*******************************
;
@   IN  SOA  ns-updates.maverick.itsc.austin.ibm.com.
                            ns-updates.maverick.itsc.austin.ibm.com. (

      95111601 ; Serial number for this data (yymmdd##)
      86400    ; Refresh value for secondary name servers
      300      ; Retry value for secondary name servers
      864000   ; Expire value for secondary name servers
      3600     ; Minimum TTL value
       300   ) ; dynamic update increment time
    IN  NS   ns-updates.maverick.itsc.austin.ibm.com.
;
localhost   IN A    127.0.0.1
;
ns-updates  IN A    200.200.200.2
martin      IN CNAME ns-updates
;
BPClient    IN A    200.200.200.14
;
```

Figure 28. NAMED.DOM File

Note: Connect lines 6 and 7 to a single line separated by one space.

A nameserver reverse file might look as follows:

```
;
;*******************************
;*  Start of Authority Records  *
;*******************************
;
200.200.200.in-addr.arpa.   IN  SOA ns-updates.maverick.itsc.austin.ibm.com.
                            ns-updates.maverick.itsc.austin.ibm.com. (
      95111601 ; Serial number for this data (yymmdd##)
      86400    ; Refresh value for secondary name servers
      300      ; Retry value for secondary name servers
      864000   ; Expire value for secondary name servers
      3600     ; Minimum TTL value
       300   ) ; dynamic update increment time

200.200.200.in-addr.arpa. IN  NS   ns-updates.maverick.itsc.austin.ibm.com.
;
;
; Addresses for the canonical names
;
2         IN PTR veronika.maverick.itsc.austin.ibm.com.
14        IN PTR BPClient.maverick.itsc.austin.ibm.com.
;
```

Figure 29. NAMED.REV File

Note: Connect lines 6 and 7 to a single line separated by one space.

3. Start the DDNS server and ignore any messages in the following
   `DDNSZONE` command that might instruct you to stop the server.

4. After you have created the files and placed them in the
    MPTN ETC NAMEDB directory, use the DDNSZONE command to create
   the public encryption key pairs for the zone resource records in the
   domain and reverse files. The `DDNSZONE` command also creates the
   DDNS.DAT file that contains the private encryption keys to sign any
   updates to the zone resource records in the domain and reverse files.

5. Since you configured the DHCP server for DDNS updates, add the
   information from the DHCPSD.DAT file to the DDNS.DAT file.

6. Finally, copy the SYSLOG.CNF file from the
    TCPIP SAMPLES ETC NAMEDB directory to the directory that contains
   the nameserver files. This file configures the logging options for the
   DDNS server and will also be examined at server startup. Normally, it
   should be there already.

   Note: KEY and SIG resource records as well as encryption keys always
   use a single line.

7. To start the DDNS Server, open the DDNS Server Services window and
   double-clicking on **DDNS Server**. The following information is presented
   to you as shown in Figure 30.

```
 --------------------------------------------
| IBM OS/2 Warp Domain Name Server (NAMED) |
|           TCP/IP Version 3.1           |
 --------------------------------------------

bootfile = C:\MPTN\ETC\NAMEDB\NAMED.BT
```

Figure 30. DDNS Server Window

Using DDNS as a Static DNS Server

Although Warp Server's DNS Server is a dynamic one, you also can
configure it as a static DNS Server if necessary. You can even
migrate an AIX DNS environment to Warp Server's DDNS
environment just by renaming the NAMED.Boot file to NAMED.BT.

Chapter 7. Remote Access through Point-to-Point Protocol

This chapter briefly describes IBM Enhanced Remote Access Services Connection Server for OS/2 Warp Server. This is an enhancement to Remote Access Services Connection Server — an optionally installable networking component of OS/2 Warp Server. However, unlike previous releases of LAN Distance and Remote Access Services, remote client versions do not come with this enhancement. They usually come with the operating system or are available separately, for example, the 8235 Client for OS/2.

In this chapter we will not describe how this component is installed, configured, used, or supported. This is discussed in redbook SG24-2008, titled *OS/2 Warp Server Functional Enhancements* (in press).

The discussion of client configuration is in Part 2, "Installing and Configuring IBM Networks Clients"

7.1 The Enhanced Remote Access Server for OS/2 Warp Server

For those users who are already familiar with the OS/2 Warp Server Remote Access Services, the major enhancement in IBM Enhanced Remote Access Services for OS/2 Warp Server is Point-to-Point Protocol (PPP) support.

The Enhanced Remote Access Server for OS/2 Warp Server allows point-to-point protocol (PPP) clients, including Windows NT, Windows 95, IBM 8235 and Shiva users, to remotely access an OS/2 Warp Server as if they were locally attached to the server. As a result, customers or employees traveling on the road or working in branch offices with multiple operating systems will have the same access to network resources and files as those working on-site.

The Enhanced Remote Access Server delivers new levels of performance and security and reduces the cost of ownership by leveraging customer's current client/server investments. Combined with recent Windows 95 and NT client enhancements, it makes OS/2 Warp Server the premier server operating system for customers running OS/2 Warp, as well as Windows 95 and NT clients.

IBM's Remote Access Server for Warp previously supported network-attached clients only. Now, however, users can dial into the Remote Access Server by modem from home or on-the-road to obtain the same access to desktop and network applications that is available to

83

network-attached clients. The PPP server can be downloaded from IBM's Software Choice home page at the following Web site:

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

Make sure you have the OS/2 Feature Install Version 1.1 product installed before you install the PPP server.

7.1.1 Client Support

The IBM Enhanced Remote Access Services 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 IBM Enhanced Remote Access Services Connection Server for OS/2 Warp Server will now support the following clients:

- Windows 95 PPP version 4.0.
- Windows NT PPP version 4.0.
- IBM OS/2 Internet Dialer.
- IBM 8235 DIALs for OS/2 Version 4.5.2 and patch 4. You can get the patch from the World Wide Web (WWW) at the following Web site:

  `http://www.networking.ibm.com/nes/nes8235.htm`
- IBM OS/2 LAN Distance.
- IBM OS/2 Remote Access Services.
- IBM 8235 DIALs for Windows version 4.1.
- LAN Distance for Windows 3.1.
- Remote Access Services for Windows 3.1.

The PPP connection support included with IBM Enhanced Remote Access Services for for OS/2 Warp Server ensures long-term compatibility with other Internet-based products on a variety of computer platforms.

7.1.2 PPP Clients System Requirements

The PPP client system requires 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.

   - 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.

7.1.3 PPP Restrictions

The following restrictions apply to PPP:

- Callback is not supported for PPP clients.

- An IBM Enhanced Remote Access Services 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 ping LAN Distance and Remote Access Services clients. LAN Distance and Remote Access Services clients cannot ping PPP clients.

- PPP clients can run LAN applications and networking software that use TCP/IP.

- 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.

- Native NetBIOS support is not available to PPP clients. To access SMB servers such as OS/2 Warp Server, clients need to have NetBIOS over TCP/IP installed and configured.

Chapter 8. IBM Neighborhood Browser Enabler for OS/2 Warp Server

This chapter describes installing and configuring the IBM Neighborhood Browser Enabler for OS/2 Warp Server. This enhancement for OS/2 Warp Server can be downloaded from the following Web site:

```
http://www.software.ibm.com/os/warp/downloads/
```

8.1 Introducing IBM Neighborhood Browser Enabler for OS/2 Warp Server

The IBM Neighborhood Browser Enabler for OS/2 Warp Server, referred to Neighborhood Browser Enabler from now on, enables your OS/2 Warp Server to function as a master browser for Windows, Windows 95, and Windows NT clients. As mentioned earlier, if you are using Windows 95 or Windows NT clients in an OS/2 Warp Server domain, and not using the Neighborhood Browser Enabler, you have to set one master browser per segment to be able to browse OS/2 Warp Server domain resources from Windows 95 and Windows NT. Steps to enable a Windows 95 workstation to be a master browser are described in 12.7.1.2, "Setting a Windows 95 Workstation to Be the Master Browser" on page 274. The master browser workstation has to be up and running all the time; it would be better to run this function on a server machine.

We recommend installing the Neighborhood Browser Enabler on the domain controller machine. However you can install it on any OS/2 Warp Server machine, but only one can be the master browser at one time. Installing Neighborhood Browser Enabler on more than one server reduces the network traffic between the master browser and clients. All the other servers running the Neighborhood Browser Enabler service are backup browsers. For performance considerations, it is recommended to install Neighborhood Browser Enabler for every 20 servers in the domain. Depending on the installation, this figure may vary.

> **CSD IP08260 Required!**
>
> If you are using OS/2 Warp Server 4.0, the CSD level IP08260 or better has to be applied. If you are using the SMP version of OS/2 Warp Server, refer to the README.1ST file found in the ZIP package. Install will not proceed unless one of the above is present.

8.1.1 Installing Neighborhood Browser Enabler

To install the Neighborhood Browser Enabler, follow the steps below:

1. Create a temporary directory on your OS/2 Warp Server drive by typing

```
MD C: BROWSER4
```

from an OS/2 command prompt.

2. Download the Neighborhood Browser Enabler BROWSER4.ZIP file either from IBM's anonymous ftp-server from address:

```
ftp://service.boulder.ibm.com
```

or

```
http://www.software.ibm.com/os/warp/downloads/
```

and save the file in the directory created.

3. Open the directory created and unzip the package to the directory by typing:

```
UNZIP BROWSER4.ZIP
```

You can use either `UNZIP` or `PKUNZIP2` commands, just pick your favorite.

4. Read the README.1ST file.

5. If the LAN Server is running, stop the server by typing

```
NET STOP SERVER
```

6. Enter the command

```
BRINST
```

at the OS/2 command prompt which installs deliverables into appropriate directories:

```
\IBMLAN\SERVICES\BROWSER.EXE
\IBMLAN\NETLIB\BROWSE32.DLL
\IBMLAN\NETLIB\BROWSE16.DLL
```

7. A reboot may be necessary depending on LAN Server's service level.

The Neighborhood Browser Enabler installation program copies the browser files to the appropriate directories, backs up the existing IBMLAN.INI file to IBMLAN.IBR, backs up some LAN server components and replaces them with new components and finally modifies the IBMLAN.INI file so that the browser service starts automatically when the server service is started.

The updated IBMLAN.INI file contains a new section:

```
[browser]
  maintainserverlist = austo
```

and a new service called `BROWSER` in the `SRVSERVICES` line, and it extends the path to new executable in [services] section.

Depending on service level, selected base LAN Server modules are backed up, then newer versions are installed:

```
\IBMLAN\SERVICES\NETSERVR.EXE
\IBMLAN\SERVICES\NETSVINI.EXE
\IBMLAN\NETPROG\NETWKSTA.200
\IBM386FS\HPFS386.IFS
\MUGLIB\DLL\NETAPI32.DLL
```

Note: The file \MUGLIB\DLL\NETAPI32.DLL is replaced only on OS/2 Warp Server SMP IP08500.

You can start the Neighborhood Browser Enabler service at any time by entering the command:

```
NET START BROWSER
```

or stop the service by using the command:

```
NET STOP BROWSER
```

Only One Subnet Supported

The Neighborhood Browser Enabler product supports Windows clients only within a single subnet; Windows clients can browse OS/2 Warp Server domain resources only in their own IP subnet.

When Neighborhood Browser Enabler is installed on the OS/2 Warp Server domain contoller machine, the domain controller also recognizes and answers to NetBIOS name types used by Microsoft networks but not by IBM networks. These types include domain controller, domain master browser, master browser, and browser service elections. In cases where Microsoft Windows clients are attached to the network, we recommend installing the Neighborhood Browser Enabler and using the appropriate IBM Networks Client for Windows.

8.1.2 How does Browser Service Work

The following lists details of the operation of Neighborhood Browser Enabler:

- Starts and stops as a LAN Server service
  - Requires server service to be started; typically starts automatically when the server service starts.
- Installation to one OS/2 Warp Server machine makes all servers in the domain visible to Windows clients.
- Runs in one of three modes:

- Master Browser

    - Registers unique NetBIOS names.

    - Periodically announces as a domain master browser.

    - Listens for other machine's announcements to unique NetBIOS names.

    - Collects announcement information.

    - Makes information about "announcers" available to clients.

    - Keeps announcement information current.

    - Designates backup browsers.

    - Participates in elections.

- Backup Browser

    - Periodically retrieves "announcers" list from master browser.

    - Makes information about "announcers" available to clients.

    - Periodically announces as backup browser.

    - Participates in elections.

- Potential Browser

    - Periodically announces as potential browser.

    - Participates in elections.

- Mode is determined dynamically by an election process.

- Installation on domain controller ensures mode is master browser.

- Mode is not known by end user.

  - Operation on server is essentially invisible.

- Effects of BROWSER service seen on Windows clients.

  - OS/2 Warp Server domains running the BROWSER service become visible within Network Neighborhood object

  - Clients can browse shared resources.

- Master Browser Mode.

  - Registers the following NetBIOS names:

      - domain [1Eh]

        A group name used for browser-to-browser communication.

      - domain [1Dh]

A unique name used by clients to communicate with the master browser.

- [\x01\x02__MSBROWSE__\x02\x01]

   A group name used for workgroup announcements.

- If server is domain controller, it also registers:

  - domain [1Bh]   (unique name)

  - domain [1Ch]   (group name)

- Receives and processes datagrams sent to these NetBIOS names.

- Creates and maintains lists of servers and domains that have announced to the master.

- Makes server and domain lists available to requesters through NetServerEnum2 API calls.

- Keeps track of the number of backup browsers and potential browsers in the domain; when another backup is needed, sends a BE_BACKUP datagram to a potential browser.

- Periodically reviews server and domain lists and removes entries that have not announced for three announcement intervals.

• Backup Browser Mode

- Registers the domain [1Eh] NetBIOS name.

- Retreieves a list of "announcers" by remoting a NetServerEnum2 API to the master.

- Responds to NetServerEnum2 API calls from clients with data retrieved from master.

- If data cannot be retrieved from master, initiates an election.

- Announces periodically.

• Potential Browser Mode

- Registers the domain [1Eh] NetBIOS name.

- Announces periodically.

8.1.3 Calling Elections

Elections are called when:

• BROWSER service requests announcement from domain master at startup.

• If master exists and BROWSER is starting on domain controller, an election is called for:

- Backup browsers cannot find master to obtain server list.

- Windows clients cannot find master to obtain backup list.

- Election datagrams are sent to domain [1Eh] NetBIOS name.

- Datagrams contain sender's version and election criteria:

  - Version is 2 (same as NT server's version).

  - Criteria is an unsigned log with various bits set to indicate server's role, services is it running.

- Sender's version and criteria compared with those of local machine:

  - Server with highest criteria wins election and becomes master.

  - Losing servers become potential browsers.

  - Tie breakers:

    - Lenght of time BROWSER service has been running.

    - Lexical value of server's name

8.1.4 Additional NetBIOS Names on LAN Adapter

The following NetBIOS names are bound to a LAN Adapter, when IBM Neighborhood Browser Enabler for OS/2 Warp Server is started at the domain controller:

Table 4 (Page 1 of 2). Additional Registered NetBIOS Names w/Neighborhood Browser Enabler		
Name	**Name #**	**Status**
ITSCSV00 0x49545343535630302020202020202020**00**	002	04 Unique
ITSCSV00 0x49545343535630302020202020202020**03**	003	04 Unique
ITSCAUS 0x49545343415553202020202020202020**00**	004	84 Group
ITSCSV00 0x49545343535630302020202020202020**20**	005	04 Unique
ITSCAUS 0x49545343415553202020202020202020**1e**	006	84 Group
ITSCAUS 0x495453434155532020202020202020**1c**	007	84 Group

Table 4 (Page 2 of 2). Additional Registered NetBIOS Names w/Neighborhood Browser Enabler		
Name	**Name #**	**Status**
ITSCAUS ¬ 0x49545343415553202020202020202**1b**	008	04 Unique
ITSCAUS 0x49545343415553202020202020202**1d**	01F	04 Unique
ADMIN_DC 0x41444d494e5f4443202020202020202**03**	00C	04 Unique
__MSBROWSE__ 0x01025f5f4d5342524f5753455f5f02**01**	020	84 Group
Note: The 16th-byte value is highlighted. The domain name is ITSCAUS, the servername is ITSCSV00, and the user ID logged on to the domain controller is ADMIN_DC.		

Chapter 9. IBM Networks Clients File and Print Graphical User Interface

9.1 Common GUI Features and Functions

The new IBM Networks Clients adds a number of features and functions that previously were unavailable for Windows 95 and Windows NT users connected to an OS/2 Warp Server domain, such as:

- Logon verification
- Logon assignments
- User profiles
- Home directory connection
- Use of aliases
- Shared applications
- DASD limits (directory limits)
- Command line administration

9.1.1 GUI Overview

The Graphical User Interface (GUI) is shown in Figure 31:
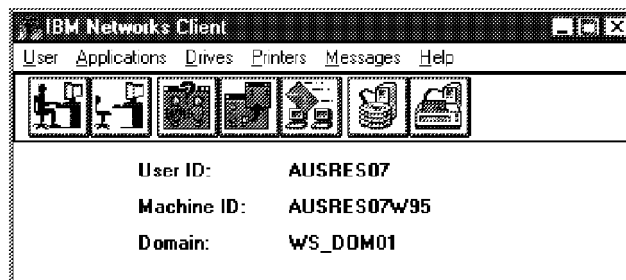
Figure 31. The IBM Networks Client GUI (Windows 95 Version)

In the Windows NT version of the GUI, there are no functions for Logon/Logoff; in the DOS LAN Services version, Peer functions are added. Otherwise, the look and feel of the GUI is much the same throughout. The available icons are discussed in Table 5 on page 96. (These, and a few other functions are also available via the menu pull-downs.)

Note: Specific GUI functions for Windows NT are discussed in section 13.6, "Client-Specific Features and Functions" on page 346; the Windows NT version of the GUI is shown in Figure 184 on page 328.

Table 5. IBM Networks Clients — Icon Overview		
Icon	**Function**	**Comments**
	Logon	The OS/2 Warp Server domain logon will be executed, you will get access to appropriate domain resources after successful validation.
	Logoff	Logoff from the OS/2 Warp Server domain.
	Logged-on Users	A list of logged-on users is displayed; you can send a message to any user in the list.
	Shared Applications	If shared network applications exist on the OS/2 Warp Server domain, they can be enabled here.
	Drive Connections	A listing of your current network drive connections. You can add or delete connections.
	Printer Connections	A listing of your current network printer connections. You can add or delete connections.
	Network Messaging	You can send messages to specific user Ids and to all users in a domain. Broadcast function is not supported.
	User's Guide	The User's Guide for the installed client.
	DASD Limits	Lets you check eventual directory limits for your home directory (or any other available directory on the domain).
	User's Guide	The User's Guide for the installed client (Primary or Coordinated).
	Drive Sharing	DLS Peer function, shares selected drives/directories.
	Printer Sharing	DLS Peer function, shares selected printers.
	Printer Manager	Lets you manage selected printers defined at the OS/2 Warp Server domain.

9.1.2 Logon Verification

When the new network client is installed, the user ID and password are appropriately set (synchronized, in the case of the IBM Networks Coordinated Logon Client for Windows NT 4.0) and the workstation is rebooted. The logon is now validated and verified by the OS/2 Warp Server domain defined during the client install. (For an example on this definition, see topic 13.2.1.2, "Installing from Diskette" on page 323, steps 9 and 10.) The logon verification is essential for the other functions discussed here.

9.1.3 Logon Assignments

The new IBM Networks Clients now recognize the logon assignments as defined for an user ID in the OS/2 Warp Server domain. However, there is no longer any need to connect separately to common OS/2 Warp Server resources. Of course, this can still be done if desired, either through this client GUI (as shown in Figure 32 and Figure 33 on page 98), the system GUI or the system command line interface.
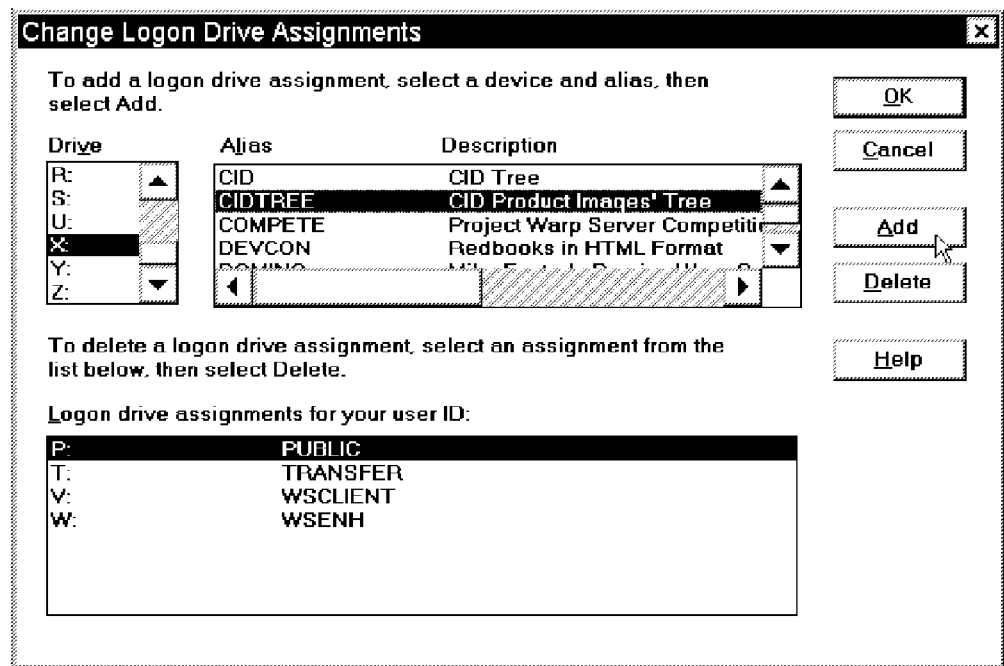
Figure 32. Change Logon Drive Assignments
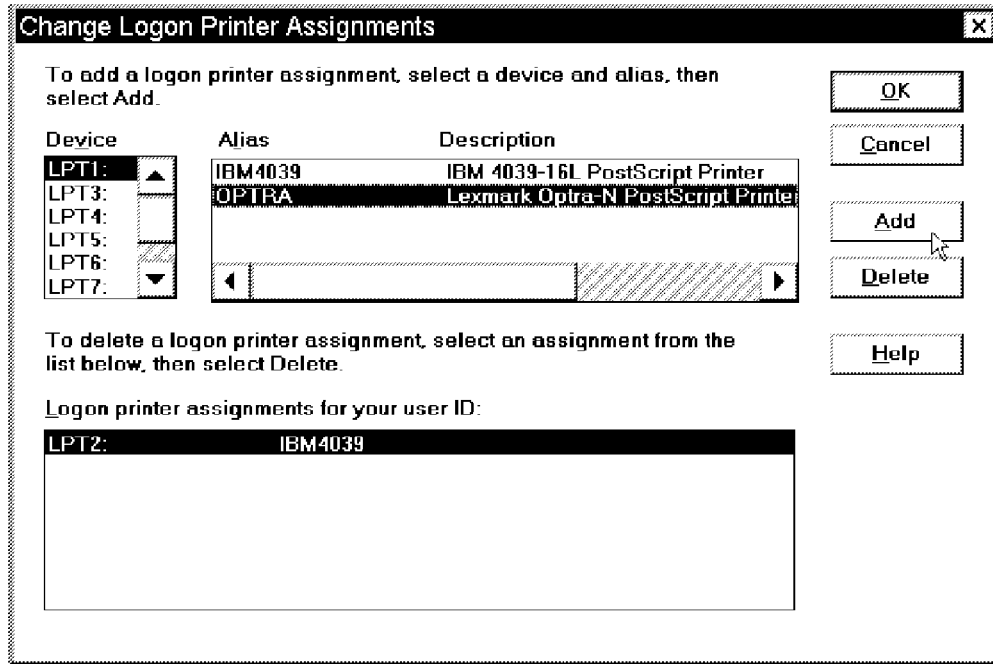
Figure 33. Change Logon Printer Assignments

9.1.4 User Profiles

When user profiles (and logon scripts) are set up, they will execute after the logon validation on the OS/2 Warp Server domain. A user profile is created on the logon server after first logon, but an eventual locally stored profile can be used if desired. (For Windows NT there are some implications to this, discussed in topic 13.6.1, "User Profiles Support" on page 347.)

9.1.4.1 User Profile vs PROFILE.BAT

We want to make sure that user profiles and the PROFILE.BAT file are different. While a user profile is a Windows 95 function that saves things like user's desktop wallpaper and color scheme, display settings, file sharing restrictions, and application restrictions, the PROFILE.BAT that resides in each user's home directory in the OS/2 Warp Server domain enables you to include commands that are executed after a successful logon. The following is an example of a PROFILE.BAT file:

```
@ECHO OFF
ECHO Executing commands after you have been successfully logged on ...
ECHO.
ECHO Assigning the Optra Network Printer as your local LPT1 Printer ...
NET USE LPT1: \\ITSCPS00\OPTRA  >NUL
ECHO.
ECHO Checking for the existence of a batch file to be executed ...
IF EXIST H:\LANUSER.BAT CALL H:\LANUSER.BAT
ECHO.
ECHO Exiting PROFILE.BAT
```

Figure 34. PROFILE.BAT File

Notes:

1. Printer assignments are usually done through the logon assignments function in OS/2 Warp Server.

2. If users want to have their own profiles run at startup time you can check for a user specific batch file stored in the user's home directory. In the example shown above, the file checked would be LANUSER.BAT in the user's home directory H:.

9.1.5 Home Directory Connection

If a home directory is defined for the user, a connection to it will be established after successful logon validation. Through the GUI, you can identify the OS/2 Warp Server hosting your home directory by clicking [**Users — Change user comment...**], as shown in Figure 35:
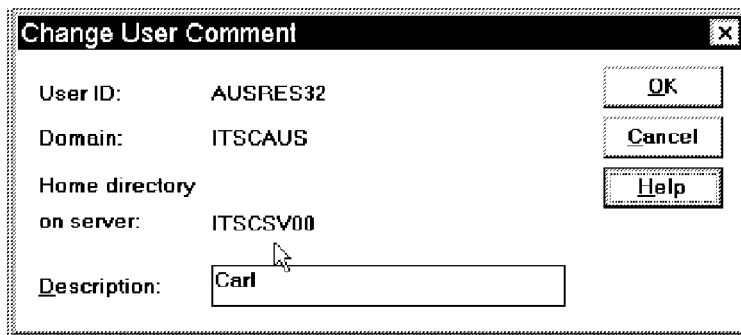
Figure 35. Change User Comment — Identifying the Home Directory

The home directory in the OS/2 Warp Server domain might be subject to limitation of disk space, as discussed in topic 9.1.7, "DASD Limits (Directory Limits)" on page 100.

9.1.6 Shared Applications

The Windows 95/Windows NT user can now run DOS/Windows shared applications on OS/2 Warp Server domains. There is no longer any need to install commonly used DOS/Windows applications locally on the workstation. (Specific Windows 95/Windows NT applications are best run off a Windows NT Server.)

The enabling of shared applications may vary across the IBM Networks Clients, details can be found in the respective chapters. More client-specific information is available through the online help function.

9.1.7 DASD Limits (Directory Limits)

The new IBM Networks Clients recognize eventual directory limits (DASD limits) as set by the OS/2 Warp Server administrator.

```
┌─ Tip to OS/2 Warp Server Administrators ─────────────────────────┐
│                                                                   │
│  Tired of users flooding precious server disk space with data that is: │
│                                                                   │
│    · Obsolete?                                                    │
│                                                                   │
│    · Redundant?                                                   │
│                                                                   │
│    · Not job-related?                                             │
│                                                                   │
│    · Otherwise unappropriate?                                     │
│                                                                   │
│  By implementing this unique OS/2 Warp Server feature, you can handle │
│  the problem! Learn more about it by checking out the OS/2 Warp Server │
│  online manual *Network Administration Tasks*, section *Limiting Space* │
│  *within Directories.*                                            │
│                                                                   │
└───────────────────────────────────────────────────────────────────┘
```

To identify the limits, proceed as follows:

1. Open the GUI by clicking [**Start — Programs — IBM Networks Client (Common) — IBM Networks Client**].

2. Select **Drives** on the main menu pull-down

3. Select **Directory Limits**, as shown in Figure 36 on page 101.
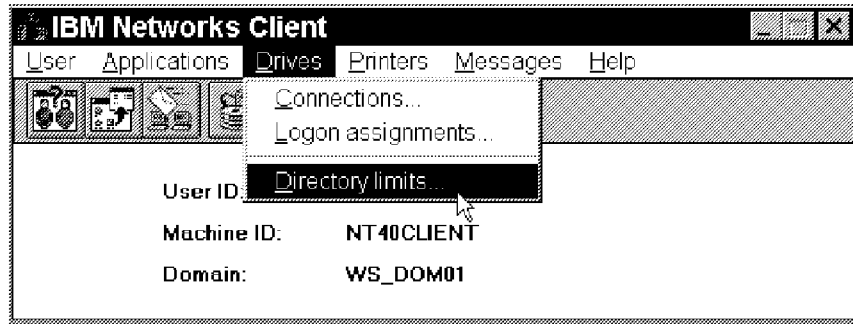
Figure 36. Selecting Directory Limits

4. A list box of possible drives to check is now displayed, see Figure 37. In this example, the home directory (U: here) is being checked.
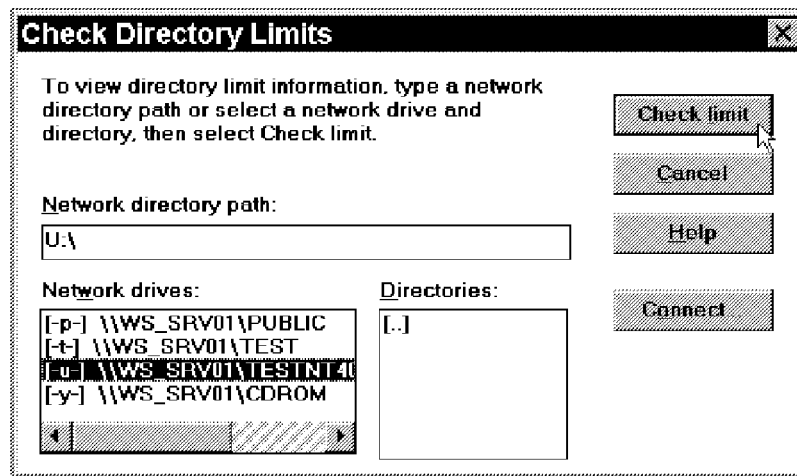
Figure 37. Check Directory Limits — Selecting directory

5. Select **Check limit** and an information panel is displayed containing statistical information related to limitations of disk space (See Figure 38 on page 102; the listed information corresponds exactly to what the OS/2 Warp Server Administrator has set for this particular drive).
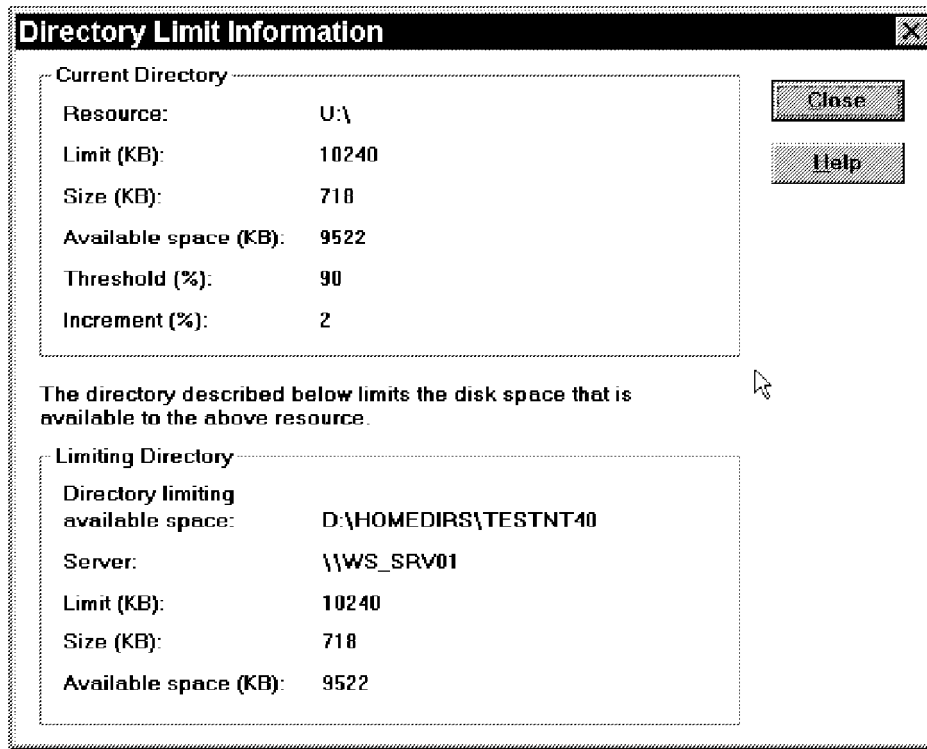
Figure 38. Directory Limit Information

9.2 Customizing the DLS GUI

As the network administrator you can customize the appearance of the
graphical user interface (GUI), restrict user access to menu bar items, or
even hide the GUI so the user can only log on and log off. You will find this
useful when you want to provide a standard workstation configuration
tailored to enable users to perform their job while preventing them from
modifying their logon assignments or connections.

To customize the GUI, follow these steps:

1. Use an ASCII editor to create a file named \WINDOWS\WDLS.INI.

2. In the WDLS.INI file include just the heading sections with the entries
   you want to change. Figure 39 on page 103 shows a sample WDLS.INI
   file containing all headings and entries.

3. Optionally, you can use the ATTRIB command to hide the WDLS.INI file,
   thereby reducing the possibility that a user can make changes to the
   file.

```
[MenuBar]
User=1
UserComment=1
Applications=1
Drives=1
DriveAssignments=1
Printers=1
PrinterAssignments=1
Messages=1
Help=1

[MainWindow]
HideMainWindow=0
ShowNormalAtStartup=1
ShowNormalAtLogon=1
LogonAtStartup=1
Toolbar=1
```

Figure 39. WDLS.INI File to Customize the DLS GUI

In the WDLS.INI file, setting 0 disables the item whereas setting 1 enables the item and is the default. The [MenuBar] section controls the menu bar items on the main window. The section [MainWindow] has the following controls:

Parameter	Description	Valid Values	Default Value
Table 6 (Page 1 of 2). WDLS.INI Parameter Values			
HideMainWindow	Hides the main window completely. This enables you to provide only logon and logoff functions by creating program icons that call the WDLS.EXE, WDLS95.EXE, or WDLSNT.EXE file with the appropriate command line parameters.	0, 1	0
ShowNormalAtStartup	Controls how the main window behaves when the user starts Windows, Windows 95, or Windows NT. The default behavior causes the window to display centered on the desktop. The =0 setting causes the main window to be displayed as a minimized icon until the user selects the icon. Then the main window is displayed centered on the desktop.	0, 1	1

Table 6 (Page 2 of 2). WDLS.INI Parameter Values			
Parameter	**Description**	**Valid Values**	**Default Value**
ShowNormalAtLogon	Controls how the main window behaves when a user logs on. The default behavior causes the main window to display centered on the desktop. The =0 setting causes the main window to be displayed as a minimized icon until the user selects the icon. Then the main window is displayed centered on the desktop.	0, 1	1
LogonAtStartup	Controls the logon window at startup. The =0 setting suppresses the logon window at startup .	0, 1	1
Toolbar	Controls the toolbar on the main window. The =0 setting suppresses the toolbar from being displayed.	0, 1	1

For example, if you want to disable the Drives Logon Assignments and Printer Logon Assignments windows, the WDLS.INI file must contain the following entries:

```
[MenuBar]
DriveAssignments=0
PrinterAssignments=0
```

Part 2. Installing and Configuring IBM Networks Clients

Chapter 10. OS/2 Warp 4

This chapter describes installing and configuring OS/2 Warp 4 File and Print Services in a plain NetBEUI and TCP/IP environment, dynamic TCP/IP:

- Dynamic Host Configuration Protocol (DHCP)

- Dynamic Domain Name Server (DDNS)

- NetBIOS Names Server (NBNS)

and Remote Access Services using the Point-to-Point Protocol (PPP) that comes with the IBM 8235 client dialing into an OS/2 Warp Server Remote Connection Server.

10.1 OS/2 Warp File and Print Client

File and Print Client is the component of OS/2 Warp 4 that allows you to connect to machines running OS/2 Warp Server on a LAN (Local Area Network), and use hardware and software resources (printers, directories, files, applications and serial devices) across the network.

It also lets you do peer networking, which means that you are allowed to share your own resources with other workstations on the network and access other systems' resources. These other systems must be running software capable of handling peer services, such as other OS/2 Warp 4 workstations or a Windows 95 machine.

10.2 Installing and Configuring OS/2 Warp 4

There are many methods of installing the OS/2 Warp File and Print Client of OS/2 Warp 4. The simplest way is to take advantage of the installation procedure of the networking components that is integrated into the OS/2 Warp installation. However, if you have not selected to install the networking components during OS/2 Warp installation time, you can always install them with the Selective Install for Networking object that resides in the System Setup's Install/Remove folder. The latter is the installation method described below.

The installation can be performed locally from a CD-ROM or remotely through the LAN. We consider the former as the default method for installing the networking components.

10.2.1 Installation Requirements

OS/2 Warp File and Print Client requires a machine running OS/2 Warp 4 in order to be installed. Although processor, RAM memory and free hard disk space requirements can vary depending on the user-selected options, applications and data installed, for getting an acceptable performance of the networking components we recommend using a machine with at least a 486 66 MHz processor, 24 MB of memory and 300 MB of free hard disk space.

You should also have a supported network adapter. A complete list of supported adapter cards and information on MAC (Media Access Control) drivers can be found in the READMAC.TXT file located in IBMCOM MACS directory on a system installed with MPTS (Multi-Protocol and Transport Services). If you have not installed OS/2 Warp 4 yet, you can extract this file from the product CD-ROM by unzipping the MACS.ZIP file located in \CID\IMG\MPTS\IBMCOM\MACS directory.

10.2.2 Installing OS/2 Warp File and Print Client

As we will describe the default method of installing the OS/2 Warp File and Print Client, you need to have your OS/2 Warp 4 product CD-ROM in the CD-ROM drive of your machine.

Open the **Install/Remove** folder from the **System Setup** folder located in the **OS/2 System** folder on the **Desktop** to see all the install and uninstall options available, as shown in Figure 40.
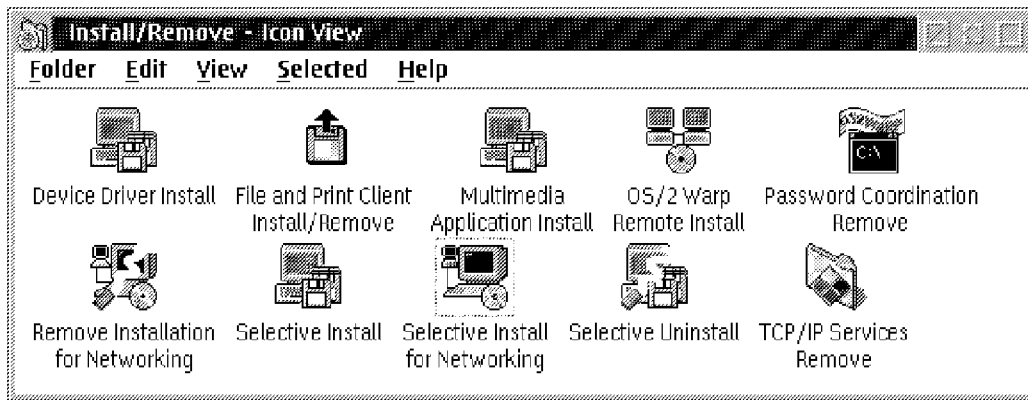
Figure 40. Install/Remove Folder

Select **Selective Install for Networking** and the Installing IBM OS/2 Warp window is displayed as shown in Figure 41 on page 109.
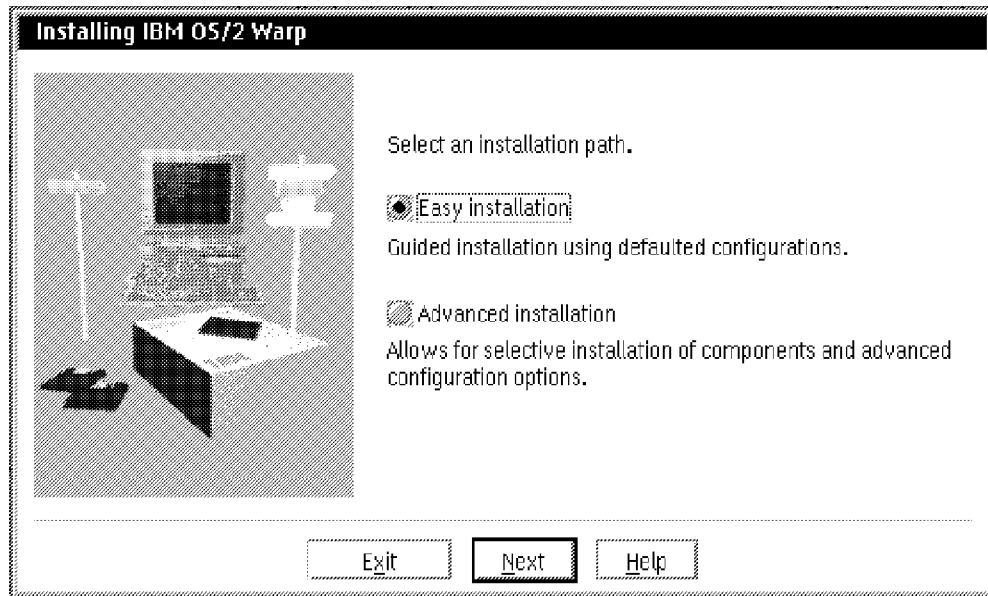
Figure 41. Installing IBM OS/2 Warp Window

INSTALL.CMD

If in OS/2 Warp 4 installation you do not select to install any networking components, the **Install/Remove** folder, shown in Figure 40 on page 108, does not contain the icons related to the selective installation for networking.

In this case, execute the INSTALL command from the root directory of the OS/2 Warp 4 product CD-ROM to start the selective installation for networking procedure. You are also presented with the Installing IBM OS/2 Warp window as shown in Figure 41.

In the Installing IBM OS/2 Warp window you are asked to select the installation path that you want to use. The **Easy Installation** program prompts you with installation questions for all networking components and default values that are selected for you. The **Advanced Installation** option lets you choose among all components of OS/2 Warp 4 and you can customize your installation with values that you select or supply.

Which Installation Path Should You Select?

The following information might help you decide which is the best installation path, according to your needs:

- The Easy Installation path allows you to configure only one adapter for your workstation. If you need to configure multiple adapters, you should use the Advanced Installation path.

- The installation of the LAN Server Administration utilities can only be perfomed by selecting the Advanced Installation path. These utilities allow you to administer your OS/2 Warp Server from your OS/2 Warp 4 workstation.

- While the Easy Installation path prompts you through the configuration windows of all the networking components available in OS/2 Warp 4, the Advanced Installation path provides an initial menu that allows you to select only the services that you need.

Generally, we recommend that you choose the Advanced Installation path. Although it requires some additional networking knowledge on your part, it gives you more control over the way the installation program of OS/2 Warp 4 sets up your networking components.

10.2.3 Easy Installation

This section guides you through the Easy Installation. If you selected Advanced Installation you may proceed with 10.2.4, "Advanced Installation" on page 123.

By selecting the **Easy Installation** option, the Type of Activities window will be displayed as shown in Figure 42 on page 111.
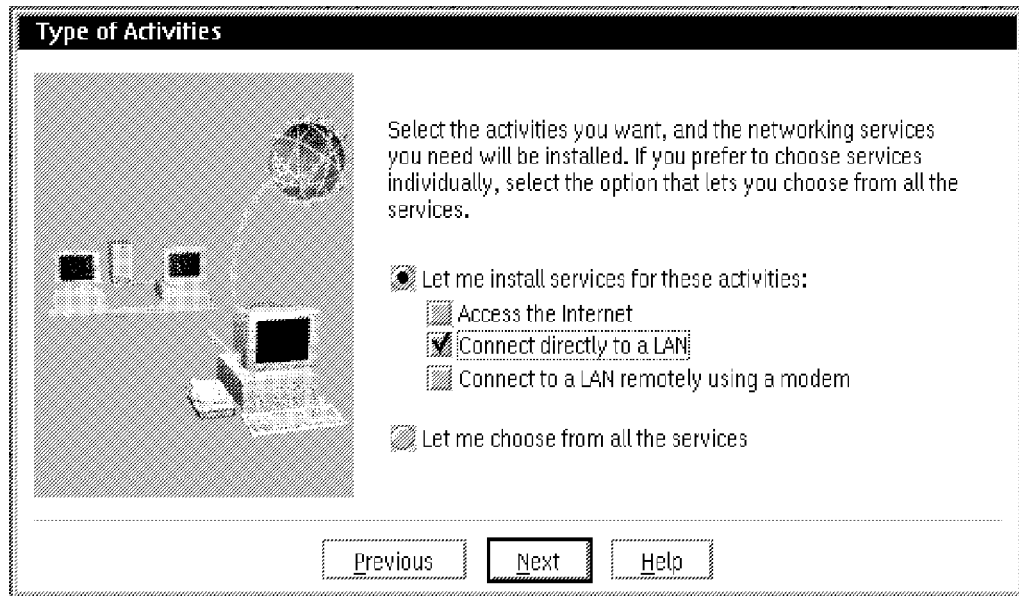
Figure 42. Easy Installation Path - Type of Activities Window

If you select the **Let me choose from all the services** option, you will be guided through a number of windows with questions about all the available networking services in the Easy Installation path: File and Print Client, NetWare Client, Mobile Office Services, System Management Client, TCP/IP Services and Remote Access Client.

For this scenario we only need to install the **File and Print Client**, so it is preferable to select the **Connect directly to a LAN** option from the **Let me install services for these activities** list. In doing so, the File and Print Client window will be displayed, as shown in Figure 43 on page 112.
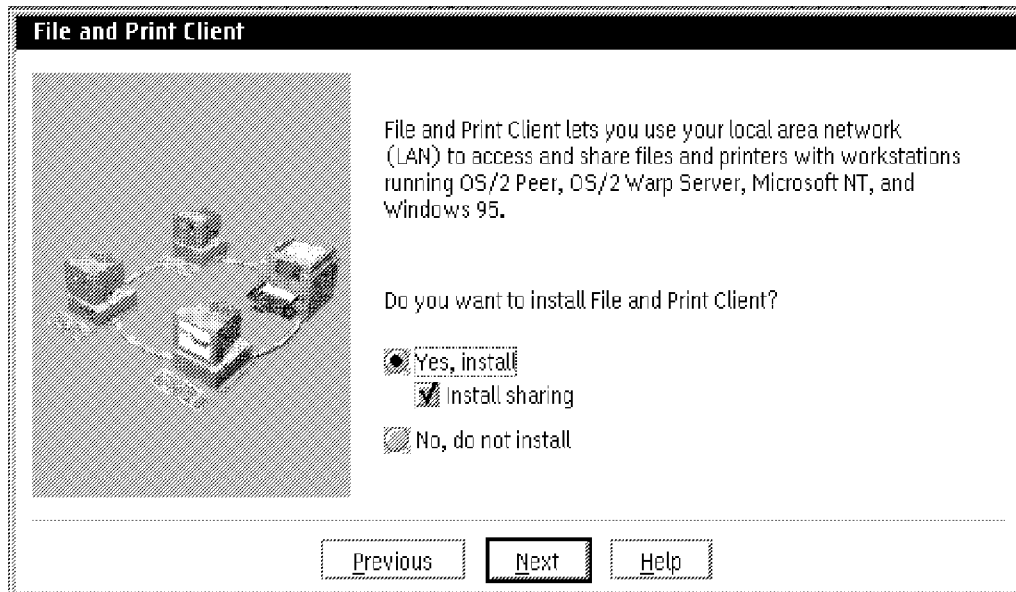
Figure 43. Easy Installation Path - File and Print Client Window

Select **Yes, install** option if you want to install the File and Print Client. If you want to allow users on other workstations to use files, printers, serial devices and applications that are on your workstation, check the check-box for **Install sharing**, too.

Select the **Next** button to arrive at the Specify Workstation Name window, shown in Figure 44 to specify the workstation name and description.
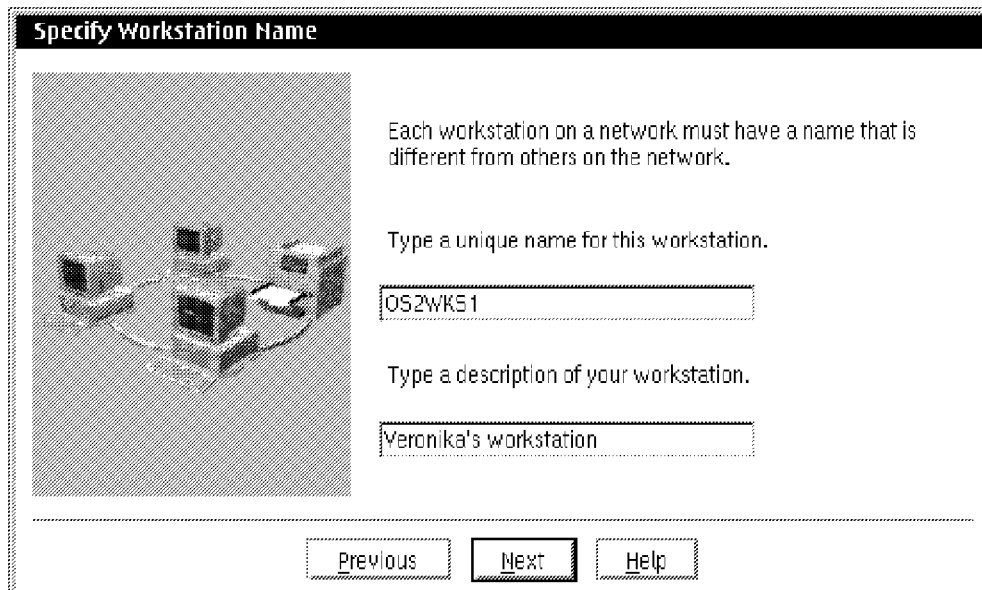
Figure 44. Easy Installation Path - Specify Workstation Name Window

Each workstation must have a unique name by which it will be known on the network. OS/2 Warp 4 chooses a default name for you based on information you have entered in previous steps (a typical workstation name offered starts with CLIENT followed by three numbers, for example, CLIENT127). However, if you want to use a name that is different from the one offered, you can enter one to fifteen alphanumeric characters in the space provided.

You can also provide a description for your system. This description will help other users on the LAN to identify your workstation. The information entered for each workstation in the LAN will appear in the File and Print Client Resource Browser folder, located in the Network folder within the Connections folder on the Desktop. The entry in this field is optional and does not have to be unique.

Once you have entered the information required, select **Next**. The Domain Name window will be presented to you as shown in Figure 45, in which you will need to provide the name of your domain.
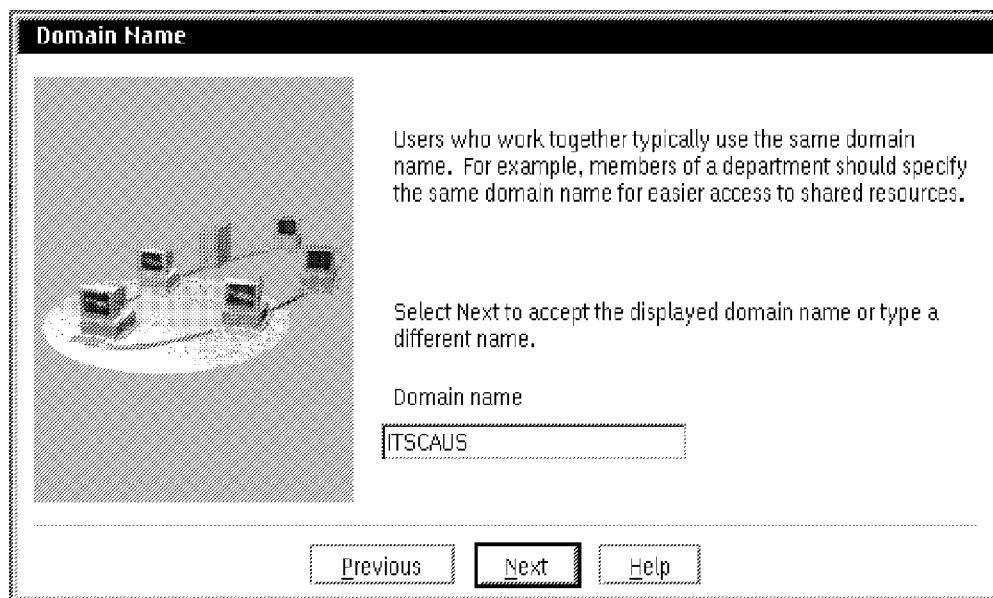
Figure 45. Easy Installation Path - Domain Name Window

The domain name defines the group of users who frequently share and use resources in a LAN. Most organizations use international standards for the domain names to be used. They are usually related to the city and the department of the organization where the domain is located. For example, our department's domain name is ITSCAUS which stands for International Technical Support Center in Austin, Texas.

If you have an OS/2 Warp Server domain on your network, you can type that name. Alternatively, you can use an existing peer network name (for

example, an OS/2 Peer or Windows 95 workgroup name) or you can even set up a new peer network. For more information about domains and workgroups, please refer to 3.2, "Local Area Network Concepts" on page 22.

By default, OS/2 Warp 4 chooses IBMPEERS as the domain name for a new peer network. You can accept the displayed name, or type 1 to 15 alphanumeric characters in the Domain name field to specify the domain of which you want your workstation to be a member.

The domain name must not be the same as the workstation name. If you use the same name for both, you will receive an information message and will not be allowed to continue the installation before you have selected different names.

IBMLAN.INI File

The information about workstation and domain names is stored in a file called IBMLAN.INI that is located in the IBMLAN directory on the disk where File and Print Client is installed.

This file contains the initialization parameters that control how your File and Print Client workstation works. In a machine with the OS/2 Warp File and Print Client installed, this file is divided into the following six sections:

```
[networks]
[requester]
[messenger]
[peer]
[replicator]
[services]
```

You can find the workstation and domain names for your machine within the [requester] section, as the Computername and Domain parameters' values, respectively.

Once the File and Print Client installation has finished, there are three ways of making permanent changes to the parameters' values of the IBMLAN.INI file:

- Change them in the Shared Resources and Network Connections notebook configuration pages.

- Use the File and Print Client Install/Remove icon located in the Install/Remove folder (shown in Figure 40 on page 108).

- Directly edit the IBMLAN.INI file with an ASCII text editor, such as the OS/2 System Editor.

Once you selected **Next** at the Specify Workstation Name window, the **Default User ID and Password** window will be presented to you as shown in Figure 46 on page 116. You are asked to specify a user ID and password for your File and Print Client.
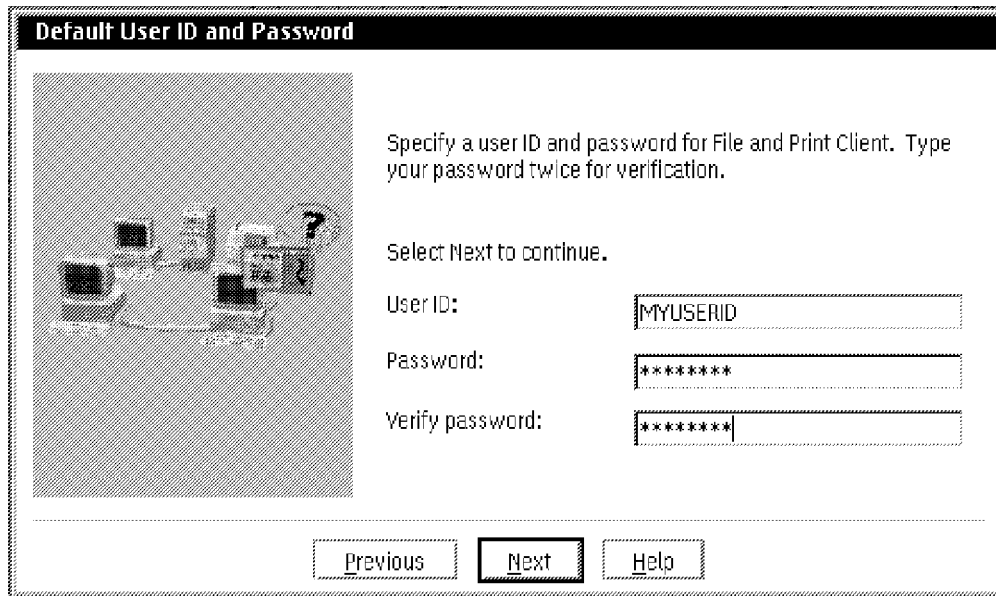
Figure 46. Easy Installation Path - Default User ID and Password Window

10.2.3.1 Three Types of Logons

There are three different kinds of logons that you can perform from the OS/2 Warp File and Print Client:

LAN Domain Logon This is a logon to an OS/2 Warp Server domain. Logging on to a LAN domain gives you access to the resources on that domain's servers.

You can log on by double clicking on the LAN Server Logon icon from the Logons folder located in the Network Services folder within the Connections folder on the Desktop, or from an OS/2 command line by using the `LOGON /VD` command (VD stands for Verification by Domain).

Local LAN Logon This means logging on your peer workstation. In order to configure and share network resources on your machine, you must first identify yourself to OS/2 Warp 4 by logging on using the peer administration user ID.

You can log on by double clicking on the File and Print Client Workstation Logon icon from the Logons folder located in the Network Services folder within the Connections folder on the Desktop, or from an OS/2 command line by using the `LOGON` command.

Local Logon   This is a facility for users who need to log on locally to their workstation. For example, users who have subsystems such as Database Manager may need to log on locally to access databases on their workstation.

You can log on from an OS/2 command line either by using the `LOGON /L` command, or just the `LOGON` command after making a LAN Logon (either to the local LAN or to a LAN domain).

If you have the same user ID and password on your peer workstation and a LAN domain, you can be connected to both of them at the same time by using a LAN domain logon. If this is to be the peer administrator user ID, and it has administrator privileges in the LAN domain, you will be able to administer both your peer network and your OS/2 LAN Server domain network resources at the same time.

Logon Command

The `LOGON` command can be used with many parameters. Syntax information is given if you type `HELP LOGON` in an OS/2 command line session.

The user ID that you enter in the Default User ID and Password window will become the default peer administration user ID for your OS/2 Warp 4 system.

User ID And Password Must Be Filled In

The user ID and password are mandatory. If you do not enter them, you will receive an information message and the installation will not continue before you have entered the required information.

The characters are displayed when you type your user ID, but to help keep your password secure, asterisks (*) are displayed when you type your password in the Password and Verify Password fields.

There are some general rules to remember when defining passwords and user IDs:

- Characters are converted to uppercase, no matter how they are entered.

- User IDs and Group IDs cannot have the following values: ADMINS, GROUPID, GUESTS, LOCAL, PUBLIC, RPLGROUP, SERVERS, SYSASID and USERS.

• User IDs and Group IDs cannot begin with any of the following: IBM, SQL and SYS.

User ID/Password

Previous versions of OS/2 included a default userid of USERID with the password of PASSWORD. This could cause a security exposure since, unless you remembered to delete this user ID, other users who knew this could use it to gain access to your system. With OS/2 Warp 4, this user ID is no longer present, eliminating this potential exposure.

This means, however, that you must remember the peer administration user ID and password that you enter during OS/2 Warp 4 installation, or you will be unable to share resources.

After entering this information, you are reminded to record your user ID and password in a secure location because you will need them to logon once the installation is complete, as shown in Figure 47.
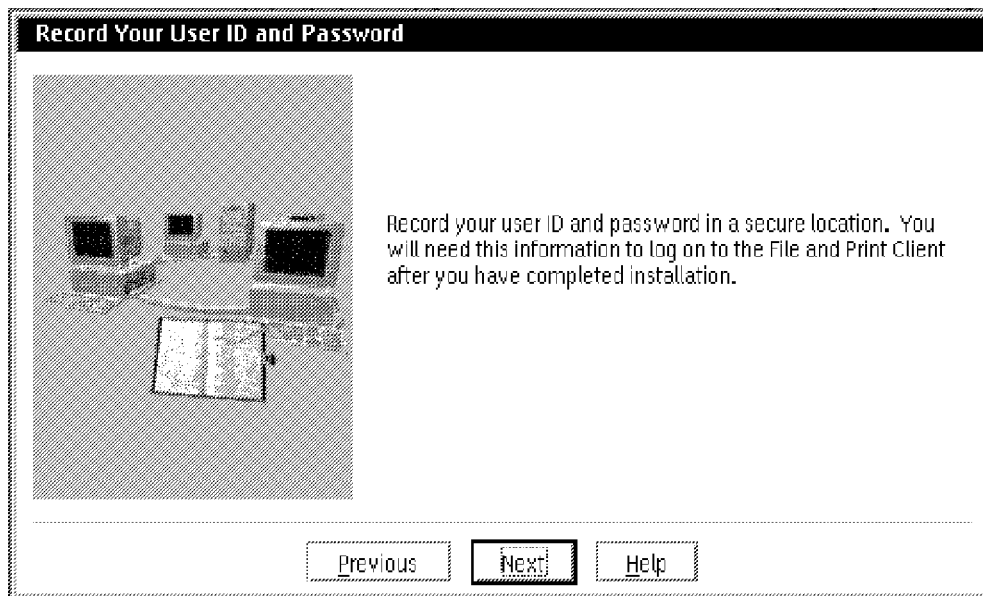
Figure 47. Easy Installation Path - Record Your User ID and Password Window

Selecting **Next** the Novell NetWare Client for OS/2 window is presented to you as shown in Figure 48 on page 119.
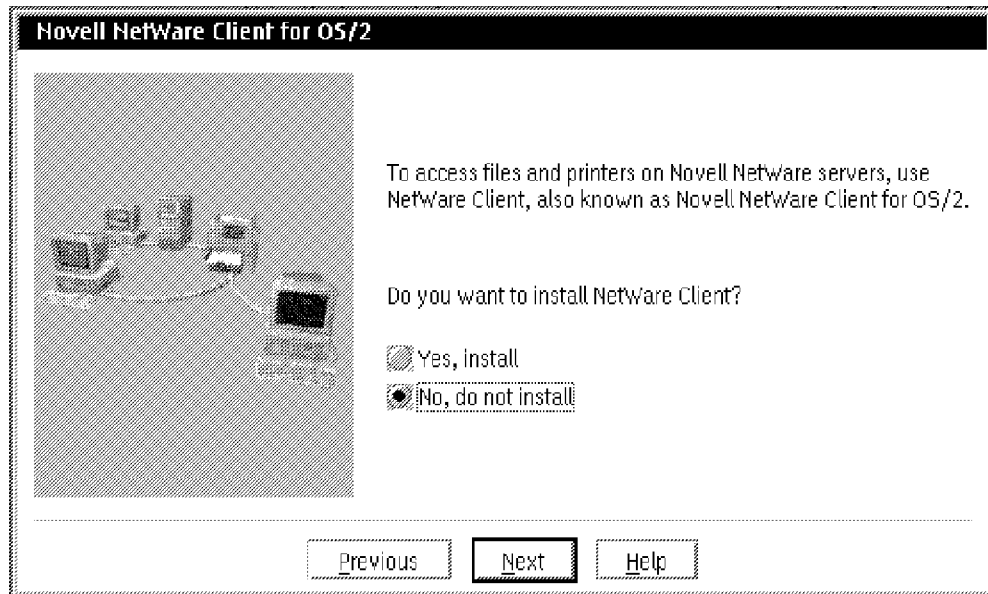
Figure 48. Easy Installation Path - Novell NetWare Client for OS/2 Window

At the Novell NetWare Client for OS/2 window you need to select to install or not to install the OS/2 NetWare client. Select **No, do not install** and **Next**, which will guide you to the TCP/IP Services window as shown in Figure 49. Figure 49.
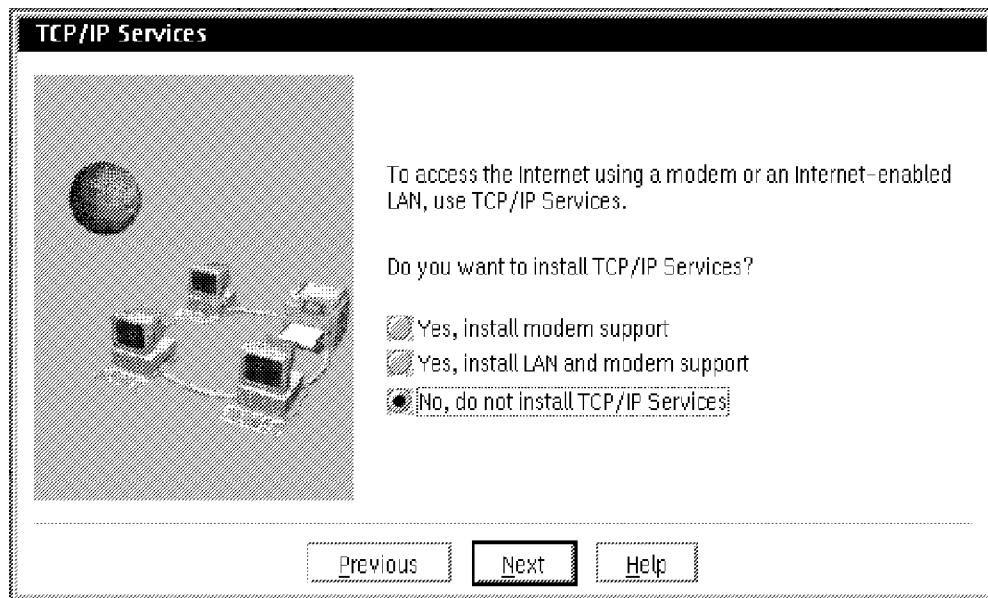
Figure 49. Easy Installation Path - TCP/IP Services Window

At this time, select **No, do not install TCP/IP Services**. We will explain this installation later in this chapter when we describe how to configure the DHCP (Dynamic Host Configuration Protocol) and DDNS (Dynamic Domain

Name Server) services. Select **Next**. to let the install program check your hardware configuration and attempt to determine what type of network adapter is present in your computer. When the system detects the network adapter, the Adapter Confirmation window is displayed as shown in Figure 50.
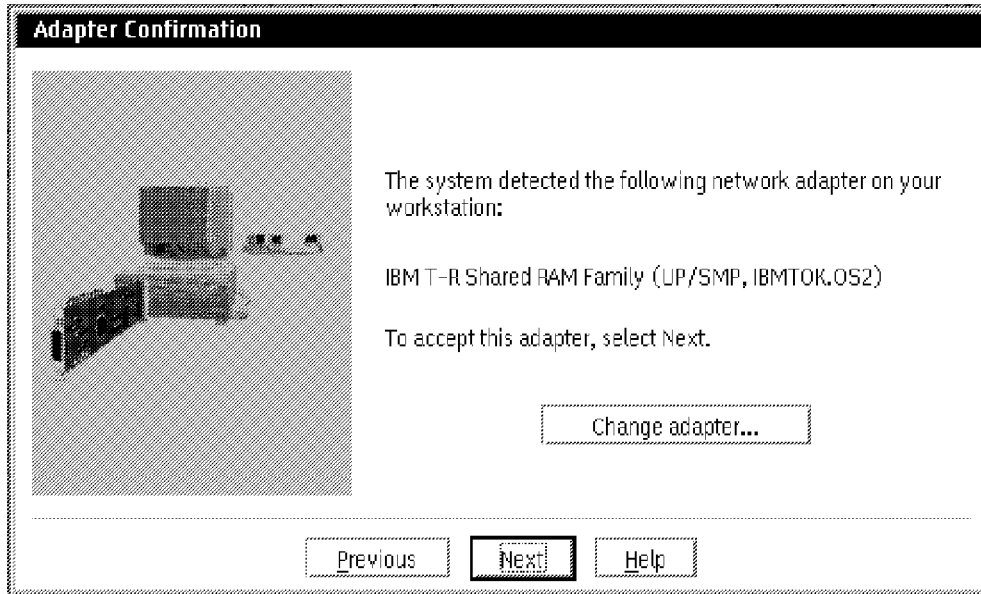
Figure 50. Easy Installation Path - Adapter Confirmation Window

In most cases, the install program will correctly identify the adapter installed in your workstation. However, because of certain bus design limitations, sometimes network adapter sniffing does not provide the expected results. In this case, select **Change adapter** to select your LAN adapter from a list of supported network adapters that is presented to you, as shown in Figure 51 on page 121.
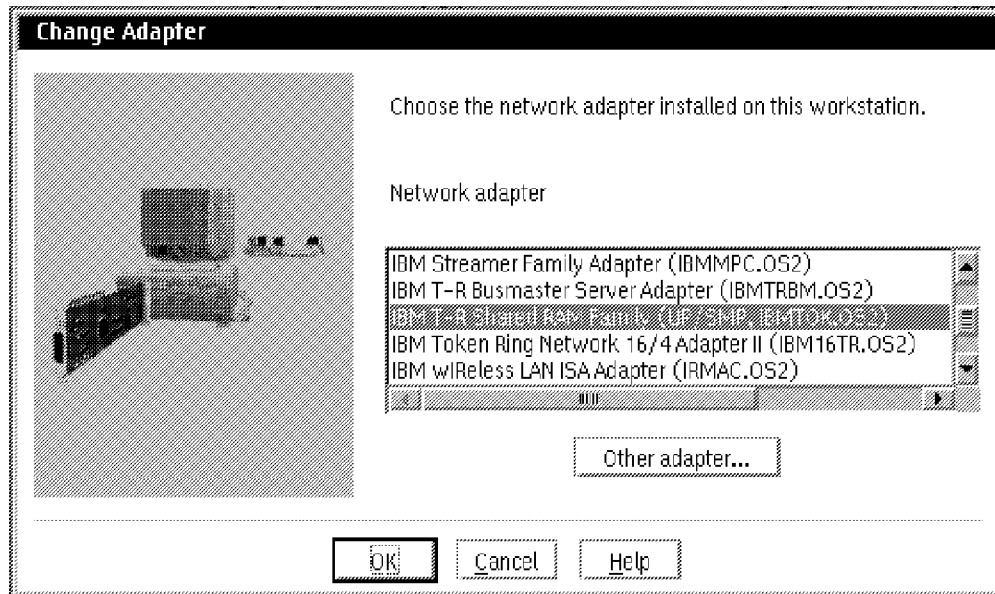
Figure 51. Easy Installation Path - Change Adapter Window

If your adapter appears in the list of network adapters, it means that this network adapter driver is on the OS/2 Warp 4 CD-ROM, so you just have to select it. If it is not in this list, you need to obtain the driver for your adapter from the adapter card's manufacturer. In this case select **Other adapter** which will present the Network Adapter Driver diskette windows as shown in Figure 52.
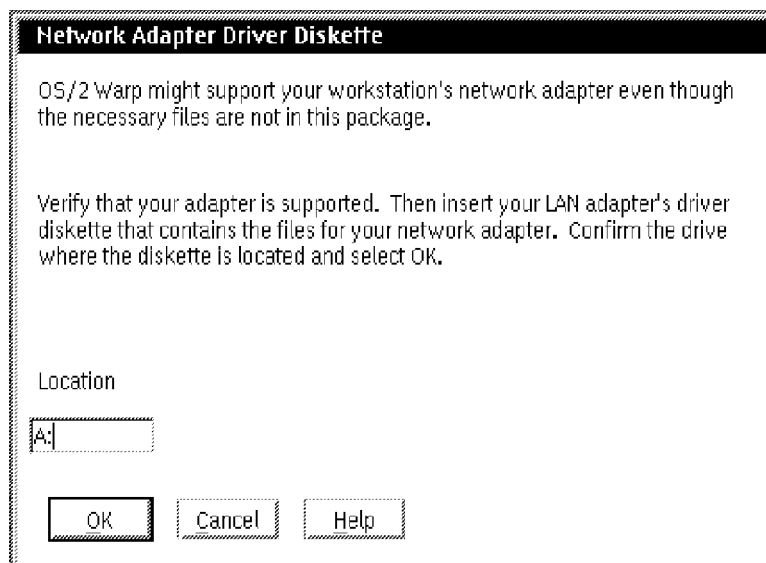
Figure 52. Easy Installation Path - Network Adapter Driver Diskette Window

Insert your LAN adapter's driver diskette to install the corresponding network adapter driver.

> **No Network Adapter?**
>
> If there is no network adapter installed in your workstation but you still
> need to install networking components (for example, for remote access),
> select the **Change adapter** button and select the **No Network Adapter**
> entry in the list of adapters.

By default, the Easy Installation path only binds the IBM OS/2 NetBIOS
protocol driver with your adapter. If you need to have more protocols bound
with your adapter, you have two possibilities:

 • Choose the Advanced Installation path instead of Easy.

 • Configure it after the installation is finished. Select the **File and Print
   Client Install/Remove** object in the Install/Remove folder (in the System
   Setup folder).

Once the network adapter configuration is finished, you will be presented
with the Ready to Install window, which contains a summary of the options
you have chosen, as shown in Figure 53.

Figure 53. Easy Installation Path - Ready to Install Window

At the Ready to Install window you can change the drive letter the install
program uses to install the products. To do so, select the product in the
Product list and then click on **Change drives...**.

If all the listed options are correct, select **Install** to start the installation.

10.2.4 Advanced Installation

If you used the Easy Installation path you may skip this section and proceed
with 10.3, "Post-Configuration" on page 141.

Select the **Advanced Installation** option from the Selective Install for
Networking window, shown in Figure 41 on page 109, to open the OS/2
Warp Setup and Installation window as shown in Figure 54.
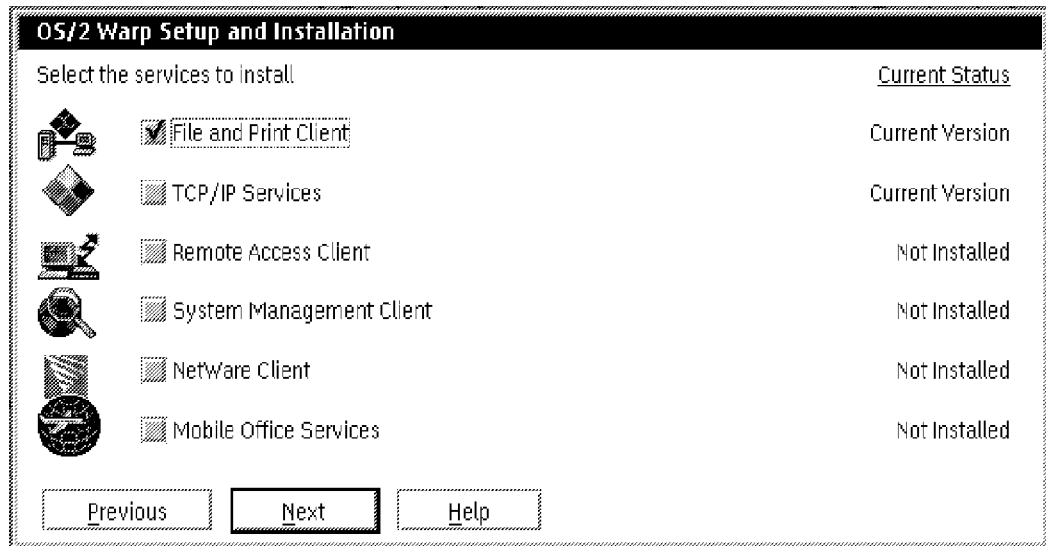
Figure 54. Advanced Installation Path - OS/2 Warp Setup and Installation Window

A list of networking components that can be installed on your workstation is
displayed:

File and Print Client   Allows you to log on to a peer network and a
                                 LAN domain and use shared applications,
                                 directories, modems and printers on servers
                                 and peer workstations, or share your own
                                 network resources.

TCP/IP Services   Allows you to use your modem or an
                                 Internet-enabled LAN connection to access
                                 resources worldwide and to communicate with
                                 users anywhere in the world.

Remote Access Client   Allows you to dial into a server and access resources over telephone lines.

System Management Client Allows a network administrator to manage hardware and software on your workstation from a central location.

NetWare Client   Allows you to use LAN resources on Novell NetWare file servers.

Mobile Office Services   Allows you to take LAN-based files with you when you travel and automatically restore the updated files to the LAN when you return.

```
┌─ Current Status ──────────────────────────────────────────┐
│                                                            │
│  You can find out which services are actually installed on your machine │
│  by checking the Current Status list in the OS/2 Warp Setup and         │
│  Installation window.  Those products that show Current Version are      │
│  already installed on your machine.                        │
│                                                            │
└────────────────────────────────────────────────────────────┘
```

In this scenario, we are considering only the installation of the OS/2 Warp File and Print Client, so select the **File and Print Client** service only. The Configuration window is displayed, as shown in Figure 55.
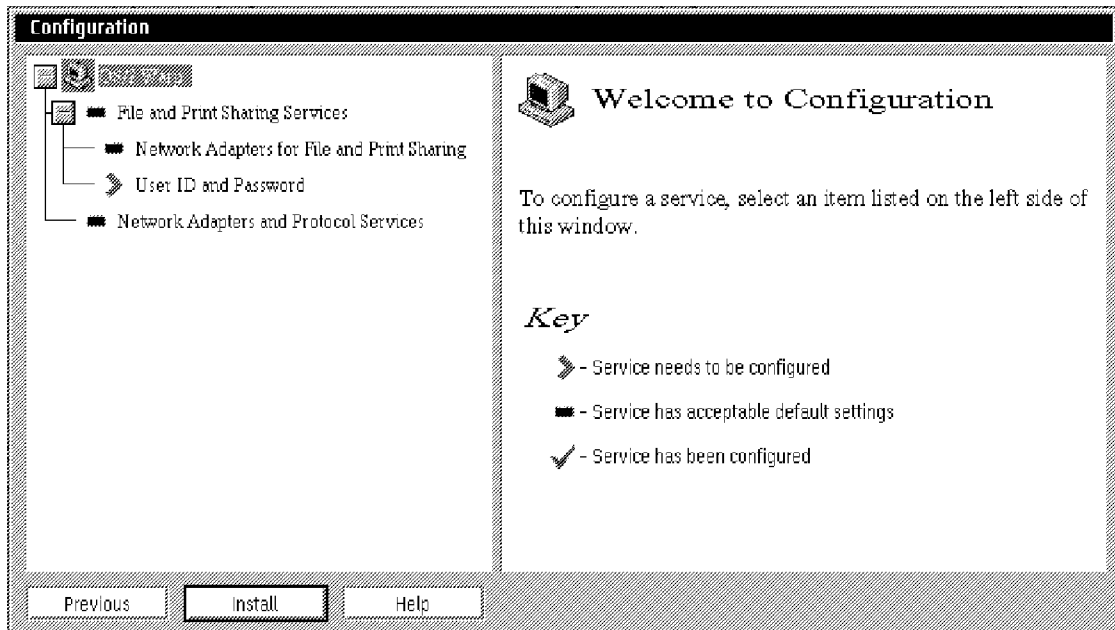
Figure 55. Advanced Installation Path - Configuration Window

The Configuration window contains two sections:

- The section on the left side of the window contains a list of items that you can configure. Symbols used here are explained below:
  - A green check mark next to an item means the item is correctly configured.
  - A red arrow means the item must be configured.
  - A blue box means the item is configured correctly with the default value.
- The section on the right side of the window is the page in which you configure the item you selected from the left item list.

Select Install Only After all Services are Configured

Do not select the **Install** button until you have completely finished configuring all items that you want to install (or at least the ones marked with red arrows). Otherwise, you receive information messages, and are not allowed to continue with the installation.

When the configuration panel for the networking components is displayed, you also see a small window titled Disk Space as shown in Figure 56. This windows displays the local drives on your computer and shows how much space is available on each one. This assists you when deciding which drives to use when installing the individual networking components.

Drive	Available	Remaining
C	281 MB	273 MB
D	456 MB	456 MB
E	999 MB	999 MB

Figure 56. Advanced Installation Path - Disk Space Window

For the installation of the File and Print Client, the only service that needs to be configured is the `User ID and Password` item, because the other items have acceptable default settings. However, we recommend going through the configuration of all the services listed to verify the default configuration values and change them to the correct ones, if necessary.

> **Configuration Order**
>
> We recommend configuring the `Network Adapter and Protocol Services` item first, because the network adapters available in the `Network Adapters for File and Print Sharing` item depend on the drivers and protocols you select in your configuration.

Before you start configuring items from the top, select **Network Adapter and Protocol Services** from the item list. The Network Adapters and Protocol Services (MPTS and LAPS) configuration window is opened for you as shown in Figure 57.
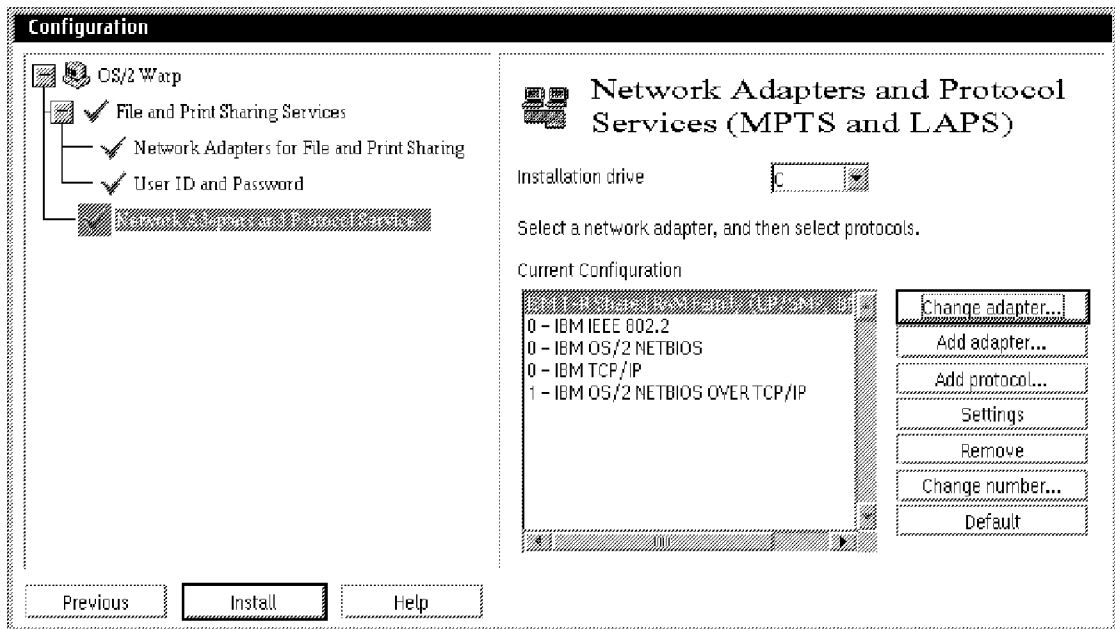
Figure 57. Advanced Installation Path - MPTS and LAPS Window

This component of OS/2 Warp 4 provides communication support to all the other networking parts of the product, and is always installed when you install any networking components. Therefore, it cannot be explicitly selected on the OS/2 Warp Setup and Installation window, shown in Figure 54 on page 123.

Network Adapter and Protocol Services attempts to detect and identify the network adapters installed in your system. However, only the first one found will be automatically included in the configuration. If you want to configure more than one adapter, you have to add the other ones manually.

The initial configuration of network protocols within the Network Adapter and Protocol Services depends on the networking components that you select to

install. By default, when installing the File and Print Client only the IBM OS/2 NetBIOS protocol will be configured.

The following table summarizes the configuration parameters and describes their purposes:

Table 7. Network Adapter and Protocol Services Installation	
Configuration Item	**Configuration Data**
Change adapter...	Press this button if you want to change a network adapter for the current configuration. This may be necessary if the installation program can not detect your adapter configuration properly.
Add adapter...	Press this button if you want to: • Add an adapter to your configuration. • Add a new adapter driver that is not supplied with Network Adapters and Potocol Services.
Add protocol...	Press this button if you want to: • Add a protocol to your configuration. • Add a new protocol driver that is not supplied with Network Adapters and Protocol Services.
Settings	Press this button if you want to change the parameters for any item in the configuration list. This will bring up a menu depending on the item you want to change.
Remove	Press this button if you want to remove an item from the configuration list. You can only remove one item at a time. **Note:** You can only remove an adapter if you have previously removed all the protocols that are associated with that adapter.
Change number...	Press this button to change the logical sequence that a protocol driver associated with more than one adapter addresses the adapter. Application programs will use these numbers when they issue calls to the network interface(s).

If you want to add an adapter to your configuration, click on the **Add adapter...** button and then select the appropriate driver from the list of Network adapter, as shown in Figure 58 on page 128.
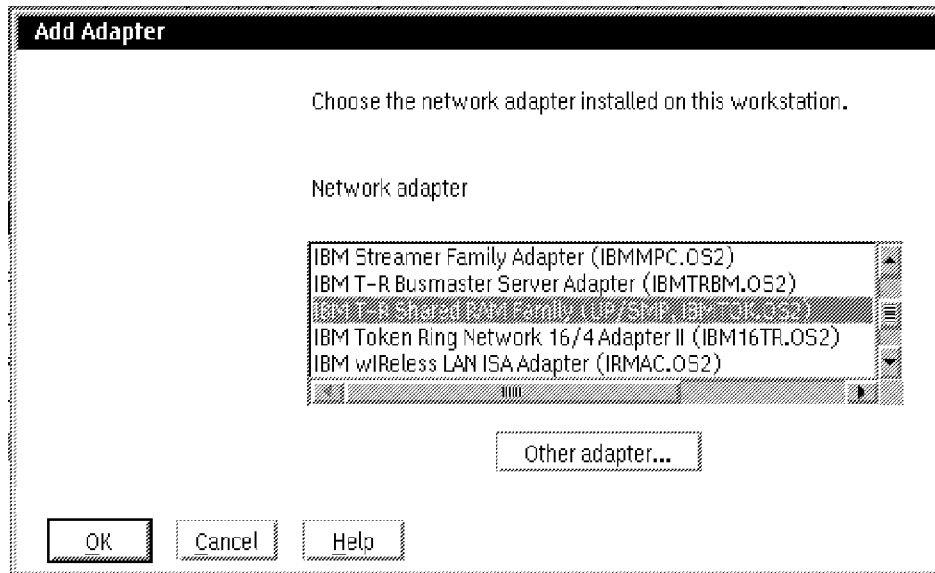
Figure 58. Advanced Installation Path - Add Adapter Window

If the network adapter in your computer is not supported by the drivers
supplied with OS/2 Warp 4 (meaning it is not listed in the Network adapter
list), but you have an NDIS-compliant OS/2 device driver for that adapter,
you can add the new adapter driver by selecting **Other adapter...** and
specifying the source drive from which the new driver will be copied to your
system.

```
┌─ Suggestion for Compatible Adapters . . . ──────────────────────────┐
│                                                                     │
│ If you have an IBM compatible token ring network adapter and you are│
│ not sure which driver you should configure to make it work, you can try│
│ using the IBMTOK.OS2 MAC device driver that usually works with most │
│ token ring adapters.                                                │
│                                                                     │
└─────────────────────────────────────────────────────────────────────┘
```

If you want to add a protocol to your configuration, select **Add protocol...** and
then select the appropriate driver from the Protocol list as shown in

```
Add Protocol

Choose the protocols to be used with the selected adapter.

Network adapter:
IBM T-R Shared RAM Family (UP/SMP, IBMTOK.OS2)

Protocol:

┌─────────────────────────────────────────────────────┬──┐
│ IBM IEEE 802.2                                        │▲ │
│ IBM Netware Requester Support                         │  │
│ IBM OS/2 NETBIOS                                      │  │
│ IBM OS/2 NETBIOS OVER TCP/IP                          │  │
│ IBM TCP/IP                                            │  │
│ NetWare NetBIOS Emulation over IPX – IBM Netwar       │  │
│                                                       │  │
│                                                       │  │
│                                                       │▼ │
├──┬─────────────────────────────────────────────┬──┬──┴──┤
│◄ │                IIIII                         │  │►    │
└──┴─────────────────────────────────────────────┴──┴─────┘

┌─────────┐  ┌────────────────┐  ┌──────────┐  ┌────────┐
│   OK    │  │ Other protocol...│  │  Cancel  │  │  Help  │
└─────────┘  └────────────────┘  └──────────┘  └────────┘
```
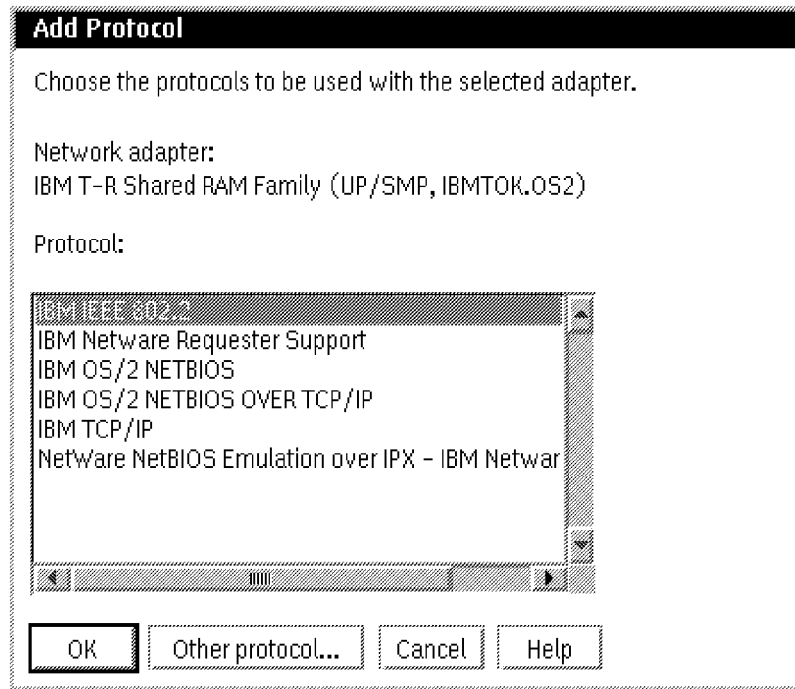
Figure 59. Advanced Installation Path - Add Protocol Window

The following are the network protocols provided by OS/2 Warp 4:

- **IBM IEEE 802.2**

    This protocol is required for some specific applications, such as:

    - IBM Communications Manager/2, that uses the IBM IEEE 802.2 protocol driver LANDD.OS2.
    - Personal Communications for OS/2, that is configured for SNA.
    - The Remote Initial Program Load (RIPL) service in OS/2 LAN Server.
    - The HP JetAdmin and Lexmark MarkVision printer utilities provided in the BonusPak of OS/2 Warp 4, which need the IBM IEEE 802.2 protocol driver to be installed to communicate with network-attached printers.

- **IBM NetWare Requester Support**

    This protocol enables an NDIS (Network Driver Interface Specificaton) compliant MAC (Media Access Control) driver to communicate with a protocol stack that complies with Novell ODI (Open Data Link Interface) specifications.

    It is required when using the OS/2 NetWare Requester to communicate between your OS/2 Warp 4 machine and a NetWare server.

- **IBM OS/2 NetBIOS**

NetBIOS (Network Basic Input Output System) is an Application Programming Interface (API) that provides a consistent interface for applications to access network resources.

OS/2 LAN Server and OS/2 Warp File and Print Client are NetBIOS applications which are normally configured to use the NetBIOS protocol stack.

Native NetBIOS has certain characteristics that limit its use in certain communications environments:

- The NetBIOS protocol can only be used on a LAN.
- The NetBIOS protocol cannot be routed.
- The NetBIOS protocol uses single route broadcasts to establish connections. Find more detailed information about NetBIOS in 4.1, "The NetBIOS Application Programming Interface" on page 27 and NetBEUI in 4.2, "The NetBEUI Protocol" on page 32.

- **IBM TCP/IP**

  This is a general networking protocol that may be used in any kind of network (for example, ethernet, token ring, broadcast networks and dedicated serial lines). It is a routable protocol, which means that it is designed to be efficiently routed from one network to another or around a Wide Area Network (WAN).

  TCP/IP is a combination of two protocols:

  - Internet Protocol (IP)

  - Transmission Control Protocol (TCP)

- **IBM OS/2 NetBIOS over TCP/IP**

  One solution to overcome the limitations of the NetBIOS protocol can be found in RFC (Request For Comment) 1001/1002 specifications, which describe how to implement the IBM NetBIOS services on top of the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocol layers.

  The NetBIOS over TCP/IP (TCPBEUI) implementation of OS/2 Warp Server and OS/2 Warp File and Print Client allows a workstation to be geographically isolated from a LAN domain or an OS/2 peer network, yet communicate with them transparently.

  More information about this NetBIOS over TCP/IP implementation is provided in:

  - 4.4, "NetBIOS over TCP/IP" on page 35

  - 4.4.1.1, "NetBIOS over TCP/IP Implementation in OS/2 Warp 4" on page 36

- Illustrating B-node, P-node and H-node.
  - 4.4.2, "How to Enhance B-node Operations in OS/2 Warp 4" on page 37
    - Illustrating RFCNAMES.LST, RFCBCST.LST, RFCADDR.EXE and Domain Name Server routing extension.
  - 4.4.2.1, "OS/2 TCPBEUI NetBIOS Names Resolution Order B-Node" on page 42
  - 4.4.2.2, "OS/2 TCPBEUI NetBIOS Names Resolution w/NetBIOS Name Server" on page 42
  - 4.4.3, "OS/2 Warp 4 Clients To Communicate with a NetBIOS Name Server" on page 42.

- **NetWare NetBIOS Emulation over IPX - IBM NetWare Requester**

  This protocol is another solution to overcome the limitations of the NetBIOS protocol. It uses the NetBIOS over the IPX protocol driver, which is a routable protocol.

  This capability is extremely useful for customers who have multi-segment networks connected by IPX routers, or who are already using IPX as the standard protocol on their networks and do not wish to introduce additional protocols.

Licensing Information

You can configure as many protocols as you need to communicate with as many servers running OS/2 Warp Server as you want (for example, you may need to connect to a print server and an application server from the same workstation). To do so, you need **one client license**, which is already included in the OS/2 Warp 4 package.

If you want to use a network protocol that is not supplied by OS/2 Warp 4, (which means that it is not listed in Protocol list shown in Figure 59 on page 129) but you have an NDIS-compliant OS/2 protocol driver for that protocol, you can add the new protocol driver by selecting **Other protocol...** and specifying the source drive from which the new driver will be copied to your system.

Adding an adapter or protocol may affect the configuration of other OS/2 Warp components, so you may want to check the items on the configuration tree after the changes are made.

For instance, adding the NetBIOS over TCP/IP protocol, as shown in Figure 57 on page 126, allows another network adapter to be selected from

the **Network Adapters for File and Print Sharing** item in the File and Print Client, as shown in Figure 63 on page 138. This is because when you configure both NetBIOS and TCPBEUI, even though a single physical network adapter is present in the workstation, both protocols must be configured on different logical adapters. That is, the numbers of the protocol drivers have to be set differently, although only one physical LAN adapter is present. This is why if you tried to configure both NetBIOS and TCPBEUI on the same logical adapter a Duplicate NetBIOS API Adapter Numbers window would be presented to you as shown in Figure 60.

```
┌──────────────────────────────────────────────────┐
│▓ Duplicate NetBios API Adapter Numbers       ▓ ▣ │
├──────────────────────────────────────────────────┤
│                                                  │
│   ⊘   LT00213:  You cannot have duplicate        │
│       logical adapter numbers for NetBIOS        │
│       application support enabled protocol       │
│       drivers.                                   │
│                                                  │
│       Select OK and then change one or           │
│       more of the logical adapter numbers.       │
│                                                  │
│   ┌────────┐   ┌────────┐                        │
│   │  OK    │   │  Help  │                        │
│   └────────┘   └────────┘                        │
└──────────────────────────────────────────────────┘
```
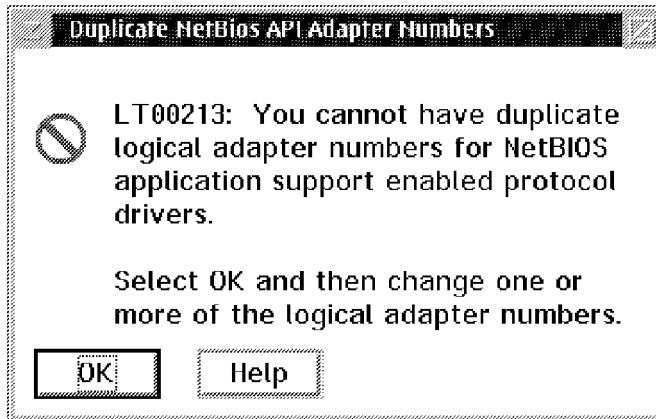
Figure 60. Duplicate NetBIOS API Adapter Numbers Window

If you want to view or change the configuration of any adapter or protocol driver, select the appropriate item on the list and then click on the **Settings** button. For example, if you select the **IBM T-R Shared RAM Family (UP/SMP, IBMTOK.OS2)** adapter driver and then click on the **Settings** button, the Parameters for IBM T-R Shared RAM Family (UP/SMP, IBMTOK.OS2) window will be displayed as shown in Figure 61 on page 133.
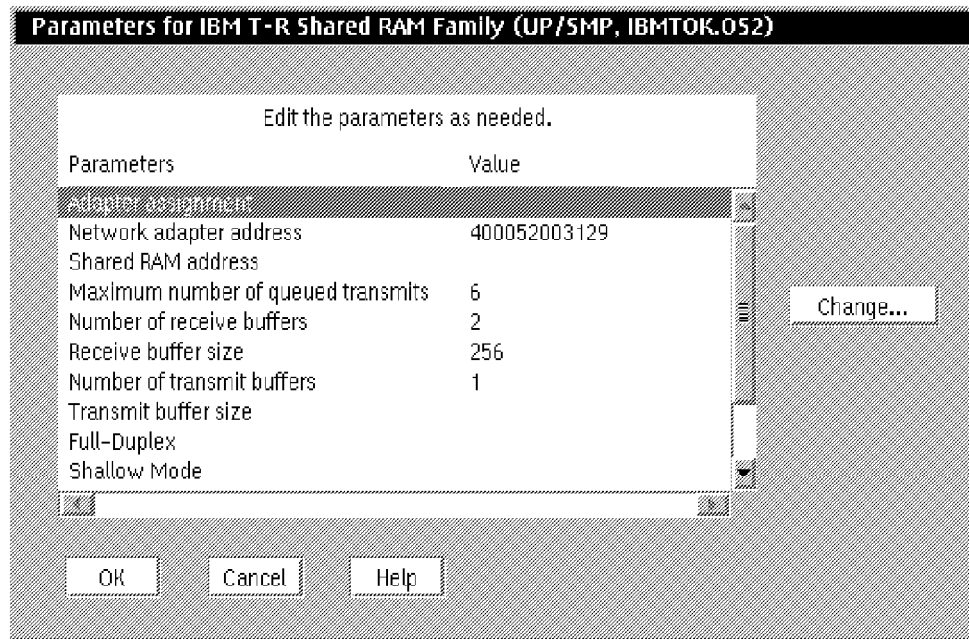
Figure 61. Advanced Installation Path - Parameters for Network Adapter Window

In the Settings window you can change the parameters for the selected adapter driver, for instance, enter a LAA (Logically Administered Address) in the Network Adapter Address field.

What If You Do Not Have a Network Adapter?

Remote access does not necessarily require the presence of a LAN adapter. You may select **No Network Adapter** entry in the list shown in the Add Adapter window. However, other networking components cannot be installed.

Next, configure the **File and Print Sharing Services** item. The File and Print Sharing Services window shown in Figure 62 on page 134 is displayed.
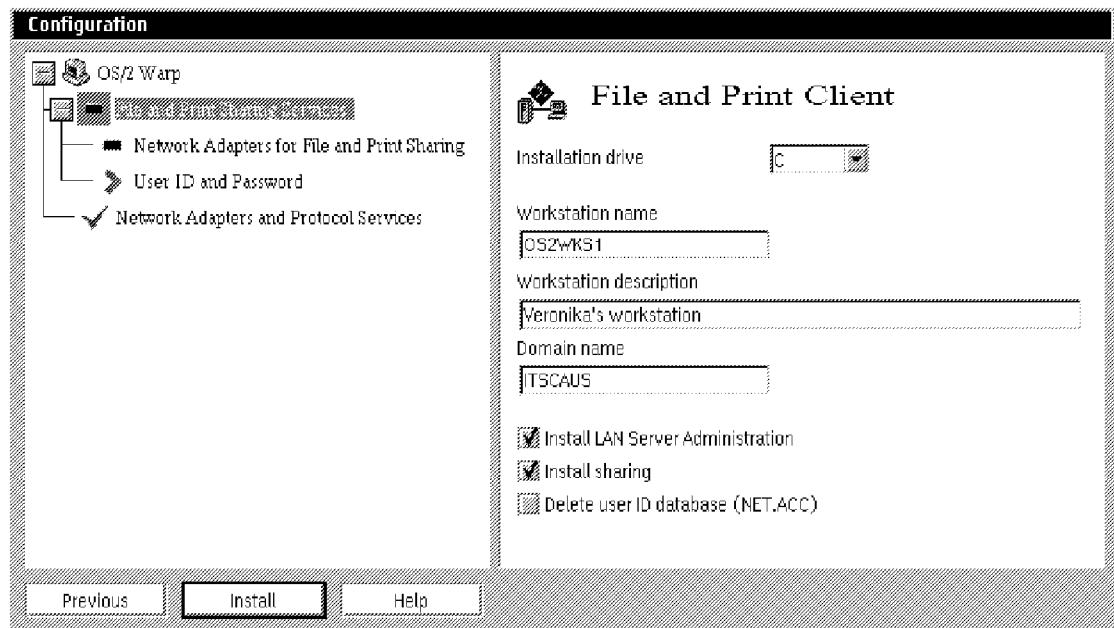
Figure 62. Advanced Installation Path - File and Print Sharing Services Window

When the Network Adapters and Protocol Services are configured, proceed with the configuration of File and Print Sharing Services. Complete the following fields:

- Installation drive

  This is the drive on which you wish to install the File and Print Client.

- Workstation name

  This is the unique name by which your system will be known on the LAN. OS/2 Warp 4 chooses a default name based on information you have typed in in previous steps (a typical default workstation name format is CLIENTxxx, for example, CLIENT127). However, if you want to use a name that is different from the one displayed, you can enter one or up to 15 alphanumeric characters in the space provided.

- Workstation description

  This is an optional description that identifies your system to other users on the LAN. The information that each workstation in the LAN enters in this field appears in the File and Print Client Resource Browser folder, located in the Network folder that resides in the Connections folder on the Desktop.

- Domain name

  The domain name defines the group of users who frequently share and use resources in a LAN. Most organizations use international standards for the domain names to be used. They are usually related to the city

and the department of the organization where the domain is located. For example, our department's domain name is ITSCAUS which stands for International Technical Support Center in Austin, Texas.

If you have an OS/2 Warp Server domain on your network, you can type that name. Alternatively, you can use an existing peer network name (for example, an OS/2 Peer or Windows 95 workgroup name) or you can even set up a new peer network. For more information about domains and workgroups, please refer to 3.2, "Local Area Network Concepts" on page 22.

By default, OS/2 Warp 4 chooses IBMPEERS as the domain name for a new peer network. You can accept the displayed name, or type one to 15 alphanumeric characters in the Domain name field to specify the domain of which you want your workstation to be a member.

The domain name must not be the same as the workstation name. If you try to use the same name for both, you receive an information message and are not allowed to continue the installation before you have selected different names.

┌─ **IBMLAN.INI File** ──────────────────────────────────────┐

The information about the workstation and domain names is stored
in a file called IBMLAN.INI located in the IBMLAN directory on the
disk where File and Print Client is installed.

This file contains the initialization parameters that control how your
File and Print Client workstation works. In a machine with the OS/2
Warp File and Print Client installed, this file is divided into the
following six sections:

```
[networks]
[requester]
[messenger]
[peer]
[replicator]
[services]
```

You can find the workstation and domain names for your machine
within the [requester] section, as the Computername and Domain
parameter's values, respectively.

Once the File and Print Client installation has finished, there are
three ways of making permanent changes to the parameters' values
of the IBMLAN.INI file:

  • Change them in the Shared Resources and Network Connections
    notebook configuration pages.

  • Use the File and Print Client Install/Remove icon located in the
    Install/Remove folder (shown in Figure 40 on page 108).

  • Directly edit the IBMLAN.INI file with an ASCII text editor, such as
    the OS/2 System Editor.

└──┘

• Install LAN Server Administration

  If you select this check box, the full Graphical User Interface (GUI) for
  the administration utilities for OS/2 Warp Server will be installed.

  Warp Server Administration utilities allow you to administer the OS/2
  Warp Server from your OS/2 Warp 4 machine. To do this, however, you
  must have administrator rights for the servers you want to administer.

  These utilities are contained in the LAN Server Administration and
  Logons folders, located in the Network Services folder within the
  Connections folder on the Desktop

• Install sharing

  There are two ways you can share and administer the resources of your
  peer network:

1. From the command line by using the following command:

   `NET SHARE`

   This option is always available regardless whether you selected the **Install sharing** button from the File and Print Sharing Services window. `NET SHARE` makes a server's or peer workstation's resource available to local area network users.

   When used without options, `NET SHARE` lists information about all resources being shared on the server or peer server. To get syntax information, type `NET HELP SHARE | MORE` at an OS/2 command line.

2. From the Graphical User Interface (GUI): there are many graphical alternatives to share and administer your workstation's resources:

   - From the Shared Resources and Network Connections notebook, located in the Network Services folder that resides in the Connections folder on the Desktop.

   - From the networking options of the resources' context menus, such as Start sharing... or Manage access...

   - From the Shares page of the resources' Properties notebooks, which can be accessed from the Properties option in their context menus.

   If you want these GUI facilities to be installed, you have to select the **Install Sharing** button from the File and Print Sharing Services window.

In either the GUI or command line interface, you must be logged on as the peer administrator to be able to share and administer your workstation's resources.

- Delete user ID database (NET.ACC)

The NET.ACC file contains user and group definitions information. There are two types of this file: one located on the domain controller machine, and one located in each OS/2 Warp File and Print Client workstation.

The User Profile Management (UPM) of the OS/2 Warp File and Print Client uses the local NET.ACC file to store user IDs and group names, which are used for the OS/2 Warp peer network. OS/2 Warp File and Print Client also stores access control profiles in this file.

If you select the **Delete user ID database (NET.ACC)** option, the local copy of the NET.ACC file will be replaced, which means that all current definitions in this file are deleted.

Select this option only if you are reinstalling over a previous version of File and Print Client and you want to start with a new default NET.ACC

file. Do not select this option if you are migrating from a previous version of OS/2 Warp 4 and want to keep this information.

Logon Verification

You can specify in the IBMLAN.INI file the type of verification you want to occur when you perform a logon.

The logon verification is represented by the 37th digit of the `wrkheuristics` parameter in the `[requester]` section, and can take the following values:

- 0   Allows you to log on without your user ID and password being verified.
- 1   Validates your user ID and password on your local workstation using the local copy of the NET.ACC file.
- 2   Validates your user ID and password on the domain controller or backup server using the domain copy of the NET.ACC.

The default value in OS/2 Warp 4 for this parameter is 1.

If you select the **Network Adapters for File and Print Sharing** item, the Network Adapters for File and Print Client window is displayed as shown in Figure 63.
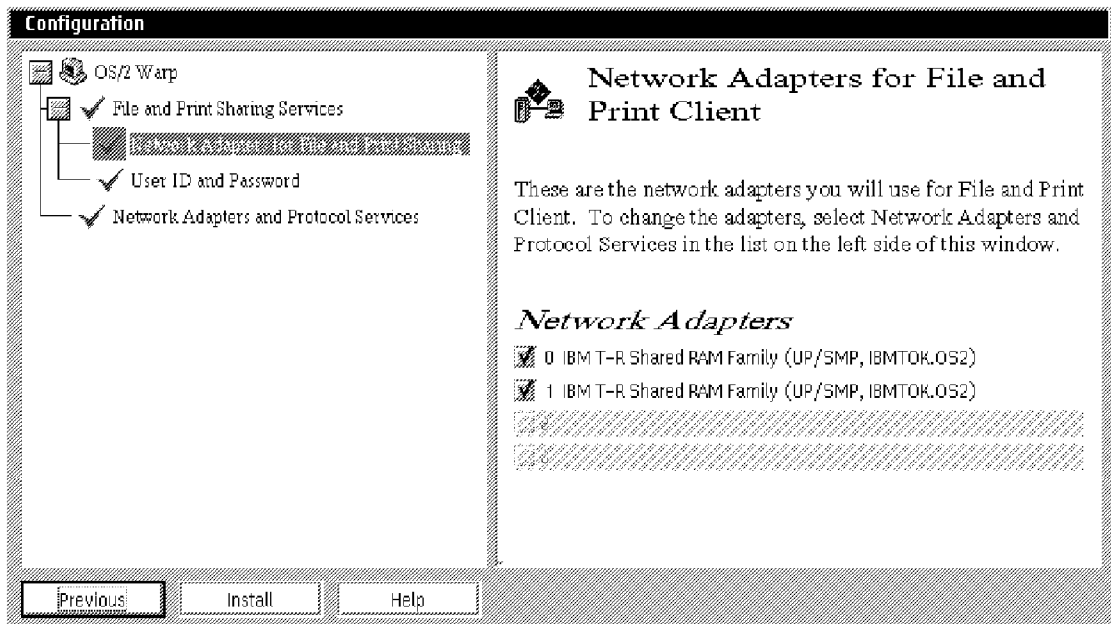
Sharing Window

Figure 63. Advanced Installation Path - Network Adapters for File and Print

You can use this window to activate one or more adapters for use with the File and Print Client, in case you have more than one network adapter installed and configured in your computer.

The available network adapters listed in this window depend on the configuration of the Network Adapters and Protocol Services item.

Note: Remember one of the previous steps when we recommended you to configure Network Adapters and Protocol Services before you configure Network Adapters for File and Print Client? If you selected TCPBEUI in this previous step, it will now appear in the list of Network Adapters as another network adapter. In this example, TCPBEUI would be network adapter 1.

Next, you need to configure the user ID and password. Type user ID and password information that will be the default peer administration user ID for your OS/2 Warp 4 system as shown in Figure 64.
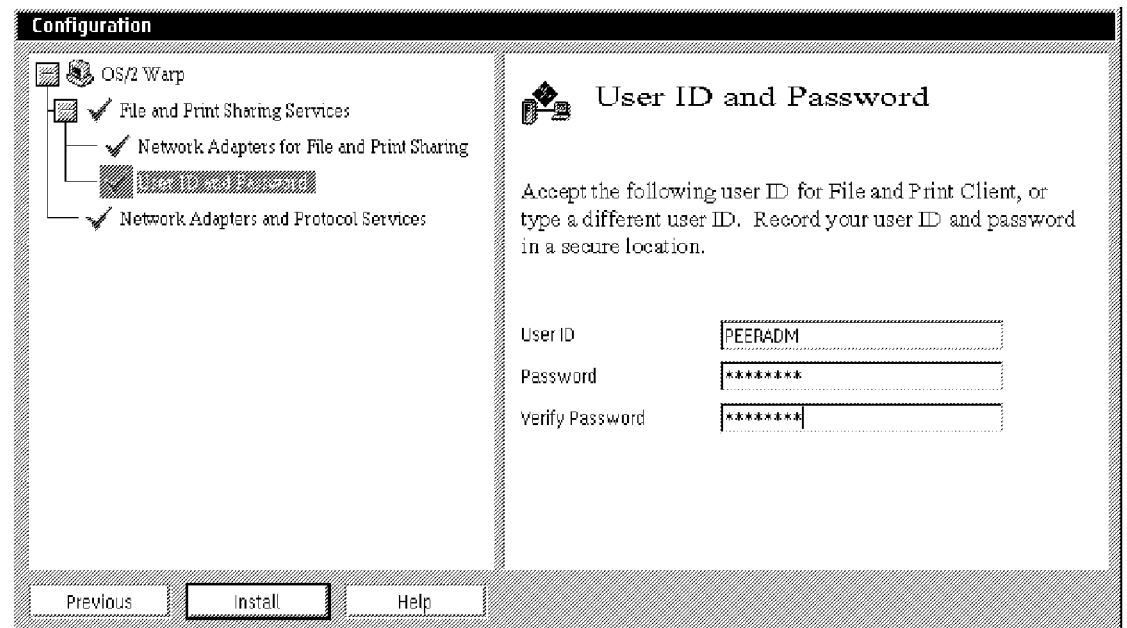
Figure 64. Advanced Installation Path - User ID and Password Window

The characters are displayed when you type your user ID, but to help keep your password secure, asterisks (*) are displayed when you type your password in the Password and Verify Password fields.

> **User ID And Password Must Be Filled In**
>
> User ID and password information is mandatory. If you do not enter them, an information window will pop up and the installation will not continue before you enter values.

There are some general rules to remember when defining passwords and user IDs:

- Characters are converted to uppercase no matter how they are entered.

- User IDs and Group IDs cannot have the following values: ADMINS, GROUPID, GUESTS, LOCAL, PUBLIC, RPLGROUP, SERVERS, SYSASID and USERS.

- User IDs and Group IDs cannot begin with any of the following: IBM, SQL and SYS.

> **User ID/Password**
>
> Previous versions of OS/2 included a default user ID of USERID with the password of PASSWORD. This could cause a security exposure since, unless you remembered to delete this user ID, other users who knew this could use it to gain access to your system. With OS/2 Warp 4, this user ID is not present, eliminating this potential exposure.
>
> This means, however, that you must remember the peer administration User ID and password that you enter during OS/2 Warp 4 installation, or you will be unable to share resources.

Once you have configured all the services listed in the Configuration window (which means that there is no item marked with the red arrow in the window), click on the **Install** button to start the installation procedure. An information window is displayed, informing you that the install program is ready to copy the files and complete the installation as shown in Figure 65 on page 141.
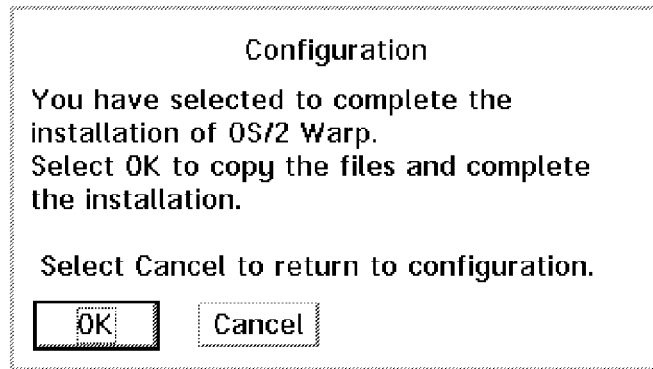
Figure 65. Advanced Installation Path - Configuration Confirmation Message

Select **OK** to start the installation of networking components.

10.3 Post-Configuration

After installing the OS/2 Warp File and Print Client on your workstation, there might be cases where you want to make modifications to your configuration, such as, add a new network adapter, change your machine's name, or make some tuning adjustments in your network configuration files. In this section you will find all the information required for making such modifications to your workstation's OS/2 Warp File and Print Client configuration.

We also describe how to configure your OS/2 Warp File and Print Client to share your network resources, and how to access resources from other peer workstations.

10.3.1 Important LAN System Files

There are some important files that contain the network configuration parameters for your workstation and can help you find out possible causes of problems that you may have encountered.

Since it is very useful to understand the function and content of each of these files, we will make a short summary of their main features, as well as the recommended backup procedures for each of them.

1. CONFIG.SYS

   This is an ASCII file, located in the root directory, that contains all configuration information, commands, and instructions that allow OS/2 to run the programs and hardware you have installed on your computer. The device driver statements included in this file have a direct correlation to the sections of the PROTOCOL.INI file, explained below.

It is important to keep a current backup of the CONFIG.SYS file. We strongly recommend backing up this file before making any changes. Since this file is not locked during operation, it can be backed up to tape or disk at any time.

2. PROTOCOL.INI

   This is an ASCII file, located in the IBMCOM directory in which Multi-Protocol and Transport Services is installed. It contains the network configuration parameters for your workstation and consists of sections that describe the function of the protocol manager, LAPS (LAN Adapter and Protocol Services) configuration information, protocol drivers and adapter drivers.

   The MPTS (Multi-Protocol and Transport Services) component of OS/2 Warp 4 creates the PROTOCOL.INI file based on the configuration of the Network Adapters and Protocol Services during the installation of any networking component of OS/2 Warp 4, such as the File and Print Client.

   Since this file is not locked during operation, it can be backed up to tape or disk at any time.

3. IBMLAN.INI

   This is an ASCII file, located in the IBMLAN directory in which File and Print Sharing Services is installed. It contains the initialization parameters for file and print sharing services configured on your OS/2 Warp 4 workstation. Parameters are placed in a separate section for each service. On a workstation running OS/2 Warp File and Print Client, there are six sections:

```
[networks]
[requester]
[messenger]
[peer]
[replicator]
[services]
```

   On a server machine, there are more sections corresponding to the network services for servers only. You can find more information about those in the OS/2 Warp Server online documentation.

   The IBMLAN.INI file includes the workstation name and the default domain name, as well as most of the network tuning parameters. It also lists the network services that are started when the requester service is started.

   Since this file is not locked during operation, it can be backed up to tape or disk at any time.

4. LANTRAN.LOG

This is a text file that contains information about the network adapter initialization while the workstation is being started.

It is written to the subdirectory that is specified by the /I parameter of the DEVICE= statement for LANMSGDD.OS2 in the CONFIG.SYS file. Usuallly this is the C: IBMCOM directory. If no /I parameter is specified, the LANTRAN.LOG file is written to the root directory of the starting drive. Since the DPATH statement in your CONFIG.SYS file points to the IBMCOM directory, you may execute the command TYPE LANTRAN.LOG from the root directory.

The information written to this file can be very helpful in cases where the system did not start properly. It is also very useful for obtaining the burned-in universal address of your network adapter, which is often required for configuration processes, such as RIPL (Remote Initial Program Load) and to verify the network adapter data rate speed.

Each workstation's start-up creates this file and will therefore overwrite previous startup information. If you plan to use the file at a later time you need to copy the log to another location of the hard disk.

5. NET.ERR

This file, located in the IBMLAN LOGS directory, contains error messages that can be of help for trouble-shooting purposes.

The content of this file can also be accessed by using the following command syntax:

```
 --NET ERROR-/COUNT:number--/REVERSE--/DELETE----------------
```

For example, it you want to view the latest item in the error log, type the following command:

NET ERROR /COUNT:1 /REVERSE

To delete the error log completely, type NET ERROR /D.

6. NET.ACC

This file, located in the IBMLAN ACCOUNTS subdirectory, contains user and group definitions.

There are two types of NET.ACC files:

- The NET.ACC file located on the domain controller, backup domain controllers, and additional servers (application servers).

  This file is used for validating user logon requests and controls access to resources owned by the servers. (For this, the NET.ACC

file is copied by the Netlogon service from the domain controller to all servers in the domain. Note that Access Control Lists (ACLs) are not replicated.

- The NET.ACC file located in each OS/2 Warp File and Print Client workstation.

  This file contains user IDs, group names and access control profiles that are used for the OS/2 Warp peer network.

This file is locked during the operation of the OS/2 Warp File and Print Client, and a utility called BACKACC located in the IBMLAN NETPROG subdirectory is provided (with both OS/2 Warp 4 and OS/2 Warp Server) to help you make backups of it. You can find more information about this utility in the online documentation provided with these products.

10.3.2 Making Changes to the Networking Configuration

There are several ways of making changes to the configuration of the networking components installed on your workstation. The following is a description of the most common methods of making modifications to your networking configuration files.

1. Using the Selective Install for Networking

   If you select the **Selective Install for Networking** object from the Install/Remove folder, located in the System Setup folder within the OS/2 System folder on the Desktop, you are presented with the Selective Install for Networking window, as shown in Figure 41 on page 109. It gives you the choice to go the Easy Installation path or the Advanced Installation path, as explained in 10.2.2, "Installing OS/2 Warp File and Print Client" on page 108.

   Using this method, you can make any configuration changes necessary to your OS/2 Warp File and Print Client. All three network configuration files (CONFIG.SYS, IBMLAN.INI and PROTOCOL.INI) will be updated.

2. Using the File and Print Client Install/Remove Program

   You can find the File and Print Client Install/Remove object within the Install/Remove folder, located in the System Setup folder that resides in the OS/2 System folder on the Desktop.

   Open it to display the IBM Peer for OS/2 Installation/Configuration window. Select the **Configure this workstation** option to make the following changes:

   - Reinstall MPTS.

   - Peer workstation name.

   - Peer workstation description.

- Domain name.

- Replace the NET.ACC file and reset the current definitions.

The File and Print Client Install/Remove Program changes the CONFIG.SYS and IBMLAN.INI files.

Hint

We do not recommend using this method to make netwoking configuration changes for the following reasons:

- It changes the location of the networking icons:

    - It deletes the Logons and the LAN Server Administration objects from the Network Services folder (located in the Network folder within the Connections folder on the Desktop)

    - It creates an OS/2 Peer folder on the Desktop and places all the networking objects in it.

- MPTS configuration cannot be changed. You can only reinstall the files. Therefore the PROTOCOL.INI file cannot be updated.

---

3. Using the Multi-Protocol Transport Services

MPTS (Multi-Protocol and Transport Services) is an OS/2 Presentation Manager application used to install and configure network adapter drivers and network protocol drivers. By means of its functional component called LAPS (LAN Adapter and Protocol Support), MPTS allows you to modify your adapter and protocol configuration.

MPTS creates the PROTOCOL.INI file and adds device driver statements to the CONFIG.SYS file. These are also the two files that are updated each time you make adapter or protocol configuration changes by using MPTS.

You can find the MPTS icon within the System Setup folder, located in the OS/2 System folder on the Desktop.

CONFIG.SYS File Changes

Every time a program makes modifications to your CONFIG.SYS file, you will be asked to shut down your system and restart the workstation to be able to complete the changes requested.

The reason for this is that the statements in the CONFIG.SYS file are executed just once, at workstation start time.

---

4. Using a Text Editor Program

If you prefer to use the command line and your knowledge of the networking configuration files is adequate, you can use a text editor program to make the required modifications to your LAN system files.

Which Method Should You Use?

If you only change the LAN adapter in your machine, it is good enough to go through the Multi-Protocol and Transport Services panels since network adapters are not taken into consideration in the IBMLAN.INI file. However, if you plan to add protocols, we recommend that you choose the Selective Install for Networking path so that all essential files will be updated.

Domain name and workstation names can be changed by going through the panels of the File and Print Client Install/Remove program. Alternatively, you may edit the IBMLAN IBMLAN.INI file using an ASCII editor, such as EPM or TEDIT, and change those names in the `[requester]` section.

10.3.3 Getting to Know the Networking Parameters

There are many configuration parameters that you can modify to improve your system's performance and adjust them to your functional requirements. The following is a summary of the most used network configuration parameters for your OS/2 Warp File and Print Client:

- **Capacity Parameters**

  In the `NETBEUI_nif` section of the PROTOCOL.INI file there are three capacity parameters:

  ```
  SESSIONS
  NCBS
  NAMES
  ```

  that correspond to capacity variables x1, x2 and x3, on the Netx statements in the `[networks]` section in the IBMLAN.INI file. Table 8 illustrates the relation between PROTOCOL.INI capacity parameters and IBMLAN.INI Netx parameters.

Table 8 (Page 1 of 2). PROTOCOL.INI Capacity Parameters vs IBMLAN.INI Netx Parameters	
PROTOCOL.INI Capacity Parameter	**Corresponding IBMLAN.INI** `Netx` **Parameter**
`SESSIONS`	`NetBEUI$,0,LM10,`**`34`**`,100,14`
`NCBS`	`NetBEUI$,0,LM10,34,`**`100`**`,14`

Table 8 (Page 2 of 2). PROTOCOL.INI Capacity Parameters vs IBMLAN.INI Netx Parameters	
PROTOCOL.INI Capacity Parameter	**Corresponding IBMLAN.INI** Netx **Parameter**
NAMES	NetBEUI$,0,LM10,34,100,**14**
Note: The corresponding parameters are highlighted.	

While the PROTOCOL.INI parameters indicate maximum numbers for the whole workstation functionality, the IBMLAN.INI parameters indicate how many resources of the maximum available are reserved for use by the OS/2 Warp File and Print Client. Therefore, x1, x2 and x3 variables must be less than or equal to the SESSIONS, NCBS and NAMES parameters, respectively.

The following is a short description of these parameters:

SESSIONS - x1 While SESSIONS specifies the maximum number of NetBIOS sessions that the workstation can allocate, x1 indicates how many of those sessions will be reserved for the OS/2 Warp File and Print Client.

NCBS - x2 While NCBS (Network Control Blocks) specifies the total number of NCB commands available to all the NetBIOS applications on the workstation, x2 indicates the number of simultaneous NetBIOS commands that the OS/2 Warp File and Print Client can post.

NAMES - x3 While NAMES specifies the maximum number of NetBIOS names assigned to the workstation, x3 indicates the number of these NetBIOS names that the OS/2 Warp File and Print Client allocates.

- **Logon Verification**

  You can specify in the IBMLAN.INI file the type of verification that you want to occur when you perform a logon.

  The logon verification is represented by the thirty 37th digit of the wrkheuristics parameter, and can take the following values:

  - 0   Allows you to log on without your user ID and password being verified.
  - 1   Validates your user ID and password on your local workstation using the local copy of the NET.ACC file.
  - 2   Validates your user ID and password on the domain controller or backup server using the domain copy of the NET.ACC.

  The default value for this parameter is 1.

- **Multiple Domains**

  Your network can have more than one domain. If this is the case and you need to connect to resources, send messages to peer workstations on other domains, or administer other domains, it is easier to access these peer workstations if their domains are listed in the `othdomains` parameter in the `[requester]` section of your IBMLAN.INI file.

  When you add a domain to the `othdomains` parameter, icons for servers and peer workstations in the domains are added to the File and Print Client Resource Browser folder (located in the Network folder within the Connections folder on the Desktop) and in the Shared Resources and Network Connections notebook (located in the Network Services folder within the Network folder in the Connections folder on the Desktop).

  The `othdomains` parameter supports up to four domain names. If you have a network with more than four domains, you can access the systems in the domains not specified in the `othdomains` parameter by using their computer names directly in your Logon panel or in your logon command.

  Alternatively, you can use the `NET CONFIG REQUESTER` command from an OS/2 command line. For example, to make the domain called CONSTELLATION visible in the File and Print Client Resource Browser folder, type the following command:

  `NET CONFIG REQUESTER /OTHDOMAINS:CONSTELLATION`

If you make changes to the IBMLAN.INI file while the OS/2 Warp File and Print Client is running, you will have to stop the client (`NET STOP REQ`) and restart it (`NET START REQ`) before the changes take effect.

```
┌─── Other Parameters . . . ──────────────────────────────────────┐
│                                                                  │
│  There are many other parameters that can be configured to adjust your │
│  system to your working requirements.  You can obtain more information │
│  about them from the online information provided in OS/2 Warp 4 and │
│  OS/2 Warp Server.                                               │
│                                                                  │
└──────────────────────────────────────────────────────────────────┘
```

10.3.4 Using the Graphical User Interface

After OS/2 Warp 4 installation, the Connections folder, as shown in Figure 66 on page 149, appears on your desktop.
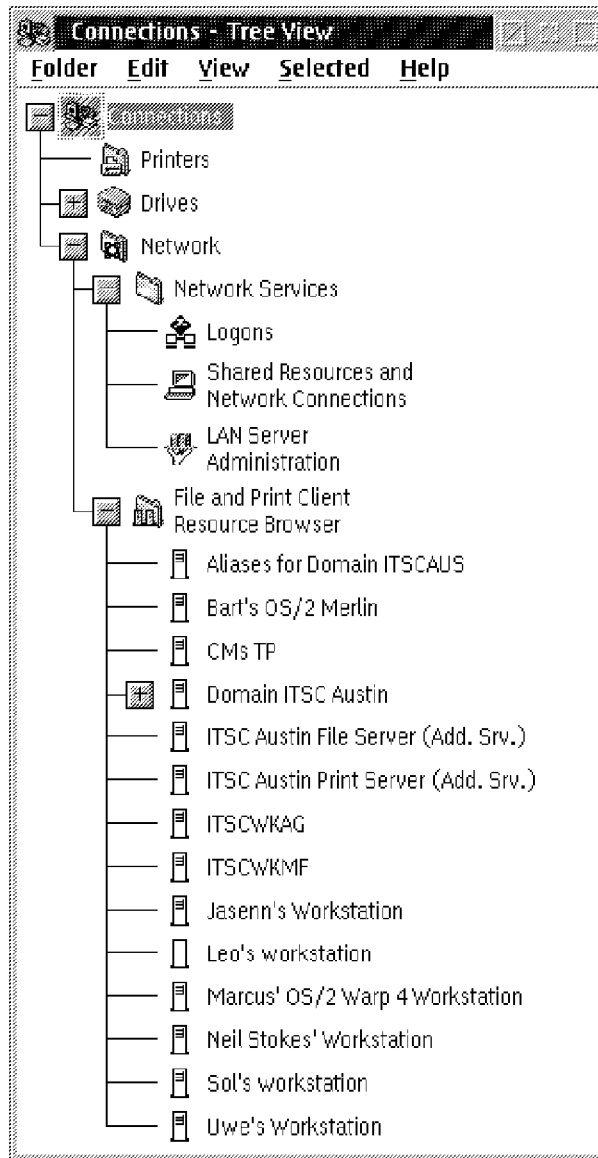
Figure 66. Connections Folder

With the functions that the Connections folder provide, you can work with and explore the LAN. For example, you can work with and manage your peer network, LAN domains, drives, printers, and the World Wide Web depending on the networking components you have installed on your workstation. The Connections folder contains the following objects:

Printers   This folder contains printer objects to manage your local and network-connected printers.

Network   This folder contains objects that enable you to administer network servers, access and share resources on the LAN or on your workstation.

Drives   This folder contains drives objects to manage your diskette drives, hard disks and CD-ROM drive.

Web Sites This folder contains objects that link to many different kinds of pages on the World Wide Web, such as education, computing, entertainment, and OS/2-related Web pages.

In this section, we focus on the Network and Printers folders:

10.3.4.1 Network Folder

When you install the OS/2 Warp File and Print Client, the Network folder appears in your Connections folder. The tools and utilities contained in this folder allow you to:

- Log on or log off from peer networks or LAN domains.

- Browse all the network resources available to you.

- Access files, directories and printers using drag and drop techniques with the Workplace Shell.

- Assign logical drive letters and ports to network resources so you can access them from applications that require a drive letter or port name.

The objects contained in the Network folder depend on the networking components you choose to install. For example, the Logons and LAN Server Administration objects appear in the Network Services folder only if you select the Install LAN Server Administration option in the OS/2 Warp File and Print Client Advanced Installation path, and the Shared Resources and Network Connections object appears in the Network Services folder only if you select the **Install Sharing** option in the OS/2 Warp File and Print Client Advanced Installation path. For more information about these options, refer to 10.2.4, "Advanced Installation" on page 123.

The following is a brief description of the objects that reside in the **Network Services** folder.

- LAN Server Administration

  The LAN Server Administration folder, as shown in Figure 67 on page 151, contains a set of utilities that allow you to administer an OS/2 Warp Server domain from your peer requester machine.
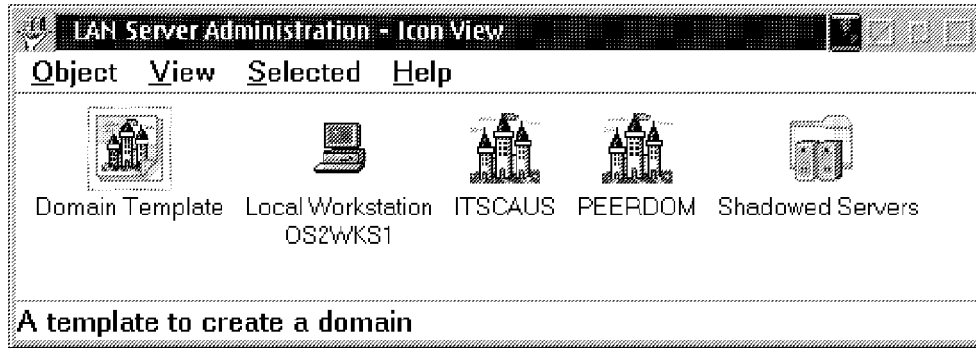
Figure 67. LAN Server Administration Folder

The LAN Server Administration Graphical User Interface (GUI) is started by using the `NETGUI` command from an OS/2 command line.

- Logons

The Logons folder, as shown in Figure 68, contains objects that allow you to log on to a peer network or LAN domain, log off, start your OS/2 Warp File and Print Client services and even manage your LAN user account from the Network User Account notebook.
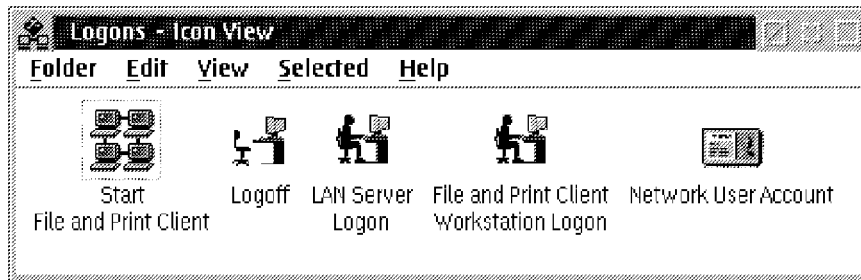
Figure 68. Logons Folder

The `LOGON` or `LOGOFF` commands are entered in an OS/2 command line session followed by parameters, for example:

`LOGON UserId /P:password /V=D`

Verfiation is done by the domain controller or backup domain controllers, depending on which server gets the logon request first.

`LOGON UserId /P:password /L`

Verification is done locally. If you are logged on to the domain and want to manage your local peer resources, you are not prompted to logon locally if the user ID and password at the local workstation are the same as defined at the domain controller.

A Logoff window from which you can select the session to log off from will be presented by typing the following command:

```
LOGOFF /L
```

For example, you can select to log off from the LAN only while staying logged on locally. If you type `LOGOFF` only you will be logged off from all sessions.

The Network User Account notebook, as shown in Figure 69, allows you to change the password for the peer network or the LAN domain to which you are logged on, provides information about your user ID, lets you change the description of your user account and, when you are logged on with sufficient access authority, allows you to make changes to your network logon assignments.

Note: Logon assignments are the connections you want to have established automatiallly to shared resources on the domain whenever you log on to that domain.
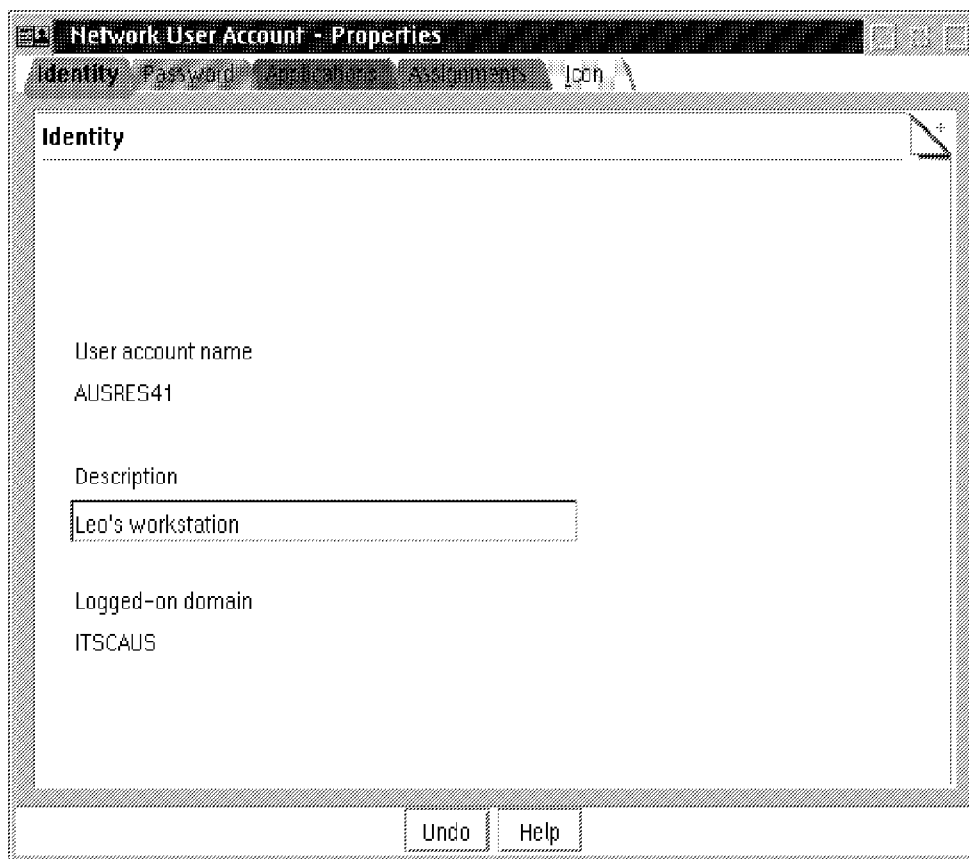
Figure 69. Network User Account Notebook

- Shared Resources and Network Connections

  In this notebook, as shown in Figure 70 on page 153, you display or create connection definitions, specify which resource on the LAN to connect to and assign the resource a local device name. These

definitions allow easily connect to and disconnect from shared resources.

You can also share your peer network resources (disks, printers or serial devices) through the Shared Resources and Network Connections notebook.
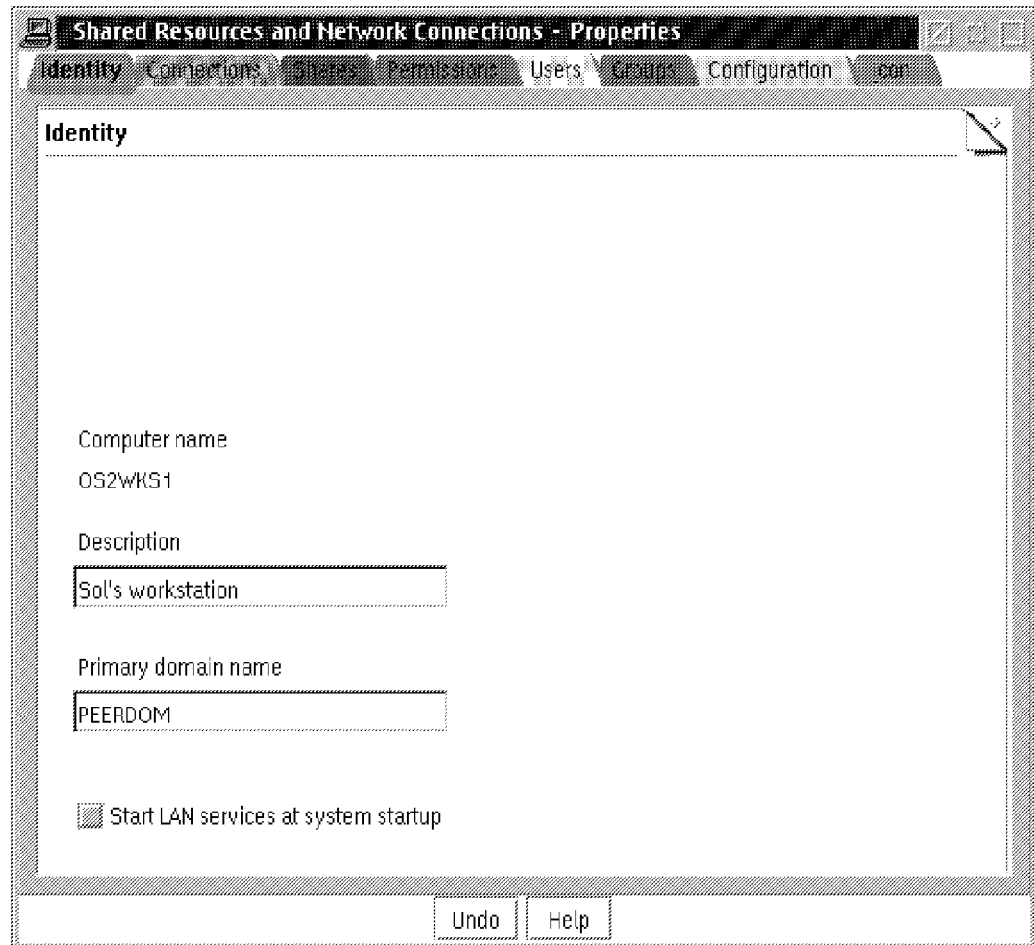
Figure 70. Shared Resources and Network Connections Notebook

Note: The entries in the Shared Resources and Network Connections notebook depend on the type of logon you perform (LAN domain or local LAN logon). The notebook shown in Figure 70 corresponds to a local LAN logon.

After installing the OS/2 Warp File and Print Client, your Network folder contains the File and Print Client Resource Browser folder as shown in Figure 71 on page 154.
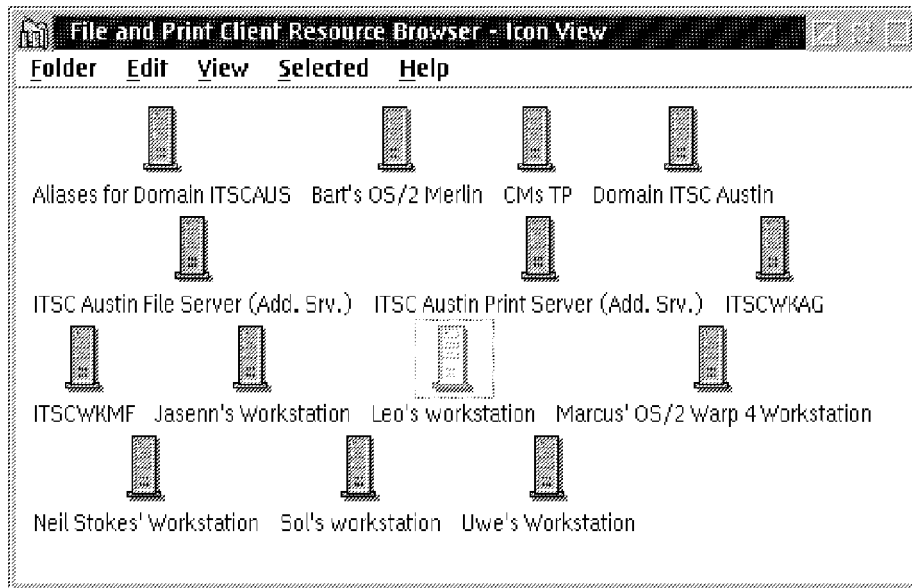
Figure 71. File and Print Client Resource Browser Folder

This folder presents all network stations in your domain you are logged-on to as well as domains that are listed in the OTHDOMAINS statement in the IBMLAN.INI file. Domain controllers, backup domain controllers, additional servers (application servers), and OS/2 Warp 4 peer workstations appear in this folder.

If you open the File and Print Client Resource Browser folder without logging on to the appropriate network environment, a dialog box is displayed asking you for your user ID and password.

Make a LAN Domain Logon First...

If you open the File and Print Client Resource Browser folder and log on at this point, you will be logged on to your peer network only. This means that you cannot browse any resources on servers, even if you normally have access to them.

To avoid this problem, log on to your LAN domain before you open the File and Print Client Resource Browser folder. If you have the same user ID and password for your peer network and your LAN domain, you can use the resource browser to view both peer and server resources.

The File and Print Client Resource Browser folder displays peer workstations to which you have access, but only displays servers and aliases for the domain to which you are currently logged on as well as domains listed in the OTHDOMAINS statement in the IBMLAN.INI file and

domains that were defined with the NET CONFIG command (see example on page 148). This is known as your browse scope.

If you want to access a resource on a server that is not within your browse scope, click your right mouse button on any of the server objects in the resource browser window to display a context menu, and select the **Access Another...** menu item. The Access another server window, as shown in Figure 72, is displayed.
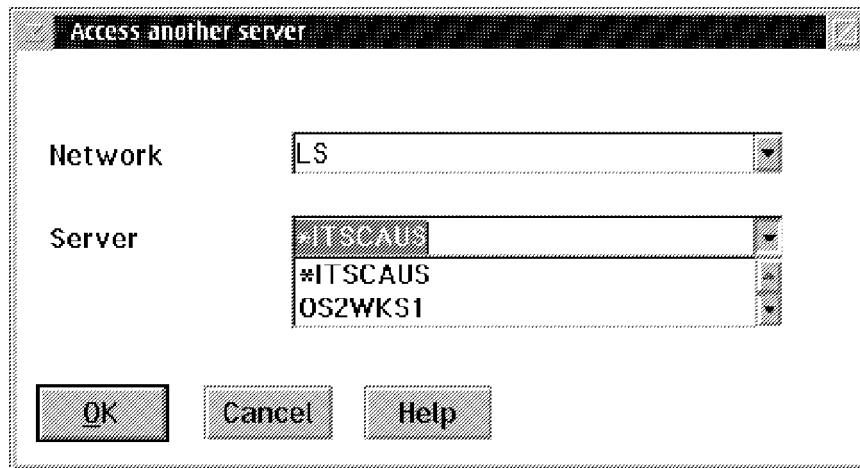
Figure 72. Access Another Server Window

All the servers within your browse scope are listed in the Server pull-down menu. Alternatively, you can enter the name of a new server, peer workstation, or domain in this field.

Note: If you enter a domain name, it must be preceded by an asterisk (*).

If you want the resources of another domain to be permanently displayed in your resource browser window, add the name of the domain to the othdomains parameter list in the IBMLAN.INI file. For more information about this parameter, refer to 10.3.3, "Getting to Know the Networking Parameters" on page 146.

From the File and Print Client Resource Browser folder, you can make either implicit or explicit connections to resources on servers or peer workstations.

• Implicit Connections

    An implicit connection allows you to access a resource from the File and Print Client Resource Browser folder without assigning the resource to a local device (drive letter or port number).

    When you open a directory folder or printer through the File and Print Client Resource Browser folder by double-clicking on that resource

object, you make an implicit connection to that directory or printer. This type of connection does not specifically assign a local device name to the resource.

- Explicit connections

  When you assign a local device name to a resource, you make an explicit connection. A local device name is a label on your workstation used to identify a shared resource on a server or peer workstation.

  The type of resource (directory, printer or serial device) that you use determines the local device name you should use:

  - Local device names for directories and files are drive letters: `D`, `E`, `F`, and so on.
  - Local device names for printers are printer port numbers: `LPT1`, `LPT2`, `LPT3`, and so on.
  - Local device names for serial devices are serial device port numbers: `COM1`, `COM2`, `COM3`, and so on.

  To assign drive letters or ports, select the **Assign Drive...** or **Assign Port** options, respectively, from the context menu of the objects in question. This is very useful if you wish to access these network resources from within an application that may need to refer to logical drive letters or ports.

  When you assign a device to a network drive, a drive object is created and placed in the Drives folder (which resides in the OS/2 System folder). However, when you assign a port number to a network printer or serial device, no printer or serial device object is created. If a printer object is needed, you can create one by shadowing the object to your desktop.

  To shadow a network object on your desktop, simply drag and drop the object from the File and Print Client Resource Browser into any folder on your desktop. This lets you group objects in the way that best suits your working requirements.

  If you access an object that is a shadow of a network object and you are not currently logged on to the network, a dialog box is automatically displayed asking for your user ID and password, so you can log on.

10.3.4.2 Printers Folder

The Printers folder, as shown in Figure 73 on page 157, contains objects for each printer that you have installed in your system, as well as templates for creating local and network printers.
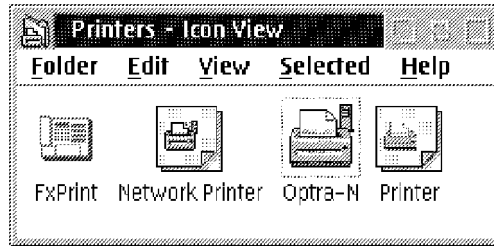
Figure 73. Printers Folder

Use the Printer template to create a local printer object or the Network Printer template to create a network printer object that connects to a network printer.

Note: If no Printer template exist in the Printers folder, create a local Printer object by using the Printer template that resides in the OS/2 System's Templates folder.

Alternatively, you can use the File and Print Client Resource Browser folder to work with network printers as explained in 10.3.4.1, "Network Folder" on page 150.

OS/2 Warp 4 needs to have the correct printer device driver installed on your workstation, even if the printer is attached to a server on the network. This is because network printing in OS/2 Warp requires a driver in your system as well as on the server.

To simplify your printers installation procedure we recommend configuring your OS/2 Warp Server to support automated download of printer device drivers to OS/2 Warp 4 clients, as explained in the next section.

10.3.4.3 Automated Printer Driver Install to OS/2 Warp 4 Workstations

When you create local printer and network printer objects, OS/2 can automatically install the OS/2 and WIN-OS/2 (if supported by WinOS/2) printer drivers for the printer object. To enable OS/2 Warp 4 to automatically install printer drivers from the server, the LAN administrator must setup a shared directory from which OS/2 File and Print Clients can automatically download required printer drivers.

To automatically install printer drivers, log on to the LAN domain. When you create a local printer object or a network printer object on your desktop, OS/2 Warp 4 first checks whether the required printer driver has already been installed on your workstation. If the driver is not installed OS/2 Warp 4 searches in the order specified for the following paths to the printer driver:

1. It searches the OS2SYS.INI system file for an application named PM_SPOOLER_DRVSHARE. The key names for this application name are server names. The key value is the path for the server to the printer drivers that can be downloaded to clients.

2. If OS/2 Warp 4 finds the application name, it uses the first key value with the path that contains the printer driver.

   For example, the following is an entry for the print server PRINTSRV on an OS/2 Warp Server domain. The user issued the NET USE command for a virtual drive X:, which contains the directory DRVS with printer drivers that can be downloaded to OS/2 Warp File and Print Clients:

   - Application Name: PM_SPOOLER_DRVSHARE
   - Key Name: LS:\\PRINTSRV
   - Key Value: X:\DRVS

3. If no PM_SPOOLER_DRVSHARE entry exists, OS/2 Warp 4 searches the print server for a directory share named PRINTDRV.

4. If OS/2 Warp 4 does not find an entry for PM_SPOOLER_DRVSHARE or a directory share named PRINTDRV, it searches the user's logon domain for a directory alias named PRINTDRV. This alias enables you to store all printer drivers in a common place for all users in the domain.

OS/2 Warp 4 uses the path it finds to automatically download printer drivers as follows:

1. Search the root of the path for packed files (*.DR_).

2. Search the root of the path for unpacked files (*.DRV).

3. Search the subdirectory OS2DRV of the path for packed or unpacked files.

4. Search the subdirectory PMDD_n of the path, where n is the printer driver diskette number and the subdirectory has the contents of the printer driver diskette.

   For example, to share all printer dirvers, the administrator can create the following directories:

   D:\DRVS.
   D:\DRVS\PMDD_1, which contains OS/2 printer driver diskette 1.
   D:\DRVS\PMDD_2, which contains OS/2 printer driver diskette 2.
   D:\DRVS\PMDD_3, which contains OS/2 printer driver diskette 3.
   D:\DRVS\PMDD_4, which contains OS/2 printer driver diskette 4.
   D:\DRVS\PMDD_5, which contains OS/2 printer driver diskette 5.
   D:\DRVS\PMDD_6, which contains OS/2 printer driver diskette 6.

10.3.5 Sharing Your Peer Network Resources

There are many resources on your OS/2 Warp 4 system that you might want to share with another user on the network. To do so, log on with the peer administration user ID and password.

The following describes the graphical alternatives to share and administer your workstation's resources.

1. Using the Workplace Shell

    To share a drive, directory or printer directly from the Workplace Shell, click your right mouse button on the object to display its context menu, and select the **Start sharing...** option. The Create a Share window, as shown in Figure 74, is displayed.
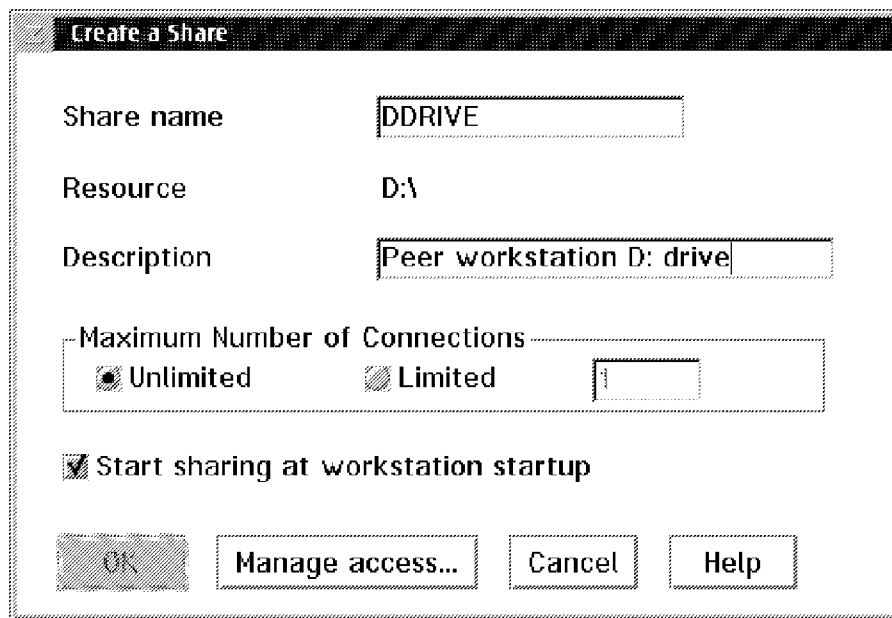
Figure 74. Create a Share Window

In this window you can specify any additional information not already known about the resource.

The Share name field determines the name by which other users will identify and connect to this resource on the network, so it should be short but descriptive. This name appears in your own Shared Resources and Network Connections notebook, explained below in this section. OS/2 Warp 4 provides a default name, but you can change it if you wish.

Note: Shared names for printers cannot be changed.

The Resource field identifies the local device name or path of the resource on your computer. Since you have already specified this information, you cannot change it here. If you find you have made a mistake and do not wish to share the resource as indicated, select the **Cancel** button to cancel sharing and then start again with the correct resource.

The Description field is optional, and simply provides additional information about the resource. You can place any other information about the resource in this field.

Maximum Number of Connections allows you to control the number of users who can concurrently access this resource. For example, if you want to share documents with your secretary team you can grant access to one or more people at a time. Select **Unlimited** to allow anyone to access the resource, or select **Limited** and specify in the field at the right the maximum number of users that can access your shared resource simultaneously.

If you want the resource to be shared automatically when you start your computer, select the **Start sharing at workstation startup** check box.

At this point, you have defined the shared resources on the LAN. However, OS/2 Warp 4 does not allow any other users to access this resource until you define access control privileges for the resource. These privileges form part of the share profile for the resource, and prevent other users from accessing your resources until you grant them access. To define access control privileges from this point, select the **Manage access...** button. You can find more information about how to manage access to resources below in this section.

If you have previously shared an object and you want to update the access profile for the resource (that is, the users who may access it and the level of access granted to each user), select the **Update share** option from its context menu. The Update a Share window, as shown in Figure 75 on page 161, is displayed.

```
┌─────────────────────────────────────────────────────────────┐
│ ▓ Update a Share                                            │
├─────────────────────────────────────────────────────────────┤
│                                                             │
│   Share name             DDRIVE                             │
│                                                             │
│   Resource               D:\                                │
│                                                             │
│   Description            ┌──────────────────────────────┐   │
│                         │ Peer workstation D: drive     │   │
│                          └──────────────────────────────┘   │
│                                                             │
│   ┌─Maximum Number of Connections────────────────────────┐  │
│   │  ● Unlimited          ▓ Limited       ┌─────────┐    │  │
│   │                                       │ 1       │    │  │
│   │                                        └─────────┘    │  │
│   └──────────────────────────────────────────────────────┘  │
│                                                             │
│   ▓ Start sharing at workstation startup                    │
│                                                             │
│   ┌────────┐  ┌──────────────────┐  ┌────────┐  ┌────────┐  │
│   │  OK    │  │  Manage access...│  │ Cancel │  │ Help   │  │
│   └────────┘  └──────────────────┘  └────────┘  └────────┘  │
│                                                             │
└─────────────────────────────────────────────────────────────┘
```
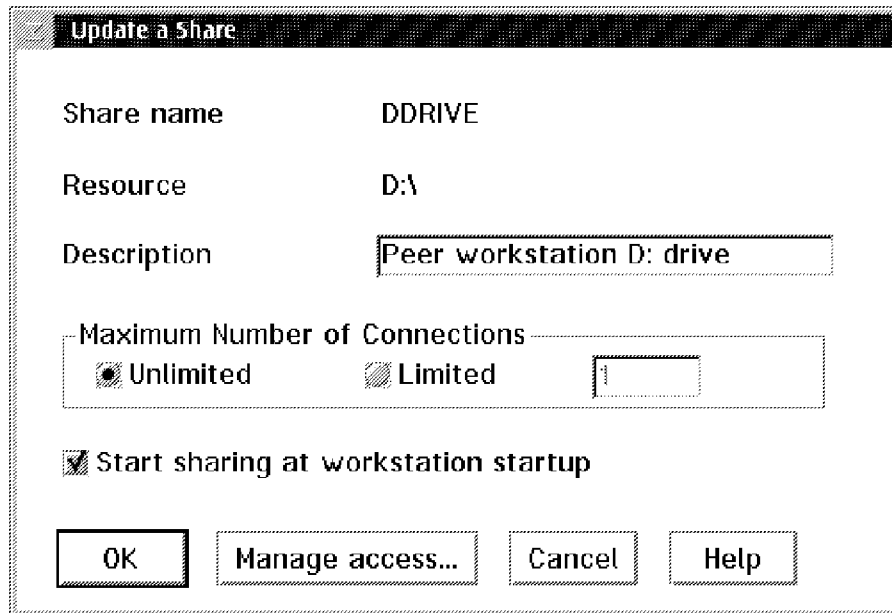
Figure 75. Update a Share Window

From this window you can modify all the information that we have just
described for the Create a Share window.

Note: When you provide information for creating a new share profile,
you cannot select the **OK** button until you have provided access
control information for your resource. Working on the **Update a
Share** window allows you to select **OK** right away, because you
have already provided access information when creating the
share profile.

Alternatively, you can open the resource's Properties notebook, and
select the **Shares** tab, as shown in Figure 76 on page 162, to start
sharing the resource.
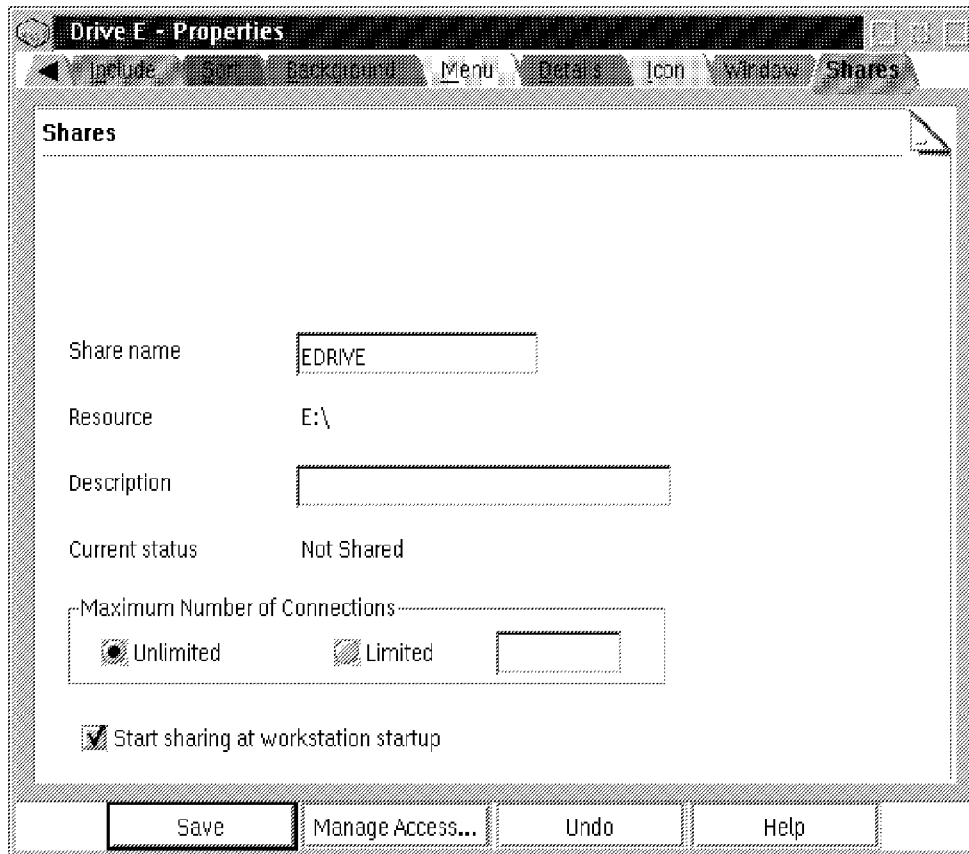
Figure 76. Resource Sharing by Using the Object's Properties Notebook

Using this method gives you the same configuration alternatives presented in the object's context menu options. In addition, there is an extra information field that indicates the current status of the shared resource.

2. Using the Shared Resources and Network Connections Notebook

The Shared Resources and Network Connections utility, located in the Network Services folder within the Connections folder on the Desktop, allows you to share resources and configure the access to them.

To share a resource, select the **Shares** tab from the Shared Resources and Network Connections notebook, as shown in Figure 77 on page 163.
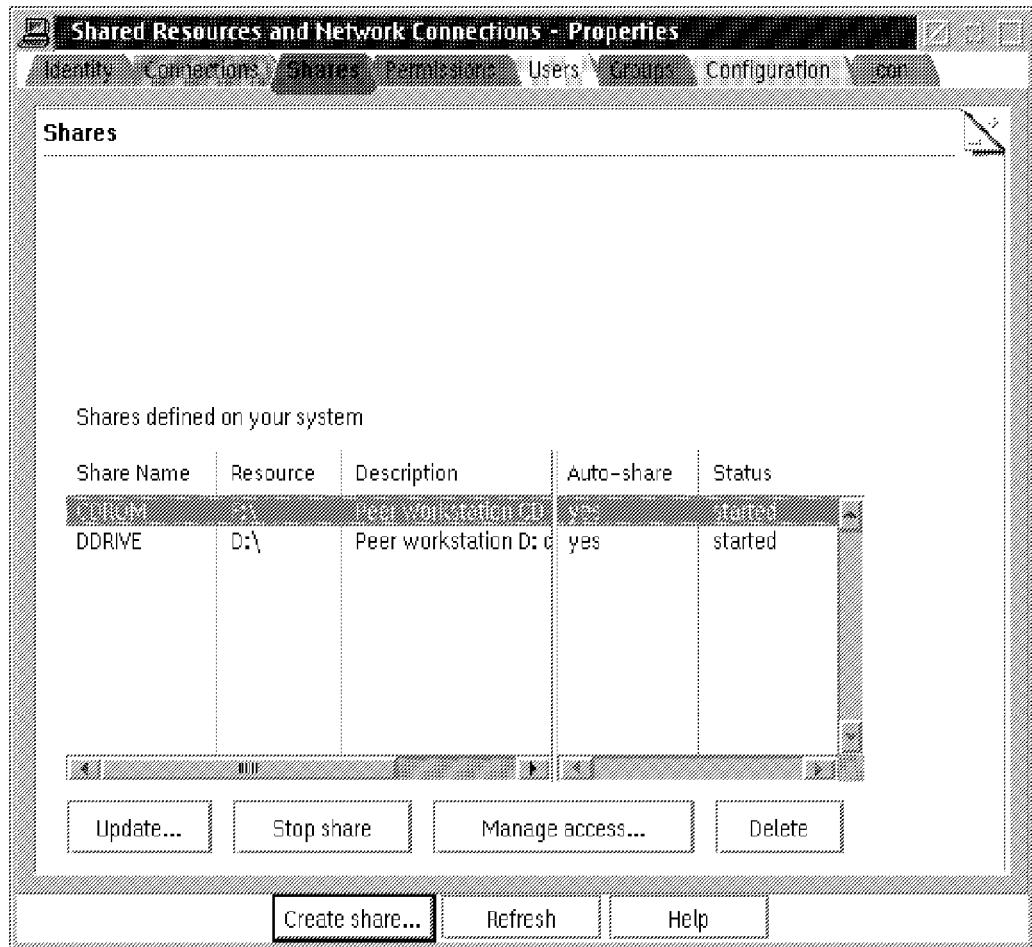
Figure 77. Shared Resources and Network Connections Notebook

Then, either drag and drop any resource object (printer, drive or directory) from your desktop or other folder into the Shares page, or select the **Create share...** button in the Shared Resources and Network Connections notebook to define a new resource to be shared.

In the former case, the Create a Share window shown in Figure 74 on page 159 is displayed, and can perform the configuration as we have just explained for this window. In the latter case, the Select a Resource to Share window, as shown Figure 78 on page 164, will be displayed.
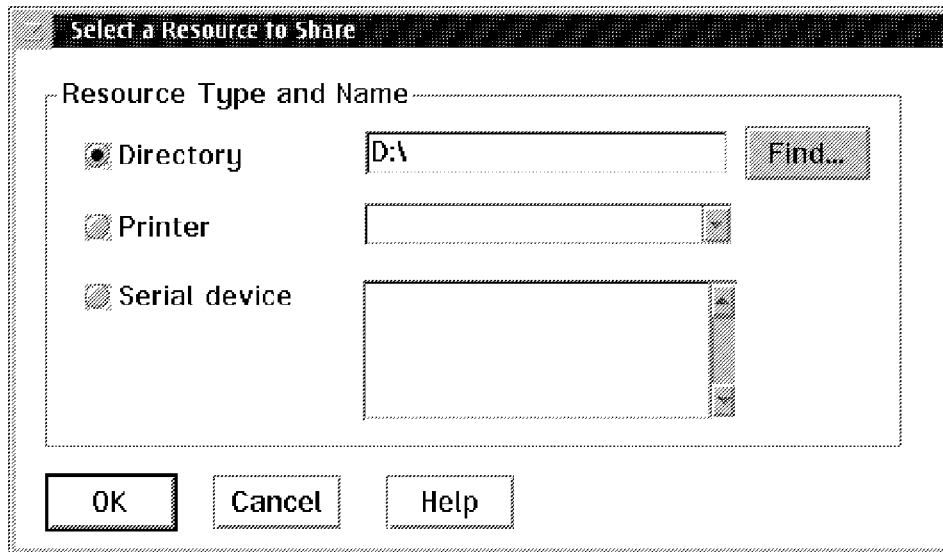
Figure 78. Select a Resource to Share Window

In this window, you can select the radio button of the type of resource you wish to share, such as Directory, Printer, or Serial device.

If you want to share an entire drive (especially one with removable media, such as a CD-ROM), select only the drive letter, such as D:, with no succeeding backslash. This avoids creating an Access Control List (ACLs) for a single CD-ROM which you might need to update for a different CD-ROM. If you want to share a directory rather than an entire drive, enter the fully qualified path to that directory.

If you are sharing an application, share the directory that contains the application and the files it needs to run. If all application files are not already in one directory, put them in the same directory to simplify sharing the application reduce the possibility of a user receiving errors while running the application.   Some applications store their Dynmaic Link Library (DLL) files in the OS2 DLL directory. If some of the files must reside in other subdirectories, it is especially important to grant access to these subdirectories for any other users who will access the application.

If you want to share a printer or a serial device, select the appropriate radio button, and select the name of the resource from the list provided.

Select the resource you want to share and click on the **OK** button to open the Create a Share window, as shown in Figure 79 on page 165.

```
┌─────────────────────────────────────────────────────────────┐
│ ▓Create a Share▓                                             │
│                                                               │
│   Share name              ┌─────────────────────┐            │
│                           │FDRIVE               │            │
│                           └─────────────────────┘            │
│                                                               │
│   Resource                F:                                  │
│                                                               │
│   Description             ┌─────────────────────┐            │
│                           │Peer workstation CD-ROM│          │
│                           └─────────────────────┘            │
│                                                               │
│   ┌─Maximum Number of Connections────────────────┐           │
│   │  ⦿ Unlimited         ▨ Limited    ┌───────┐  │           │
│   │                                    │1      │  │           │
│   │                                    └───────┘  │           │
│   └───────────────────────────────────────────────┘          │
│                                                               │
│   ☑ Start sharing at workstation startup                     │
│                                                               │
│   ┌────────┐ ┌────────────────┐ ┌──────────┐ ┌────────┐      │
│   │  OK    │ │ Manage access...│ │  Cancel  │ │  Help  │      │
│   └────────┘ └────────────────┘ └──────────┘ └────────┘      │
└─────────────────────────────────────────────────────────────┘
```
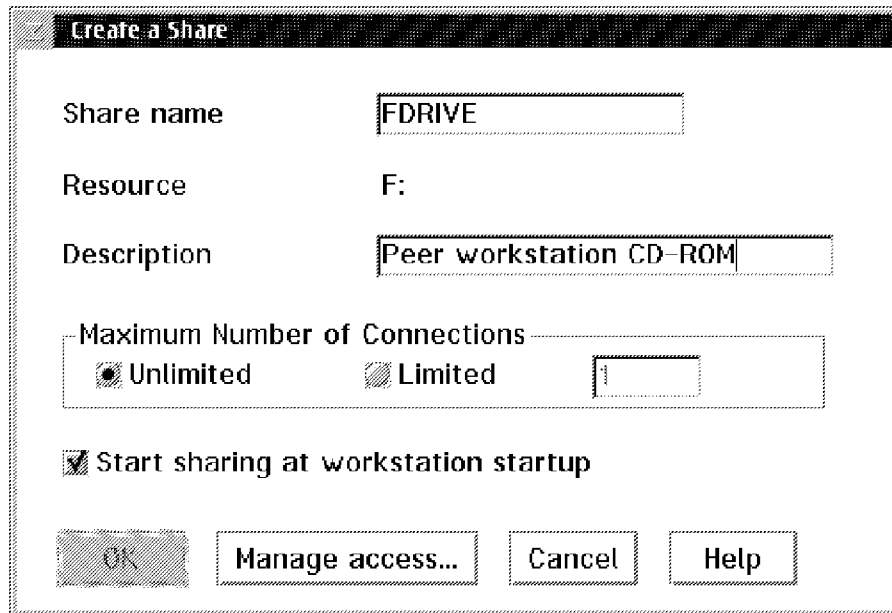
Figure 79. Create a Share Window

Sharing a CD-ROM

You should always keep in mind that when you share a CD-ROM,
you only need to specify its corresponding drive letter, as shown in
the example in Figure 79, and not the root directory F: . This allows
you to change the CD-ROM from the CD-ROM drive, and still be able
to make the resource available without modifying its access control
list.

In this window you can configure the same information described above
for the Create a Share window.

10.3.5.1 Managing Access to Resources

When you share disks and directories as resources on the network, you
must grant access to these resources before anyone in the network can
access or use them. In this way, OS/2 Warp 4 ensures that the information
on your computer is secure, and not available to unauthorized users.

Note that by default, OS/2 Warp 4 allows all users access to printers or COM
ports that you share as resources. You do not need to define specific
access control privileges for printers or COM ports.

Before sharing or accessing resources on the LAN, each user needs to log
on to their computer locally, just as you do. Their user ID identifies them to
their computer, and to your computer when they access resources on your
computer. You can tell OS/2 Warp 4 to allow different users to access

different resources, and only the users that you specify will be able to access your resources.

In order to simplify matters when you are granting access to resources, OS/2 Warp 4 lets you create groups of users, and then assign levels of access to the entire group. In this way, you do not need to assign levels of access to every individual user. This speeds up the process.

When you grant access to a resource, you create an access control profile for that resource which is stored as part of the share profile for the resource. The access control profile specifies which users have access to a shared resource on your computer, and what type of access these users have. A detailed view of all existing access control profiles on your workstation is provided by the Permissions page in your Shared Resources and Network Connections notebook, as shown in Figure 80.
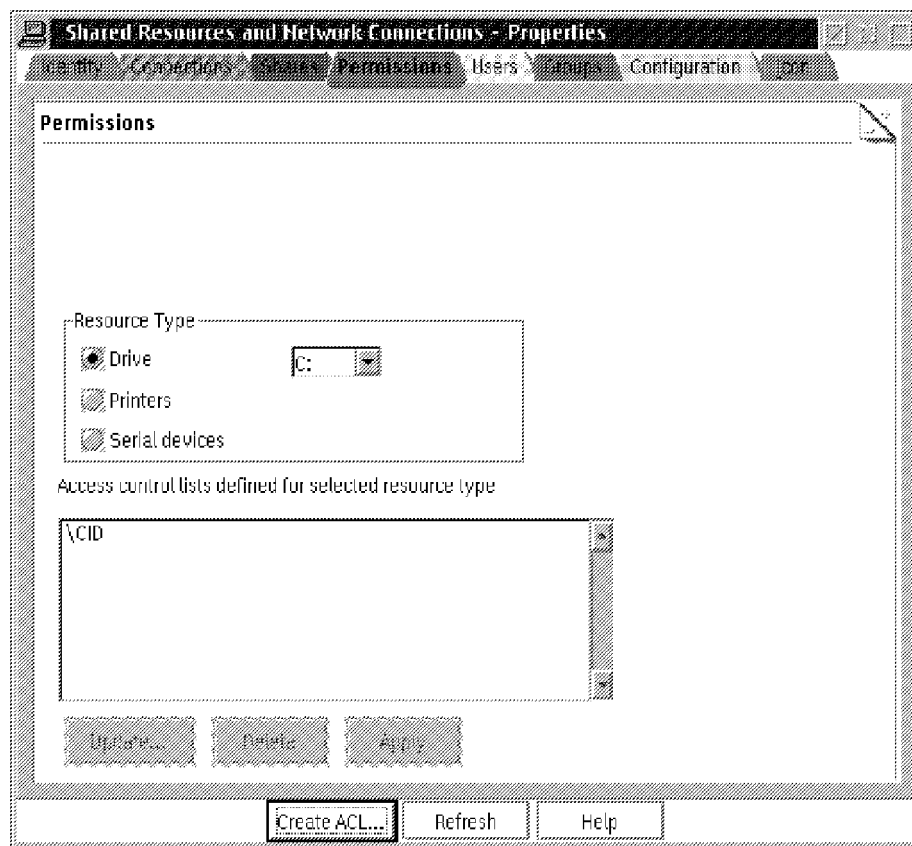
Figure 80. Shared Resources and Network Connections - Permissions Page

You can create access control profiles in any of the following ways:

• Select the **Manage access...** button on the resource object's context menu.

- Select the **Manage access...** button on the Shares tab in the resource's Properties notebook.

- Select the **Manage access...** button from the Shares page in the Shared Resources and Network Connections notebook.

Each case the Manage Access window, as shown in Figure 81, is displayed.

Figure 81. Manage Access Window

In this window, you can specify the type of access that you want for your resource. You can manage access to your resources in one of two ways:

Basic access   Allows all users to have the same level of access to your resource. For example, read access only.

Customized access Specifies different levels of access for different users on the network.

The following is a more detailed description about how to define basic and customized accesses:

- **Basic Access**

  If you want to grant the same level of access for all users, select the **Basic - one access for all users** option from the Manage Access window, as shown in Figure 81 on page 167, and then decide which level of access you want to give users accessing this resource: No access, Read only or Read/Write access.

  If you want to keep a record of who accesses this resource, select the **Audit this resource** check box. When you select this option, any future access to this resource is recorded in the audit log.

  Select the **OK** button to receive the message as shown in Figure 82, letting you know that the access permissions have been created.

  ```
  Create Access Permissions

  ⚠  The access permissions have been
      created.

  ┌──────┐
  │  OK  │
  └──────┘
  ```
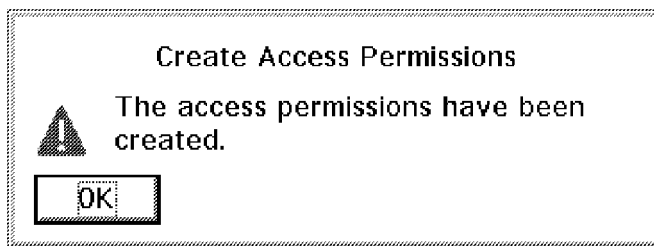
  Figure 82. Create Access Permissions Information Message Window

  If this resource is a directory that has subdirectories, OS/2 Warp 4 asks whether you wish to apply this level of access to the subdirectories as well, as shown in Figure 83.

  ```
  Apply Access Permissions

  ❓  This directory has subdirectories.
      Select OK to apply the access
      permissions to the subdirectories.

  ┌──────┐   ┌──────────┐
  │  OK  │   │  Cancel  │
  └──────┘   └──────────┘
  ```
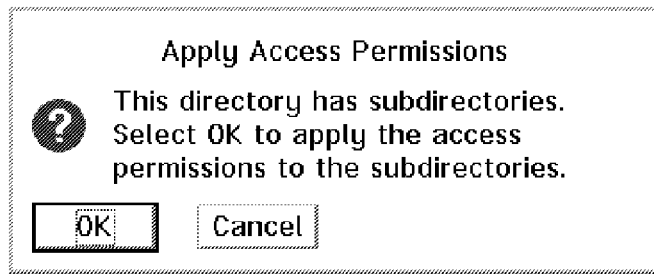
  Figure 83. Apply Access Permissions Information Message Window

  Select **OK** to apply the access to all subdirectories.

  ┌─ **Apply ACLs** ──┐
  │   │
  │ The apply function replaces ACLs that exist down the tree.   │
  │   │
  └──┘
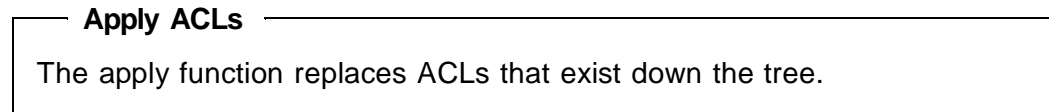
  Select **Cancel** to apply the specified level of access to the parent directory only. No network users will have access to the subdirectories unless they are specified as administrators on your machine.

Notes:

Perform the follwing tasks to change the user's level of privileges:

1. Type `UPMACCTS` from an OS/2 command line.

2. Select **Select destination...** from the Actions pull-down menu.

3. Select the radio button for **Local workstation** and select **OK**. Then select **Manage Users...** from the Manage pull-down menu.

4. In the User ID list double-click on the user you want to make updates to and select **Update user information...**. The Actions pull down menu also allows you to add user IDs.

· **Customized Access**

If you want to grant different levels of access to different users, select the **Customized** option in the Manage Access window. Selecting this button causes the contents of the window to change, as shown in Figure 84.
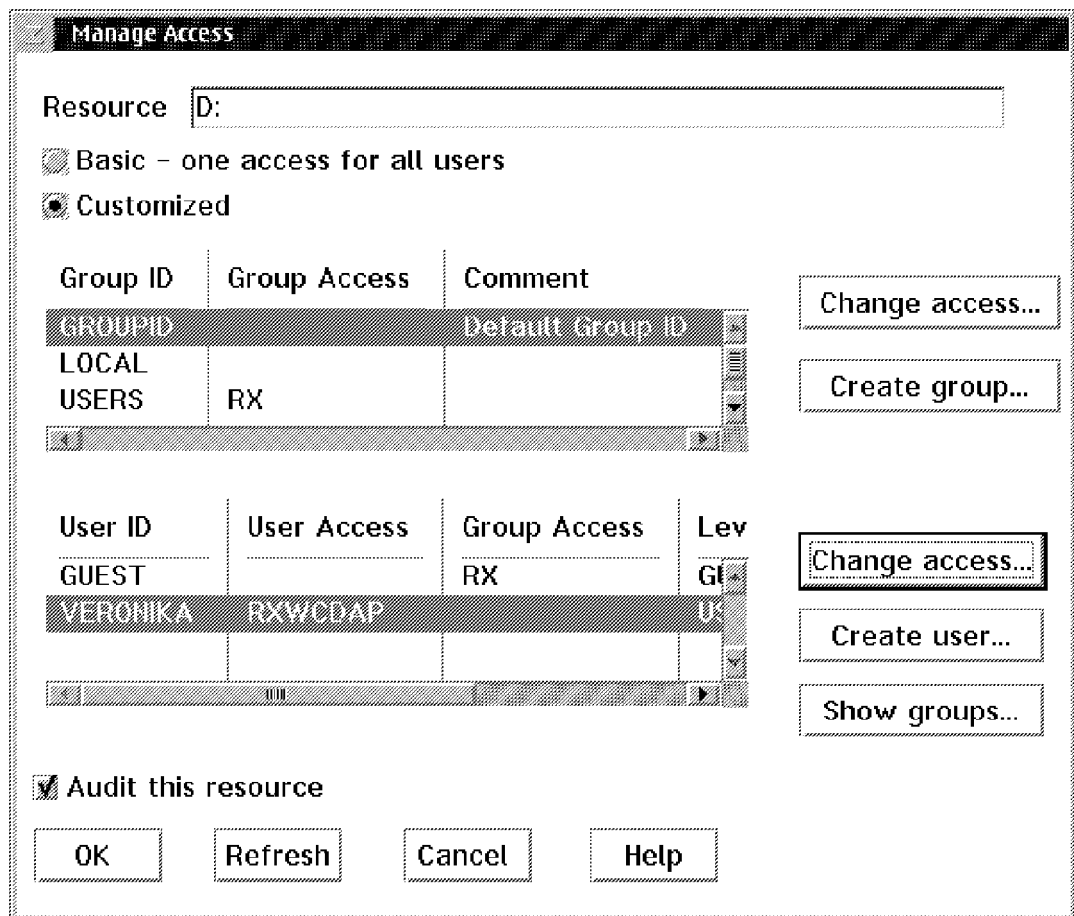
Figure 84. Manage Access Window

All users and groups of users defined in your OS/2 Warp 4 system are listed in this window, along with their current access permissions for this resource.

In the upper part of this window you can see the list of groups that are already defined in your peer network. There are two buttons:

- `Change access...`

- `Create group...`

If you select a group and click on the **Change access...** button, the Change Access Permissions window, shown in Figure 85, is displayed.

```
┌──────────────────────────────────────────────────────┐
│ Change Access Permissions                            │
│                                                      │
│  Resource name     │D:│                             │
│                                                      │
│  User or group name  │GROUPID                      │ │
│  ┌─Access Permissions──────────────────────────────┐ │
│  │ ░None             ░Create                       │ │
│  │                                                 │ │
│  │ ░Read             ░Delete                       │ │
│  │                                                 │ │
│  │ ░Write            ░Attributes                   │ │
│  │                                                 │ │
│  │ ░Execute          ░Permissions                  │ │
│  │                                                 │ │
│  └─────────────────────────────────────────────────┘ │
│                                                      │
│  ┌────────┐   ┌────────┐   ┌────────┐              │
│  │   OK   │   │ Cancel │   │  Help  │              │
│  └────────┘   └────────┘   └────────┘              │
└──────────────────────────────────────────────────────┘
```
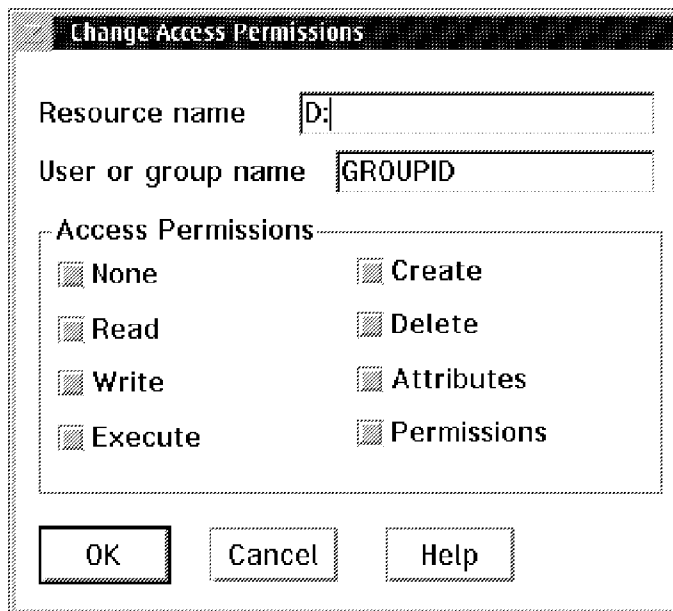
Figure 85. Change Access Permissions Window

In the Change Access Permissions window you can change the access permissions for the selected group.

You can also create a new group by clicking on the **Create group...** button. The Create a Group window, as shown in Figure 86 on page 171, is displayed.
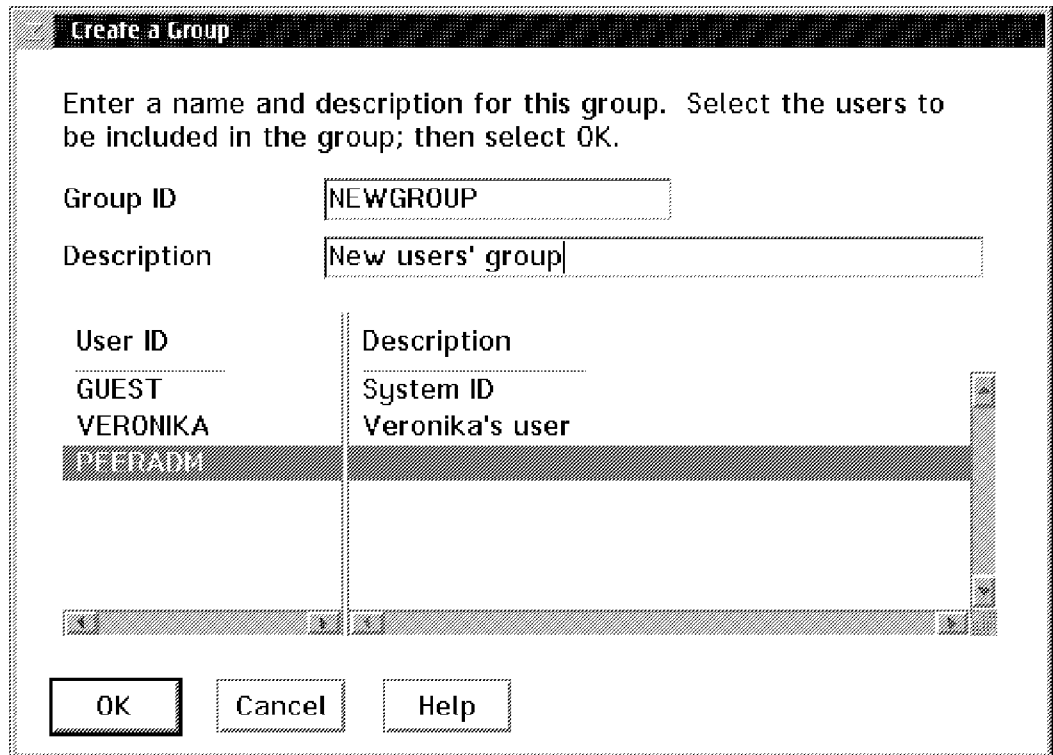
Figure 86. Create a Group Window

In the Create a Group window enter the name and descripton of the new group that you want to create, as well as the users to be included in it.

In the lower part of the Manage Access window, shown in Figure 84 on page 169, you can see the list of users that are already defined in your peer network, and you have three buttons to select: `Change access...`, `Create user...`, and `Show groups....`

Select a user and click on the **Change access...** button to open the Change Access Permissions window, as shown in Figure 85 on page 170. In this window can change the access permissions for the selected user.

You can create a new user by clicking on the **Create user...** button. In this case, the Create a User Account window, as shown in Figure 87 on page 172, is displayed.
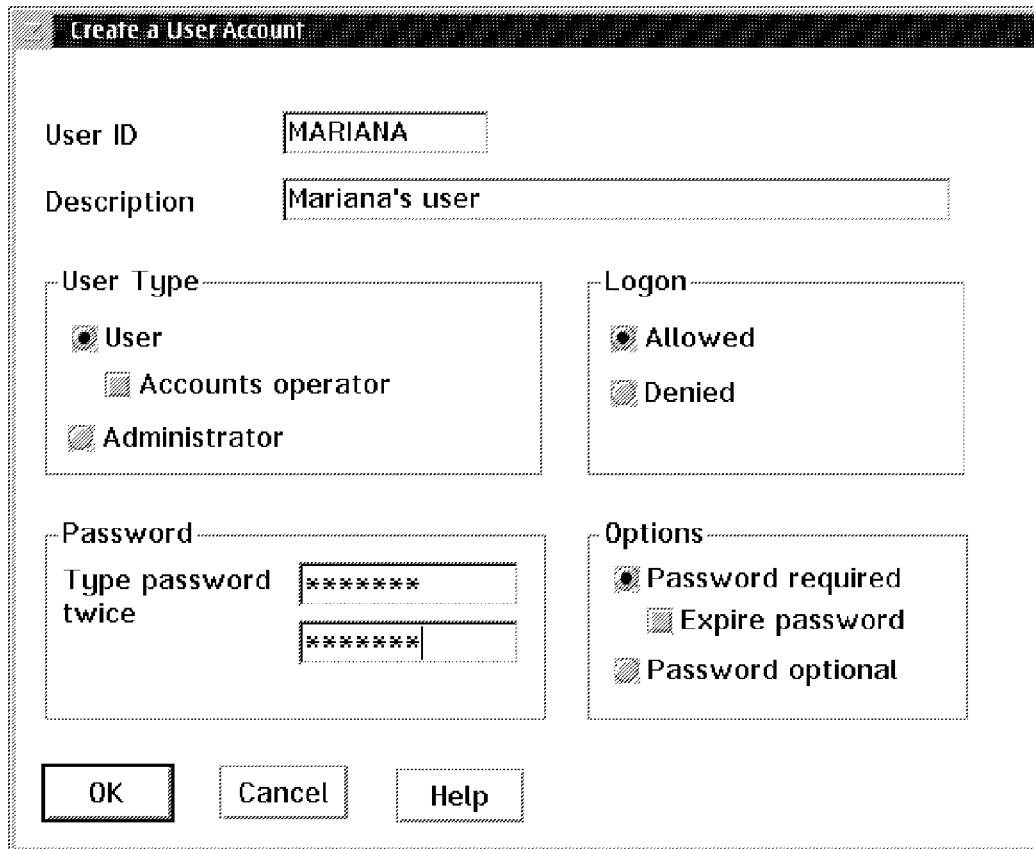
Figure 87. Create a User Account Window

In the Create a User Account window you need to provide the following information:

User ID   This field identifies each user to your OS/2 Warp 4 system.

Description   This field is optional. You can enter a description for each user if you wish.

User Type   Select the radio button that indicates the level of access authority you want to give to this user account.

User access allows the user to access resources according to the access privileges you assign.

Administrator access allows the user to access and manage all user accounts, resources and connections on your system.

If you want the user to manage other users and groups on your workstation, select the **Accounts operator** check box. A user with accounts operator privilege can add, change or delete users and groups, but cannot create or change user

accounts that have administrator or accounts operator privilege.

Logon   Select one radio button to indicate whether the user acount is allowed to log on to your system. If you select **Denied**, the user is restricted from logging onto your system, but the user account is maintained so you do not have to recreate it if you need it again later.

Password   If you want the user to provide a password for logon, enter that password here.

Options   Select a radio button to indicate whether the user acccount must specify a password to log on to your workstation.

If you want the initial password to expire the first time the user logs on, select the **Expire password** check box. The user is then required to change the password during the first logon.

After entering the desired information, select the **OK** button to create the new user account. You can now add this user account to a group of users and define access privileges for the account.

You can also display the groups a selected user is a member of by selecting the **Show groups...** button from the Manage Access window.

10.4 Dynamic TCP/IP in OS/2 Warp 4

OS/2 Warp Server comes with superior dynamic TCP/IP servers, such as a DHCP (Dynamic Host Configuration Protocol) server and a DDNS (Dynamic Domain Name Server) server. OS/2 Warp 4 clients can take full advantage of dynamic TCP/IP by obtaining an IP address from a DHCP server while keeping their host names regardless of the current IP address that was given by the DHCP server along with all other necessary TCP/IP information, such as router address, DNS (Domain Name Server), and so on. Following redbooks describe dynamic TCP/IP in OS/2 Warp Server and OS/2 Warp 4 in detail:

 • SG24-2602-00 *Inside OS/2 Warp Server Volume 1: Exploring the Core Components*

 • SG24-4786-00 *OS/2 Warp Server, Windows NT, and NetWare: A Network Operating System Study*

Section 6.1, "Dynamic TCP/IP in OS/2 Warp Server" on page 61 briefly defines the basic concepts of Dynamic TCP/IP and explains how to configure the Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS) servers of OS/2 Warp Server

This section explains how to configure the Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS) Clients of OS/2 Warp 4.

10.4.1 Installing and Configuring the Dynamic TCP/IP Client for OS/2 Warp 4

If you have not installed the TCP/IP Services on your workstation, you must install them to be able to configure the Dynamic TCP/IP Client for OS/2 Warp 4.

We describe the default method of installing the Dynamic TCP/IP Client for OS/2 Warp 4, so you need to have your OS/2 Warp 4 product CD-ROM in the CD-ROM drive of your machine.

Open [**Desktop** — **OS/2 System** — **System Setup** — **Install/Remove**] to see all the installation and uninstallation options available, as shown in Figure 88.
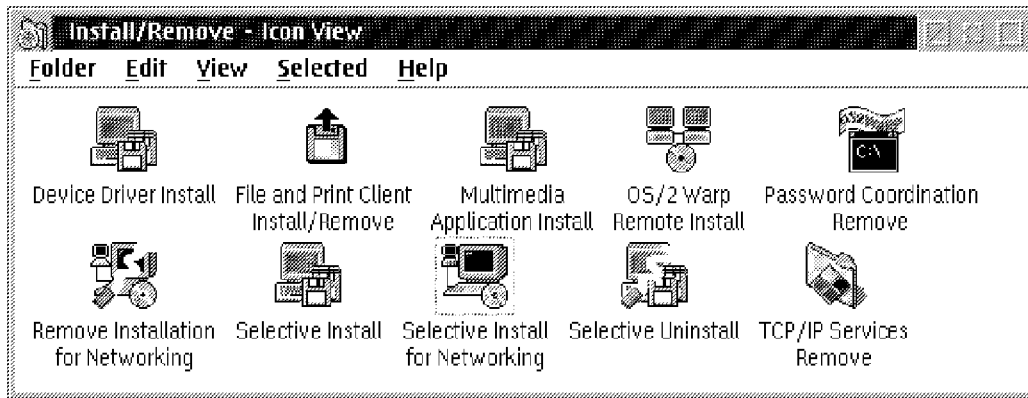
Figure 88. Install/Remove Folder

Open the **Selective Install for Networking** oject to display the Installing IBM OS/2 Warp window, as shown in Figure 89 on page 175.

Installing IBM OS/2 Warp

Select an installation path.

⦿ Easy installation
Guided installation using defaulted configurations.

◯ Advanced installation
Allows for selective installation of components and advanced configuration options.

Exit   Next   Help
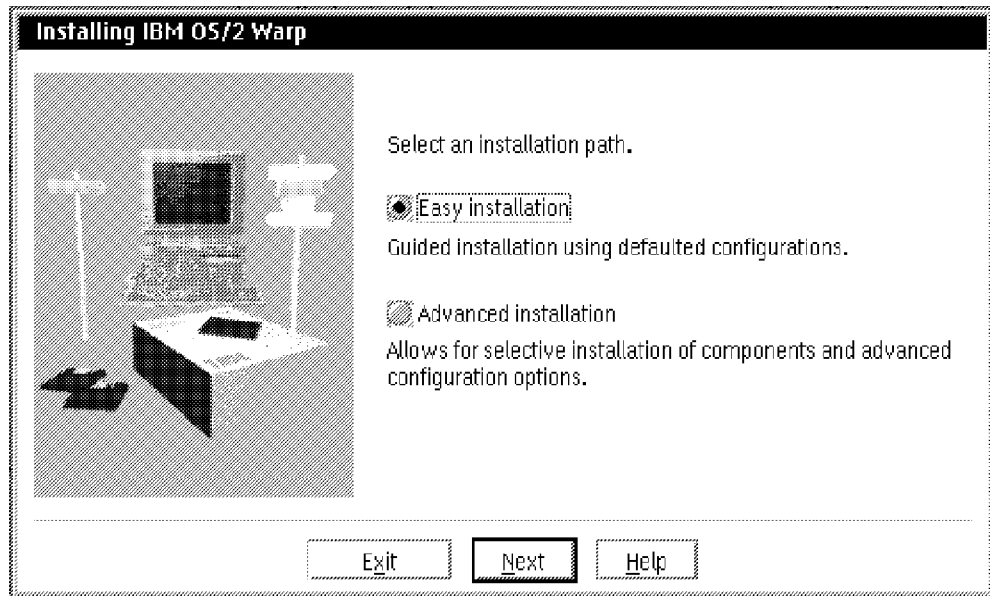
Figure 89. Installing IBM OS/2 Warp Window

10.4.1.1 Installing TCP/IP Services through the Easy Installation Path

From the Installing IBM OS/2 window choose between the Easy Installation and Advanced Installation paths. This section describes the Easy Installation path. Installing TCP/IP services through the Advanced Installation path is described in 10.4.1.2, "Installing TCP/IP Services through the Advanced Installation Path" on page 179.

Selecting the **Easy Installation** path prompts you to the Type of Activities window, as shown in Figure 90 on page 176, in which you have to select the **Let me choose from all the services** option to be able to configure the TCP/IP, DHCP, and DDNS services.
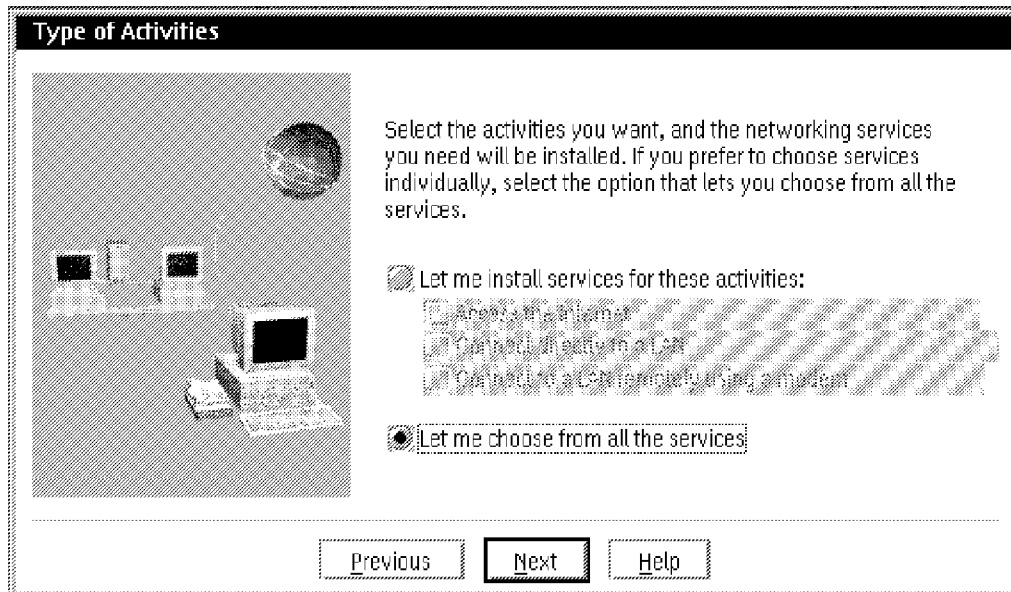
Figure 90. Type of Activities Window

Then you will have to go through all the installation windows for all the networking components included in OS/2 Warp 4, and when you are prompted to the TCP/IP Services window, shown in Figure 91, select the **Yes, install LAN and modem support** option.
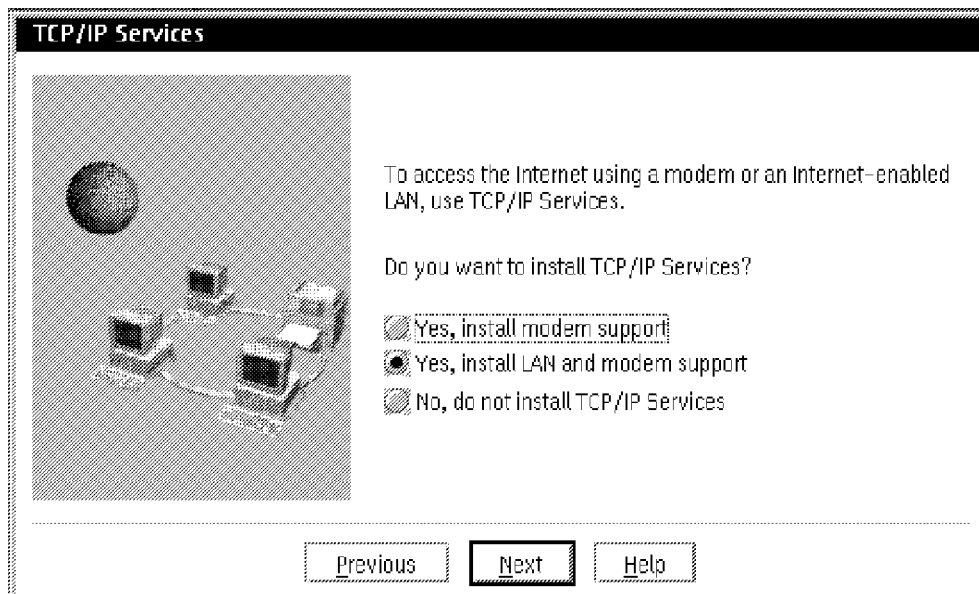
Figure 91. TCP/IP Services Window

If you do so, the TCP/IP Address Distributed? window, shown in Figure 92 on page 177, is displayed.
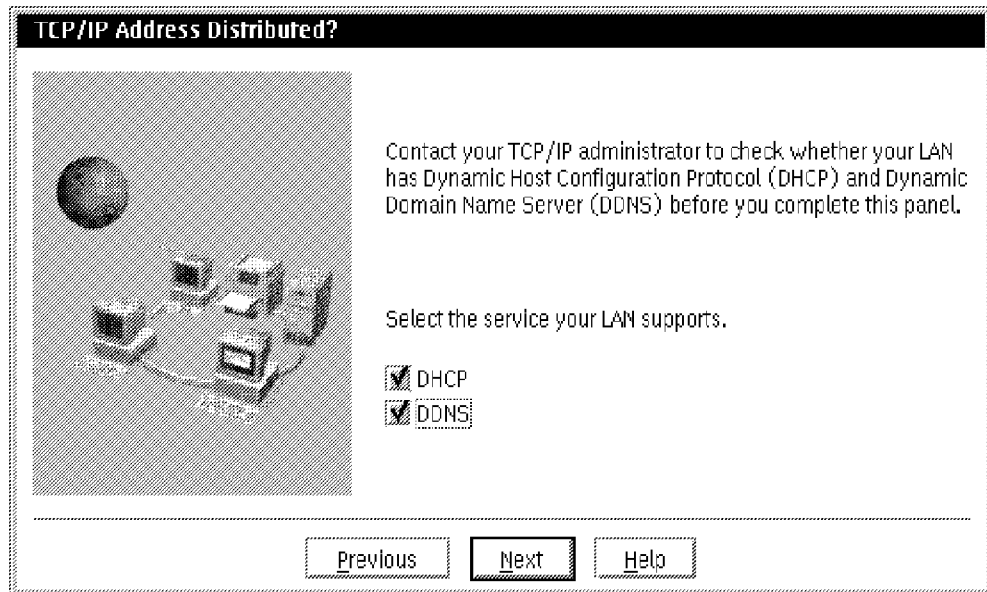
Figure 92. TCP/IP Address Distributed? Window

In this window you can select the **DHCP** and **DDNS** services by checking its corresponding checkmarks. Select these options only if a DHCP and DDNS server is available to your workstation through the LAN.

Note: The **DDNS** option is selectable only if you have previously selected the **DHCP** service.

Select **Next** to display the TCP/IP Services Configuration window, as shown in Figure 93 on page 178.
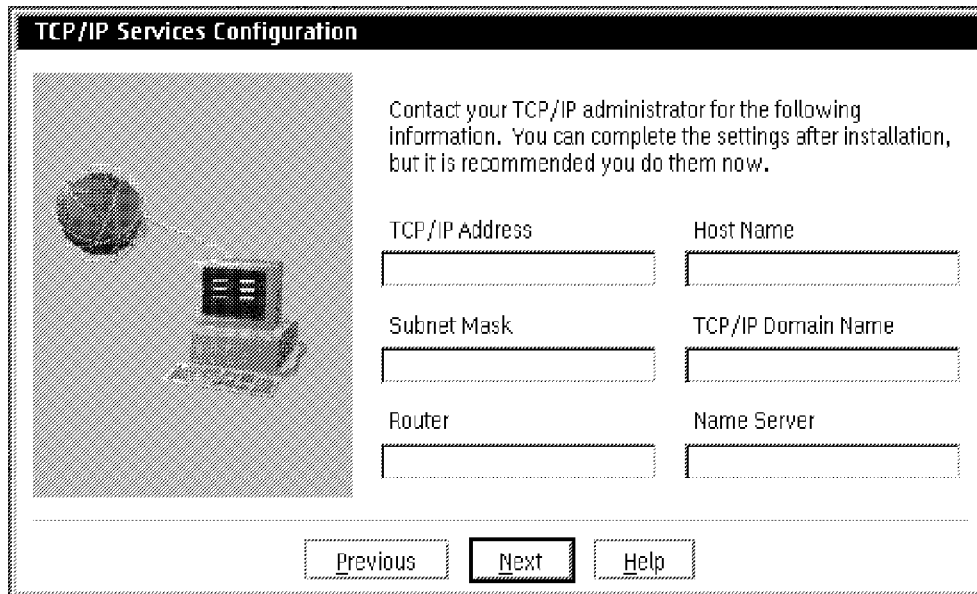
Figure 93. TCP/IP Services Configuration Window

You do not need to provide any information in this window since all TCP/IP configuration information for your workstation is provided by the DHCP and DDNS server. Proceed by selecting the **Next** button.

Note: TCP/IP configuration information is needed if you do not plan to have DHCP and DDNS servers in your network.

Although your workstation is configured with DHCP/DDNS support, an information window, as shown in Figure 94, appears informing you that TCP/IP was not configured.
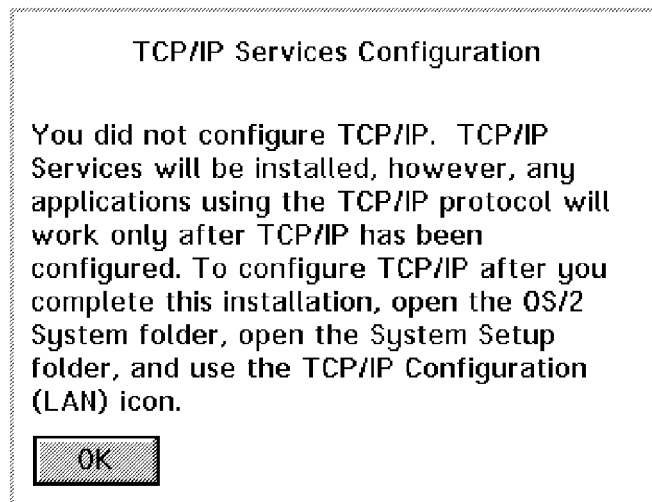
Figure 94. TCP/IP Services Configuration Information Message Window

Ignore this information message. Your dynamic IP client will work as soon as the installation is completed.

10.4.1.2 Installing TCP/IP Services through the Advanced Installation Path

Select the **Advanced Installation** path in the Installing IBM OS/2 Warp window as shown in Figure 89 on page 175. You do not need to go through the installation windows for all networking components available in OS/2 Warp 4. When prompted to the OS/2 Warp Setup and Installation window, shown in Figure 95, select the **TCP/IP Services** option.

Figure 95. OS/2 Warp Setup and Installation Window

When you select the **TCP/IP Services** option, the Configuration window as shown in Figure 96 on page 180 is displayed.
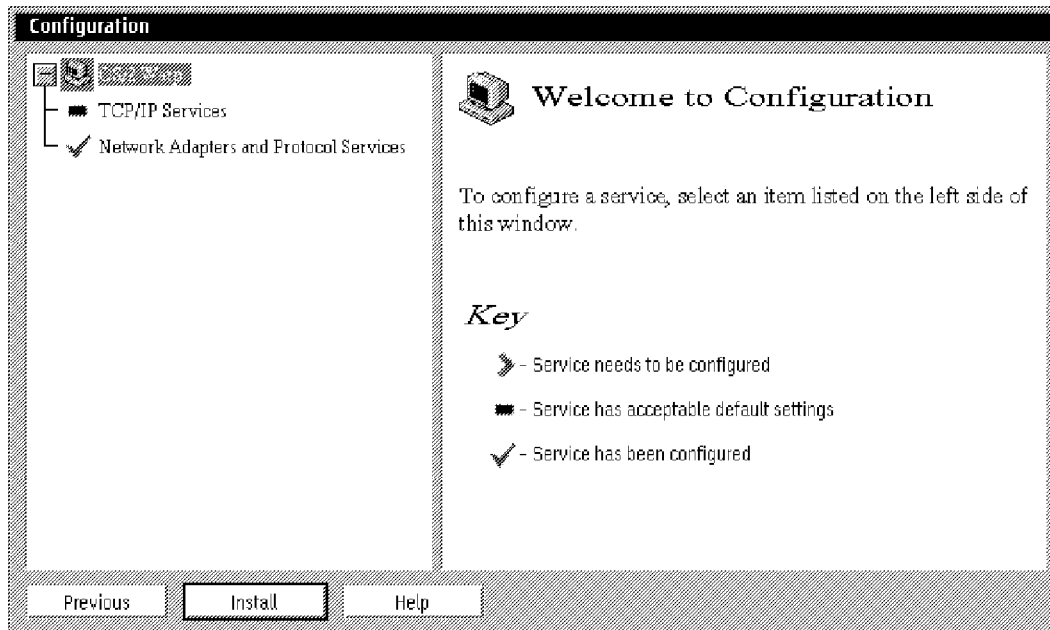
Figure 96. Configuration Window

Start by selecting and configuring the **Network Adapters and Protocol Services** item, as shown in Figure 97.
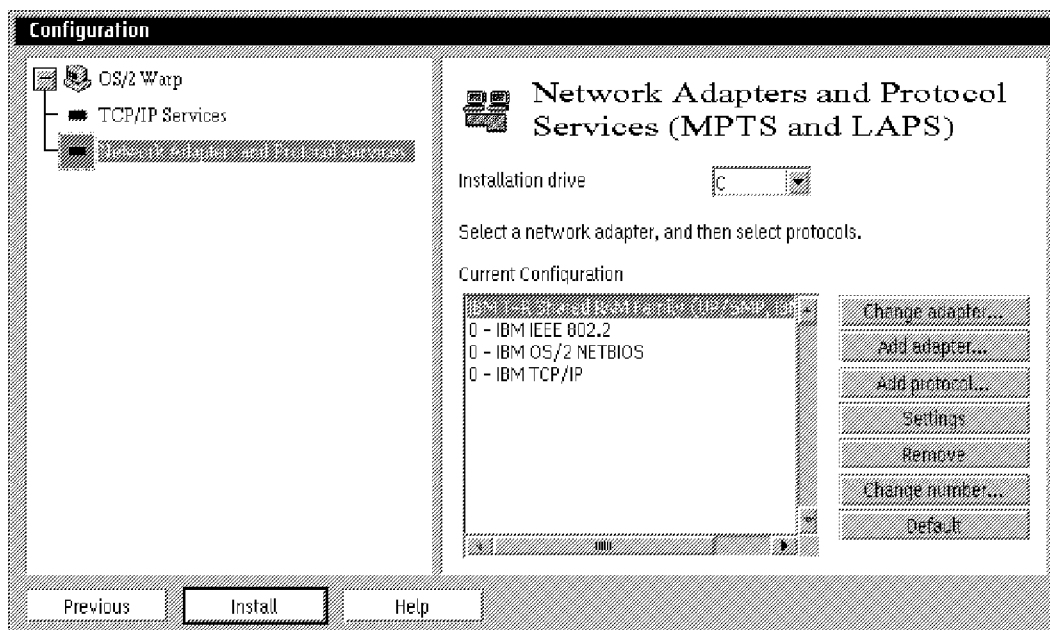
Figure 97. Network Adapter and Protocol Services Window

In this window you can select and configure the network adapter and protocol drivers that you want to use. If you need more information about

how to make this configuration, refer to 10.2.4, "Advanced Installation" on page 123, or the online documentation available with OS/2 Warp 4.

Note: In case you are presented with the error message as shown in Figure 98, remove the IBM OS/2 NetBIOS over TCP/IP protocol in the list of Network Adapter and Protocol Services. We recommend that you start with the DHCP configuration, and then add the IBM NetBIOS over TCP/IP protocol in the list of Network Adapters and Protocol Services.
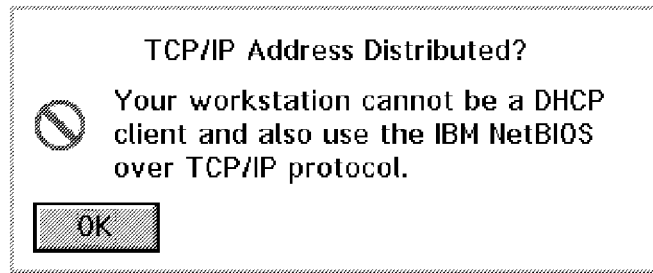
Figure 98. TCP/IP Address Distributed Error Window

Once you have configured the Network Adapter and Protocol Services, you need to configure the **TCP/IP Services** item from the Configuration window, as shown in Figure 99.
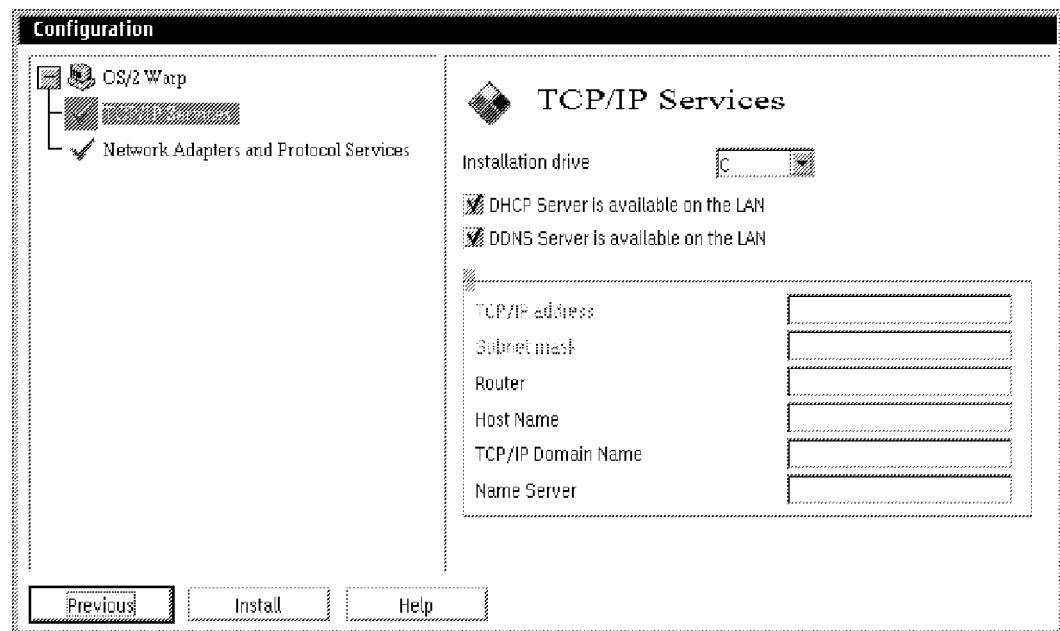
Figure 99. TCP/IP Services Window

To install the DHCP and DDNS services for OS/2 Warp 4, select the **DHCP Server is available on the LAN** and **DDNS Server is available on the LAN**

options. Make sure there is a DHCP server and DDNS server available in your LAN.

Note: The **DDNS Server is available on the LAN** option can be selected only if you have previously selected the **DHCP Server is available on the LAN** option.

As soon as you select these two options, the input fields of TCP/IP address and Subnet mask options are greyed out. Depending on the setup of the DHCP server (that is, whether or not it povides more IP information to DHCP clients) you can type configuration information for Router, Host Name, TCP/IP Domain Name, and Name Server. If there was not any TCP/IP configuration, the following information message window, as shown in Figure 100, is displayed:
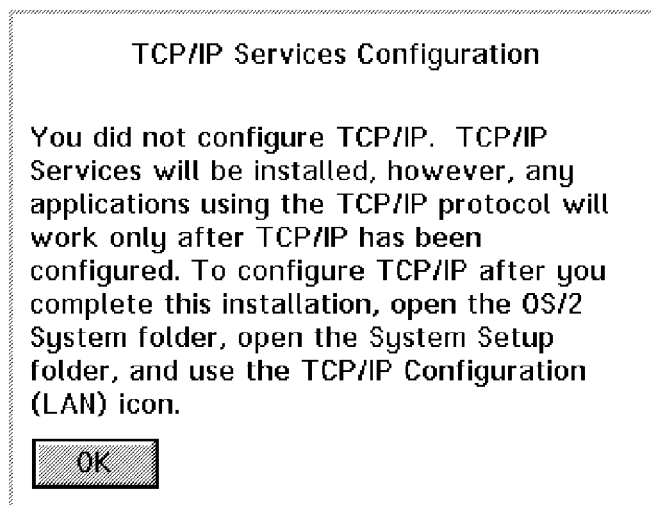
Figure 100. TCP/IP Services Configuration Information Message Window

As stated in 10.4.1.1, "Installing TCP/IP Services through the Easy Installation Path" on page 175, you can ignore this message. Your dynamic IP client will work as soon as the installation is completed.

In 10.4.1.1, "Installing TCP/IP Services through the Easy Installation Path" on page 175 and 10.4.1.2, "Installing TCP/IP Services through the Advanced Installation Path" on page 179 we illustrated the installation and configuration of DHCP and DDNS services during the installation of the TCP/IP services networking component of OS/2 Warp 4. If TCP/IP services are installed on your OS/2 Warp 4 workstation, you can modify your TCP/IP configuration using the TCP/IP configuration program. Use the Warp Center: [**Warp Center — System Setup — TCP/IP Configuration (LAN)**] or execute the `TCPCFG` command from an OS/2 command line. To modify your TCP/IP configuration to use DHCP/DDNS server, check the boxes for **Automatically,**

using DHCP and the **also, using DDNS** options from the Network settings notebook, as shown in Figure 101 on page 183.
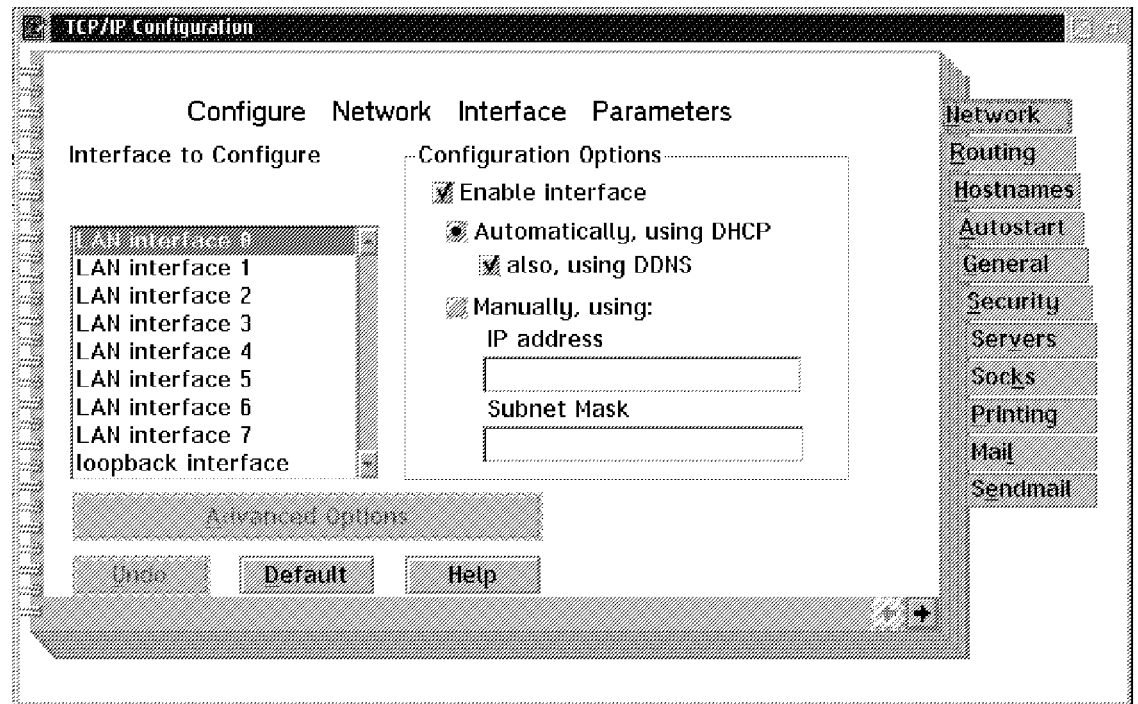
Figure 101. TCP/IP Configuration Notebook

Once you have made modifications, save the changes by closing the window. Restart your workstation so your machine can get the TCP/IP configuration information from the DHCP and DDNS server.

The procedures described above are basically everything you need to do to set up a dynamic IP client for OS/2 Warp 4.

If your DHCP server is configured and running correctly, it will deliver all TCP/IP configuration information to your workstation. You can verify TCP/IP configuration information by using the DHCP client and DDNS client utilities that come with OS/2 Warp 4. For more detailed information, see 10.4.2, "OS/2 Warp 4 Dynamic IP Utilities" on page 184.

10.4.1.3 Configuring the Dynamic IP Client for User Class Support

DHCP is supported by Windows 95 and Windows NT Workstation clients. However, the dynamic IP client in OS/2 Warp 4 supports DHCP servers configured for user classing, such as the OS/2 Warp Server DHCP server.

DHCP classing refers to mechanisms in DHCP that administer groups of hosts independent of where they are located in a network. There are two types of DHCP classing:

User Classing   User classing is a general mechanism for network administrators to define groups of users with common configuration requirements. For example, a class called `IBM_MOBILE_CLIENTS` can be created in OS/2 Warp Server so that their hosts are served by a separate range of IP addresses than others on the same subnet or across many subnets.

At the OS/2 Warp 4 dynamic IP client, the DHCPCD.CFG file, located in the MPTN ETC directory, contains information about the client's class. The default class name is `IBMWARP_V3.1`.

To configure the client for a different class, you need to modify the **User Class** entry in the DHCPCD.CFG file. You can make this change by editing the file with an ASCII editor, searching for the line that starts with `option 77` and changing the entry with the appropriate class name, as shown below:

```
option 77 "IBM_MOBILE_CLIENTS"             # User Class
```

Vendor Classing Vendor classing is a special-purpose mechanism for DHCP vendors to specify the "make and model" of the requesting client software. Vendors can use this option to optimize the operation of DHCP when the client and server are the same brand.

DHCP clients use DHCP `option 60` to indicate to DHCP servers what vendor type they are. The vendor class is also specified in the default DHCPCD.CFG file provided as `IBMWARP_V31`. You should not change this value.

10.4.2 OS/2 Warp 4 Dynamic IP Utilities

OS/2 Warp 4 provides two dynamic IP utilities, located in the System Setup folder:

DHCP Monitor

DDNS Configuration

10.4.2.1 DHCP Monitor

The DHCP client program runs as a background process, does not display messages and cannot be viewed. To view DHCP client configuration status and events, select the **DHCP Monitor** program in the System Setup folder or

execute the command DHCPMON.EXE from an OS/2 command line. The following information is presented:

- Current IP address.
- IP address lease time.
- DDNS host name registration (when applicable).
- DHCP options accepted and configured.
- DHCP client protocol state.
- DHCP client operational messages.

The DHCP Client Monitor Summary window is shown in Figure 102.
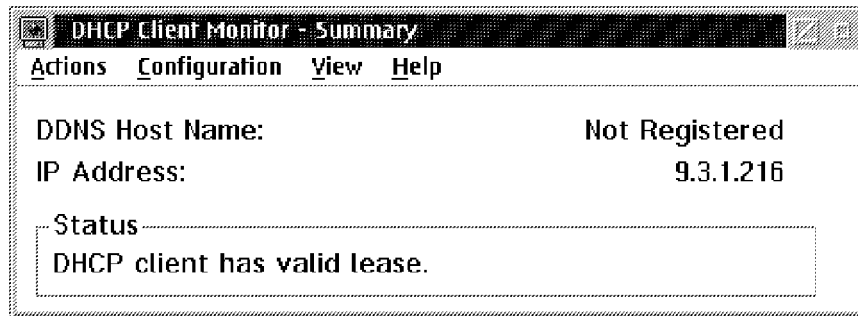
Figure 102. DHCP Client Monitor - Summary Window

The DCHP Client Monitor - Summary window displayes the following information:

DDNS Host Name If you enabled your workstation to use the Dynamic Domain Name Services, this field displays your current DDNS host name.

IP Address The IP address field displays the IP address assigned to you by the DHCP server.

Status This box displays the most recent DHCP status. The information in the Status box is refreshed every 5 seconds.

Other information, such as the remaining lease time for your IP address, is given by selecting the **Details** item from the **View** pull-down menu. The DHCP Client Monitor - Details window is displayed, as shown in Figure 103 on page 186.
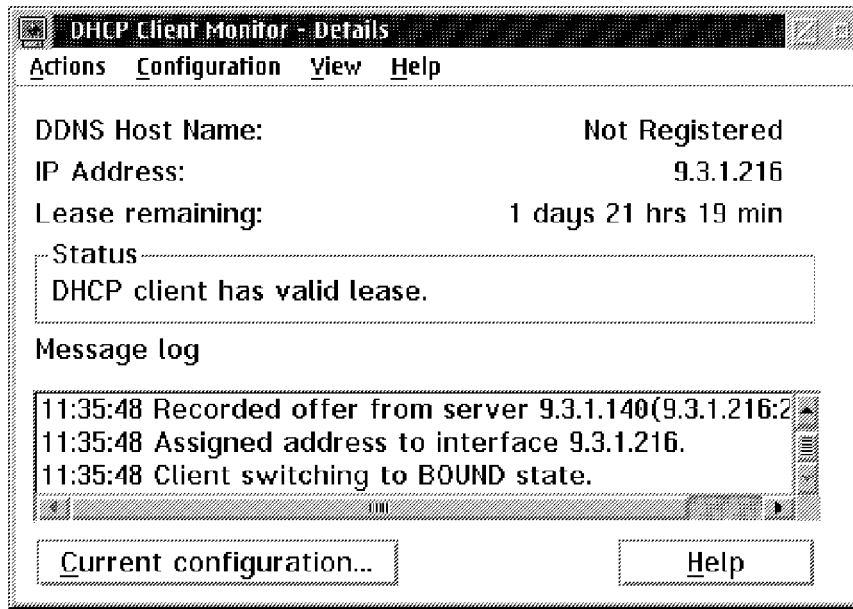
Figure 103. DHCP Client Monitor - Details Window

In the DHCP Client Monitor - Details window click on the **Current configuration...** button to check the parameters supplied by the DHCP server, as shown in Figure 104.
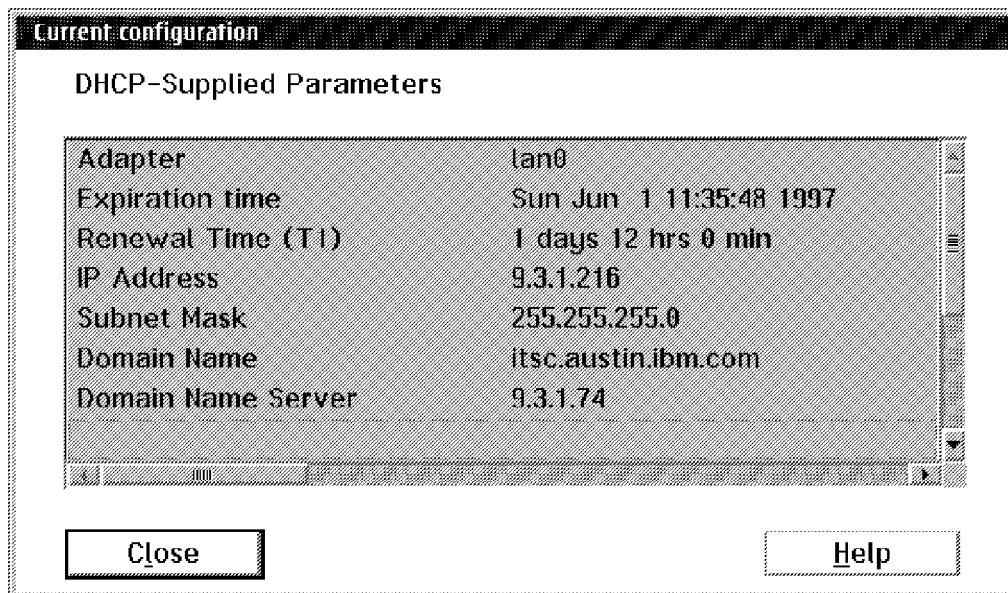
Figure 104. Current Configuration Window

Select the **Current configuration...** option from the **Configuration** pull-down menu to obtain additional configuration information.

10.4.2.2 DDNS Configuration

When you configure TCP/IP for DHCP and DDNS support and restart your workstation, the DDNS Client Configuration window, as shown in Figure 105, is automatically displayed.
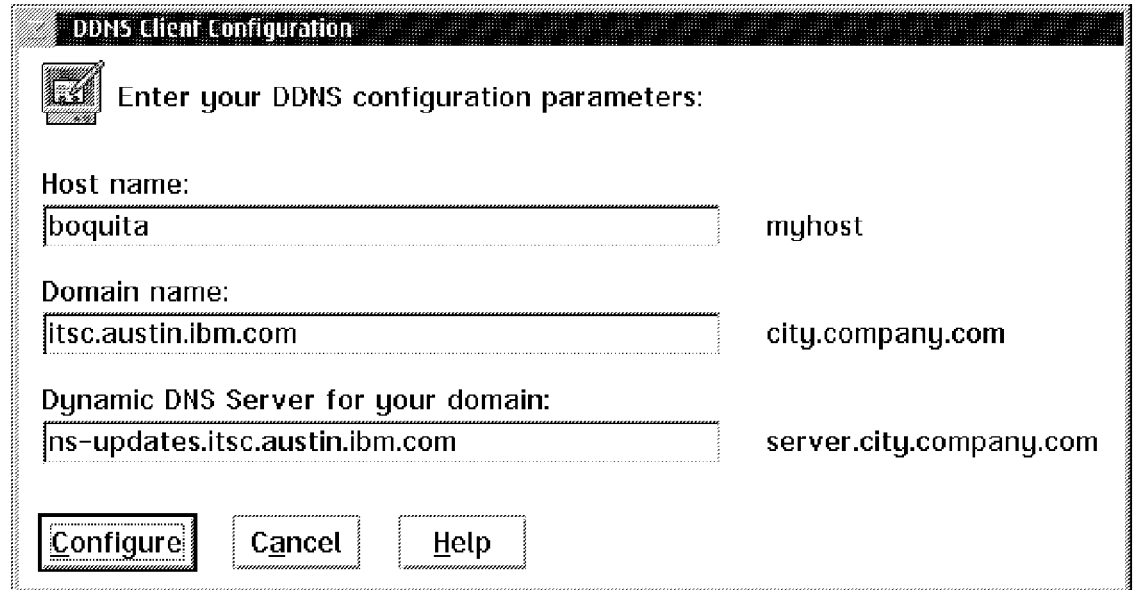
Figure 105. DDNS Client Configuration Window

If you do not want to configure your DDNS client, you can do so at a later time by opening the DDNS Configuration icon, located in the System Setup folder.

In the DDNS Client Configuration window, the information for your domain name and Dynamic DNS Server is automatically filled in. However, you must enter your Host name information. Once you have entered your host name and clicked on the **Configure** button, you are the owner of that host name, assuming your host name is not currently owned somebody else.

A file named DDNS.DAT will be copied from the DDNS server to your workstation's MPTN ETC directory. This file contains a digital signature and ensures that only you are allowed to change your host name.

Notes:

1. If you think that this kind of security is not enough, you can take advantage of having the DDNS.DAT file made available to users who are actually authorized for dynamic DDNS updates. To do this, supply the DDNS.DAT file on a diskette or on a user's home directory to establish a pre-secured environment for the dynamic DDNS client.

2. To make sure only authorized clients can retrieve dynamic IP addresses, you can establish TCP/IP classes, as explained in 10.4.1.3, "Configuring the Dynamic IP Client for User Class Support" on page 183.

10.5 Remote Access Services

With the introduction of IBM Enhanced Remote Access Services Connection Server for OS/2 Warp Server, OS/2 Warp 4 users now have a choice of two methods to dial into a LAN remotely:

- OS/2 Warp Server Remote Access Connection Server
- OS/2 Warp Server Remote Access Connection Server with PPP (Point-to-Point Protocol) enhancement

Without the PPP enhancement, OS/2 Warp Server Remote Access Connection Server fully supports OS/2 Warp 4 clients without any additional software. All components necessary for a OS/2 Warp 4 client to remotely dial in comes with the OS/2 Warp Server and OS/2 Warp 4 product. For information on how to work with "traditional" remote access services in OS/2 Warp Server refer to the IBM redbook SG24-4602, titled *Inside OS/2 Warp Server, Volume 1: Explore the Core Components*.

Unlike previous releases of LAN Distance and Remote Access Services, remote client versions do not come with the PPP enhancement. To allow OS/2 Warp 4 clients to dial in remotely using PPP, the IBM 8235 Dial-In Access to LANs Client for OS/2 needs to be purchased separately.

Refer to 7.1, "The Enhanced Remote Access Server for OS/2 Warp Server" on page 83 for more information.

10.5.1 IBM 8235 Dial-In Access to LANs Client for OS/2

IBM 8235 Dial-In Access to LANs Client for OS/2 (from now on, 8235 DIALs Client/2) is a multiprotocol, dial-in software package for OS/2 Warp 4, that lets you dial in to any IBM 8235 Dial-in Access to LAN Server for Token Ring and Ethernet (8235 DIALs Server) to use resources on a remote network, as if you were locally connected to it.

The 8235 DIALs Server, formally called IBM 8235 Dial-In Access to LAN Server for Token Ring and Ethernet, consists of a hardware device that attaches to a LAN (either token ring or ethernet) and a telephone network. This hardware works along with the 8235 software to provide the following functions:

- Physically attach the LAN to up to eight modems.

- Send data from the LAN to the remote workstations, and from the remote workstations to the LAN.

- Minimize traffic between the workstations and the LAN by filtering and compressing the data.

- Provide security.

When you make a dial-in connection, the 8235 DIALs Server answers the call and prompts you for a password (if one is required). Once you are connected you can work exactly as if you were in your office connected directly to the network, performing your usual activities such as using file servers, sending e-mail and even emulating host sessions. With the 8235 DIALs Client/2, higher level network applications treat the remote link as if it were a local link.

The 8235 DIALs Client/2 software communicates with remote networks by using the workstation's serial communications (COM) port and device drivers to emulate the operation of a locally attached LAN adapter. The 8235 DIALs Client/2 COM port device drivers provide the same software interfaces as LAN adapter device drivers to network program applications, such as OS/2 Warp File and Print Client. This makes the communication between your modem and the network transparent to the network software, enabling you to run the same network applications as locally attached users.

10.5.1.1 Installation Requirements
Before proceeding with the installation of the 8235 DIALs Client/2, make sure that you have:

- A personal computer running OS/2 Warp 4 (that is, a 486 processor machine or higher).

- A high-speed modem: V.32 or faster (using a slower modem greatly reduces performance when running certain appications and protocols).

- A modem cable, if you use an external modem.

- A standard telephone line.

- MPTS (Multi-Protocol Transport Services). This is an OS/2 Presentation Manager application used to install and configure network adapter drivers and network protocol drivers. It is included in the OS/2 Warp 4 product CD-ROM.

- OS/2 Warp Server with the Enhanced Remote Access Server for OS/2 Warp Server. See 7.1, "The Enhanced Remote Access Server for OS/2 Warp Server" on page 83 for more details. The Enhanced Remote

Access Connection Server for OS/2 Warp Server is available through IBM's Software Choice home page, at the following Web site:

```
http://www.software.ibm.com/os/warp/swchoice/
```

Furthermore, if you plan to have your 8235 DIALs Client/2 dial into OS/2 Warp Server with the Enhanced Remote Access Server for OS/2 Warp Server, you need to provide a patch for the IBM 8235 DIALs for OS/2 version 4.5.2 client. You can get the patch from the World Wide Web (WWW) at the following Web site:

```
http://www.networking.ibm.com/nes/nes8235.htm
```

In addition, your network administrator needs to give you:

- A user ID and password, if required.
- The phone number to use to dial into the network.
- The network protocols available on the LAN.
- The correct device drivers to install on your workstation.

10.5.1.2 Installation and Configuration

The 8235 DIALs Client/2 is licensed for use to purchasers of the IBM 8235 Dial-In Access to LAN Servers for Token Ring and Ethernet.

In order to install 8235 DIALs Client/2, put the product diskette in your floppy drive and run the A: SETUP2 command from an OS/2 command session. The DIALs Client/2 Setup window, as shown in Figure 106 on page 191, is displayed.

Figure 106. DIALs Client/2 Setup Window

Selecting the **OK** button guides you to the Install Directory window, as shown in Figure 107.
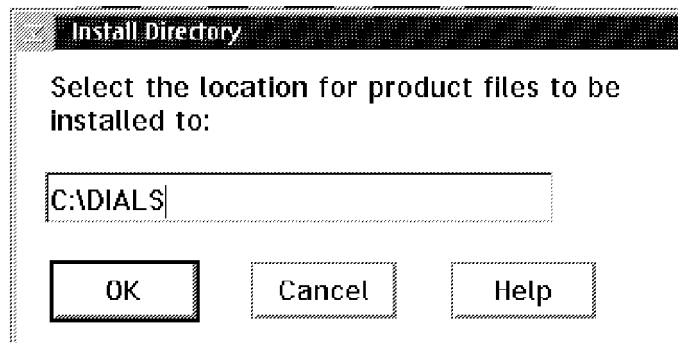
Figure 107. Install Directory Window

In this window, select the subdirectory in which you want the 8235 DIALs Client/2 product files to be installed. The default path is C: DIALS. After entering the desired path, select the **OK** button to start the 8235 DIALs Client/2 installation procedure. A progress indicator, as shown in Figure 108 on page 192, shows the status of the installation.
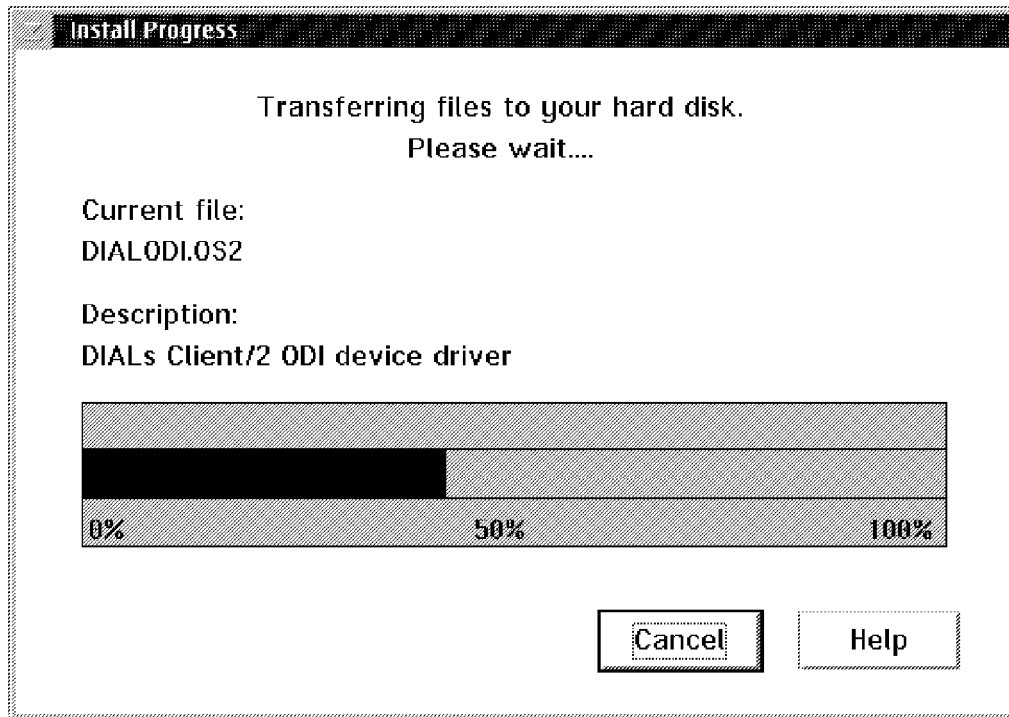
Figure 108. Install Progress Window

When the installation is complete, you are guided to the Configuration
window, as shown in Figure 109.
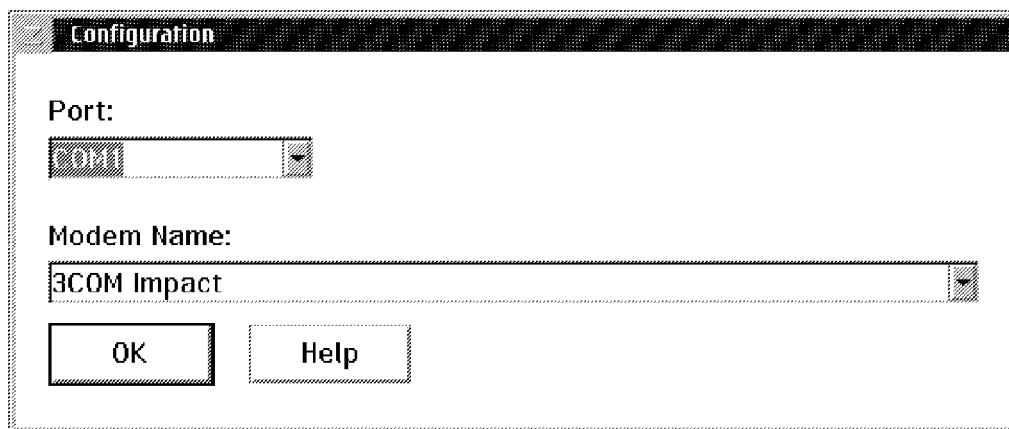
Figure 109. Configuration Window

In this window, provide the **Modem Name** that you are using and the Port to
which the modem is connected. For more information about port and
modem configuration, please refer to 10.5.1.5, "Modifying the Port and
Modem Settings" on page 204.

Once you have made the selections in the Configuration window, select **OK**
to complete the installation. The Install Complete message window, as
shown in Figure 110 on page 193, is displayed.
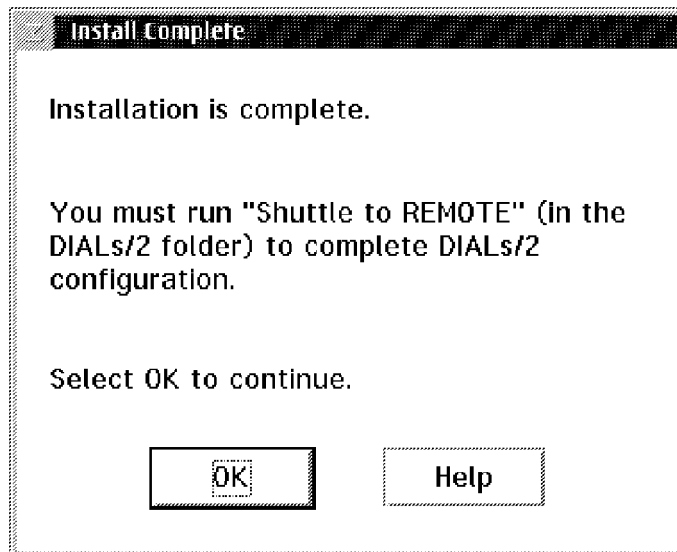
Figure 110. Install Complete Window

Select **OK** to leave the 8235 DIALs Client/2 installation program. There is
now a new folder called DIALs/2 on your desktop. This folder, as shown in
Figure 111, contains all your 8235 DIALs Client/2 program icons.
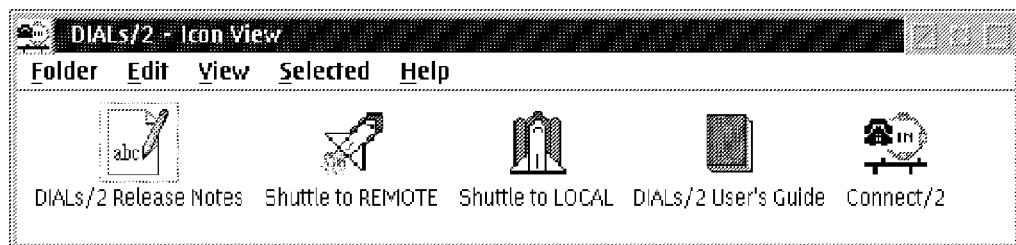
Figure 111. DIALs/2 Folder

In the DIALs/2 folder there are two icons called Shuttle to REMOTE and
Shuttle to LOCAL. When you check the properties settings of these icons as
shown in Figure 112 on page 194 and Figure 113 on page 195, they execute
the same program, called SHUTTLE2.EXE. Each icon, however, passes
along different parameters.
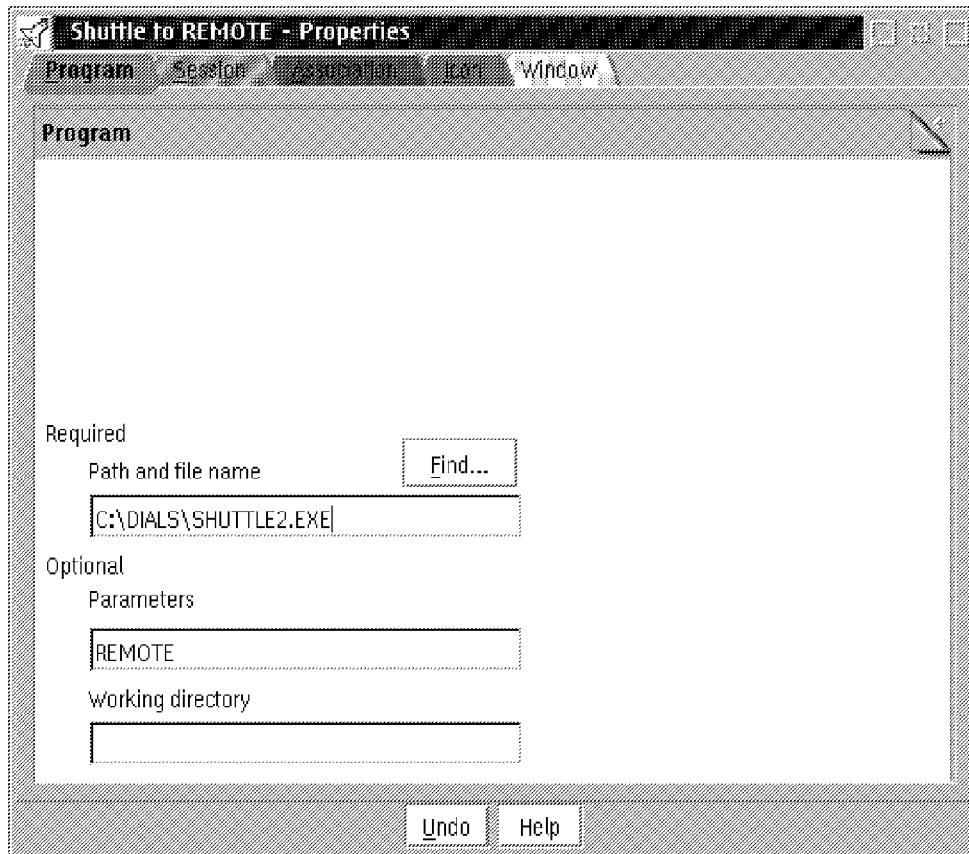
Figure 112. Shuttle to REMOTE - Properties Window

The command to enable your 8235 DIALs Client/2 to remotely dial into a LAN is:

```
C: DIALS SHUTTLE2 /REMOTE
```

whereas the command to enable your 8235 DIALs Client/2 to work in a LAN is:

```
C: DIALS SHUTTLE2 /LAN
```

as shown in

Figure 113. Shuttle to LOCAL - Properties Window

The SHUTTLE2.EXE program allows you to use the same workstation at work and on the road. It lets you have two versions of your configuration files:

 • One version for directly connecting to the LAN in the office.

 • One version for your remote connection from the road.

To set up your workstation to use the SHUTTLE2 program you must be running a local configuration, which means that you have to be directly attached to a LAN. The configuration must also use NDIS drivers, as ODI-only configurations are not supported at this time.

Click on the **Shuttle to REMOTE** icon (as asked in the Install Complete window shown in Figure 110 on page 193) to exchange the startup files (CONFIG.SYS and PROTOCOL.INI) you run for your local attachment with the startup files that are necessary to run remotely. The Shuttle Complete window, shown in Figure 114 on page 196, is displayed.
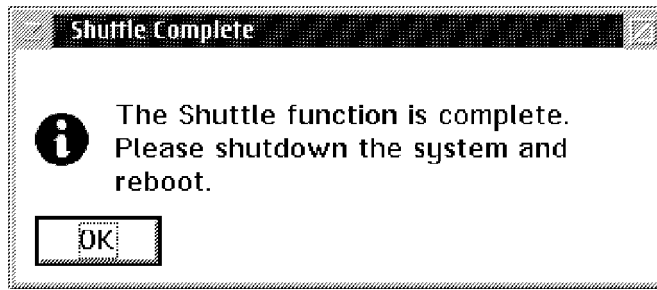
Figure 114. Shuttle Complete Window

Shut down and restart your system and your workstation will be configured to run remotely.

Note: The startup files are backed up to the SHUTTLE2 subdirectory and the working copies of the startup files are located in their respective directories with file extensions of .LAN for local attachment and .DIA for remote access.

Before you shut down your machine each day, you should think about the next place you plan to use it. If you plan to work in the office, for example, click the **Shuttle to LOCAL** icon. This will configure your workstation for a local connection the next time you start up your workstation. Do this each time before you shut down to reduce the amount of time you spend configuring your workstation.

In the Adapter and Protocol Configuration window shown in Figure 115 on page 197, note that when you start your workstation to work remotely, the currently configured MAC driver has changed to DIALs Client/2 Support.
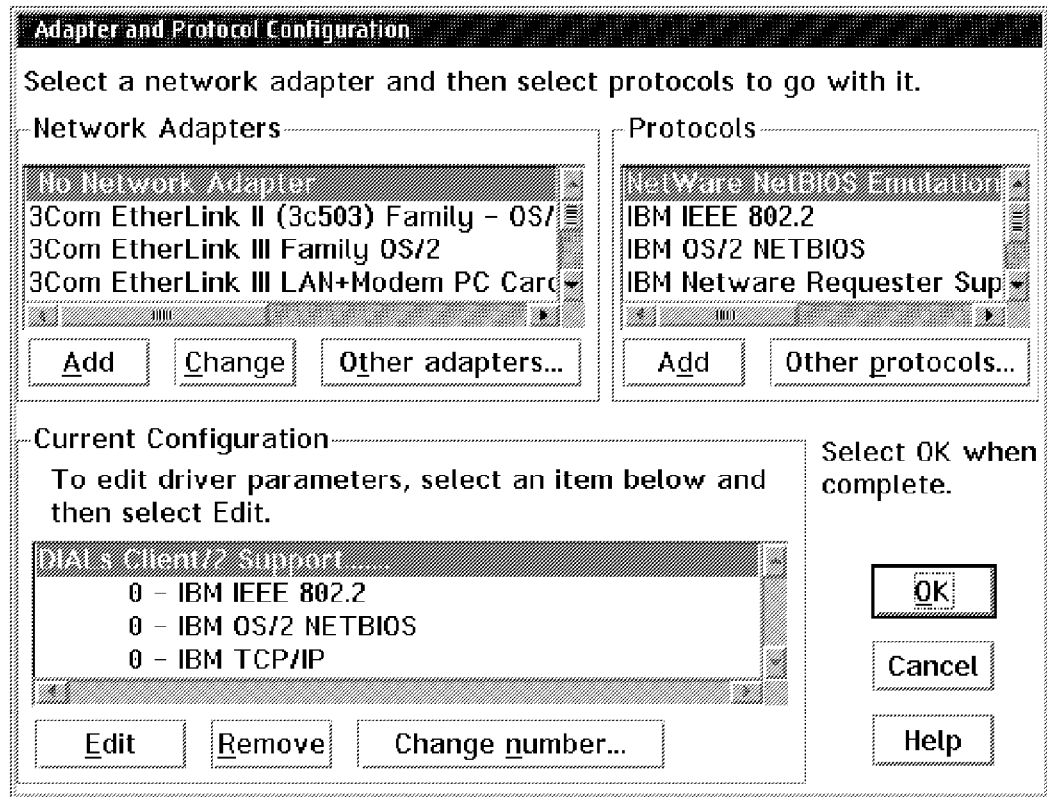
Figure 115. Adapter and Protocol Configuration Window

10.5.1.3 Creating Connection Files

In the DIALs/2 folder, as shown in Figure 111 on page 193, you can find the Connect/2 icon. This application manages the configuration of modems, phone numbers, password and other items that establish connections between the remote workstation, the 8235 DIALs Server and the LAN. DIALs Connect/2 needs to be active only while connecting and disconnecting. However, it can remain loaded during the connection to provide information about the status of the call, traffic statistics, modem configuration and more.

A separate connection file needs to be created for every remote network you want to access. The connection file contains all of the information DIALs Client/2 needs to connect to the remote network. When you create a connection file for dialing in to a remote network, save the connection file and use it each time you want to connect to that particular network. To run the DIALs Connect/2 application to create a connection file, the network administrator for the remote network must give you:

- The telephone number to dial.

- A valid user name and , if required, a password.

- The network protocols required to make the connection.

In this section we explain how to create a dial-in connection file to be used to access a remote network.

Open the **Connect/2** object located in the DIALs/2 folder. The DIALs Connect window, as shown in Figure 116, is displayed.
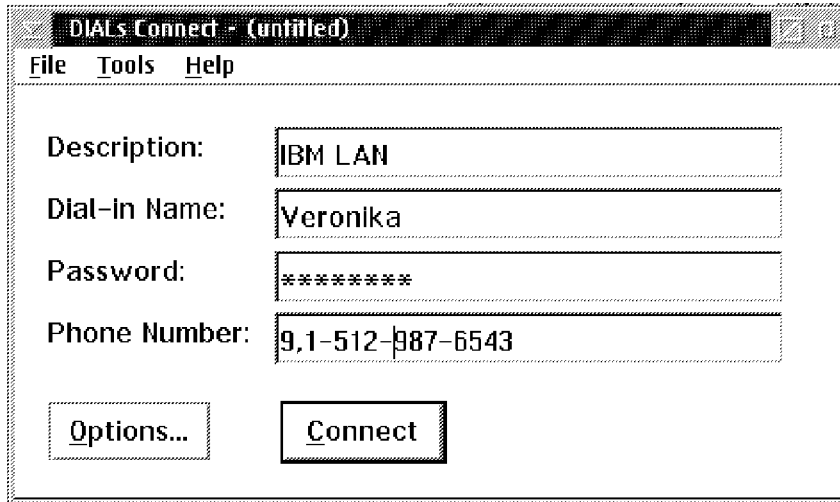
Figure 116. DIALs Connect Window

```
┌─ DIAL.OS2 Driver Not Loaded ────────────────────────────────────┐
│                                                                  │
│  If you receive the message "DIAL.OS2 driver not loaded", make sure that
│  the drivers are configured correctly (you can check this out in the
│  Adapter and Protocol Configuration window).                     │
│                                                                  │
│  Although you cannot connect to a remote network unless the DIAL.OS2
│  driver is loaded, you can still create and save a connection file.
│                                                                  │
└──────────────────────────────────────────────────────────────────┘
```

In the DIALs Connect window, configure the following items:

Description In the Description box you can enter a description of this connection file as, for example, IBM LAN. This field is optional and can be up to 64 characters long.

Dial-in Name In this box enter your dial-in user name provided by the network administrator, for example, Veronika. Dial-in user names are not case sensitive and can be up to 64 characters long.

Your dial-in user name is specific to the 8235 DIALs Server you are calling. It does not necessarily match your user

name for using other services on the remote network such as your file server or e-mail ID.

Password If your network administrator has assigned a password, enter it in the **Password** box. Passwords are not case sensitive and are displayed as asterisks (*) when typed. Alternatively, you can enter the password when prompted during the connection process. For security reasons, passwords are not saved to the connection file.

Phone Number In the Phone Number field you should enter the telephone number of the network you are calling. The number should be entered exactly as you would dial it manually, using up to 56 numbers (including commas and hyphens). For example, if you were dialing a long-distance call from your office where you have to dial a "9" to reach an outside line, enter 9,1-512-838-6543. You can use the commas if you need to add a pause (usually 2 seconds for each comma you use, but this varies with your modem settings). Hyphens are optional. This allows you to enter long distance prefixes and telephone company charge codes.

> **Note:** Keep in mind that many modems cannot handle more than 36 characters for dialing, so if DIALs Client/2 reports an error while dialing, this might be the cause.

Click on the **Options** button and the Connection File Options window, as shown in Figure 117 on page 200, is displayed.
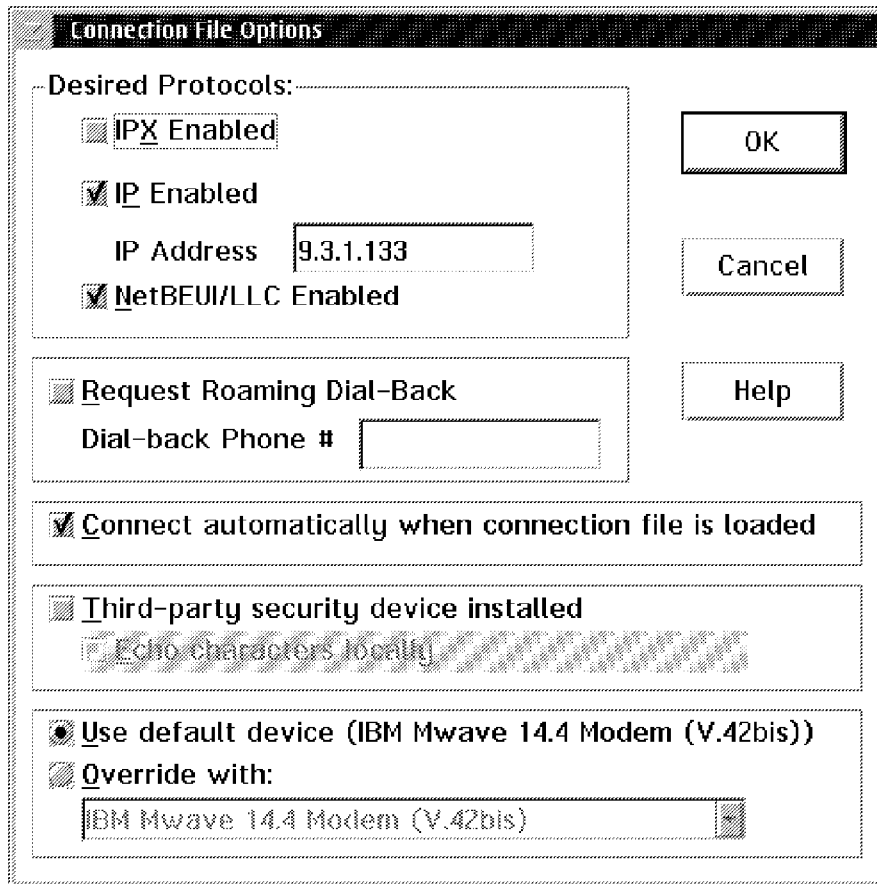
Figure 117. Connection File Options Window

In this window you need to set up the desired networking protocols and other features that you want to use for this connection. You can make the following configurations:

· **Desired Protocols**

In this box you can enable the network protocols that you want to use when connected. The available options are listed below:

IPX Enabled   Enables the IPX protocol for your dial-in connection, providing access to Novell network services. To use Novell services, you must also install the NetWare Client for OS/2 software on your workstation (this product is included in the OS/2 Warp 4 product CD-ROM).

IP Enabled   Enables the Internet Protocol (IP) for your dial-in connection, providing access to all IP services on the remote network. To use IP services, you must have a TCP/IP software package installed on your workstation. If your network administrator has

provided an IP address, enter it here. Otherwise, do not change the IP Address field from the default of `0.0.0.0`.

NetBEUI/LLC Enabled Enables the NetBEUI and LLC protocols for your dial-in connection, providing access to all services on the remote network that use those protocols. You have to enable this option if you plan to log on to an OS/2 Warp Server or work with Personal Communications 3270 Emulation configured to run over SNA.

You can enable any combination of IPX, IP and NetBEUI/LLC by selecting the check box next to each protocol. However, you are able to use a selected protocol only if the remote server also supports that protocol. The table below lists some examples of common network applications and their corresponding protocols:

Table 9. Common OS/2 Network Applications and Protocols	
Network Application	**Protocol**
OS/2 Warp Server	NetBEUI/LLC
Communications Manager/2; Personal Communications 3270 configured through SNA	NetBEUI/LLC
TCP/IP	IP
Novell NetWare	IPX

Note: When using the IP protocol, leave the IP Address field set to `0.0.0.0` unless your network administrator instructs you to enter an IP address. In most cases, the dial-in workstation receives its IP address from the network, not from the value entered in this field.

- **Request Call-Back**

  If your user ID is set up on the 8235 DIALs Server to support call-back, you should select this check box.

  Call-Back lets you tell the 8235 DIALs Server to call your modem back at the telephone number you specify so you can reverse the charges for the telephone call. Not all 8235 DIALs Servers support call-back, and not all users are set up to use this feature.

  To enable Call-Back, you should enter the call-back telephone number in the Dial-back Phone # field. The telephone number you enter in this field must include any access codes needed by your modem to dial the

phone number from the remote site (such as, for example, 9 to use an outside line and 1 for long distance calls).

- **Connect automatically when connection file is loaded**

  Select this check box to automatically set up this connection whenever the connection file is opened. If you do not enable this option, you must click the **Connect** button to make a connection after you open the connection file.

  Note: If you select this check box, you must make an icon for the connection file for 8235 DIALs Client/2 to connect automatically, as explained below in this section.

- **Third-party security device installed**

  This selection tells 8235 DIALs Client/2 to use a third-party security device that are set up on the 8235 DIALs Server. If you select this check box, you will typically have to enter an additional password after connecting to the remote modem, but before you have access to the 8235 DIALs Server.

  If you are not sure whether to select this check box, contact the network administrator for the remote network.

  Dialing in manually requires you to enter the modem configuration and dial-in strings. Third-party security device installed, when selected, automatically does that part of the connection process under software control.

  You can also select the **Echo characters locally** option to tell 8235 DIALs Client/2 to display characters on the screen as you type them.

- **Use default device / Override with**

  This option tell 8235 DIALs Client/2 to use the default installed communications device or to override the device with another device.

Once you have finished your connection file configuration, if you select the **OK** button in the **Connection File Options** window, you return to the **DIALs Connect** window. Save your connection file by selecting the **Save** or **Save as...** options from the File pull-down menu, as shown in Figure 118 on page 203.
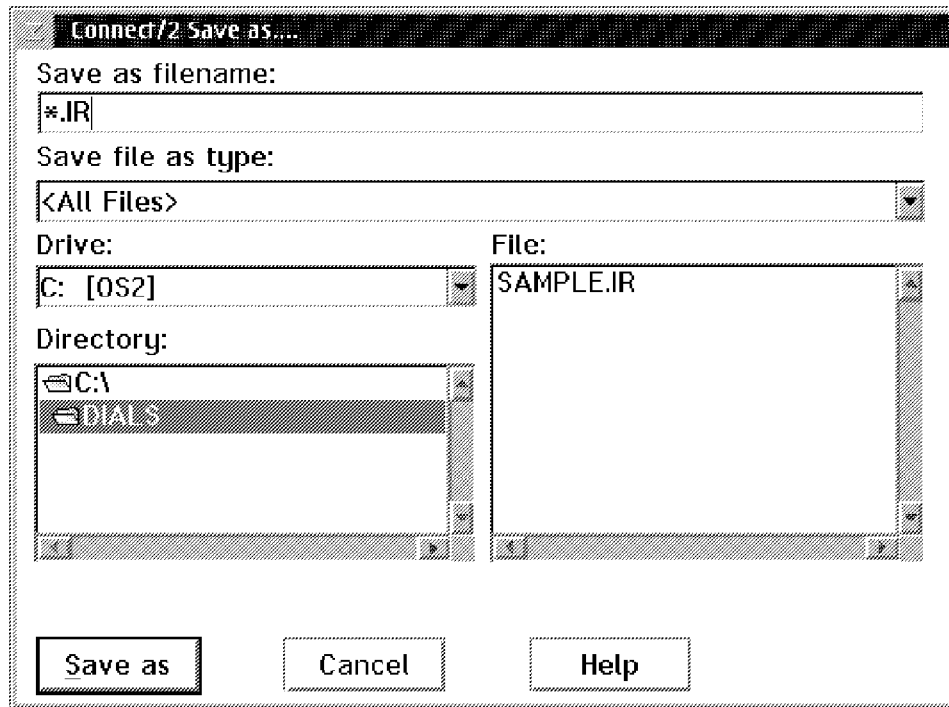
Figure 118. Connect/2 Save as... Window

10.5.1.4 Creating an OS/2 Desktop Icon

After you have created and saved a DIALs connection file using Connect/2, create an OS/2 desktop icon to easily identify and open the connection file.

To create the icon, open the corresponding connection file by double clicking on the **Connect/2** icon located in the DIALs/2 folder, and then select the **Open...** option from the **File** pull-down menu.

When you open the connection file for which you want to create the icon, select the **Make Icon...** option from the **File** pull-down menu. The Create Desktop Icon window, as shown in Figure 119, is displayed.
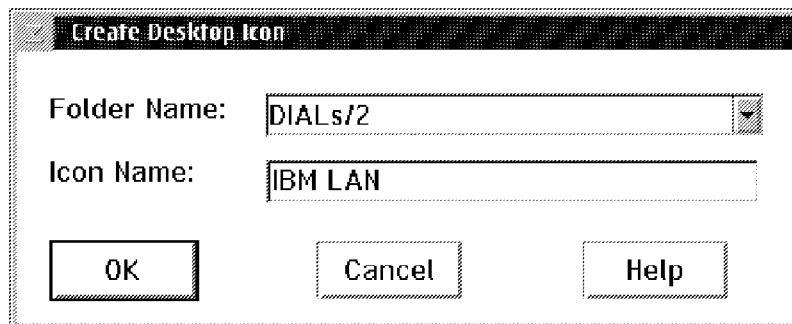
Figure 119. Create Desktop Icon Window

In this window, enter the following information:

Folder Name Enter the name of the desktop folder in which 8235 DIALs Client/2 will create the icon for the current connection file. You can enter the name in this field and press **Enter**, or select the drop-down arrow to the right of the **Folder Name** box and then select the folder from the list. The default is DIALs/2, the folder created by the DIALs Client setup program.

Icon Name This is the name for the icon you create, up to 26 characters. The default is the name that you have specified in the Description box for the opened DIALs connection file.

Fill in these two fields and when press the **OK** button to create the icon in the specified folder, as shown in Figure 120.
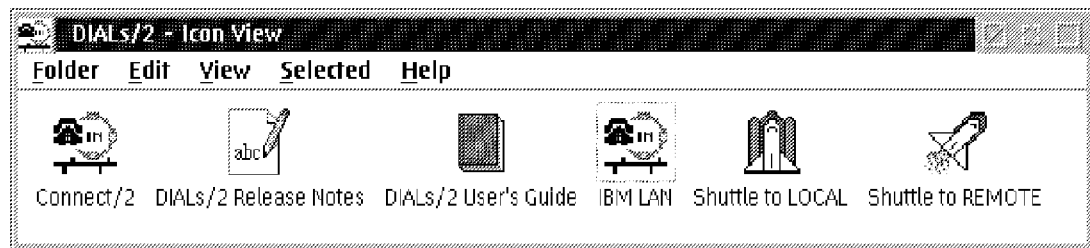
Figure 120. Connection file Icon Within DIALs/2 Folder

From now on, each time you need to perform this connection, just double click on the corresponding icon.

10.5.1.5 Modifying the Port and Modem Settings

When you installed 8235 DIALs Client/2, you specified the kind of communications device you are using, and in which port it was connected on your workstation. If this information changes, you need to change the settings in DIALs Client/2 to match. For example, if you were using a 9600 bps modem when you installed 8235 DIALs Client/2 and you replaced it with a 28800 bps modem, you need to change the settings in DIALs Client/2 to take advantage of the higher speed.

When you set up the communications ports in the 8235 DIALs Client/2, you tell DIALs Client/2 what kind of modem or other communications device you are using, as well as the COM port to which it is attached (or what driver to use in the event the communications device is not a COM port). You can also tell 8235 DIALs Client/2 what speed to use for this connection (in bps), how to initialize the modem for the best possible connection and so on.

To set up the comunications ports for the 8235 DIALs Client/2, you must open the **Connect/2** program, located in the DIALs/2 folder on the desktop,

and choose the **Port Setup** option from the **Tools** pull-down menu. The Port
Setup window, as shown in Figure 121 on page 205, is displayed.
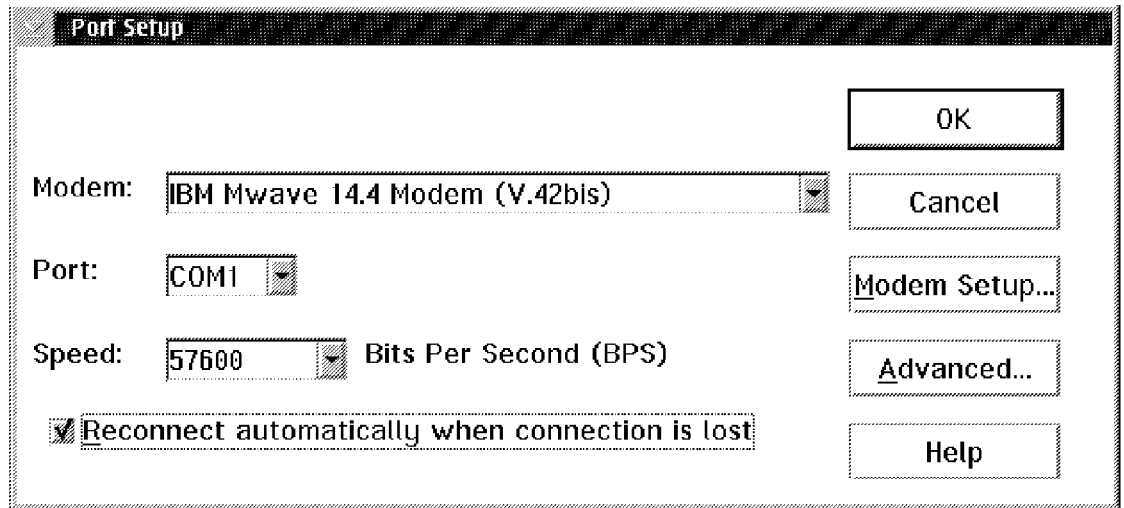
Figure 121. Port Setup Window

In this window, you can:

- Select the type of modem you are using, from the **Modem** drop-down
  list. If the modem you want is not in the list, you can click the **Modem
  Setup...** button to add your modem to the list, as shown in Figure 122 on
  page 206.
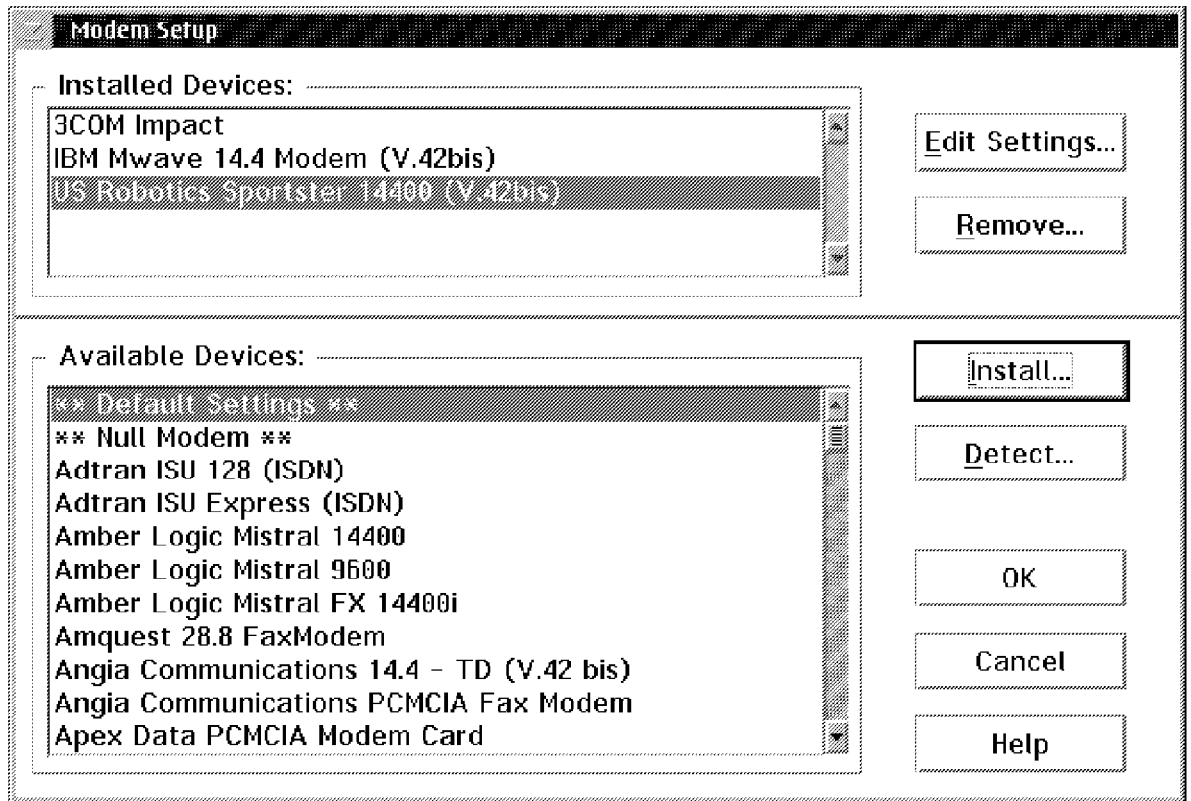
Figure 122. Modem Setup Window

- Select the COM port to which the modem is attached from the **Port** drop-down list.

- Accept the default speed selected in the **Speed** drop-down list or select another speed.

  In most cases, you should accept the preset value for the communications speed. This speed is usually the highest speed your modem supports. However, if you experience a high number of communications errors, choosing a lower number on this drop-down list might eliminate the errors.

- Select the **Reconnect automatically when connection is lost** check box if you want the DIALs Client/2 software to automatically attempt to reestablish a lost modem connection.

  Note that Connect/2 must be running at the time the connection was lost in order for the automatic reconnection to occur. If you do not select this check box, you are prompted to reconnect when the modem connection is lost.

Chapter 11. DOS LAN Services for DOS with or without Windows

This chapter describes installing and configuring DOS LAN Services Version 5.0 in a plain NetBEUI and TCP/IP environment, NetBIOS Name Server (NBNS), and dynamic TCP/IP:

- Dynamic Host Configuration Protocol (DHCP)

11.1 DOS LAN Services Overview

The following sections introduce fuctional details of DOS LAN Services.

11.1.1 Functional Overview DLS Under DOS

The following functions are provided by DOS LAN Services in a plain DOS environment:

- File redirection.

- Print redirection.

- Named pipe redirection.

- Memory conservation.

- Automatic session/optional *persistent connection* reconnect.

- Mailslot support.

- LAN API support.

- Password encryption support.

- Receiver support.

- Message support.

- Data buffering/caching.

- Peer Support (client single-connection resource sharing); User level security (rather than share level security in DOS LAN Services 4.0) which enforces the use od user IDs and passwords. DLS Peer has a NET.ACC file and supports NET USER, NET ACCESS, and NET GROUP.

- DOS based DLS graphical user interface.

- Command line administration of OS/2 LAN/Warp Server.

- Network DDE/Clipboard for Windows.

11.1.2 Functions Not Supported by DOS LAN Services (DLS)

The following functions are not supported in DLS:

- Use of shared serial devices (except for a serial printer configured at the server as a shared printer and assigned as a LPT port to DLS clients). This is a DOS restriction and not a DLS restriction.

- Start from `DOSSHELL`.

- Run while `DOSSHELL` is running unless redirectors are loaded in real-mode.

- Perform remote administration of an OS/2 LAN/Warp Server from the DLS GUI.

- Will not install if the path exceeds 127 characters after adding the path for the DLS code. (This is another DOS limitation.)

- Will not install if the environment memory is not big enough. In this case include the

  ```
  SHELL=C: DOS COMMAND.COM C: DOS  /E:512 /P
  ```

  statement in your CONFIG.SYS file to increase the environment memory to 512 bytes from the default 256 bytes.

- Run in an OS/2 Virtual DOS Machine (VDM).

- Change connections from a domain controller to a backup domain controller if the domain controller goes down.

11.1.3 Functional Overview within DLS Windows Interface

The DLS Windows (`WDLS.EXE`) interface provides access to the following functions:

- Logon and Logoff.

- Change logon password.

- Change logon assignments.

- Change user description.

- View, connect, and disconnect OS/2 LAN/Warp Server shared file aliases.

- View, connect, and disconnect OS/2 LAN/Warp Server shared printers.

- View, install, and use OS/2 LAN/Warp Server shared applications.

- Message support.

- List logged-on users.

- Manage print jobs in shared print queues (peer function).

- View directory-limit (DASD limits) information for a shared directory.

- Share local directories and printers (peer function).

- Send and receive messages from other network users.

- Queue, log, print, and view messages.

11.1.4 Functions not Supported by DLS Windows

The following functions are not supported in DLS in a Windows environment. DLS Windows cannnot:

- Have private network applications.

- Logon/logoff a medialess Remote-IPL requester.

- Start the virtual redirector if Windows is loaded from a network drive.

- Use the Basic Redirector.

- Work with Windows 32-bit file access.

- Work with 32-bit NDIS Vxd device drivers.

11.1.5 DOS LAN Services Graphical User Interface

As previously mentioned, you may access network resources from DOS workstations by using any of the three interfaces provided by DOS LAN Services:

- DOS LAN Services Graphical User Interface (`NETGUI.EXE`)

- Windows interface (`WDLS.EXE`)

- Command line interface (the DOS command prompt)

The Graphical User Interface provided with DOS LAN Services replaces the DOS LAN Requester EZVU-based full-screen interface and now supports DBCS (Double Byte Character Set) and mouse input. This can be used on DOS clients with or without Windows and enables the user to perform the following tasks:

- Log on and log off to or from an OS/2 LAN/Warp Server domain, modify logon assignments and reestablish persistent connections

- Change logon password and user comment

- List users logged on to the domain

- Modify the appearance of the graphical user interface

- Share directories and printers with other users on the network

- View directory-limit information for a shared directory (Windows only)

- Send and receive network messages

- Define private and public applications

The DOS LAN Services graphical user interface can run in graphics mode on any monitor or video adapter combination supporting VGA graphics or higher. The graphical user interface gains no benefit from higher resolution graphics.

If a workstation does not support VGA, the graphical user interface may be run in text mode by specifying the `/T` switch after the `NETGUI` command.

The DOS LAN Services graphical user interface is packaged with DOS LAN Services and is presented as an installation option of DOS LAN Services as mentioned in 11.3, "Installing DOS LAN Services" on page 219. For a functional overview of the graphical user interface of DOS LAN Services, also in conjunction with the graphical user interface functions provided in IBM Networks Clients for Windows 95 and Windows NT, see 9.1, "Common GUI Features and Functions" on page 95. Basic GUI features and functions are covered in the GUI chapter (9.1, "Common GUI Features and Functions" on page 95).

11.1.6 Peer Services

This service is included to enable DOS requesters to share the resources of your DOS workstation with other OS/2 Warp Server DOS and DOS/Windows clients, OS/2 LAN Requesters, and other Server Message Block (SMB)-based network products, such as Windows 95 and Windows NT. Peer services for DOS clients has a single-session restriction.

Note: OS/2 Warp 4 offers unlimited peer sessions.

The peer service in DOS LAN Services 5.0 now supports user level security, rather than share level security. User IDs and passwords must be used. User information as well as access rights information is now stored in the NET.ACC file. DLS Peer supports the following commands:

```
NET USER
NET ACCESS
NET GROUP
```

11.1.6.1 Working with DLS Peer Services

To avoid problems when working with DLS Peer Services, remember the following:

1. Remember, DLS peer has its own NET.ACC file which enforces you to define user IDs at the peer workstation.

2. Log on with USERID PASSWORD as an administrator the first time you logon at the peer.

```
LOGON USERID PASSWORD /LSLOGON:NO
```

3. Create a new user account (for example NEWUSER with the password of PASSWORD)

```
NET USER NEWUSER PASSWORD /ADD
```

4. Create an access profile for the resource to be shared (for example, the directory C: NET)

```
NET ACCESS C: NET /ADD
```

5. Grant access to users, for example to the previously created user ID.

```
NET ACCESS C: NET /GRANT NEWUSER:RWCDA
```

or whatever access is desired. R stands for Read-only, W stands for Write, C stands for Create, D stands for Delete, and A stands for Attributes.

6. Share the resource using the DLS GUI or command line:

```
NET SHARE NETDIR=C: NET
```

assuming that NETDIR is the desired share name.

Each user defined on the DLS Peer is automatically placed in the group USERS so that you can grant access to the group, rather than granting access to each individual user. The group USERS is automatically given Create access to the DLS peer print queue. Remember that only one user can access a peer resource at a time.

To share a CD-ROM drive, perform the following steps:

- Verify that the CD-ROM drive works locally with the DLS Peer service started (NET START PEER).

- Share the drive (E:) not the root directory of the CD-ROM (E:), assuming the E: drive is the CD-ROM's drive letter.

- Add the '/S' (share) parameter to the MSCDEX statement in the AUTOEXEC.BAT file.

11.1.6.2 Local Logon to the DLS Peer Workstation
In the previous section you performed a local log on to the DLS peer workstation and did not perform a domain logon. To access peer resources, only a local logon is necessary. If your user ID and password are the same both locally and on the domain, then a local logon also allows you access to domain resources; however, you must provide the full UNC name (`server sharename`) when making the server connection, because aliases are not interpreted with a local logon. In order to use aliases, you must be logged on to the domain.

With only a local logon and no domain logon, you do not receive your domain logon assignments. However, DLS attempts to reconnect any persistent connections for that workstation. If your user ID has permission to use these reconnected resources, then you are granted access. If you do not have permission, then the connection may be made (for example, port LPT1 may connect to LASERQ), but you could not actually use the resource.

For each user that logs on at a workstation, DLS maintains an unreadable password file with the extension PWL. This file contains a local password, domain password (if the user has logged on to a domain), and peer services passwords (if the user has used peer resources requiring passwords).

11.1.7 Reduced Memory Requirements

Given the limitations of DOS and conventional memory, it is obviously critical to minimize its use. Continuous efforts are focused on increasing the amount of conventional memory available for DOS applications. The result is that on an 8086/8088-based workstation configured as a basic redirector running DOS versions earlier than 5.0 and LAN Support Program, less than 500 KB of conventional memory remains available to applications. A similarly configured 386 or 486 workstation running IBM PC-DOS 7.0 with the virtual mode redirector, which is included with other DOS LAN Services enhancements, would leave over 600 KB of conventional memory available.

Note: It is important to remember that the virtual redirector does not maintain the redirections after you close Windows 3.x and return to DOS. In our examples, we chose to use the full redirector that maintains redirections after you close Windows 3.x.

As a strictly Windows client, DOS LAN Services does not actually use any conventional memory when configured as a virtual redirector, since it runs as a Windows virtual device driver (DLSHELP.SYS).

Note: DLSHELP.SYS cannot work in conjunction with IFSHELP.SYS. The DLS install routine deletes the `DEVICE=C: WINDOWS IFSHELP.SYS` statement from the CONFIG.SYS file.

The following sample DOS startup files illustrate how to configure a system using PC-DOS 7.0 and multiple configurations to be either a DOS only DOS LAN Services client, a Windows for Workgroups DOS LAN Services client, or a standalone DOS XMS system with optimum memory configurations for each configuration.

These sample files come from a 486 workstation with 16 MB RAM and an IBM Auto 16/4 Token Ring ISA Adapter installed. The amount of UMB space available varies depending on the hardware and BIOS configuration of the system, since hardware drivers are loaded into this memory area.

```
[MENU]
menuitem=DLS, DOS LAN Services Client (DOS Only LAN Client, Low RAM)
menuitem=WFW, Windows w/Full Redir (Windows LAN Client)
menuitem=DOS, Local DOS machine (NO LAN, High RAM)
menucolor=7,1
menudefault=DLS,30

[DLS]
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE NOEMS  <-----------See Note 1
DOS=HIGH,UMB
STACKS=9,256
devicehigh=C:\NET\PROTMAN.DOS /i:C:\NET
devicehigh=C:\NET\IBMTOK.DOS
devicehigh=C:\NET\DLSHELP.SYS
LASTDRIVE=Z  <-----------------------------See Note 2

[WFW]
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE NOEMS
DOS=HIGH,UMB
STACKS=9,256
DEVICEHIGH=C:\NET\PROTMAN.DOS /i:C:\NET
DEVICEHIGH=C:\NET\IBMTOK.DOS
DEVICEHIGH=C:\NET\DLSHELP.SYS   <----------See Note 3
LASTDRIVE=Z

[DOS]
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE NOEMS
DOS=HIGH,UMB
STACKS=0,0   <-----------------------------See Note 4

[COMMON]
FILES=30
BUFFERS=10   <-----------------------------See Note 5
DEVICEHIGH=C:\DOS\SETVER.EXE
```

Figure 123. CONFIG.SYS File with Menu Choice

```
@ECHO OFF
SET PATH=C:\NET;C:\NWDBPATH;C:\WINDOWS;C:\DOS;%PATH%;
SET TEMP=C:\DOS
GOTO %CONFIG%

:DLS
LH C:\DOS\SMARTDRV.EXE 128 2048
LH C:\DOS\MOUSE.COM
LH C:\DOS\DOSKEY.COM
LH SHARE
C:\NET\NET START
GOTO END

:WFW
LH C:\DOS\SMARTDRV.EXE 128 2048
LH SHARE
C:\NET\NET START   <---------------------- See Note 6
WIN
GOTO END

:DOS
LH C:\DOS\SMARTDRV.EXE 128 2048
LH C:\DOS\MOUSE.COM
LH C:\DOS\DOSKEY.COM
CLS
GOTO END

:END
```

Figure 124. AUTOEXEC.BAT File with Menu Choice

```
[network]
computername=WINDOSDLS
lanroot=C:\NET
autostart=full
username=TESTDLS
domain=WS_DOM01
lslogon=yes
reconnect=yes
passwordcaching=yes
timesync=no
```

Figure 125 (Part 1 of 2). The DOS LAN Services NETWORK.INI File

```
[install]
peer=yes
gui=yes
windows=yes
protocol=netbeui
minidls=no                    **for minidls only
installed=no                  **for minidls only
target=c: WSRCLNT\             **for minidls only

[Password Lists]
TESTDLS=C:\NET\TESTDLS.PWL
```

Figure 125 (Part 2 of 2). The DOS LAN Services NETWORK.INI File

Notes:

1. This uses a basic memory configuration without exceptions for devices such as video cards and network cards. Some devices may require additional switch settings or RAM exceptions to work properly. Refer to the manuals accompanying the device. Some greater RAM savings may result from using RAMBOOST included with IBM PC-DOS 7. This example uses the Multiple Boot Configuration available in IBM PC-DOS 7 and should work with other DOS versions supporting Multiple Boot. Consult the user's manuals to make any syntax changes, if necessary, or to implement any RAM saving function or software native to your specific DOS version.

2. This sample uses LASTDRIVE=Z. Each additional drive letter consumes approximately 80 bytes of memory. Additional RAM savings can result from using lower drive letters.

3. This device driver replaces the IFSHELP.SYS included with Windows for Workgroups.

4. Reducing this setting to STACKS=0,0 saves additional conventional memory but may cause some systems to hang.

5. Increasing the BUFFERS can increase performance in systems but will result in greater RAM usage.

6. This Windows sample configuration uses the Full Redirector to allow both Windows and DOS applications to have access to LAN and Peer resources.

PCMCIA configuration examples are provided in D.1, "DOS LAN Services Configured for PCMCIA Machines" on page 387.

11.1.8 Persistent Connections

Persistent connections are connections that are reestablished automatically from one logon to the next. They are based on the workstation, not the user ID, and are different from the user logon assignments. Only a local logon is required for persistent connections. Be aware that if you need to access reconnected resources on a domain server or on an OS/2 peer server (where user-level security is used), then it is easiest if you keep your user ID and password the same on your local workstation, the domain, and the OS/2 peer server. Otherwise, you must specify the password with the NET USE command, or you must use the GUEST account.

Each time a user logs off, the current connection information (to both OS/2 Warp Servers and peer servers) is stored in the DLS workstation NET CONNECT.DAT file. When another user or the same user logs back on at that workstation, DOS LAN Services attempts to reconnect to those resources. It is important to realize that *connecting to a resource and accessing that resource are two different actions*; in order to actually use the resource, the user ID must have the proper permissions.

You can choose not to have automatic reconnections made for a subsequent local logon by specifying reconnect=no in the NETWORK.INI file.

11.1.9 Local Logon vs Domain Logon

You can perform both a local logon and a domain logon. To access peer resources, only a local logon is necessary. If your user ID and password are the same locally and on the domain, then a local logon also allows you to access domain resources; however, you must provide the full UNC name (server sharename) when making the server connection, because aliases are not interpreted with a local logon. In order to use aliases, you must be logged on to the domain.

With a local logon and no domain logon, you do not receive your domain logon assignments. However, DOS LAN Services attempts to reconnect any persistent connections for that workstation. If your user ID has permission to use these reconnected resources, then you are granted access. If you do not have permission, then the connection may be made (for example, port LPT1 may connect to LASERQ), but you could not actually use the resource.

For each user that logs on at a workstation, DOS LAN Services maintains an unreadable password file with the extension PWL. This file contains a local password, domain password (if the user has logged on to a domain) and peer services passwords (if the user uses peer resources requiring passwords).

11.1.10 Performance Enhancements

DOS LAN Services provides a significant increase in performance in comparison with DOS LAN Requester, especially in instances where the emphasis is on random read access. This is due to the ability of DOS LAN Services requesters to use big buffers as cache and the use of a read ahead function.

11.1.11 Network Dynamic Data Exchange and Clipboard

The network Dynamic Data Exchange (DDE) and clipboard feature available under DOS LAN Services in a Windows environment extends DDE and clipboard capabilities across the network. This feature does not create a network clipboard; it allows other users to access your local clipboard and enables you to access other user's clipboards.

11.1.12 Common Configuration File Structure

The DOSLAN.INI file, which contains requester configuration parameters for DOS LAN Requester, has been replaced in DOS LAN Services with a NETWORK.INI file. It is structured in a similar way to the OS/2 Warp Server and OS/2 Requester's IBMLAN.INI, but requires less in terms of manual configuration for tuning purposes because it automatically sets parameters based on the amount of XMS memory available in the workstation.

See 11.5.2, "NETWORK.INI Parameters" on page 236 for descriptions of the NETWORK.INI parameters. A typical NETWORK.INI file is shown in Figure 125 on page 214.

11.2 General Windows Information

In this chapter we share some Windows-related information with you that you might not know.

- To run Windows in 386 enhanced mode you need to have at least 200 KB of unused conventional memory and 1024 KB of available extended memory.

    - The more programs you run simultaneously, the more memory you will need.

    - Windows will put 24 BB of buffer into the UMB area if it is available. Otherwise conventional memory is used.

- The more conventional memory available to DOS before Windows starts, the better it is. Windows bases the amount of memory available to non-Windows (DOS) applications executed from within Windows on what is available before Windows starts.

- Windows only uses extended memory (XMS), so unless you are running a DOS application that requires expanded memory (EMS), always specify `DEVICE=C: DOS EMM386.EXE NOEMS` in the CONFIG.SYS file.

  Note: You might need to pass include and exclude memory frame information for DOS LAN Services to orderly open LAN adapters. The EMM386.EXE program is not smart enough to exclude memory frames that are used by LAN adapters (ROM/RAM area).

- Windows can use swap files to simulate memory. Use a large permanent swap file if possible. Don't use 32-bit file access.

- Delete unused icons and associated files to save disk space and RAM.

- Windows takes over all memory mamangement when it loads. Memory excluded by EMM386.EXE is ignored unless you specify them in the Windows SYSTEM.INI file (`EmmExclude=` in section [386Enh]).

  - To prevent Windows frm scanning the upper memory area for unused memory address space, specify `EmmExclude=A000-FFFF`. If Windows hangs unexpectedly there might be a conflict with an unseen adapter (for example, high resolution video adapters), so excluding all upper memory can quickly help to isolate this.

- SMARTDRV.EXE does not work with networked drives.

  - When `DOS=HIGH` is set in the CONFIG.SYS file, you can specify `BUFFERS=30` with DOS 5.x, 6.x, or 7.x without using any conventional memory.

  - If you insist on using SMARTDRV.EXE, then set the `WinCacheSize` value and `InitCacheSize` value to the same number so Windows can reduce the cache size if it needs more memory.

- If DOS applictions are being launched from Windows and they fail with an out of memory error, try setting the `Min Menory` in the PIF file lower than the default of 128 KB.

- If you are using IBM Token-Ring Network 4/16 Adapter II (NDIS-only) be sure the PROTOCOL.INI file has the entry `WindowsEhnaced=Yes`.

- Add `MaxBPs=768` to the [386Enh] section of the SYSTEM.INI file to prevent Windows from hanging after several hours of usage due to insufficient breakpoints. (Each time you go in and out of a Windows application, a breakpoint (BP) is used and not released until exiting Windows)

- Shadow RAM and network adapters may have memory conflicts. Disable Shadow RAM using your computer's `SETUP` utility.

11.3 Installing DOS LAN Services

Step-by-step installation instructions are provided in the *OS/2 Warp Server: Up and Running* manual that comes with the product. As previously discussed, DOS LAN Services provides a number of new features. To take full advantage of these components, take the time to carefully plan your installation. For example, decide whether you could make better use of resources that are currently connected to workstations by implementing the DOS peer service. Or, enable users to discover the benefits of workgroup computing by allowing them to access data residing on each other's workstations through the Network DDE and clipboard feature.

You need to have PC-DOS or MS-DOS installed Version 5 or higher. We recommend using PC-DOS 7 to gain maximum memory management capabilities that come with the product. All scenarios described in this chapter are based on PC-DOS 7. Before you install DOS LAN Services, make sure that `HIMEM.SYS` is laoded from your CONFIG.SYS along with the `DOS=HIGH` statement. The `EMM386.EXE` device driver can be included in the CONFIG.SYS file when DOS LAN Services is installed and configured properly. If this device driver is already part of your CONFIG.SYS file, the LAN adapter might not open if memory was allocated by EMM386.EXE. DOS LAN Services needs this to open the adapter. We recommend removing this statement and running `RAMSETUP` (or `MEMMAKER` for MS-DOS-based machines) at another time, to optimize memory allocation.

Properly running DOS and Windows environments fully depend on sophisticated memory management. Proceed with the following steps:

Note: The installation procedure is the same for DOS with or without Windows installed.

 1. If you have not created the DOS LAN Services product diskettes yet, do so by inserting the OS/2 Warp Server CD-ROM in your CD-ROM drive. Then type the following command at an OS/2 command line:

    `E: INSTUTIL`

    assuming the E: drive is your CD-ROM's drive letter.

    The OS/2 Warp Server Install Utilities window is be presented. Select the radio button for **Make 3.5-inch product diskettes** and when complete, select **OK**. Next, select the radio button for **IBM LAN Server 5.0 (23 diskettes)**, then select **OK**. Finally, select the **Skip** button until the Insert Diskette window prompts you to insert the first diskette for DOS LAN Services.

    Note: You need to have four formatted (empty) diskettes ready to create the DOS LAN Services product diskettes.

Refresh IPx8260/IPx8265

There is a refresh code of DOS LAN Services Version 5.0 available on the Internet. The refresh code is part of IBM OS/2 LAN Server for Warp Server FixPak. Point to the following Web site to get it:

`http://service2.boulder.ibm.com/pspfixpk/`

Note: The letter 'x' in IPx8260 stands for the country letter. The US version of the FixPak would be IP08265. In some countries only IPx8260 is available.

---

2. Insert the DOS LAN Services Diskette 1 in your client's diskette drive and type the following command:

`A: INSTALL`

Note: Several undocumented parameters can be passed to INSTALL.BAT

/I	(Upper case "i") Disables hardware detection. Use only if Install will not run without it. Install will prompt you to specify your hardware configuration.
/L1	Specifies the location of the remote install error log file.
/L2	Specifies the location of the remote install history log file.
/N	Use this option if your adapter/transport is configured and you want to install the services provided by DOS LAN Services without changing the adapter/transport information. `DEVICE=C: NET DLSHELP.SYS` is added to the CONFIG.SYS file. Everything else is left whatever configuration existed before.
/R	Required for remote install. Provides the location of the response file.

There are two install programs in DOS LAN Services Version 5.0:

- INTSTALR.EXE

  Same as DOS LAN Services Version 4.0 and need 440 KB of conventional memory to run.

- INSTAL16.EXE

  Uses DOS16M (protect-mode installer) libraries and needs only 200 KB to run.

The DOS16M support used by INSTAL16.EXE does a lot of hardware checking and may result in GPFs (Windows General Protection Fault) on

non-tested hardware. A workaround is to use the `/I` parameter with INSTALL.BAT, or just try INSTALR.EXE.

3. Press **Enter** at the Install DOS LAN Services window.

4. Type the subdirectory in which you want to install DOS LAN Services. The default directory is C: NET

5. Enter the machine name as prompted. This name identifies you in the network. Make sure this name is different than the domain name. However, it can be the same name as the user ID you enter later. The machine name can have up to 15 characters.

6. Enter the user name (user ID) as prompted. This name can have up to 20 characters and can be the same as your machine name.

7. Enter the domain name as prompted. This name can have up to 15 characters.

8. At the options list, select either **The listed options are correct** or make changes to the options by moving the bar to the options to be changed. For example, if you want to change the default protocol driver from IBM NetBEUI to one of those listed below, scroll up to Protocol Driver, press **Enter**, then scroll up to Change driver for protocol and press **Enter** again. With DOS LAN Services, the following protocol drivers come with the product:

   - **Other protocol**

     This options allows you to install protocol drivers other than those listed below. You are prompted to specify the location of the protocol driver file.

   - **IEEE 802.2 Support**

     Select this option if you want to have both, NetBIOS and 802.2 bound to the LAN adapter. DOS LAN Support Program is installed with the following DXM drivers:

     - DXMA0MOD.SYS

     - DXMC0MOD.SYS

     - DXMT0MOD.SYS

     which require about 37 KB of conventional memory (as with DOS LAN Services version 4.0).

   - **TCPBEUI (Real-Mode)**

     Select this option if you want to have NetBIOS over TCP/IP installed in a native DOS and DOS/Windows environment. If you exit Windows, network connections will remain. This option takes about

92 KB of conventional memory and can talk to OS/2 LAN/Warp Server only if they are running TCPBEUI. Also see 11.6, "TCP/IP and TCPBEUI Options in DOS LAN Services" on page 243 for more details.

- **TCPBEUI (Real-Mode) and IBM NetBEUI**

  Select this option to install native NetBIOS and NetBIOS over TCP/IP bound to the LAN adapter. This solution is suitable for native DOS and DOS/Windows environments. If you exit Windows, network connections will remain. This option takes about 144 KB (92 KB + 52 KB) of conventional memory and can talk to OS/2 LAN/Warp Servers if they are running TCPBEUI or NetBEUI. Each stack has a lana # to go to:

  - lana 0 is the default for NetBEUI

  - lana 1 is used for TCPBEUI if NetBEUI is installed

  Note: The messenger and peer services work only on lana 0. This means that if you send a message from DLS client 'A' that has NetBEUI and TCPBEUI to DLS client 'B' that has only TCPBEUI installed, the messenger will use NetBEUI through lana 0, which client 'B' cannot hear.

  Also see 11.6, "TCP/IP and TCPBEUI Options in DOS LAN Services" on page 243 for more details.

- **TCPBEUI (Windows Protect-Mode)**

  Select this option to install NetBIOS over TCP/IP. This solution is suitable for Windows environments only. Once you exit Windows to the DOS prompt, all network connections are disconnected. This solution uses only 2 KB to 4 KB of conventional memory and can work with OS/2 LAN/Warp Servers if they are running TCPBEUI.

  Notes:

  a. If you install only the protect-mode version of TCPBEUI, you are not be able to start the peer, messenger, or netpopup services. As with DOS LAN Services 4.0, these services require Full Redirector to be started first.

  b. The GA (General Availability) code of DOS LAN Services 5.0 that comes with OS/2 Warp Server requires Windows for Workgroups. ServicePaks IPx8260 and IPx8265 offer newer versions of DOS LAN Services that will work with Windows 3.1 or higher.

  Also see 11.6, "TCP/IP and TCPBEUI Options in DOS LAN Services" on page 243 for more details.

- **TCPBEUI (Windows Protect-Mode) and IBM NetBEUI**

  Select this option to install native NetBIOS and NetBIOS over TCP/IP bound to the LAN adapter. This solution is suitable for Windows environments only. If you exit Windows, network connections are disconnected. This option requires about 54 KB to 56 KB of conventional memory and can talk to OS/2 LAN/Warp Server if they are running TCPBEUI or NetBEUI. Each stack has a lana # to go to:

  - lana 0 is the default for NetBEUI

  - lana 1 is used for TCPBEUI if NetBEUI is installed

  Notes:

   a. The messenger and peer services work only on lana 0. This means that if you send a message from DLS client 'A' that has NetBEUI and TCPBEUI to DLS client 'B' that only has TCPBEUI installed, the messenger will use NetBEUI through lana 0, which client 'B' cannot hear.

   b. The GA code of DOS LAN Services 5.0 that comes with OS/2 Warp Server requires Windows for Workgroups. ServicePaks IPx8260 and IPx8265 offer newer versions of DOS LAN Services that will work with Windows 3.1 or higher.

  Also see 11.6, "TCP/IP and TCPBEUI Options in DOS LAN Services" on page 243 for more details.

- **IBM NetBEUI**

  This option installs the NetBIOS interface. This solution is suitable for DOS and DOS/Windows environments. NetBEUI is loaded in real-mode so connections remain in case you exit Windows. This option takes about 52 KB of conventional memory.

9. If configured for TCPBEUI, you need to provide additional TCP/IP information, such as:

   - `IPAddr=`

     Local IP address of your workstation

   - `SubNetMask=`

     Subnet mask of your IP network

   - `GatewayAddr=`

     Router address

   - `DNSAddr=`

     Address of the primary domain name server

Note: The install program does not do syntax checking or validation. The install panels scroll up to reveal more parameters that can be set, for example, DHCP support (`BootP=DHCP`).

DHCP Support

The following parameters must be set to enable DOS LAN Services client to retrieve an IP address and other IP configuration information from an DHCP server:

- `BootP=[value]`

  where `[value]` can be `Never`, `Attempt`, `Always`, or `DHCP`. We recommend the `BootP=DHCP` setting.

- `DHCPClientID=[value]`

  where `[value]` is the class to which the DHCP client belongs. See 68 for more information about classing.

Since dynamic DNS is not supported by DOS LAN Services, the client needs to get the host name from the DHCP server. More information is provided in 11.6.1, "Setting Up DHCP Support" on page 243.

- The option titled Graphical User Interface installs the DOS GUI. Select not to install this option when you do not plan to run the GUI in native DOS. This will not affect the GUI for Windows.

- The option titled Peer Services enables users to share resources such as files and printers with other users in the network. Select not to install it to go without peer services.

- The option titled Windows Support installs Windows-specific files. At next startup of Windows, the `DLSSETUP` command is run. This command creates the DOS LAN Services folder. Select the GUI from this folder.

10. At the summary list of options, press **Enter** when you do not have to make changes to your configuration. Otherwise scroll up to the option you want to make changes to. For example, if the network card was not recognized successfully, you can change the settings by scrolling up to the option titled Network card, pressing **Enter**, then scrolling up to Change driver for network card and press **Enter**. These network cards are supported by default:

3Com Etherlink II or IITp (8 or 16-bit)
3Com Etherlink III
3Com Etherlink/MC
Cabletron E2100 Series DNI
IBM LAN Adapter for Ethernet (IBMENI.DOS)

IBM Ethernet Credit Card Adapter
IBM Token-Ring (All Types)
IBM Token-Ring (MCA)
IBM Token-Ring II
IBM Token-Ring 4/16Mbs
IBM Token-Ring 4/16Mbs (MCA)
IBM Token-Ring Network 4/16 Adapter II
Intel EtherExpress 16 or 16TP
Intel TokenExpress EISA 16/4
Intel TokenExpress 16/4
Novell/Anthem NE2000
Novell/Anthem NE/2
Olicom 16/4 Token-Ring Adapter
Proteon Token-Ring (P1392)
SMC (WD) Ethercard PLUS/A (MCA)
SMC (WD) Ethercard PLUS/A Elite 16 Combo

If the network adapter you use is not in the list, select **Network card not shown in the list below...** and specify the location of the OEMSETUP.INF file for the OEM adapter you want to use (see 11.3.2, "Installation of OEM Network Adapters" on page 226 for more details).

11. Insert diskettes as prompted. Reboot your workstation once all files are copied to the hard disk.

11.3.1 Network Adapter Specific Hints and Tips

Use the following list to determine if any additional configuration is required so that your selected network adapter functions correctly with DOS LAN Services, or if there are restrictions in using your adapter with DOS LAN Services.

Token Ring Network Adapter Problem Determination

A token-ring open lobe cable condition on a DOS LAN Services workstation does not produce an error message that indentifies it as such. If you have a workstation with a token-ring adapter that appears to boot correctly and then exhibits the following symptoms, the underlying cause may be a cabling problem:

- NET START executes slowly, but is successful with netgui specified as an option for the autostart parameter of the NETWORK.INI file.

- Logging on from the command line using the NET LOGON command reports:

  NET2182: The requested service has already been started

- A local logon from the DOS LAN Services Windows graphical user interface is successful.

- A validated logon from the DOS LAN Services Windows graphical user interface results in a failure, stating that the user has no privileges on the network.

IEEE 802.2 Support on Ethernet Adapters

If you have an Ethernet adapter and require IEEE 802.2 support through the DXME0MOD.SYS and DXMT0MOD.SYS device drivers, or if Windows or DOS memory managers are used with the LAN Support Program, you need to specify that application programs should be prevented from intercepting the X'5C' interrupt issued by the NETBIOS device driver. This is achieved by adding `CF=Y` to the DXMT0MOD.SYS line in CONFIG.SYS.

IBM Etherstreamer MC32 and NET START

If you receive a `NET 54: The network is busy` error while performing a NET START on a system with the IBM Etherstreamer MC32 adapter installed, add `NET START NETBIND` to AUTOEXEC.BAT before the line `C:\NET\NET START`.

IBM ISA Ethernet (10Base2,T) Adapter

If you are using the PS/ValuePoint ISA 10Base-T/10Base2 Ethernet Adapter, be sure that you run the DOS LAN Services installation program with the `/I` parameter, and then run DOS LAN Support Program using the `DXMAID` command.

11.3.2 Installation of OEM Network Adapters

If you are installing DOS LAN Services to run on a network adapter that is not on the list of supported adapters displayed by the installation program, see if an OEMSETUP.INF file resides on the driver diskette supplied with the adapter. If so, you can use the file with the DOS LAN Services installation program to configure your adapter by using the steps detailed in this section. If this file does not exist, configure the adapter by following the instructions that came with it, after installing DOS LAN Services.

To use the OEMSETUP.INF file as input to the DOS LAN Services installation program, follow these steps before running INSTALL.EXE. The following examples are taken from the Olicom Token-Ring Network 16/4 Adapter driver diskette.

 1. Edit the OEMSETUP.INF file and verify that it contains both a `[disks]` section and an adapter section that contains a `devdir` parameter. If so, proceed as follows. Otherwise, configure this adapter separately,

according to the OEM supplied instructions, after installing DOS LAN Services.

2. In the [disks] section, verify that the symbol (usually `A` or `1`) is defined as the absolute path (minus any drive letter) to where the adapter driver resides. The name of the driver may be determined by reading the OEM supplied documentation shipped with the adapter.

> For example, if the driver called `olitok16.dos` is located in the following path of the OEM supplied diskette:
>
> `\MSLANMAN.DOS\DRIVERS\TOKENRNG\OLITOK16`
>
> you need to ensure that the [disks] section contains the following line:
>
> `1=\OLICOM\MSLANMAN.DOS\DRIVERS\TOKENRNG\OLITOK16 ,....`
>
> where "`....`" represents the adapter description text that should not be changed.

3. The adapter section containing the `devdir` parameter would need to have the following contents:

```
[oli164a]
    devdir=1:olitok16.dos
    device=olitok16.dos,@devdir\olitok16.dos
```

where `1` is the symbol defined in the [disks] section.

4. Run the DOS LAN Services installation program. When presented with the list of adapters, choose **Network card not shown on the list below** to be prompted to the location of the OEMSETUP.INF file. Enter the fully qualified path (including the drive letter) of where the file is located.

For example, if the file is in the root directory of the OEM-supplied disk, insert the disk in drive A:, type `A:\`, and press **Enter**.

The DOS LAN Services installation should then proceed normally.

11.3.3 Important TCP/IP Utilities

DOS LAN Services comes with three important TCP/IP utilities:

- `PING`

  Tests connection to a specific IP address.

- `WPING`

  Ping Utility under Windows (must add PROTOCOL and SERVICES files in ETC directory)

- `NBUTIL`

Provides a local name chache on the DLS client to associate a server name with an IP address. If the server and client are not on the same segment, you must run NBUTIL every time you boot the client. We recommend executing NBUTIL from the AUTOEXEC.BAT file. The syntax is:

```
--NBUTIL--[server name]--[IP address]-------------------------
```

Instead of using a local name cache that contains server name-to-IP address mapping information, see 11.6.2, "DLS and NetBIOS Name Server" on page 246 for a more superior solution.

11.3.4 DLS Module Descriptions

Once DOS LAN Services is installed, the following files are found in the NET directories:

DOSNET.LIB   LAN Server APIs for DOS applications.

INSTALR.EXE   Installer main program which needs 440 KB of conventional memory to run.

INSTAL16.EXE   Alternate installer program which only needs 200 KB of conventional memory to run. It uses DOS16M (protect-mode installer) libraries.

INSTALL.MSG   Installer error and warning messages.

NETWORK.INF   Used by the installer to configure LAN adapter cards.

NETWORK.INI   Contains the default parameters used by the NET START command and other services (for example, Peer services).

NET.EXE   Contains the following services:

- Start code, that is the NET START service name

- Redirector

- NetBEUI

- Loader

- Spawns CMDS.EXE (command line interface)

- Spawns CMDS16.EXE (protected mode command lines interface)

NET.MSG   Error and warning messages used by all interfaces; it contains messages in the range between 1 and 7450; all numbers up to three digits are prefixed with "Error", for

example, `Error 231`, and all four-digit numbers are prefixed with "NET", for example, `NET3682`.

NETH.MSG   Cause and action text for error messages in NET.MSG.

CMDS.EXE   Command line interface; spawned by NET.EXE.

CMDS16.EXE   Protected mode command line interface; spawned by NET.EXE.

DLSHELP.SYS   Redirector helper module. Hooks interrupt and passes requests on the redirector. Replaces Windows' IFSHELP.SYS.

PEER.EXE   Peer service; file amd local print device sharing and management. Can be started by the `NET START PEER` command.

PQ.SPL   Print queue management file used by peer service.

PQ.SEP   Separator page used by peer service for shared printers.

NETGUI.BAT   Starts the DOS GUI and reloads it after running an application.

DZG4.EXE   Actual DOS GUI executable; acronym for "DLS Zinc GUI 4.0".

SUPPORT.DAT   Contains all DOS GUI panels for graphics and text modes.

GUI.MSG   Error and warning messages used by the DOS GUI and WDLS.EXE (Windows GUI); message numbers are between NET7450 and NET7600.

GUIH.MSG   Cause and action text for error messages in GUI.MSG.

INT10.DLL   Dynamic Link Library used by DOS GUI for protected mode interrupt 10 support.

MOUSE.DLL   Dynamic Link Library used by DOS GUI for protected mode mouse support.

UNICODE.DAT   Used by DOS GUI for mapping between hardware and UNICODE code pages (Asian versions of DLS 4.0 only).

UNICODE.FNT   Used by DOS GUI in graphics mode (Asian versions of DLS 4.0 only).

PS55PRT.EXE   PS/55 printer support for DOS-J (Asian versions of DLS 4.0 only).

CONNECT.DAT   Stores persistent connection information, that is, UNCs and associated drive and print device.

USERID.PWL   Password list file for an individual user ID; stores passwords for connections and logon.

NETPOPUP.EXE   Provides message popup.

MESSENGER.EXE Receives messages and either logs them or passes them on to NETPOPUP.EXE.

MESSAGES.LOG Default message log file.

CONNECT.TXT   DLS troubleshooting document.

WDLS.EXE   Windows interface of DOS LAN Services.

DLSNET.DRV   Dynamic Link Library used by WDLS.EXE.

DLSNET.HLP   Windows help file.

NETAPI.DLL   LAN Server APIs for Windows applications.

PSSPL.DLL   LAN Server print APIs for Windows applications.

RUNLSAPP.EXE Invokes WinExec to run applications.

WINDLS.DLL   Dynamic Link Library used by WDLS.EXE, SLDNET.DRV, and RUNLSAPP.EXE.

WINPOPUP.EXE Hand-shakes with NETPOPUP.EXE.

DLSSETUP.EXE   Modifies the WIN.INI and SYSTEM.INI files to pint to DLSNET.DRV.

FMSHARE.DLL   Hook into Windows 3.1 File Manager for directory sharing (active only when peer service is started).

VNETBIOS.386   Real mode to protect mode NetBIOS layer used by Virtual Redirector (VREDIR.386)

VNETSUP.386   Virtual Redirector support module. Used for reading INI information and initialization of the redirector.

VREDIR.386   Virtual Redirector used in Windows 3.1 enhanced mode.

NETWKSTA.EXE Basic Redirector.

REDIR.EXE   Full Redirector.

11.3.5 DLS Initialization Process

The following is a decription of what services and drivers are initialized, depending on the parameters passed to the NET START command.

- NET START NETBIND

    - NET.EXE will execute:

        NETBIND

- NET START NETBIOS (Use for Virtual Redirector)

    - NET.EXE will execute:

        NETBIND
        NETBEUI.EXE   (Inside NET.EXE)

- NET START BASIC

    - NET.EXE will execute:

        NETWKSTA.EXE (Inside NET.EXE)
        NETBEUI.EXE   (Inside NET.EXE)

- NET START FULL

    - NET.EXE will execute:

        REDIR.EXE   (Inside NET.EXE)
        NETBEUI.EXE   (Inside NET.EXE)

- NET START PEER (Requires Full Redirector)

    - NET.EXE will execute:

        SHARE.EXE (If not already loaded)
        PEER.EXE

- NET START MESSENGER (Requires Full Redirector)

    - NET.EXE will execute:

        MESSENGER.EXE

- NET START NETPOPUP (Requires Full Redirector and Messenger)

    - NET.EXE will execute:

        NETPOPUP.EXE

11.3.5.1 Commands Executed from NET.EXE

The following commands may be passed to the NET.EXE module to influence
the behavior of DOS LAN Services or retrieve information from DOS LAN
Services:

- NET START [service]

    where [service] can be requester, peer, messenger or netpopup service to
    be started.

- NET STOP [service]

    where [service] can be requester, peer, messenger or netpopup service to
    be stopped.

- NET CONFIG

displays your current requester settings, for example:

```
Machine ID                    \\ITSCDLSWKUZ
User ID                       ADMIN

Software version              IP08000
Requester version             5.00
Requester root directory       C:\NET

Requester domain              ITSCAUS
```

- NET VER

  displays the version of the requester, for example:

  ```
  DOS LAN Services Full Redirector Version 5.00
  (C) Copyright International Business Machines Corporation 1993,19
  (C) Copyright Microsoft Corp. 1992.  All rights reserved.
  ```

- NET HELP

  provides information about commands and error messages. For more
  information about a specific requester command, type the command line
  name followed by /? (for example, NET VIEW /?).

11.4 DOS Memory Management

The following sections give you hints and tips to improve memory
consumption in DOS and DOS/Windows-based machines.

11.4.1 Redirector Conventional Memory Usage

The following section shows how much memory each redirector consumes.

Basic   Uses 49 KB of conventional memory. The basic redirector
provides all standard requester functions such as connecting,
disconnecting and browsing. It requires less memory and disk
space and should be used if you:

- Have limited memory available on your workstation

- Do not wish to use aliases to identify resources

- Do not plan to use Windows

- Have a workstation with limited processing power, such as
  an 8086 or 8088

Full   Uses 99 KB of conventional memory. The full redirector provides
advanced network functions such as named pipes, increased
performance and full API support.

Predir Protected-mode redirector not supported in a Windows environment. Uses 53 KB of conventional memory: 49 KB for protected-mode redirector and 4 KB for DOS16M stub. Same functionality as the Full Redirector.

Virtual Uses 0 KB of conventional memory. The virtual redirector provides the optimum memory availability since it does not use conventional memory, running as a Windows virtual device driver.

Peer Uses 49 KB of conventional memory:

- 33 KB for peer services

- 4 KB for RTIME

- 8 KB for PSPRINT

- 4 KB for DOS16M Stub

11.4.2 How to Increase Amount of Lower Memory

What to do when you need more lower memory:

1. Before you do anything else, we recommend creating an emergency boot diskette (DOS startup diskette). Sometimes your system will hang if a memory conflict occurs due to changes made in the CONFIG.SYS file and you may need to use a boot diskette to change the CONFIG.SYS file. Occasionally, machines reboot after memory conflicts and your machine enters a loop (boot - memory conflict - reboot - memory conflict - and so on).

2. Use `HIMEM.SYS`, `EMM386.EXE`, `DOS=HIGH,UMB`, `DEVICEHIGH`, and `LOADHIGH` (load device drivers and programs into upper memory blocks (UMB).

3. Check the shared ROM/RAM setup on adapters to reconfigure with the maximum contiguous UMB area. Most LAN adapters come with setup diskettes that allow you to change ROM and RAM areas of your LAN adapter.

4. Change the order in which the drivers and programs load. When loading a program into upper memory, DOS checks the first UMB to see if the driver or program will fit. If the driver or program is too large for the UMB it is not loaded high, even if another UMB area is large enough for it to fit.

   Note: Remember, when you upgrade to new drivers or programs, the new ones may be a different size and thus change your UMB usage.

5. Try including unused upper memory blocks. Some UMB areas that you can use are:

B000-B7FF This area is used by monochrome monitors, so if you use a color monitor you can include this area and gain an additional 32 KB of UMB area. However, using this range with Super VGA (SVGA) that use 128 KB page frames will cause problems.

BB00-BFFF This area is used for VGA color text buffers and provides an additional 20 KB of UMB area. The only way to know if you can use this range is to try it. Do not use it with Windows.

E000-EFFF This area is the extended BIOS area. Different PCs use parts of this area so you may end up with different ranges (on some PCs it is EA00-F3FF). The only way to know if you can use this range is to try it or use a utility, such as SCANDATE or MANIFEST.

F600-FDFF This area is used by ROM Basic. If you do not use any Basic programs, including this range will provide additional 32 KB of UMB area. The `EDIT` program is a Basic program and on an IBM PC or PS/2 running PC DOS 5 it uses ROM Basic. Later releases of PC DOS do not use ROM Basic.

11.4.3 How to Solve a Memory Conflict

If you experience memory conflicts, such as a LAN adapter that does not open, try these tips:

1. Try to recreate the problem by loading all device drivers and programs into lower memory (remove `LOADHIGH` and `DEVICEHIGH` statements).

   a. One by one, add the drivers and programs back into upper memory until you get the failure.

   b. Change the order in which the drivers and programs are loaded (as much they will let you) so that the failing driver or program is loaded into another area of memory.

2. Check the shared ROM/RAM setup on adapters (LAN adapters and, especially, sound cards) and reconfigure with the maximum contiguous UMB area. On some cards you need to set jumpers differently to do so. Modern cards come with setup diskettes that let you reconfigure ROM/RAM areas.

   Note: When checking the settings, look for shared ROM/RAM addresses that overlap memory areas in use by other adapters.

11.4.4 Configuring DLS Windows

To properly work with DOS LAN Services and Windows make sure of the following items:

- Either the Full Redirector or the Virtual Redirector must be used with Windows.

- To properly configure the Windows SYSTEM.INI file, run `DLSSETUP` from [**File** — **Run**]. Specify C: NET DLSSETUP.EXE at the Run command line.

  These statements are be added to the SYSTEM.INI file for non-RIPL 80386 and above PCs to the listed sections:

  ```
  [Boot]
  NETWORK.DRV=DLSNET.DRV

  [Boot.Description]
  NETWORK.DRV=IBM DOS LAN Services

  [386Eenh]
  NETWORK=vnetbios.386, vnetsup.386, vredir.386
  ```

  Note: The [386Enh] section only applies for Virtual Redirector. For Full Redirector (no transition to Virtual Redirector) use:
  ```
  NETWORK=*dosnet, *vnetbios
  ```

  DLS will also set up a new program group titled IBM DOS LAN Services.

Even if the Full Redirector was started before starting WIndows, the Virtual Redirector will load if the SYSTEM.INI contains the lines:

```
[386Eenh]
NETWORK=vnetbios.386, vnetsup.386, vredir.386
```

If you only use Windows applications, use the Virtual Redirector, not the Full Redirector, since this will free up memory for the Windows applications.

11.5 DOS LAN Services and the NETWORK.INI

When DOS LAN Services is initialized by the `NET START` command, the parameters in the NETWORK.INI file are read and used to customize DLS's configuration. The NETWORK.INI file DLS bypasses DOS limitations that do not allow more than 127 characters in a command line. The NETWORK.INI file allows all parameters to be passed to the `NET START` command.

11.5.1 Optimizing NETWORK.INI

Perform the following steps to optimize your DOS LAN Services configuration:

1. To optimize network performance, use the default configuration of `AUTOCACHE=YES`. This provides 30 times 8 KB buffers in XMS (Extended Memory Specification) for caching data.

2. To optimize for conventional memory, use either the Basic Redirector (50 KB) or set AUTOCACHE=NO for the Full Redirector. This reduces memory by about 10 KB.

   - AUTOCACHE=YES   REDIR.EXE is 98 KB

   - AUTOCACHE=NO   REDIR.EXE is 88 KB

3. All NETWORK.INI parameters from the [network] section are valid for the Virtual Redirector except for AUTOCACHE.

4. The Virtual Redirector uses 1/8th of all free XMS for buffer allocation.

11.5.2 NETWORK.INI Parameters

The following table provides details of the parameters in the [Network] section, [Messenger] section, [netpopup] section, and [Peer] section of the NETWORK.INI file.

Table 10 (Page 1 of 6). NETWORK.INI Parameter Values			
Parameter	Description	Valid Values	Default Value
computername	Identifies the workstation to the network	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } Ù ` ~	Name specified at installation
lanroot	Directory where DOS LAN Services is installed and starts	Fully qualified path (drive letter and path)	C:\NET
autologon	Starts the logon command when DOS LAN Services is started and prompts user to logon to a domain	Yes, No	Yes
autostart	Indicates which services to start when NET START is entered	NetBEUI, Basic, Full, Messenger, Netpopup, Peer	Basic
username	Identifies the user to the network	Up to 20 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } Ù ` ~	Name specified at installation
domain	Name of the domain that the workstation belongs to	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } Ù ` ~	Name specified at installation

Table 10 (Page 2 of 6). NETWORK.INI Parameter Values			
Parameter	**Description**	**Valid Values**	**Default Value**
reconnect	Specifies whether persistent connections are reconnected when logging on	Yes, No	Yes
lslogon	Specifies whether logon verification is to be performed by the domain controller	Yes, No	No
numbigbuf	Indicates the number of big buffers to use (Full and Virtual Redirectors) **Note:** Overridden by autocache=yes	0 to 4096	2
sizebigbuf	Specifies the size of big buffers in KB (Full and Virtual Redirectors) **Note:** Overridden by autocache=yes	4096 to 32768	4096
numworkbuf	Specifies the number of work buffers to use	2 to 16	2
sizworkbuf	Specifies the size of work buffers to use in KB	512 to 16384	1024
extraheap	Allocates extra heap space for the redirector, and should be tuned for file-intensive applications such as databases	1024 to 32768	0
keepconn	Time to keep dormant connections	0 to 65000	60
sesstimeout	Time to keep dormant sessions.	10 to 30000	90
autocache	Automatically allocates numbigbuf, sizbigbuf, and extraheap based on the amount of XMS memory available, overriding the individual values set for these parameters, and is recommended to increase performance	Yes, No	Yes
printbuftime	Specifies the amount of time, in seconds, before a print job is sent to the server after the print job is submitted	0 to 65535	60

Table 10 (Page 3 of 6). NETWORK.INI Parameter Values			
Parameter	**Description**	**Valid Values**	**Default Value**
lanas	Specifies the number of LAN adapter cards used by the workstation	0 to 7	1
ripl	Identifies a remote IPL workstation	Yes, No	No
passwordcaching	Indicates that passwords are to be cached to a file and saves passwords to servers in a password protected file, so the user does not have to enter a password for each server that they access	Yes, No	Yes
multilogon	Indicates whether the user ID can be logged on at multiple workstations	Yes, No	Yes
browsealias	Defines whether netnames or aliases are displayed when using the Browse option in a Windows environment	Yes, No	Yes
timesync	Specifies if the time on the local machine should be synchronized with the time at the domain controller at logon	Yes, No	Yes
biglie	Determines whether to lie about drives > 2 GB	Yes, No	Yes
rawread	Turns on/off SMB readblock raw at the DLS requester	Yes, No	Yes
lazyclose	Determines whether to pend closing of files	Yes, No	Yes
securelogon	Turns on/off if local logons will fail if a domain logon fails	Yes, No	No
clisync	Turns on/off if the GUI will synchronize the domain name, user name, and so on, each time a call is made from a Windows DOS session	Yes, No	No
mailslots	Use mailslots	Yes, No	Yes
numdgrambuf	Number of datagram buffers	0 to 16	3
sbinterval	Interval of time between sideband timeouts	0 to 65535	120

Parameter	Description	Valid Values	Default Value
sbtimeout	Time before timing out a sideband request	0 to 65535	3
sbcount	Count before disabling sideband	0 to 65535	5
tempdisk	Temporarily sets the drive letter that NET USE uses to run PROFILE.BAT	Z	First available drive letter
logfile	The name of the file where received messages are logged	Alphanumeric characters. See the DOS user guide for valid characters when creating filenames	MESSAGES
sizemesbuf	Indicates the size of message buffers to use, in KB	512 to 4096	512
nummsgnames	Indicates the number of message names to be added to the workstation	2 to 8	2
msgtimeout	Indicates the length of time, in seconds, a message is displayed if Esc is not pressed. If the value is -1, the message is displayed until Esc is pressed	-1 to 1800	60
A20Monitor	Saves the state of the A20 line during task switching. Some memory managers fail when set to 1. If you experience hangs and are using a memory manager this value should be set to 0	0 or 1	1
NumRdrs	Indicates the workstations that can connect to you at one time (only valid on the peer stand alone product; set value to 1 on LAN/Warp Server product)	3 to 251	10
NumShares	Indicates the number of resources you can share	2 to 256	10
NumReqs	Indicates the number of request buffers the Peer uses when it starts	3 to 6	3

Table 10 (Page 4 of 6). NETWORK.INI Parameter Values

Table 10 (Page 5 of 6). NETWORK.INI Parameter Values			
Parameter	**Description**	**Valid Values**	**Default Value**
`XmitSize`	Indicates the size (bytes) of transmit buffers the Peer will use when transferring data	512 to 32768	2048
`TaskTimeSlice`	Indicates the amount of time (ticks) the foreground/background will each run. The default is 5 for foreground and 4 for background (54). Value Ticks 0 2 1 4 2 6 3 10 4 14 5 22 6 30 7 42 8 56 9 72	00 to 99	54
`OpenMode`	Indicates the mode file will be opened when an open request is received. • 0 = Use Open mode application requested. • 1 = DENY_NONE sharing mode if read-only access to .exe or .com files. COMPATIBILITY-mode for .bat files or write access to .exe or .com files. • 2 = DENY_NONE sharing mode if read-only access to .exe or .com files. DENY_WRITE sharing mode if read-only access to .bat files. COMPATIBILITY-mode if write access to .exe, .com, or .bat files. • 3 = DENY_NONE sharing mode on all compatibility mode opens.	0 to 3	3

Table 10 (Page 6 of 6). NETWORK.INI Parameter Values			
Parameter	**Description**	**Valid Values**	**Default Value**
`FileShareSize`	Specifies number of bytes allocated for the DOS storage area used to record file-sharing information. If SHARE.EXE is started before the Peer, the values that specified when SHARE.EXE is started are used.	512 to 32768	2048
`Share Locks`	Defines the maximum number of active locked ranges in files that you can share with the peer. If SHARE.EXE is started before the Peer, the values specified when SHARE.EXE is started are used.	20 to 1000	20.

Notes:

1. This parameter must be manually added to the NETWORK.INI file to change the default. The installation program does not add this parameter to the NETWORK.INI file.

2. This parameter is overridden by `autocache=yes`.

3. Browsing for aliases is valid only on Warp Server domains. If this parameter is set to Yes, aliases are browsed. If no aliases exist on the domain, netnames are browsed automatically. If this parameter is set to No, browsing for aliases is not attempted.

4. Logon assignments are reestablished when you log on to their domains. Additional connections made to shared directories or printers (known as persistent connections) are also reestablished, providing that you log on at the same workstation.

5. If this parameter is not specified, DOS LAN Services synchronizes the time on the local machine with the time at the domain controller at logon. The length of time that it takes to log on will be reduced if `timesync=no` is added to the `[network]` section of NETWORK.INI; however, the time at the local machine will not be synchronized with the domain controller.

6. Parameters for Virtual Redirector which must be in [NETWORK] section of the SYSTEM.INI file.

11.5.2.1 DOS LAN Services Performance Tuning

The default installation parameter values have been selected to provide the optimum performance/memory utilization ratio. The DOS LAN Services `autocache` parameter, when set to `yes`, automatically allocates the values of `numbigbuf`, `sizbigbuf` and `extraheap` based on the amount of XMS memory available. However, if a performance problem is identified, set `autocache` to `no` and manually adjust the values of the following parameters:

- **Work Buffers** are used to construct SMBs prior to their delivery to the server. The `sizworkbuf` parameter specifies the size of work buffers; however, this value rarely needs to be changed because small data

read requests are processed through the cache provided with big buffers.

- **Big Buffers** are used, as with previous versions of requesters, to process large file transfers. However, with DOS LAN Services, they are now also used for file caching which provides an obvious performance advantage.

11.5.3 PROTOCOL.INI Parameters

The following table provides details of the parameters in the [NetBEUI] section of DLS's PROTOCOL.INI.

Table 11 (Page 1 of 2). PROTOCOL.INI Parameter Values				
Keyword	**Type**	**Min**	**Max**	**Default**
NCBS	INT	1	255	12
PIGGYBACKACK	INT	0	1	1
BINDINGS	STRING	0	0	0
DRIVERNAME	STRING	0	0	0
ALWAYS_LOAD	STRING	0	0	0
SESSIONS	INT	1	254	6
NAMECACHE	INT	0	255	0
NAMES	INT	1	254	17
PACKETS	INT	1	1000	50
LOOPPACKETS	INT	0	1000	1
DATAGRAMPACKETS	INT	2	1000	2
TI	INT	0	65535	30000
T1	INT	1	65535	500
T2	INT	1	65535	200
ADAPTRATE	INT	0	65535	1000
WINDOWSERRORS	INT	0	10	1
NETBIOSTIMEOUT	INT	0	10000	500
STACKSIZE	INT	512	4096	2048
NETBIOSRETRIES	INT	1	50	2
DLCRETRIES	INT	1	65535	5
MAXIN	INT	1	127	1
MAXOUT	INT	1	127	1
PIPELINE	INT	1	200	20
MAXTRANSMITS	INT	1	10000	5
MINTRANSMIT	INT	0	9999	2

Table 11 (Page 2 of 2). PROTOCOL.INI Parameter Values				
Keyword	**Type**	**Min**	**Max**	**Default**
LANABASE	INT	0	255	1
SIDEBAND	INT	0	1	1
NETFLAGS	INT	0	0FFFFh	0
MAXDATARCV	INT	512	16384	4168
4168				
CHAINX5C	INT	0	1	1
ETHERAND_TYPE	CHAR	—	—	"I"
DOSTRACEMASK	INT	0	0FFFFh	0
Note:				

1. Possible Values are:
 	
    "I" - IEEE 802.2
    "D" - DIX				

11.6 TCP/IP and TCPBEUI Options in DOS LAN Services

There are many options in DOS LAN Services' TCP/IP and TCPBEUI. The following illustrates how to set up a DOS LAN Services client to participate in a dynamic TCP/IP environment.

11.6.1 Setting Up DHCP Support

To have DOS LAN Services clients participate in a dynamic TCP/IP environment, install one of the TCPBEUI redirectors as described in 11.3, "Installing DOS LAN Services" on page 219.

  1. Change the default protocol driver from IBM NetBEUI to TCPBEUI, scroll up to Protocol Driver, press **Enter**, then scroll up to Change driver for protocol and press **Enter** again. The Protocol list window is displayed.

  2. At the Prococol list window, as shown in Figure 126 on page 244, select the TCPBEUI option of your choice.

```
Install for DOS LAN Services


        Please select the protocol used on your network.

        ------------------------------------------------------
        | Other protocol.                                     |
        | Install 802.2 support.                              |
        | TCPBEUI (Real-Mode)                                 |
        | TCPBEUI (Real-Mode) & IBM NetBEUI                   |
        | TCPBEUI (Windows-Protect-Mode)                      |
        | TCPBEUI (Windows-Protect-Mode) & IBM NetBEUI        |
        | IBM NetBEUI                                         |
        ------------------------------------------------------

```

Figure 126. DOS LAN Services Protocol List Window

3. For example, scroll to TCPBEUI (Real-Mode) and press **Enter**.

4. At the following windows scroll up to Edit settings for protocol driver and press **Enter**. The settings for your protocol driver window is displayed as shown in Figure 127.

```
Install for DOS LAN Services


        The settings for your protocol driver are listed below. If
        all the settings are correct, select "The listed options
        are correct'. Then press Enter. If you want to change a
        setting, use the Up Arrow or Down Arrow key to select it.
        The press Enter to see alternatives for that setting.

        Protocol Driver : TCPBEUI (Real-Mode)
        ------------------------------------------------------
        | ARP Cache TimeOut in seconds=300                    |
        | DHCP Client ID=                                     |
        | Virtual Circuits=16                                 |
        | VC Receive Buffers=6                                |
        | VC Send Buffers=6                                   |
        | Receive Window in Bytes=2920                        |
        | Send Window in Buffer=8                             |
        | Use Memory Option=UMB                               |
        |                                                     |
        |The listed options are correct                       |
        ------------------------------------------------------

```

Figure 127. TCPBEUI Settings Part 1

5. Other options like BootP support appear when you scroll up the window. The following options are displayed, as shown in Figure 128 on page 245.

```
       ----------------------------------------------------------
      | Drivername=ntsts$                                      |
      | Select for Token-Ring Media=Token-Ring                  |
      | Bootp=Never                                            |
      | IP Address=                                            |
      | Subnet Mask=                                           |
      | Gateway IP Address=                                    |
      | Domain Name Server IP Address=                          |
      | Domain Name=                                           |
      | Broadcast Address=Host-1s                              |
      | TCP Heart Beats=Standard                               |
       ----------------------------------------------------------
```

Figure 128. TCPBEUI Settings Part 2

6. For dynamic TCP/IP, scroll the bar up to Bootp and press **Enter**. There are four setting options:

   Never

   Attempt

   Always

   DHCP

   Select **DHCP**

   Note: If you previously filled out TCP/IP configuration, such as local IP address, gateway IP address, and so on, delete this information in order for the client to retrieve an IP address from a DHCP server.

7. If your DHCP server was set up to support classes and there is a class for, DLS, for instance, you need to type DLS in the option for `DHCPClientID=DLS.`

8. When all settings are made, select **The listed options are correct** until the installation process of DOS LAN Services is finished.

DLS and DDNS Support

DOS LAN Services client does not support communication with a Dynamic DNS (DDNS) server to update the user's host name with the retrieved IP address from the DHCP server. Therefore, configure your DCHP server to provide the user's host name with the new IP address.

11.6.2 DLS and NetBIOS Name Server

To have DLS clients to communicate with a NetBIOS Name Server such as
Shadow from NTS (see 5.1, "The Shadow NetBIOS Name Server" on
page 47) rather than using the DLS's NBUTIL utility to map NetBIOS names
to IP addresses, provide additional statements to the [NTS$NTSTS] section of
the PROTOCOL.INI file.

Note: These statements cannot be added and configured through the DLS
installation program.

```
NODETYPE=H-Node
NBNSAddr=[9.3.1.81]
NBDGAddr=[9.3.1.81]
```

assuming that 9.3.1.81 is the IP address of the NetBIOS Name Server.

Figure 129 displays a PROTOCOL.INI file with included statements to
support communications with a NetBIOS Name Server (NBNS).

```
[network.setup]
version=0x3100
netcard=ibm$genibmtok,1,IBM$GENIBMTOK
transport=nts$ntsts,NTS$NTSTS
lana0=ibm$genibmtok,1,nts$ntsts
```

Figure 129 (Part 1 of 2). DLS-PROTOCOL.INI with NetBIOS Name Server Support

```
[NTS$NTSTS]
BootPFlag=Never
DNSAddr=[9.3.1.74]
GatewayAddr=[9.3.1.74]
NetSubNetMask=[255.255.255.0]
IPAddr=[9.3.1.83]
NodeType=H-Node
NBNSAddr=[9.3.1.81]
NBDGAddr=[9.3.1.81]
Token-Ring
DriverName=ntsts$
VCs=16
VCReceiveLarge=6
VCSends=6
RcvWindow=2920
UseMemory=UMB
BINDINGS=IBM$GENIBMTOK
LANABASE=0

[protman]
DriverName=PROTMAN$
PRIORITY=nts$ntsts

[IBM$GENIBMTOK]
DriverName=IBMTOK$
```

Figure 129 (Part 2 of 2). DLS-PROTOCOL.INI with NetBIOS Name Server Support

Chapter 12. IBM Networks Client for Windows 95

This chapter describes installing and configuring IBM Networks Client for Windows 95 in a plain NetBEUI and TCP/IP environment, dynamic TCP/IP:

- Dynamic Host Configuration Protocol (DHCP)
- Dynamic Domain Name Server (DDNS)
- NetBIOS Names Server (NBNS) / Windows Internet Name Server (WINS)

and Remote Access Services using the Point-to-Point (PPP) protocol dialing into an OS/2 Warp Server Remote Connection Server.

12.1 Hardware Requirements for IBM Networks Client for Windows 95

The same hardware requirements apply to IBM Networks Client for Windows 95 installation as are required for Windows 95 installation with network support:

- IBM PC or compatible computer
- 386DX processor or higher
- 8 MB memory or more
- Windows 95-compatible network adapter

12.2 Software Requirements

The following software components must be installed and configured prior to installing and runing IBM Networks Client for Windows 95:

- The Client for Microsoft Networks
- An appropriate network adapter device driver
- A supported protocol (NetBEUI or TCP/IP)

TCP/IP or NetBIOS over TCP/IP?

The actual protocols used are NetBEUI or NetBIOS over TCP/IP, but the NetBIOS over TCP/IP protocol is transparent in Windows 95 and is referred to TCP/IP only.

The NetBIOS over TCP/IP is not transparent in the new OSR-2 (OEM Service Release 2) version of Windows 95. For more information, see 12.9, "The OEM Service Release 2 of Windows 95" on page 316.

Other network client support drivers are not required to install or run IBM Networks Client for Windows 95. If a network adapter was detected during the Windows 95 installation, client support for NetWare Networks and protocol support for IPX/SPX-compatible protocol are automatically added to the network configuration. However neither of these are required unless you want to attach to NetWare-based networks. Some applications may need IPX/SPX-compatible protocol to function over the network. For example, many network games like Doom II support only the IPX/SPX protocol.

If you have problems getting Windows 95 networking to function, go through the following check list:

- Is the appropriate network adapter device driver installed?
- Is the network operational?
- Is the network adapter functioning correctly?
- Is the Client for Microsoft Networks installed correctly?
- Is the NetBEUI or TCP/IP protocol installed properly?

For more information, refer to the *Microsoft Windows 95 Users Guide* or see 12.7, "Windows 95 Networking" on page 269.

12.3 Installing IBM Networks Client for Windows 95

This chapter details IBM Networks Client for Windows 95 installation. We discuss installing IBM Networks Client for Windows 95 with a floppy drive and a shared network drive.

12.3.1 IBM Networks Client for Windows 95 Installation Using a Floppy Disk

The following illustrates installing IBM Networks Client for Windows 95 with diskettes. If you plan to install IBM Networks Client for Windows 95 over the network, you may skip this section and proceed with 12.3.2, "IBM Networks Client for Windows 95 Installation from IBM OS/2 Warp Server" on page 259. To begin the installation, perform the following steps:

1. Click on the **Start menu** and select [**Settings** — **Control Panel**] as shown in Figure 130 on page 251.
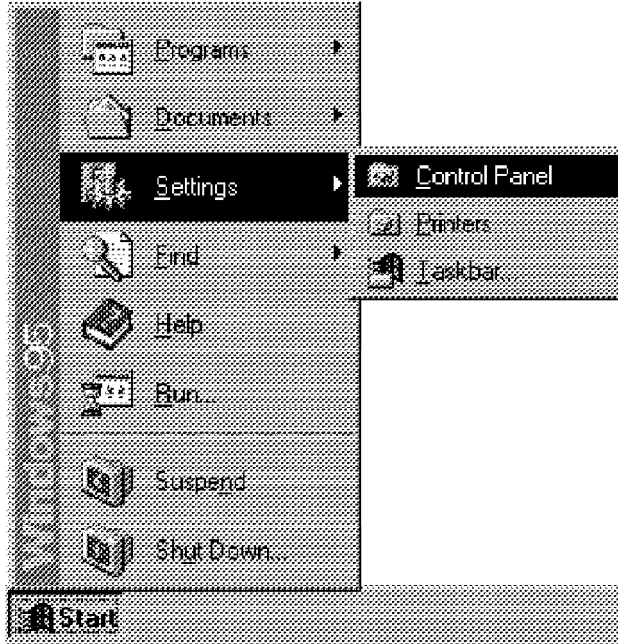
Figure 130. Use the Start Menu to Open the Control Panel

2. In the Control Panel folder, double-click on the **Network** icon as shown in Figure 131 on page 252.

Figure 131. Double-Click on the Network Icon in the Control Panel

3. The Network notebook is displayed as showed in Figure 132 on page 253). Select the **Configuration** tab.
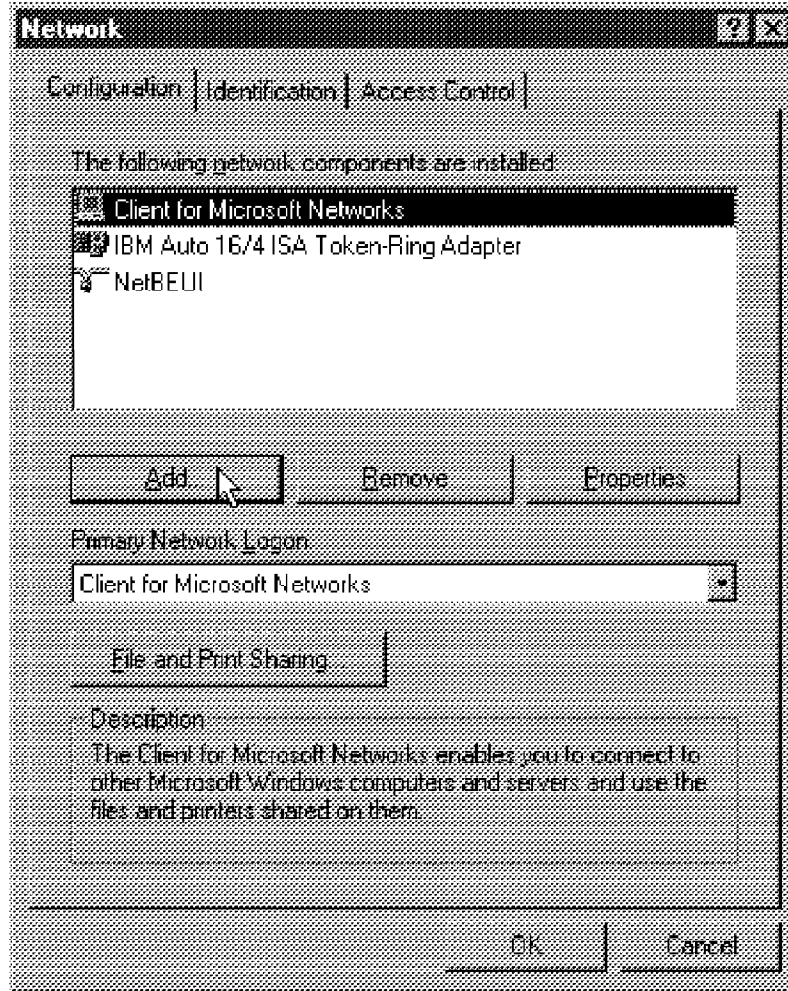
Figure 132. Use the Network Notebook to Install and Configure the Network

IBM Networks Client for Windows 95 requires the Client for Microsoft
Networks being installed and configured properly. If Windows 95 detects
a network adapter during the Windows 95 installation, the Client for
Microsoft Networks is already present in the list of installed components.
If Client for Microsoft Networks is not present, you must install it as
decribed in the *Microsoft Windows 95 Users Guide*.

Tip

Consider removing the IPX/SPX protocol. The Client for NetWare
Networks and IPX/SPX-compatible protocol are not needed to run
IBM Networks Client for Windows 95. Before removing these
components, make sure you are not using applications that need
IPX/SPX protocol to communicate over the network, such as Doom II.

In this example NetBEUI is the used protocol. If you want to install and configure IBM Networks Client for Windows 95 with TCP/IP, see 12.7.10, "Installing TCP/IP for Windows 95" on page 298 for more information.

4. To install IBM Networks Client for Windows 95, click the **Add...** button and the Select Network Component Type window is displayed (Figure 133). Select the network component type to be the **Client** and click the **Add...** button.
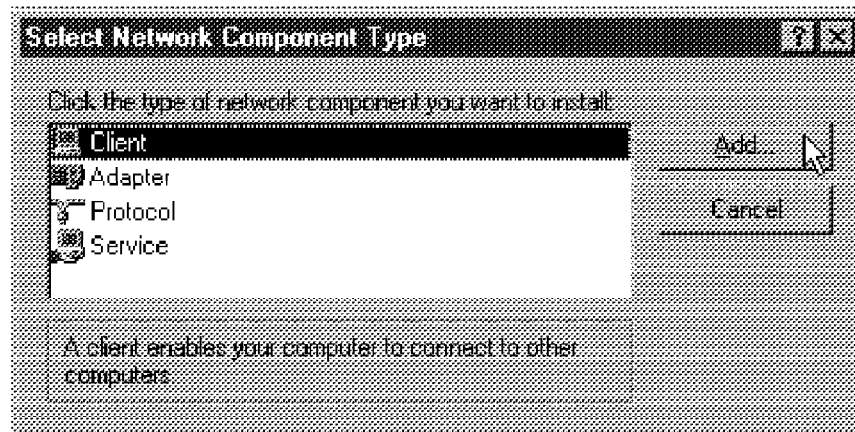
Figure 133. Select Network Component Type Window

5. When the Select Network Client window is displayed (Figure 134 on page 255), click the **Have Disk...** button.
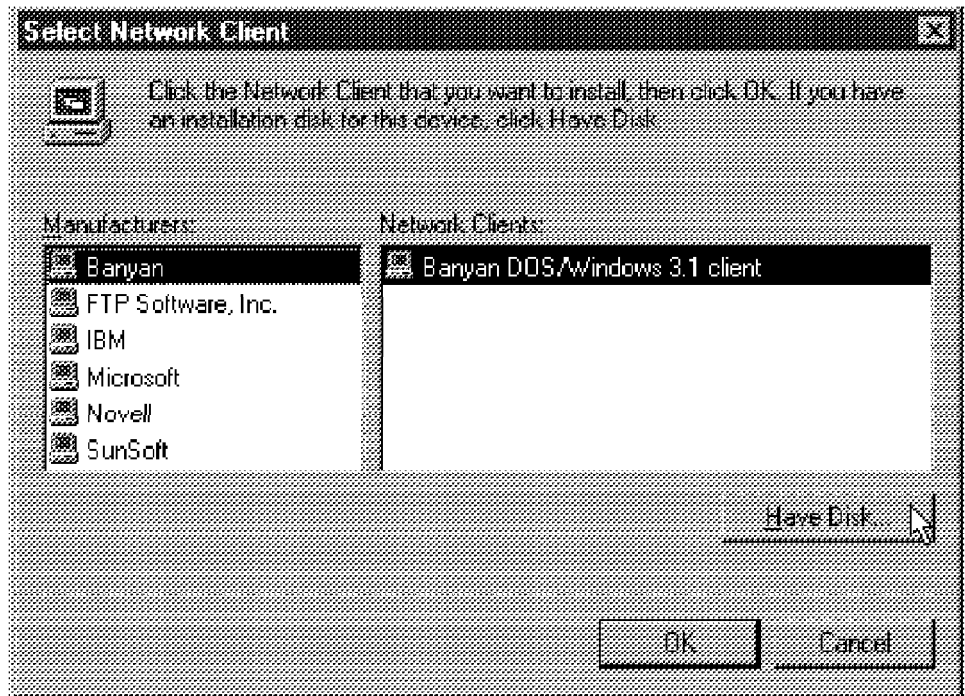
Figure 134. Select Have Disk... to Install IBM Networks Client for Windows 95

6. In the Install From Disk window, set the source files path to be **A:** ,
   insert the IBM Networks Client for Windows 95 diskette into the A: drive
   and select **OK** (Figure 135).
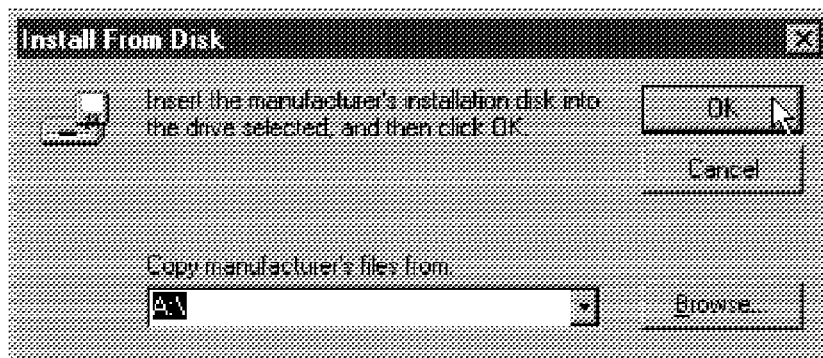
Figure 135. Enter the Source Files Path

7. From the Select Network Client window, select **IBM Networks Client for
   Windows 95** and click **OK** (see Figure 136 on page 256). The system
   may prompt you to insert a Windows 95 disk depending on the
   installation method used. If prompted, insert your Windows 95 disk or
   enter the correct path for the Windows 95 installation files and press **OK**
   to continue.
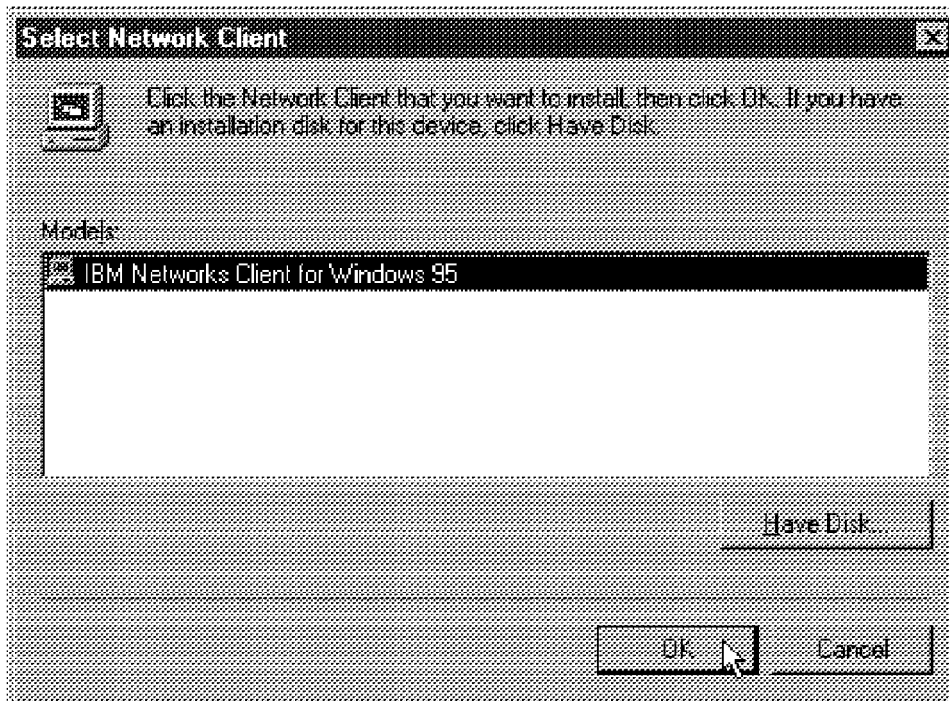
Figure 136. Select IBM Networks Client for Windows 95

8. After all files are copied, the Network notebook is displayed (see Figure 137 on page 257) and IBM Networks Client for Windows 95 is added to the installed network components list. To set the primary network logon, use the **Primary Network Logon** drop-down list to select **IBM Networks Client for Windows 95**.
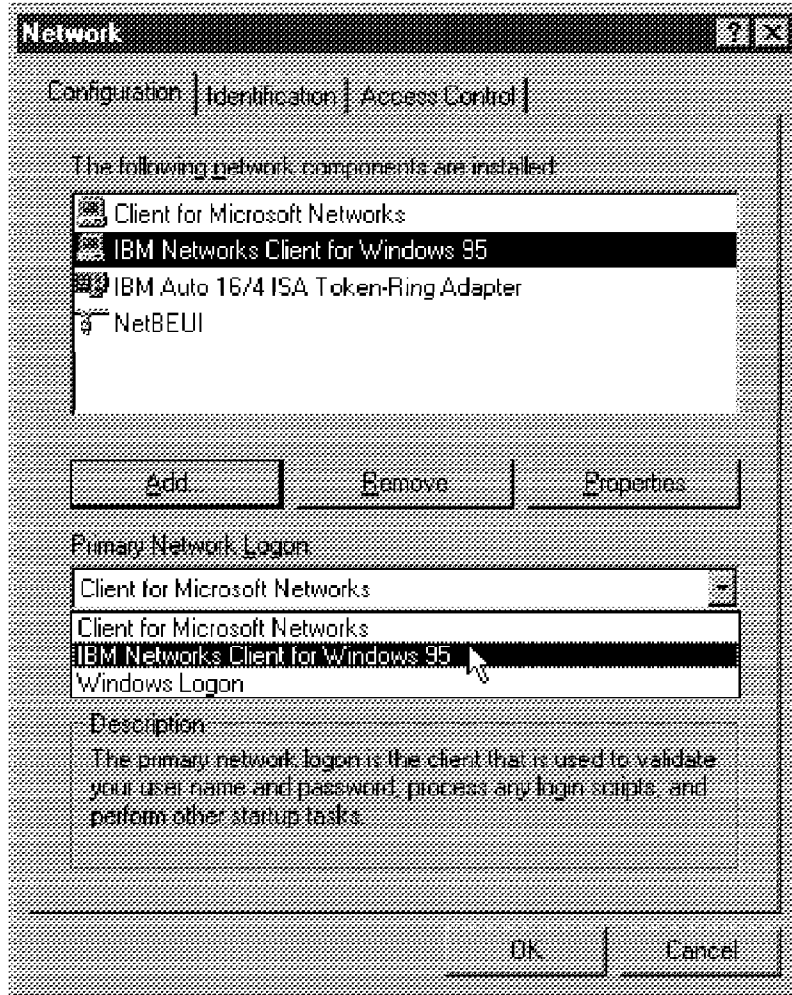
Figure 137. Select IBM Networks Client for Windows 95 as the Primary Network Client

9. Select **IBM Networks Client for Windows 95** from the Following network components are installed list and click the **Properties** button. Define the OS/2 Warp Server domain name to be logged on in the Domain name edit box (Figure 138 on page 258). You need to have a valid user account and password in this domain to log on the domain. If you do not have a user account, contact your OS/2 Warp Server administrator.
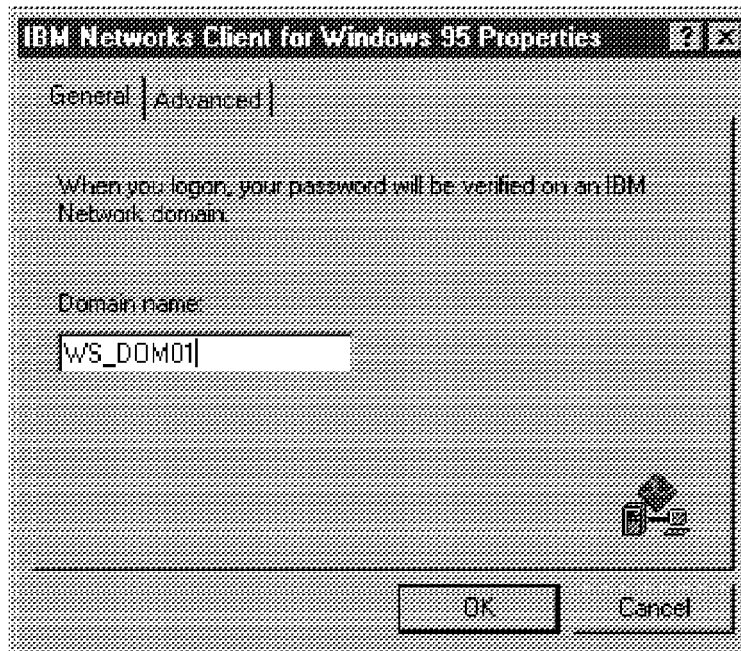
Figure 138. Define the OS/2 Warp Server as the Default Logon Domain

> ┌─ **Note** ───┐
>
> You can log on to only one domain at a time. OS/2 Warp Server
> supports cross-domain resources, so it is possible to get file and
> printer resources transparently from more than one domain. You
> can find more information about creating cross-domain resources in
> the redbook SG24-4786, titled *OS/2 Warp Server, Windows NT and
> NetWare: A Network Operating System Study*.
>
> └──┘

10. IBM Networks Client for Windows 95 supports Windows 95 system
    policies. Select the **Advanced** tab to define how the system policy
    download is done. The system policies can be downloaded from the
    Netlogon share on the domain controller, or you can define an optional
    network path in the Specify System Policy path and filename edit field
    (Figure 139 on page 259). If system policies are not used in your
    environment, unselect the **Enabled automatic System Policy download**
    check box. For more information, see 12.7.7, "Windows 95 System
    Policies" on page 292.
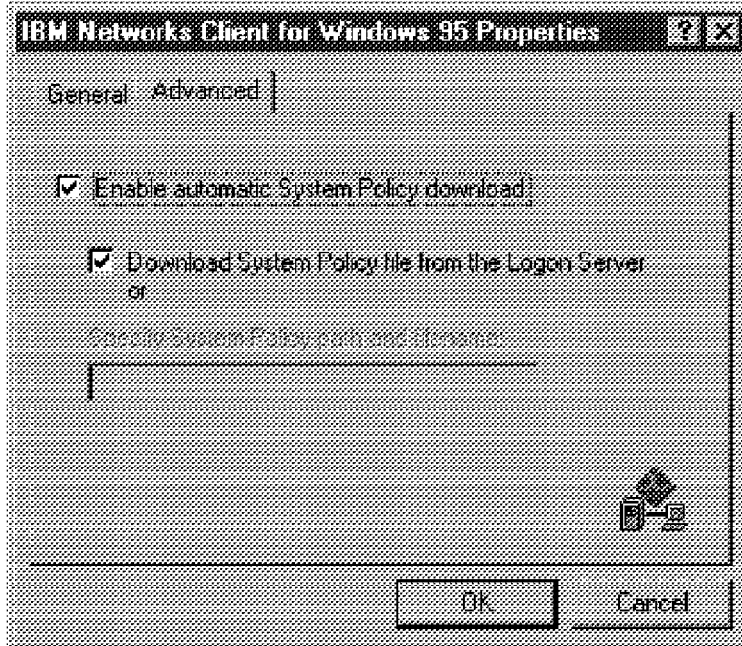
Figure 139. Automatic System Policy Download Can Be Disabled

11. Select **OK** to close the properties window. Select the **OK** button in the
    Network notebook to accept the changes. Select **Yes** to reboot the
    machine. The new settings are not effective until the system is
    rebooted.

12.3.2 IBM Networks Client for Windows 95 Installation from IBM OS/2 Warp Server

The following illustrates installing IBM Networks Client for Windows 95 over
the network. If you installed IBM Networks Client for Windows 95 in the
previous step, you may skip this section and proceed with 12.5, "Logging on
to an OS/2 Warp Server Domain" on page 264.

IBM Networks Client for Windows 95 can be installed from a shared network
resource. Installation from the network requires that Microsoft Windows 95
network support is installed and functional.

Directory Share

The directory share where the IBM Networks Client for Windows 95 code
is copied must point to the root directory. If you copy all the files from
the diskette to a subdirectory of the directory share, the installation will
fail.

The following example shows how to create a network share and install the products using that share. Assuming the directory share is to be created on the server's D: drive, perform the following operations on your OS/2 Warp Server system to create the directory share:

1. Create a directory named D: IBMWIN95.

   MD D: IBMWIN95

2. Copy all the files from the IBM Networks Client for Windows 95 diskette into the D: IBMWIN95 directory.

   COPY A:*.* D: IBMWIN95

3. Create a shared resource by typing:

   NET SHARE IBMWIN95=D: IBMWIN95

4. Create an Access Control List (ACL) to the resource by typing:

   NET ACCESS D: IBMWIN95 /ADD GUESTS:RX USERS:RX

When the directory share is ready, go to your Windows 95 system and perform the following steps:

1. Follow the steps 1 through 5 listed in section 12.3.1, "IBM Networks Client for Windows 95 Installation Using a Floppy Disk" on page 250.

2. In the Install From Disk window, select **Browse...**.

3. In the Open window, select **Network...** (Figure 140).
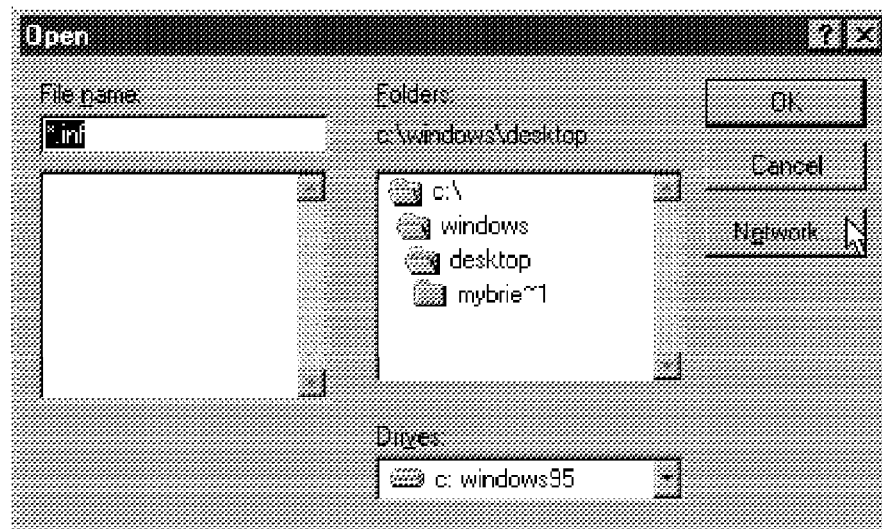
Figure 140. Select Network from the Open Window

4. Select any available drive letter from the Drive list.

Enter the correct UNC (Universal Naming Convention) path in the Path field. The UNC path consists of the server name and the share name. For example:

```
WS_SRV01 IBMWIN95
```

where `WS_SRV01` is your server name, and `IBMWIN95` is the shared resource name created on the OS/2 Warp Server (see Figure 141).

Figure 141. Map the Shared Network Resource to a Logical Drive Letter

5. Unselect the **Reconnect at logon** check box to make the connection one time only.

6. Click **OK** and the Open window is displayed again.

7. From the Drive list, select the drive letter that was mapped to the shared resource (performed in the step 4).

   Verify that IBMNET32.INF is displayed in the File name field and click the **OK** button (Figure 142).
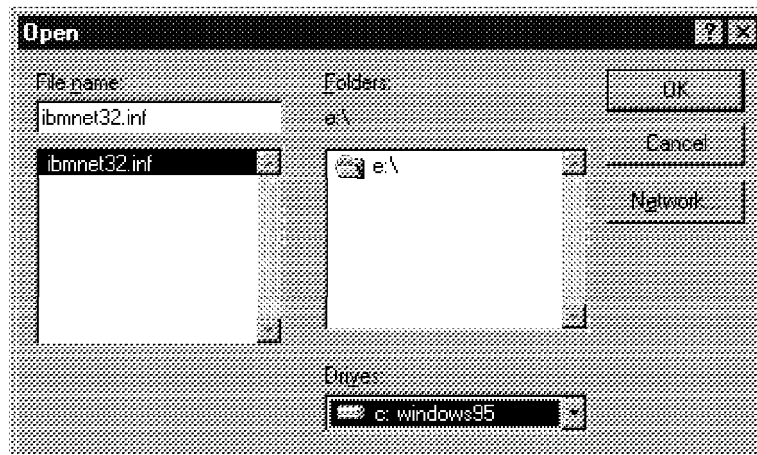
Figure 142. Make the Mapped Network Drive the Source Path

8. The Install From Disk window is displayed. Verify that the mapped network drive drive letter is displayed in the Copy manufacturer's files from field and click **OK**.

9. Continue installation with steps 8 through 12 as described in 12.3.1, "IBM Networks Client for Windows 95 Installation Using a Floppy Disk" on page 250.

12.4 IBM Networks Client for Windows 95 Uninstall

IBM Networks Client for Windows 95 is uninstalled in the following way:

1. Open [**Start** — **Settings** — **Control Panel**].

2. Double-click on the **Network** icon.

3. From the Network notebook, select **IBM Networks Client for Windows 95** and click-on the **Remove** button (Figure 143 on page 263).
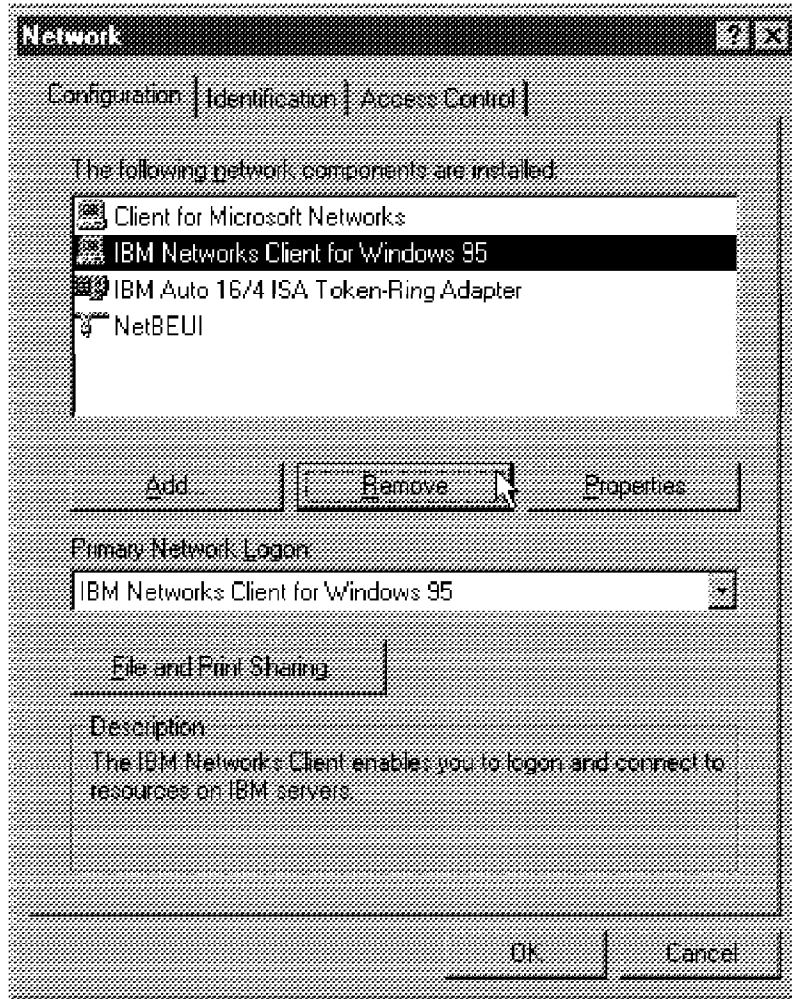
Figure 143. Select the Component to Remove and Click the Remove Button

4. Select **Yes** in the System Settings Change window to reboot the system
   (Figure 144).
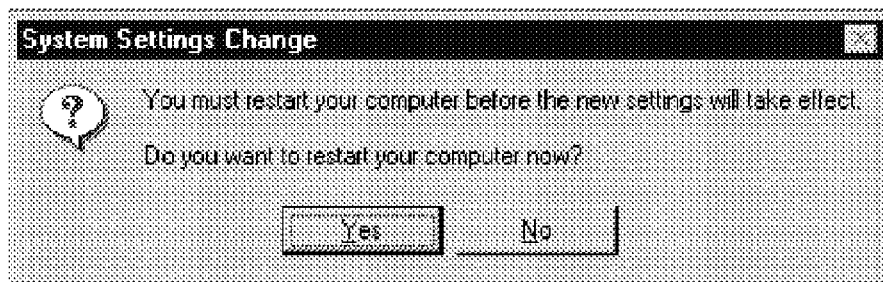
Figure 144. You are Prompted to Reboot the System

12.5 Logging on to an OS/2 Warp Server Domain

When you installed and configured Windows 95 networking and the IBM Networks Client for Windows 95, you can log on the OS/2 Warp Server domain and use its resources. When you restart the machine, the logon window is different from the previous logon window. Instead of the Microsoft networks logon dialog, the IBM Networks Client logon window appears, as shown in Figure 145.
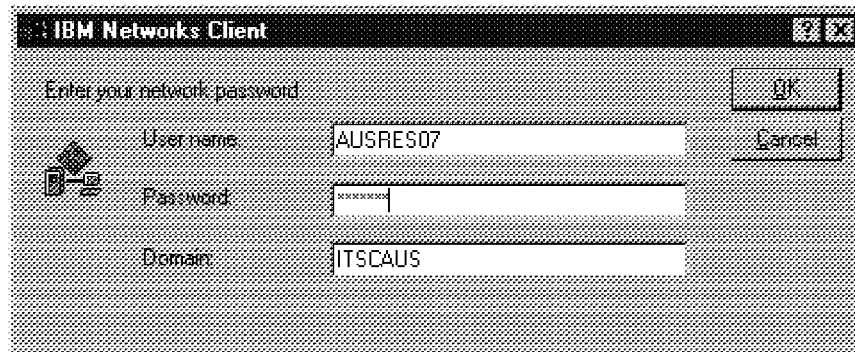
Figure 145. The IBM Networks Client for Windows 95 Logon Window

Enter your user ID and password and enter the OS/2 Warp Server domain you want to logon if the correct domain name is not already displayed. Select the **OK** button to get all your OS/2 Warp Server assigments and resources from your Windows 95 workstation. The OS/2 Warp Server domain logon assigments are read every time directly from the logon server; any changes made to logon assigments are effective after the next network logon.

Quick Logon

If you use OS/2 Warp Server's logon assignments function, consider selecting the radio button for **Quick Logon** at the Client for Microsoft Networks Properties window, as shown in Figure 151 on page 276. Your logon will go faster because the Microsoft code will not try to reconnect to logon assignments that already exist.

IBM Networks Client for Windows 95 also supports profile batch file execution; the PROFILE.BAT file is executed during the logon process if the PROFILE.BAT is defined at the logon server. The last Windows 95 logon name is stored in the Windows 95 registry and is used as a default user name in the next logon, unless the administrator set a registry entry at the local Windows 95 workstation not to display the last logon name. To change the registry, use the registry editor for Windows 95.

When you log on from a Windows 95 workstation the first time, you are prompted to enter the Windows password after the domain logon. Windows 95 creates a local user account and saves the local password. Local user accounts make it possible for every user on the machine to have a customized desktop and Start menu. The user profiles function is not enabled as default, but can be activated at any time later on.

To enable user profiles, select [**Start** — **Control Panel** — **Passwords**] and the Password properties notebook is displayed. Select the **User Profiles** tab and select the policy to be used on the workstation.

Tip

Store your user profiles on the server so the user will have the same desktop on any Windows 95 workstation from which they log on. This feature is called Roaming User.

Before you define the Windows password, you must provide the domain password and Windows 95 password. If the two passwords are the same, Windows 95 does not display the Windows 95 logon dialog. If the passwords do not match, you are prompted to enter a Windows 95 password.

If you do not want to use the local password function, you can set the local password to be a null string. In this case Windows 95 does not prompt for the local logon at all.

If you mainly use OS/2 Warp Server domain resources but want to use resources from a Windows NT domain as well, use a Windows password. When you enter your Windows password, Windows 95 creates a password list file for your user account in the Windows directory. For example, if your user account is the same in OS/2 Warp Server domain and Windows NT domain but the passwords are not synchronized, every time you connect to a Windows NT resource you are prompted for the password. If you enter the local Windows password, all the other passwords are cached, so provide them only once.

The local Windows password may raise some problems as well. If you change your domain password, the domain password and local password are no longer synchronized. To complete the logon procedure, you must enter the local password and the domain password.

Password Caching Not Recommended

If you use the password caching function you have a time bomb waiting to explode. Any code other than the original code of Windows 95 (when it was rolled-out in August 1995) has a new encryption algorithm that OS/2 Warp Server cannot read.

The password list file is found in the Windows directory with the same name as the used user account, and with the extension *.PWL. If your local and domain passwords are unsynchronized, delete the .PWL file that carries your user ID and remove the corresponding entry in the SYSTEM.INI file from the [Password Lists] section. The following is a sample section from the SYSTEM.INI file:

```
[Password Lists]
GUEST C:\WINDOWS\GUEST.PWL
ANNE C:\WINDOWS\ANNE.PWL
AUSRES07 C:\WINDOWS\AUSRES07.PWL
TESTW95 C:\WINDOWS\TESTW95.PWL
```

for example, if you want to create a new password list file for user TESTW95, delete the file C: WINDOWS TESTW95.PWL, remove the line TESTW95=C: WINDOWS TESTW95.PWL from the SYSTEM.INI [Password Lists] section and complete the logon procedure again. You are prompted for the domain password (these operations do not affect the domain password in any manner), the local password and any other passwords you need to get your resources.

12.5.1 How to Change Passwords

To change your password, follow the steps below:

1. Select [**Start** — **Control Panel** — **Passwords**]. The Password properties notebook is displayed.

2. Select **Change Windows Password** and make sure that both IBM Networks Client and Microsoft Networking are checked. This keeps the local and network password synchronized.

Note: If you use the IBM Networks Client GUI to change passwords, only the IBM domain password is changed. This immediately causes the password to be out of sync with the workstation password and you may be unable to connect to some resources. Resynchronizing the passwords is as easy as following the steps above. However, in step 2, select only those passwords that have not been updated.

12.6 Installing a Network Printer in Windows 95

Although you get all the logon assigments and resource definitions from an OS/2 Warp Server domain, you still must manually install the Windows 95 printer driver. At the time of the writing of this redbook, automatic printer driver download from an OS/2 Warp Server is implemented only in OS/2 Warp 4. If the domain administrator has defined LPT ports to be assigned to printer queues, you still get these port assigments, but Windows 95 applications are not able to use them. You have to create a Windows 95 network printer to use a network printer.

Logon and follow the steps below to install a network printer driver:

1. Select [**Start** — **Settings** — **Printers**].

2. Double-click on the **Add Printer** icon.

3. Click the **Next** button to begin the Add Printer Wizard.

4. Provide the printer queue name in the UNC format (`server queue`) or click the **Browse** button amd use the graphical user interface to select the printer queue to be used, as shown in Figure 146. Click the **Next** button to continue.
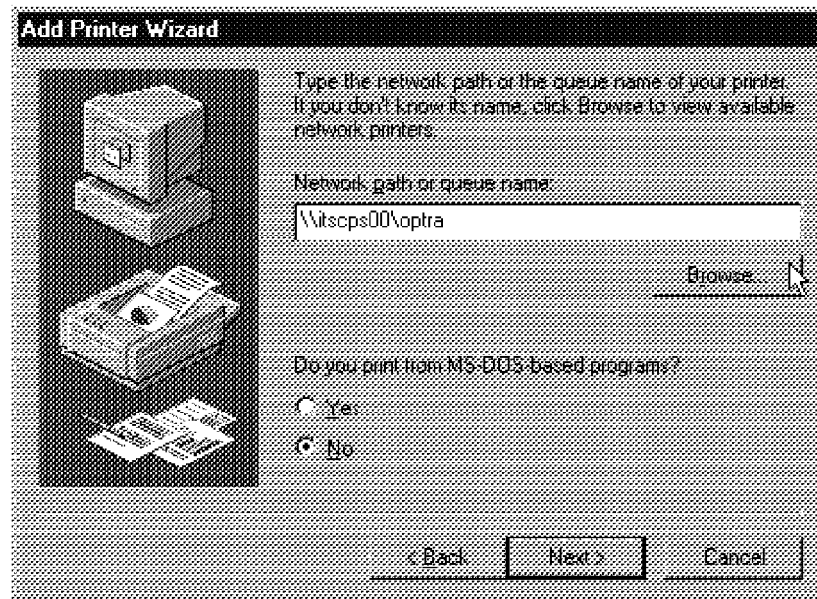
Figure 146. Enter the Print Queue Name

5. Select the appropriate printer driver from the list, as shown in Figure 147 on page 268, or click the **Have Disk** button to install the printer driver from a diskette or from a network share. Click the **Next** button when ready.
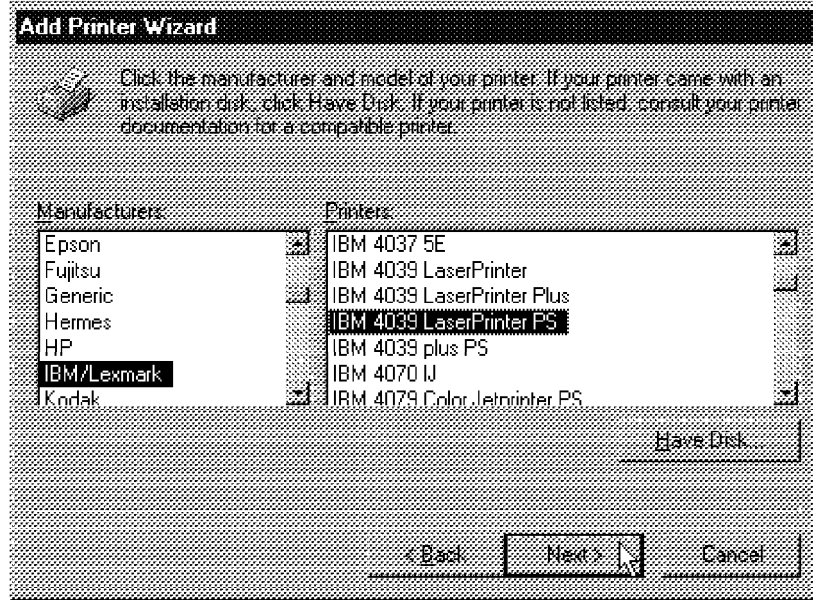
Figure 147. Select the Appropriate Printer Driver

6. Enter the symbolic printer name and select one of the default printer
   radio buttons, as shown in Figure 148. Click the **Next** button to continue.
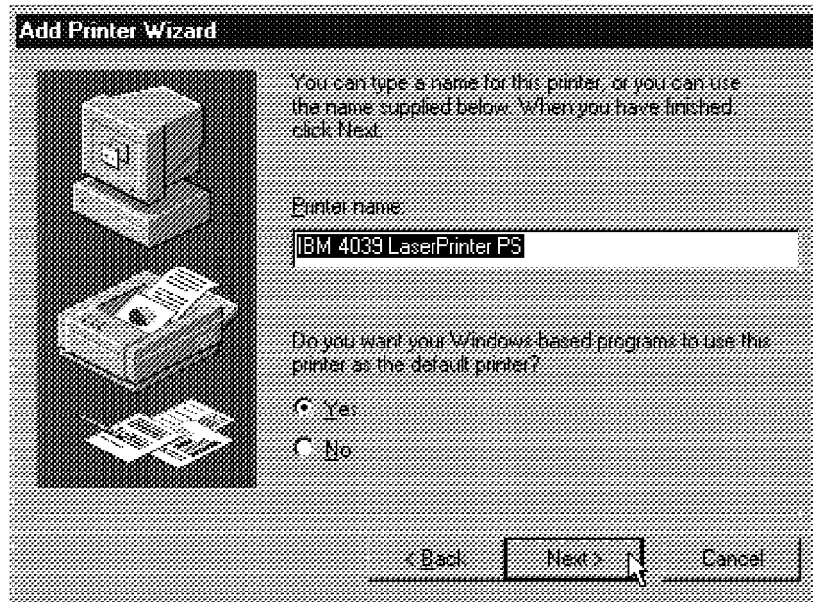
Figure 148. Enter the Printer Name

7. Select the appropriate choice to test or skip the test print-out and click
   the **Finish** button to complete the printer installation.

12.7 Windows 95 Networking

This section provides more information on how to set up Windows 95 networking in different situations. We discuss what computer identification means and how bindings work.

12.7.1 Computer Identification on the Network

Every computer using LAN (Local Area Network) resources has to be uniquely identified on the network no matter if the computer is connected to an OS/2 Warp Server domain, a Windows NT domain or just a member in a workgroup. Computer names are used to address data between computers on the network and therefore duplicate names are not allowed.

When the networking portion of the operating system is started, the computer tries to register its name on the network. If the computer is a primary domain controller on the network, the server tries to register both the domain name and the server name. A workstation only tries to register its own computer name. If the same computer name already exists on the network, networking support cannot be started.

Registration is based on broadcasting network messages over the network. The workstation that wants to join the network sends a message telling other network clients that it is trying to register its name (see Figure 149 on page 270, item 1). The registering network client sends this message several times within a defined time-out. If that name is already in use, the client that owns the name sends a response message to the network client that is trying to register (see Figure 149 on page 270, item 2).

If Windows 95 detects a duplicate computer name on the network, the error message `Error 38: The computer name you specified is already in use` `the network` is displayed, and the network logon is not completed (see Figure 149 on page 270, item 3).
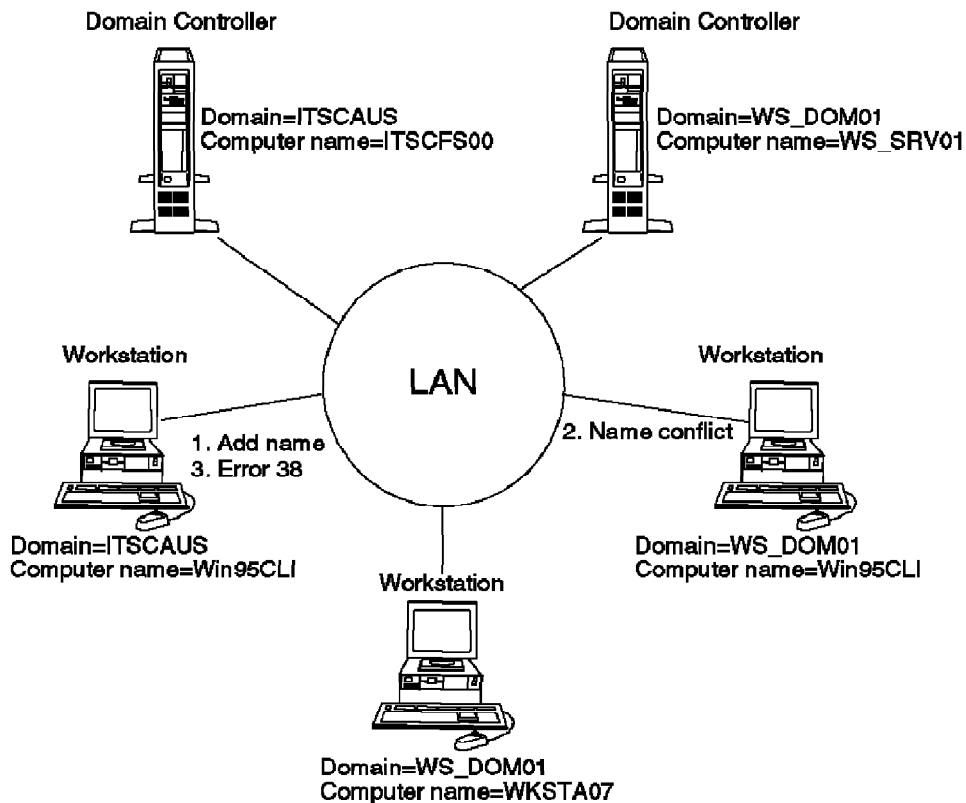
Figure 149. Conflicting Computer Names

A Windows 95 computer name can be up to 15 characters long and can contain numbers or letters and some symbol characters (!, #, $, @, %, &, (,), -, ., ^, _, {, } and ~). The name must not be made up exclusively of periods (.). Though many special characters are allowed, only - (dash) and _ (underscore) are recommended. The computer name is not case sensitive.

The following are examples of legal computer names:

```
Win95Cli01
AUSRES07
COMPUTER015
WS3L117
```

The following computer names, however, are illegal for the reasons specified:

```
COMPUTERTHATISINHALL  (name too long)
WKS=22  (illegal character)
```

`WS_DOM01` (if the domain name is WS_DOM01)
`wksta 12` (spaces are not allowed)

Keep Names 8 Characters or Shorter

If you plan to enforce `MULTILOGON=NO` keep the computer name and the domain name 8 characters or less. See Table 17 on page 297 for more details.

The computer name can be the same as your logon name, but this is not a recommended practice. It is a good idea to make the computer name and the user name different.

The computer name is known as a NetBIOS name in the IBM and Microsoft world. The actual NetBIOS name on the network consists of the user-defined name of up to 15 characters and a one-byte resource type definition. The 16th-byte (one character takes one byte to save) is in the range of [00h]-[FFh] and identifies the NetBIOS name type:

- Domain controller
- Server
- Workstation
- User ID

The User ID can be equal to the workstation name since its 16th-byte values are different. Table 12 illustrates the 16th-byte values and its corresponding NetBIOS name registration.

Table 12 (Page 1 of 2). 16th-Byte Values Used by Microsoft Components		
The Value of the 16th-byte (hex)	**Usage**	**Used By IBM**
<computername>[00h]	Workstation service	Yes
<computername>[03h]	Messenger service	Yes
<computername>[1Fh]	NetDDE service	No
<computername>[20h]	Server service	Yes
<username>[03h]	Messenger Service	Yes
<domain_name>[1Dh]	Master Browser	No
<domain_name>[1Bh]	Domain Master Browser	No

Table 12 (Page 2 of 2). 16th-Byte Values Used by Microsoft Components		
The Value of the 16th-byte (hex)	**Usage**	**Used By IBM**
<domain_name>[00h]	Domain name	Yes
<domain_name>[1Ch]	Domain Controllers	No
<domain_name>[1Eh]	Browser service elections	No
Note: OS/2 Warp Server recognizes and uses this value if the Neighborhood Browser Enabler is installed on the domain controller. For more information about installing and using Neighborhood Browser Enabler, see 8.1, "Introducing IBM Neighborhood Browser Enabler for OS/2 Warp Server" on page 87.		

Application servers use different techniques to register their names on the network. For example, IBM DataBase2 (DB2) allows the user to define a computer name of up to 8 characters. DB2 adds extra identification characters to make the name unique on the network and easier to distinguish as an DB2 server NetBIOS name.

12.7.1.1 Setting the Computer Name in Windows 95

To set the computer name, go to the **Control Panel** and double-click on the **Network** icon. Select the **Identification** tab in the Network notebook and enter the computer name in Computer name field and select **OK** to save the settings. Select **Yes** in the System Settings Change window to reboot the system.

If your workgroup name is the same as your OS/2 Warp Server domain name you can browse your OS/2 Warp Server domain servers and resources in the Network Neighborhood. The Network Neighborhood icon is on the Windows 95 desktop after the network component is set up. To join a workgroup other than your OS/2 Warp Server domain, define the workgroup in the Workgroup field. The restrictions that apply to the workgroup name also apply to the computer name (Figure 150 on page 273).

Note: Windows 95 computer names and all NetBIOS names are converted to uppercase and are not case sensitive.
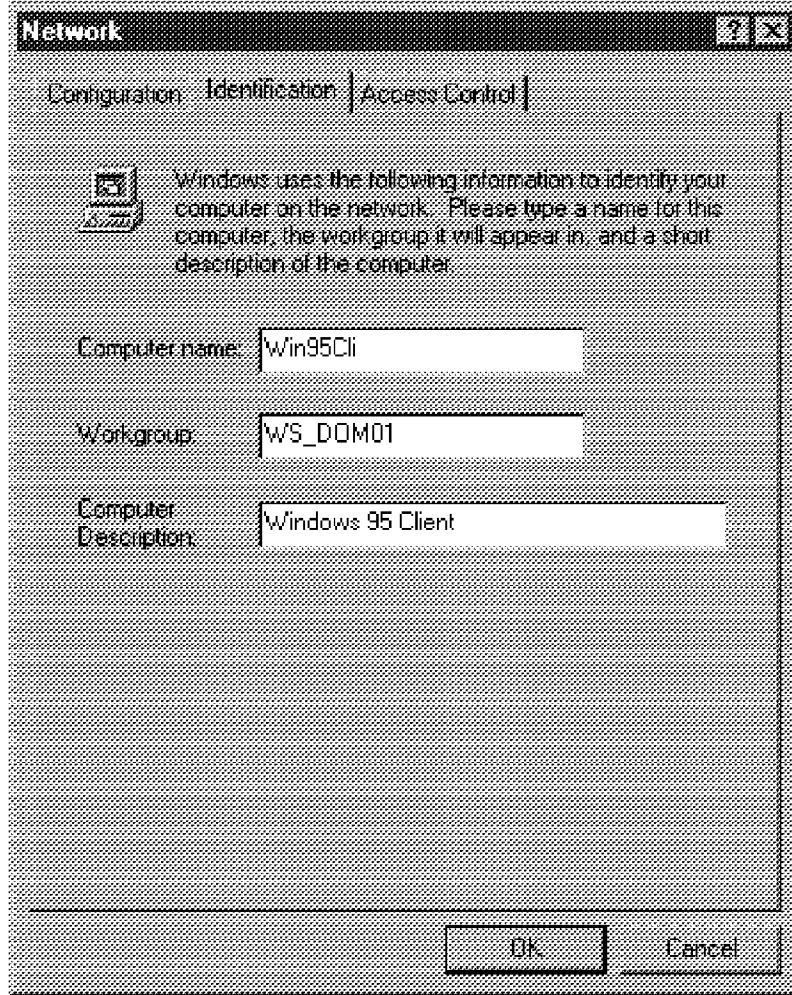
Figure 150. A Computer Name Must Be Defined

We recommend installing the IBM Neighborhood Browser Enabler for OS/2 Warp Server on your primary domain controller. See 8.1, "Introducing IBM Neighborhood Browser Enabler for OS/2 Warp Server" on page 87 for more information about installing and using the product. The Neighborhood Browser Enabler enables your OS/2 Warp Server to be the master browser computer for the domain.

> **Increasing Network Browsing Performance**
>
> To drastically increase the performance of network browsing we recommend installing IBM Neighborhood Browser Enabler for OS/2 Warp Server on your primary domain controller and disabling Windows 95 Master Browser on all Windows 95 clients. Each Windows 95 client with the Master Browser function enabled (see 12.7.1.2, "Setting a Windows 95 Workstation to Be the Master Browser" on page 274) causes an election of the Master Browser when turned on. This causes an enormous amount of network traffic.

12.7.1.2 Setting a Windows 95 Workstation to Be the Master Browser

If you do not use IBM Neighborhood Browser Enabler or do not have any Windows NT workstations in your network, configure at least one Windows 95 workstation to run File and Printer Sharing for Microsoft Networks and enable the Master Browser function to gain Network Neighborhood functionality for other Windows 95 workstations. Activate the Master Browser function the following way:

1. Select [**Start** — **Settings** — **Control Panel** — **Network**].

2. Enable File and Print Sharing by selecting the **File and Print Sharing** button and checking the **I want to be able to give others access to my files** check box.

3. Select **File and printer sharing for Microsoft Networks** service from the list and click the **Properties** button.

4. Set Browse Master value to **Enabled** and LM Announce to **Yes**.

5. Select **OK** for the File and printer sharing for Microsoft Network properties and the Network notebook. Reboot the computer when prompted.

12.7.2 Client for Microsoft Networks

With the Client for Microsoft Networks you can log on to a Windows NT domain. The Client for Microsoft Networks can execute logon scripts and download system policies, but does not automatically connect to your home directory as a Windows NT workstation does. If you have a home directory on a Windows NT server to which you want to connect, either make a permanent connection to the home directory or write a logon script that connects to the home directory.

The following steps illustrates how to make a permanent connection to the home directory. Be sure, however, the home directory is already properly set up at the NT server.

1. Click the right mouse button on the **Network Neighborhood** icon.

2. Select **Map Network Drive** in the pop-up menu.

3. Select a free drive letter for the home directory (for example H:).

4. Enter the UNC (Universal Naming Convention) name in the **Path** field. The UNC name consists of the Windows NT server name and the resource share name, for example, `NT_SRV01 HOME`, where `HOME` points to your home directory defined on the Windows NT server. Alternatively, you can enter `NET USE H: /HOME` in a command line.

5. Make sure that the **Reconnect at logon** choice is selected, to make the connection permanent.

6. Click the **OK** button to make the connection.

Select **Client for Microsoft Networks** from the Network notebook and click on the **Properties** button to configure primary the Windows NT domain. You can leave the Log on to NT domain check box unchecked if your primary logon client is IBM Networks Client for Windows 95. NT domain definition does not have any effect when Client for Microsoft Networks is not the primary logon client. If you log on to a Windows NT domain, check the box and define your Windows NT domain in the Windows NT domain filed (Figure 151 on page 276).
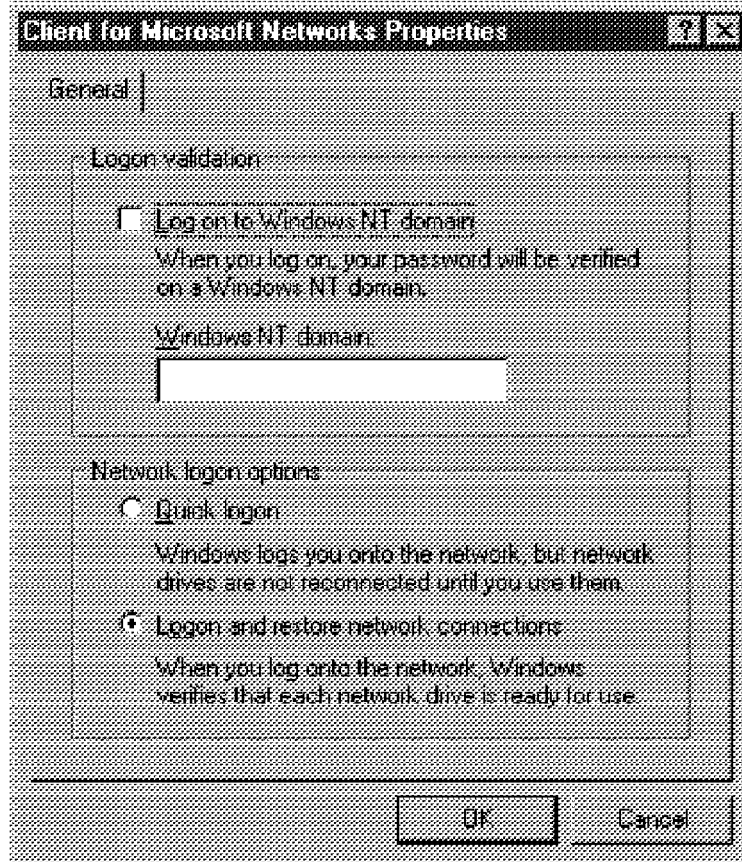
Figure 151. Client for Microsoft Networks Properties Window

The Client for Microsoft Windows Properties notebook has radio buttons to select Network logon options. You can choose the Logon and restore network connections option or Quick logon. If you use OS/2 Warp Server's logon assignments function, consider selecting the radio button for **Quick logon**. Your logon will go faster because the Microsoft code will not try to reconnect to logon assignments that already exist.

12.7.3 IBM Auto 16/4 ISA Token-Ring Adapter

In this section we discuss configuring a network adapter, setting protocol bindings, and adjusting device driver parameters. Bindings are similar for every adapter, but device driver parameters vary a lot. For example, there are only two settings for the IBM Token-Ring Credit Card Adapter II. On the other hand, the IBM Auto 16/4 ISA Token-Ring Adapter has 13 settings.

12.7.3.1 Bindings

Bindings are used to define which protocols are enabled on each adapter card. If there is only one network adapter card installed in the computer, all

the protocols have to be bound to at least one adapter. If a protocol is not bound to an adapter, it is not functional.

If there is more than one network adapter card installed, the set up of the network adapters can be complex. in the example shown in Figure 152, the NetBEUI, SPX/IPX and TCP/IP protocols are bound to the IBM Auto 16/4 ISA Token-Ring Adapter.
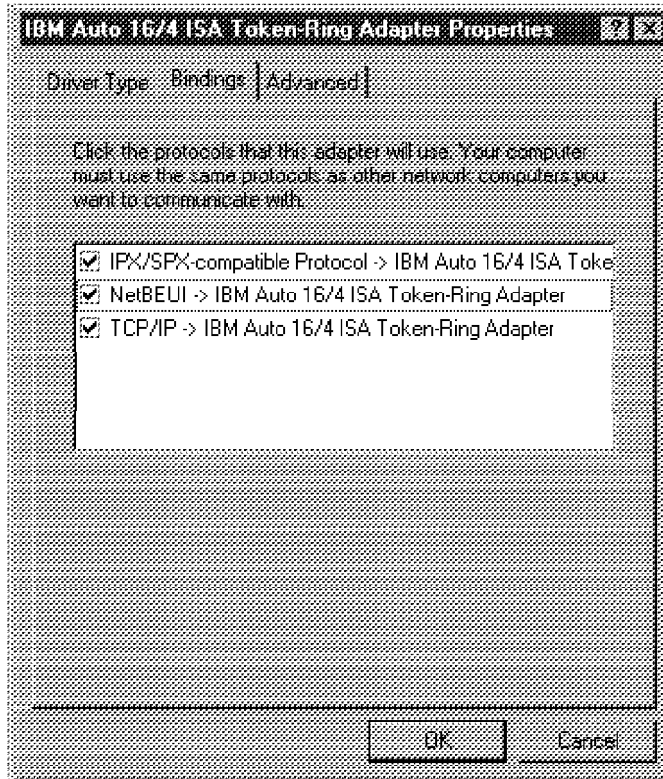
Figure 152. Three Bindings for One Network Adapter

In the Network notebook and the Bindings tab of the network adapter, the same format is used to display bindings if more than one network adapter card is installed. If only one network adapter card is installed, only the protocol is shown because there is only one possible adapter for binding.

When a new network adapter is added, Windows 95 automatically binds every installed protocol and client to the adapter. You can see all bindings, installed clients, and network adapters listed in the Network notebook. There is a small icon in the front of every row in the list that specifies the type of the product, as shown in the table below.

Table 13. Component Type Icons in the Network Notebook		
Icon	**Component Description**	**Example Components**
	Network client	• IBM Networks Client for Windows 95 • Client for Microsoft Networks
	Network adapter	• IBM Auto 16/4 ISA Token-Ring Adapter • IBM Credit Card Adapter and compatible
	Protocol	• NetBEUI • TCP/IP • IPX/SPX-compatible protocol
	Service	• File and printer sharing for Microsoft Networks • HP JetAdmin

In the example shown in Figure 153 on page 279, the active protocols for the ethernet network adapter are NetBEUI, IPX/SPX, and TCP/IP. The NetBEUI and IPX/SPX protocols are run on the token-ring adapter. To remove unwanted bindings, select the protocol to be removed and click on the **Remove** button from the Network notebook. Multiple selections cannot be made; so the operation must done for every protocol removed. When ready, select **OK** from the Network notebook and reboot the computer when prompted.

In the same fashion, you can remove protocols, adapters, and client products. Select the component from the list you want to remove and click on the **Remove** button. Remember to select the **OK** button and reboot the machine to activate the changes. If you remove a network adapter, you also remove its bindings.
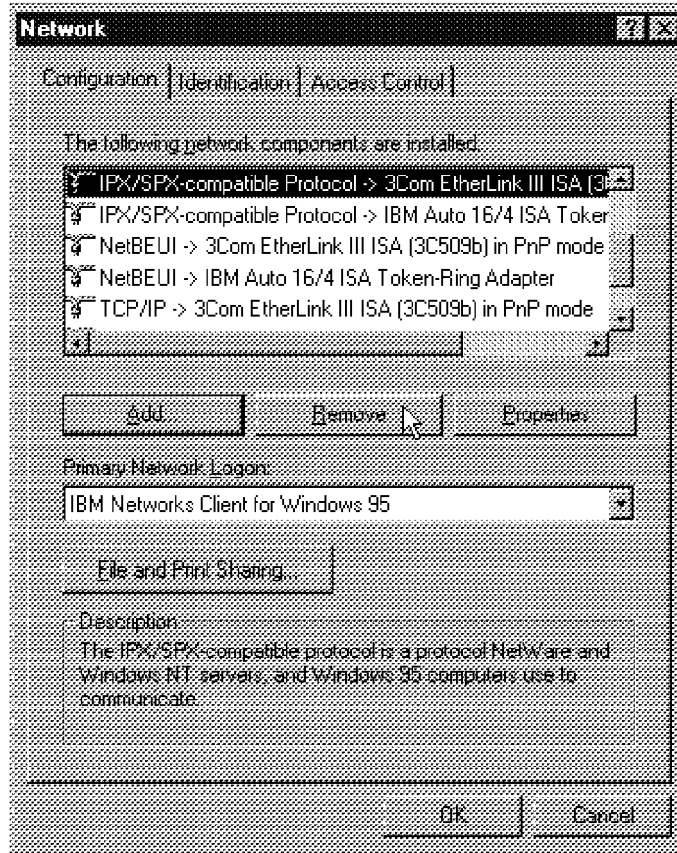
Figure 153. Network Configuration Window

> **Tip**
>
> If you make changes to the network configuration and want to cancel
> them, close the Network notebook by clicking the **Cancel** button instead
> of the **OK** button. If you select the **OK** button, changes cannot be
> undone.

In the scenario shown in Figure 154 on page 280, only NetBEUI is bound to
the Ethernet adapter. However, all three protocols are bound to the
Token-Ring adapter.
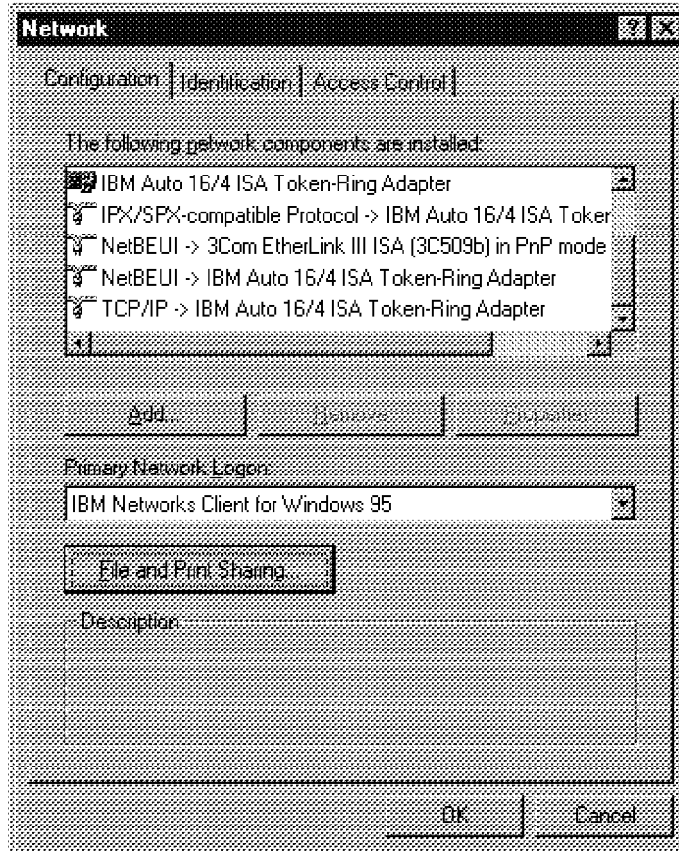
Figure 154. Bindings Are Listed in the Network Notebook

Note

IBM Networks Client for Windows 95 and Client for Microsoft Networks require the NetBEUI or TCP/IP protocol to be bound on the LAN adapter. If you remove these protocols, network clients are removed automatically, and no network logon window appears after rebooting.

12.7.3.2 Advanced Options

IBM Auto 16/4 ISA Token-Ring Adapter advanced options include hardware-dependent settings such as memory address, used IRQ, and maximum packet size. Settings and setting ranges vary depending on the driver and driver version. For instance, the IBM Auto 16/4 ISA Token-Ring Adapter, has several settings (Figure 155 on page 281), but other drivers have only a few settings.
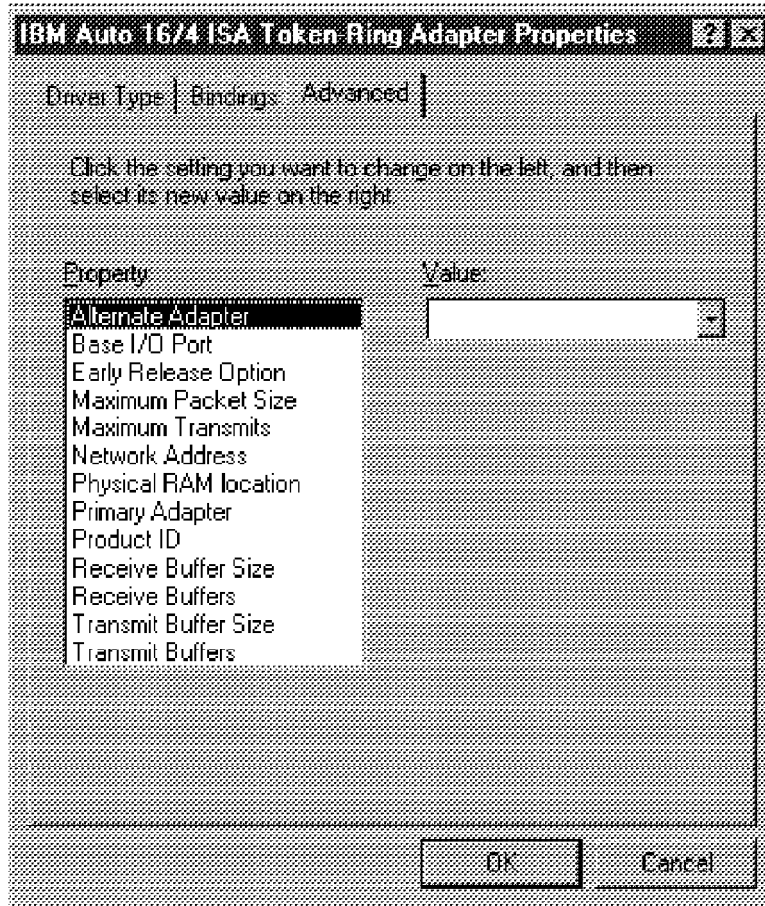
Figure 155. Network Adapter Card Drivers May Have Different Options

12.7.4 The NetBEUI Protocol

The NetBEUI protocol is commonly used as the main LAN protocol because of its easy installation, configuration (see 4.2, "The NetBEUI Protocol" on page 32. For more details, also see 4.1, "The NetBIOS Application Programming Interface" on page 27) and speed. It is one of the fastest protocols available. We discuss more of the Windows 95 NetBEUI characteristics in the following sections.

12.7.4.1 Bindings

You can determine which network protocols are being used by the network clients. Select the **NetBEUI** protocol from the installed components list in the Network notebook and click the **Properties** button to define which clients will use the NetBEUI protocol (see Figure 156 on page 282).
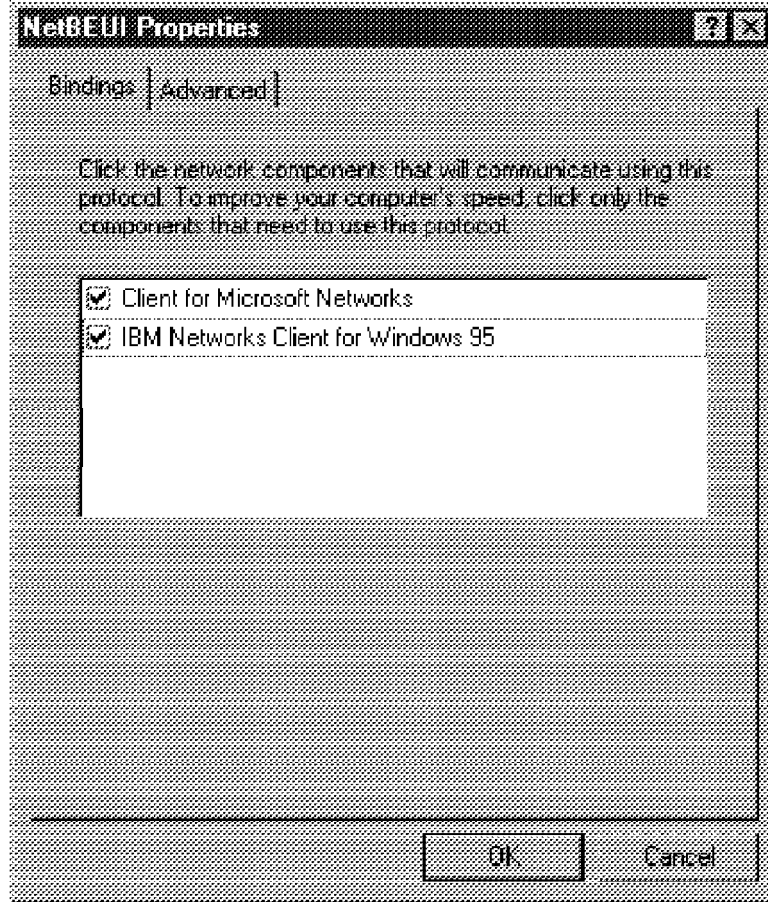
Figure 156. The NetBEUI is Bound to Every Client Product as a Default

For example, the binding function is useful if you want to install NetBEUI and TCP/IP without the NetBIOS API to ensure file and print services over NetBIOS and Internet application over TCP/IP. Install both protocols, open TCP/IP Properties, click on the **Bindings** tab, unselect all the client components in the list, and select **OK**. Select the **No** button from the attention dialog box (Figure 157) to prevent binding the protocol to any clients. However, the protocol is still be bound to the network adapter card.
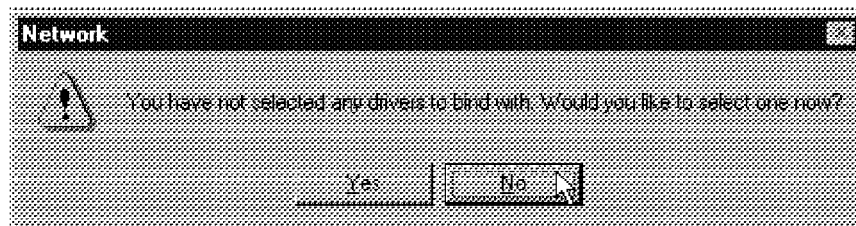
Figure 157. Sometimes Bindings Are Not Wanted

12.7.4.2 Advanced Options

NetBEUI advanced options includes NetBEUI resource settings:

Table 14. NetBEUI Advanced Options			
Resource	**Default Value**	**Maximum Value**	**Description**
Maximum sessions	10	117	Maximum number of sessions
NCBS	12	255	Maximum number of Network Command Blocks

If you use many LAN resources and applications that reserve NetBIOS resources, you may run out of resources. If necessary, increase NetBEUI resources by selecting the **NetBEUI** protocol from the Network notebook list and click the **Properties** button. Select the **Advanced** tab and enter the appropriate values for resources (Figure 158 on page 284). For example, every `NET USE` command to each server requires one new session. Once the NetBIOS session has been established, the workstation and server negotiate a higher-level protocol to use. Future file or printer resources requests against a server use that same NetBIOS session.
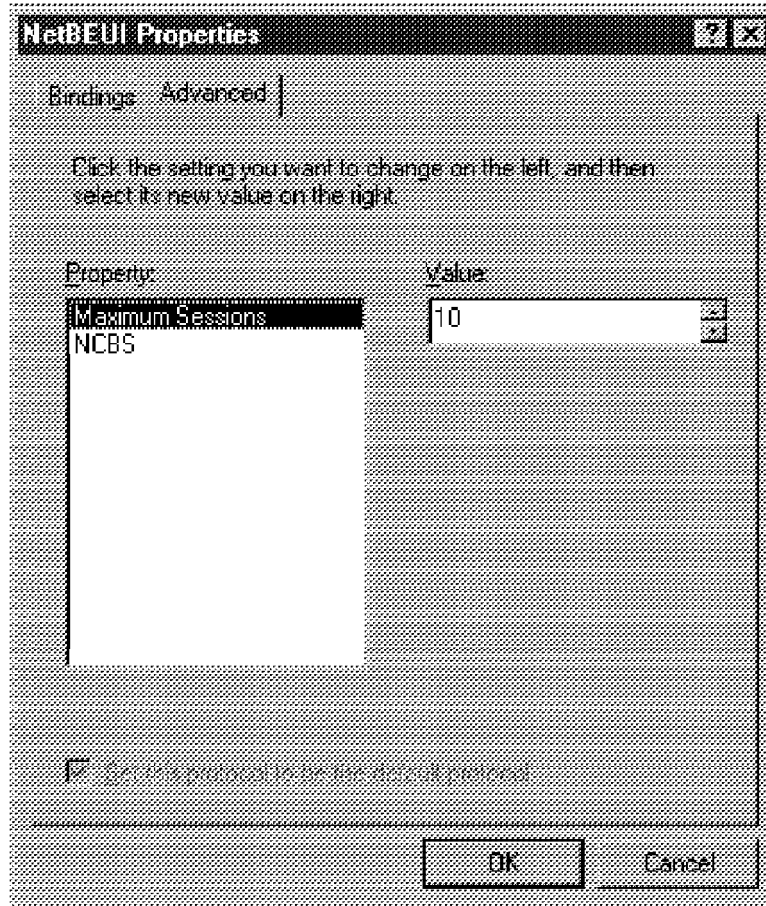
Figure 158. Increasing NetBEUI Resources

NetBIOS/NetBEUI

The difference between NetBIOS and NetBEUI is that NetBIOS is an API (Application Programming Interface), and NetBEUI is a protocol that carries NetBIOS frames. The NetBIOS functionality can be implemented over multiple protocols like NetBEUI, IPX/SPX or TCP/IP. (see 4.2, "The NetBEUI Protocol" on page 32. for more details; also see 4.1, "The NetBIOS Application Programming Interface" on page 27).

12.7.5 The Windows 95 TCP/IP Protocol

The following chapter discusses installing and configuring TCP/IP for Windows 95. We provide information on how to replace NetBEUI with TCP/IP when using network clients like Client for Microsoft Networks and IBM Networks Client for Windows 95.

12.7.5.1 NetBIOS Over TCP/IP

There are many factors to consider when the LAN communication protocol used is TCP/IP instead of NetBEUI. Network clients (both Client for Microsoft Networks and IBM Networks Client for Windows 95) cannot use native TCP/IP for file and print sharing. They need the NetBIOS interface. In Windows 95, NetBIOS over TCP/IP is transparent and cannot be enabled or disabled from the Network notebook. If you install TCP/IP, you also get NetBIOS support.

NetBIOS/NetBEUI vs NetBIOS over TCP/IP

NetBIOS/NetBEUI and NetBIOS over TCP/IP are two ways of communicating over a network, however, from a users's point of view, the two protocols offer the same services. The implementation, however, is very different. A computer using only NetBEUI cannot communicate with a computer using only TCP/IP; although they get the same services from the network.

There are many reasons why you should use the TCP/IP protocol instead of the NetBEUI protocol, such as :

- NetBIOS addressing is done on only one level; it cannot be divided into subnets like TCP/IP.

- The NetBEUI protocol uses broadcasting techniques to register and find other NetBIOS names, which causes extra network traffic.

- The NetBEUI protocol cannot be routed like TCP/IP or IPX/SPX.

There are also drawbacks when using TCP/IP instead of the native NetBEUI protocol:

- NetBIOS API calls must be mapped into the TCP/IP protocol, which costs time.

- NetBIOS packet already contains the sender and receiver information; but IP uses its own addressing method, which reduces the actual effective packet data size (the same size of packet on the network but less data in the packet and more addressing information).

- NetBIOS name resolution has to be implemented if broadcasting is not allowed.

When using (NetBIOS over) TCP/IP as the network clients protocol, a workstation has to find dependencies between NetBIOS names and IP addresses. This can cause problems, because every workstation using peer or server services has to know the NetBIOS name/IP address pair to connect to a peer or file server or an application server. However, every

workstation on the network does not have to know all workstation NetBIOS names and IP addresses, just those addresses it communicates with. The same NetBIOS computer name rules and restrictions mentioned in 12.7.1, "Computer Identification on the Network" on page 269, apply to the TCP/IP implementation as well.

Broadcasting is the easiest way to resolve the IP address of a known NetBIOS name. The computer that needs to know an IP address sends a broadcast message to the network and waits for another computer to answer and send its IP address in return. Broadcasting is the default communications technique and therefore, it does not require any configuration. The best way is to set up a NetBIOS name server and get the name resolution services without broadcasting (see 5.1, "The Shadow NetBIOS Name Server" on page 47).

In many instances, if TCP/IP traffic is routed, broadcasts are not delivered to other segments. This may be due to low-speed connection between segments, or the router is configured to prevent broadcast traffic from one segment to another. If broadcasts are masked in the router, NetBIOS name resolution must be implemented in another manner such as a static LMHOSTS file (see 12.7.5.4, "The LMHOSTS File" on page 287) or a NetBIOS name server such as Shadow (see 5.1, "The Shadow NetBIOS Name Server" on page 47).

There are five definitions of how a TCP/IP workstation can find the IP address corresponding to a NetBIOS name, as shown in Table 15.

Table 15. The NetBIOS over TCP/IP Node Types		
Node Name	**Name Registration Method**	**Name Resolution Method**
B-node	Broadcast	Broadcast
P-node	NetBIOS name server	NetBIOS name server
M-node	Broadcast	Tries broadcast first, but switches to p-node if answer is received
H-node	NetBIOS name server, if not found switches to b-node	NetBIOS name server, if not found switches to b-node
Microsoft enchanced	WINS proxies or Windows Sockets	Local LMHOSTS file or WINS proxies or Windows Sockets

The M-node is never used, only defined. You cannot set the node type directly in Windows 95, but the operating system takes care of the proper node-type setting. You can check the node-type used by typing `winipcfg` in the command line and selecting the **More Info** button.

If you have not defined a WINS server and you are not using DNS, the workstation is automatically a B-node. If there is a DNS configured, a workstation is an H-node by default.

12.7.5.2 NetBIOS Names Resolution Order B-Node

Windows NT 3.51, Windows NT 4.0, and Windows 95 NetBIOS name resolution is achieved in the following order:

1. NetBIOS name cache

2. NetBIOS name server

3. IP subnet broadcast

4. Static LMHOSTS file

5. Static HOSTS file

6. DNS server

NetBIOS Name Cache

To see the NetBIOS name cache content, use commands `nbtstat -c`, `nbtstat -n` and `nbtstat -r` to see the remote name cache, local NetBIOS names and the names resolved by broadcasting or from WINS. You can get more information about options by entering `nbtstat -?` in the DOS prompt.

12.7.5.3 NetBIOS Over TCP/IP Performance Considerations

The overhead using TCP/IP compared to NetBEUI can be anything between 10 percent to 75 percent depending on the applications and services used. On the other hand, it is quite possible that the user does not notice any difference performance-wise. When using application servers like IBM DB2/2 server or Lotus Notes server, we recommended using native TCP/IP instead of NetBIOS over TCP/IP.

12.7.5.4 The LMHOSTS File

The LMHOSTS file contains the mappings between the IP addresses and the computer (NetBIOS) names. By default, there is a sample LMHOSTS file LMHOSTS.SAM in the Windows directory that can be used as a template to create the working LMHOSTS file. The LMHOSTS file format is similar to the HOSTS file; you define the IP address, the NetBIOS name and extra options if needed (see Table 16 on page 288).

Table 16. Some LMHOSTS Options	
Option	**Description**
#PRE	The entry is preloaded into the name cache.
#DOMAIN:<domain>	Associates the entry with the domain <domain>; the #PRE option must always be used in conjunction with this option.
#INCLUDE <filename>	Includes definitions from an external file; the include file name can be a UNC name to load the file from a file server.
#BEGIN_ALTERNATE	Start the list of alternate include files.
#END_ALTERNATE	Ends the list of alternate include files.
#text	Remark text.

A typical LMHOSTS file could look like this:

```
#
#A sample LMHOSTS file
#
9.3.1.21    ITSCSV00    #PRE #DOMAIN:ITSCAUS
9.3.1.14    ITSCFS00    #PRE #additional server
9.3.1.21    ITSCAUS     #PRE #DC IP assigned to the domain name
#
```

Remember always to use capital letters in computer names and in options because the file is case sensitive. There has to be a carriage return character (Enter) at the end of the last row to be read. An easy way to make sure that the file format is correct is to start the file with a single pound sign on the first row and a single pound sign on the last row.

The LMHOSTS file is loaded in the computer at startup and is therefore static. If any changes are made, the computer has to be rebooted to load the new definitions. The LMHOSTS file information is used if NetBIOS name server is not present, cannot resolve the name, or if the broadcast fails.

The problem when using the local LMHOSTS file is that if a server's IP address changes or a server is added or removed, the LMHOSTS file may no longer be valid. Because the file is local it has to be updated on every client workstation. A solution is to define only the server entry in the LMHOSTS file and use the #INCLUDE option to load the complete definition file from a server. In this way you can avoid extra work if IP addresses are changed. However, the implementation is still non-dynamic, remaining file based, and has to be maintained manually.

If you still cannot connect to your logon server residing behind a router, there may be a conflict between the defined domain and workgroup names. Set the workgroup name to be different from the OS/2 Warp Server domain name in the Network notebook.

Workgroup Name vs Domain Name

Be aware that, when using LMHOSTS in a Windows 95 TCP/IP environment, the workgroup name must be different to the domain name. For example, when you have the names the same, and the LMHOSTS file looks like the following (xxx and zzz stand for IP addresses):

```
xxx.xxx.xxx.xxx      BADM80              #PRE      #DOM:BOBSUPPORT
xxx.xxx.xxx.xxx      "BOBSUPPORT      \0x00"   #PRE
zzz.zzz.zzz.zzz      NTINTERDC           #PRE      #DOM:NTINTERDOM
```

the scenario fails.

When the names are different and the order of LMHOSTS is changed as follows:

```
xxx.zxx.xxx.zxx      "BOBSUPPORT      \0x00"   #PRE
xxx.xxx.xxx.xxx      BADM80              #PRE      #DOM:BOBSUPPORT
zzz.zzz.zzz.zzz      NTINTERDC           #PRE      #DOM:NTINTERDOM
```

the scenario works.

The reasons for these are as follows:

- In our failed login, where the domainname=workgroupname, we broadcast and register the workgroup BOBSUPPORT. At this point, everything on the local subnet is BOBSUPPORT, and the NetBIOS name BOBSUPPORT is resolved to a hardware address of zeroes. Because of this, the LMHOSTS file is never consulted for the IP address of BOBSUPPORT and never gets the proper domain suffix. Windows 95 then sends an Arp request for the hardware address for the IP address of xxx.xx.xxx.xx, which in the LMHOSTS is BADM80, the primary domain controller for BOBSUPPORT, with no suffix.

- In our successful login, there is no attempt to resolve BOBSUPPORT until domain logon validation. There is nothing in the Arp cache telling Windows 95 where BONSUPPORT is located (as opposed to a broadcast), so it must attempt to resolve it. Per B-node resolution, it first broadcasts and then consults LMHOSTS file. Since it's not looking for BADM80, it goes to the next entry, BOBSUPPORT, and not only gets the proper IP address, but the proper domain suffix.

Another solution is to add one extra entry to the LMHOSTS file and install the Neighborhood Browser Enabler on the domain controller server. The Windows 95 client tries to find a domain name with the 16th-byte [1Ch], but by default an OS/2 Warp Server does not know how to answer to this query. If a NetBIOS name contains any special characters, the name must be surrounded by double quotes. The LMHOSTS file would look like this:

```
#
#A working sample LMHOSTS. file when using network
#connections over a router
#
#The three lines work as decleared below:
#
#The DC is registered with the domain name
#The domain itself is registered with the DC IP address
#The domain name is registered with 16th byte (or character) 1Ch
#
9.3.1.140    WS_SRV01              #PRE #DOM:WS_DOM01
9.3.1.140    WS_DOM01             #PRE
9.3.1.140   "WS_DOM01      \0x1C" #PRE
#
#
#Additional domain definition
#
9.3.1.21     ITSCSV00              #PRE #DOM:ITSCAUS
9.3.1.21     ITSCAUS              #PRE
9.3.1.21    "ITSCAUS       \0x1C" #PRE
#
#Additional servers for extra file resources
#
9.3.1.59     ITSCFS00
9.3.1.14     ITSCPS00
9.3.1.21     ITSCSV00
#
```

Be Careful with the LMHOSTS File

If you define an incorrect IP address for a server in the LMHOSTS file, you cannot connect to the server. If the domain controller IP address is not defined correctly, you cannot even log on to the domain.

12.7.6 Windows 95 Networking Model in More Detail

Windows 95 uses NDIS 3.1 (Network Driver Interface Specification) drivers with the same functionality as the NDIS 3.0 and NDIS 2.x drivers used in Windows NT, Windows for Workgroups 3.11 and OS/2. NDIS 3.1 drivers have some enchancements like Plug-and-Play support for network adapters. Both

Microsoft and IBM use NDIS specification for network drivers. However, NetWare uses Open DataLink Interface (ODI) specification (refer to Figure 159 on page 291, the device driver interface).
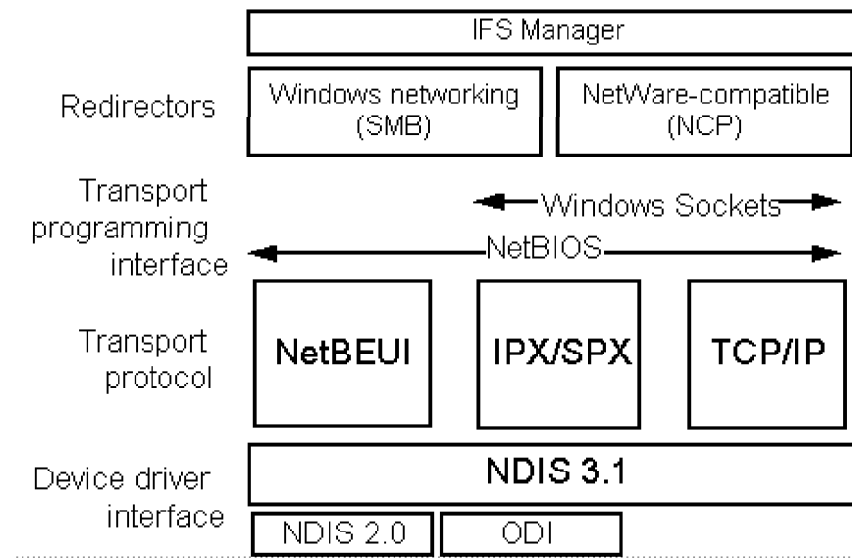
Figure 159. The Windows 95 Networking Structure

The protocol stacks are loaded over the NDIS network driver. The protocol stacks commonly used are NetBEUI, TCP/IP and IPX/SPX. Other protocols include Microsoft DLC to connect to AS/400 systems or IBM LLC2 to connect to mainframe systems. All NetBEUI, TCP/IP and IPX/SPX protocols provide the NetBIOS programming interface for applications. An application developer does not have to decide on the actual underlying communications protocol, but they can use the common NetBIOS interface regardless of the user's network implementation (see Figure 159, transport protocol).

The Windows sockets is another abstraction layer in the Windows 95 networking structure. TCP/IP and IPX/SPX can carry sockets. Many applications use sockets to communicate on the network, such as Windows 95 FTP and IBM Dynamic IP Client for Windows 95.

After a NetBIOS session has been established between two participants, Windows 95 (like OS/2) starts using the SMB (Server Message Block) protocol. Server Message Block is the protocol that LAN Manger/LAN Server clients and servers use to communicate with each other. Client systems use this protocol to request file, print, and communications service from server systems over a network (refer to Figure 159 and see 4.3, "Server Message Block (SMB)" on page 33 for more information).

12.7.7 Windows 95 System Policies

Windows 95 allows easier user and system management through system policies. The system policies include user-level profiles and hardware-level profiles. User-level profiles include user's desktop wallpaper and color scheme, display settings, file-sharing restrictions and application restrictions. Hardware-level profiles include logon-behavior settings, minimum Windows password length and settings to run programs or services during the startup process. System policies allow administrators to restrict user access to system configuration changes by restricting which icons and menu options are available on a user's desktop.

To use system policies you have to enable Windows 95 user profiles in the following way:

1. Select [**Start** — **Control Panel** — **Passwords**] to display the Password properties notebook.

2. Select the **User Profiles** tab and select the **customized preferences** radio button. Check the **Include desktop icons** and **Include Start Menu** check boxes, unless you do not want users to have personalized desktops or Start menus.

3. Reboot the machine to make these settings effective.

Use the System Policy Editor (POLEDIT.EXE) tool to create and edit Windows 95 system policies. The executable file is found on the Windows 95 installation CD in the directory ADMIN APPTOOLS POLEDIT. Install the system policy editor in the following way:

1. Select [**Start** — **Settings** — **Control Panel** — **Add/Remove Programs**].

2. Select the **Windows setup** tab.

3. Select the **Have disk** button.

4. In the Copy files from entry field, enter `d:` ADMIN APPTOOLS POLEDIT, where `d:` is your Windows 95 installation CD-ROM drive.

5. Select the componenets to be installed. If you want to use group policies, install the group policies component on every Windows 95 workstation. The system policy editor component is not required on the workstations; it is only needed to create and edit policies.

6. Select **OK** to complete the installation process.

12.7.7.1 How to Implement System Policies in an OS/2 Warp Server Environment

The CONFIG.POL system policy must be stored in the logon server. The default path is the domain controller share, which is

\\LogonServer\NETLOGON. The NETLOGON share points to
C:\IBMLAN\REPL\IMPORT\SCRIPTS where C: is the OS/2 Warp Server
installation drive.

We recommend specifying a different path. If you want to use another file
name, directory or share, define the path and file name in the IBM Networks
Client for Windows 95 settings. Users that need to download system
policies must have read (R) and execute (X) access rights to the network
share.

Create the system policy profile and save the file in your domain controller
server's NETLOGON share with the name CONFIG.POL.

```
┌─ Non-FAT Partition Required ─────────────────────────────────────────┐
│                                                                       │
│  System policies must be saved on a non-FAT partition on the server.  If │
│  the OS/2 Warp Server installation drive is formatted as FAT, you have to │
│  define the system policy to be downloaded from a share on an HPFS or  │
│  HPFS386 drive.                                                        │
│                                                                       │
└───────────────────────────────────────────────────────────────────────┘
```

If your user name or the computer name is defined in the system policy to
have restrictions or settings, the policy is downloaded during the logon
process. The user profile is stored on your home directory (if defined) to file
USER.DAT, and the user profile is also copied to your local machine's
Windows 95 registry database. This enables you to get the same profile
from all workstations, but it also means that the profile is downloaded to
every machine you use to log on to the network. The recent documents list
is always stored for every user when the user profiles function is enabled.
Other options, like personalized desktop, Network Neighborhood and the
Start menu can be enabled as well.

```
┌─ Group Policies ─────────────────────────────────────────────────────┐
│                                                                       │
│  All Windows 95 systems that use group policies must have             │
│  GROUPPOL.DLL installed:                                              │
│                                                                       │
│   1.  Select [**Start** — **Control Panel** — **Add/Revove Programs** — **Windows** │
│       **Setup** — **Have Disk**].                                     │
│                                                                       │
│   2.  Insert the Windows 95 CD-ROM and type the following path:       │
│         E: ADMIN APPTOOLS POLEDIT.                                    │
│                                                                       │
│   3.  Select **Group Policies**.                                      │
│                                                                       │
└───────────────────────────────────────────────────────────────────────┘
```

The personal Windows desktop is created in your home directory if a home
directory is defined and the desktop is included in user settings. The

desktop is copied to the local directory
C: WINDOWS PROFILES UserID DESKTOP, where UserID is the logon name
used. If you start the computer without networking and make the Windows
logon, System Policy is read directly from the local disk and the same
restrictions and settings apply as those downloaded during the last network
logon.

```
┌─── Use the Windows 95 Logon Function to Log on to the System ───

  The system policy is downloaded only when the logon is done from a
  Windows 95 system logon window. Open the logon window by restarting
  the computer or selecting [Start — Shut down — Close all programs and
  log on as a different user?]. If you log on or log off using the GUI
  interface, you are still using the system policy loaded in the startup
  logon.

```

You can view and edit the Windows 95 registry database with the REGEDIT
command. REGEDIT is run by selecting [**Start** — **Run...**] and typing REGEDIT.

Note: Changing the Windows 95 registry database can cause your system
to fail. Do not change any values if you do not know how they affect
the system.

12.7.8 The Windows 95 NET Commands

The LAN Server NET commands are accessed using the NETLS command.
This functionality supplements the Microsoft NET commands. You can get a
brief description of Microsoft NET commands just by typing the command
NET in the command line. The following is the output:

```
For more information about a specific Microsoft NET
command, type the command name followed by /?
(for example, NET VIEW /?).

NET CONFIG   Displays your current workgroup settings.
NET DIAG     Runs the Microsoft Network Diagnostics program to
             display diagnostic information about your network.
NET HELP     Provides information about commands and
             error messages.
NET INIT     Loads protocol and network-adapter drivers without
             binding them to Protocol Manager.
NET LOGOFF   Breaks the connection between your computer and
             the shared resources to which it is connected.
NET LOGON    Identifies you as a member of a workgroup.
NET PASSWORD Changes your logon password.
NET PRINT    Displays information about print queues
```

```
                    and controls print jobs.
NET START    Starts services.
NET STOP     Stops services.
NET TIME     Displays the time on or synchronizes your computer's
             clock with the clock on a Microsoft Windows for
             Workgroups, Windows NT, Windows 95, or NetWare time ser
NET USE      Connects to or disconnects from a shared
             resource or displays information about
             connections.
NET VER      Displays the type and version number of the
             workgroup redirector you are using.
NET VIEW     Displays a list of computers that share
             resources or a list of shared resources
             on a specific computer.
The command was completed successfully.
```

The following limitations apply to the Microsoft Windows 95 NET command interface:

- The server cannot be administrated from a Windows 95 workstation using the Microsoft NET commands. There are no NET USER, NET ACCOUNTS, or NET ADMIN commands available from Microsoft Windows 95 NET commands.
- Logon and logoff can only be done from the GUI interface or the standard Windows 95 logon function.
- There is no NET ALIAS command.

Some very basic network operations can be done from the command line including:

- Use NET USE to assign network resources, for example:

  NET USE P: WS_SRV01 PUBLIC

  assigns the drive letter P: to alias PUBLIC on the server WS_SRV01.

  Note: In Microsoft's terminology, OS/2 Warp Server's alias PUBLIC is a share name.

- Use NET TIME to display the server time if the TIMESYNC parameter is not set to automatically synchronize the workstation time to the sever time. For example:

  NET TIME /SET

  sets the workstation time to the timesource server time.

> **Domain Defintion Changes through the GUI**
>
> Use the GUI interface, not the command interface, to make changes to your domain definitions.

12.7.8.1 IBM Networks Client for Windows 95 NETLS Commands

The IBM Networks Client for Windows 95 supports the following `NETLS` commands using the command line interface:

- `NETLS ADMIN`

- `NETLS ALIAS`

- `NETLS DASD`

- `NETLS HELP`

    - only on `ADMIN`, `ALIAS`, `DASD`, `SEND`, `USE`, or `WHO`

- `NETLS SEND`

- `NETLS USE [alias]`

- `NETLS WHO`

To access all `NET` commands using IBM's NET.EXE, run DLSNET.BAT. This batch file renames the Microsoft NET.EXE program as NET95.EXE, and NETLS.EXE as NET.EXE. The IBM NET.EXE (NETLS.EXE) will execute the commands mentioned above. If the command is not one of the above, it sends the command to Microsoft's NET95.EXE program to be processed.

Note: If you enter Windows 95 MS DOS mode (from the shutdown menu) you can only use the `NET HELP` and `NET USE` commands.

12.7.9 SYSTEM.INI Changes

The IBM Networks Client for Windows 95 creates two new sections in the SYSTEM.INI file:

- `[Network]`
- `[Domain List]`

These settings are valid for the GUI (Graphical User Interface) only and do not affect Windows 95 startup logon behavior in any way.

12.7.9.1 The Network Section

The `[Network]` section sets the logon behavior. By default, only one option is added:

```
[Network]
passwordcaching=no
```

All possible keywords used in this section and their legal values are listed in Table 17 on page 297.

Table 17 (Page 1 of 2). Windows 95 SYSTEM.INI Parameters

Parameter	Description	Valid Values	Default Value
lslogon	Is the logon validated by the domain controller.	Yes, No	No
securelogon	If the domain logon fails, should a local logon work.	Yes, No	No
multilogon	Indicates whether the user ID can be logged on at multiple workstations. If set to No, a user must first perform log off to log on from another workstation.	Yes, No	Yes
browsealias	Indicates whether netnames or aliases are displayed when using the browse option in Windows 95.	Yes, No	Yes
timesync	Indicates whether the client should synchronize its time to that of the IBM TIMESOURCE server. If you want to automatically synchronize the Windows 95 workstation clock, set this parameter to Yes and enable the Timesource service at the domain controller.	Yes, No	No
reconnect	Reconnects persistent connections at logon.	Yes, No	Yes
forcelogoff	Used by earlier releases to logoff Windows 95 before an IBM domain logon. This parameter is no longer necessary.	Yes, No	No
quietlogoff	Controls the prompting panels during a logoff if there are open files or active connections. If set to Yes, logoff is done without futher prompting.	Yes, No	No

Table 17 (Page 2 of 2). Windows 95 SYSTEM.INI Parameters			
Parameter	Description	Valid Values	Default Value
`passwordcaching`	Caches passwords in a caching file. This saves passwords to servers in a password protected file so the user does not have to enter a password for each server that is accessed. Since Microsoft Windows 95 FixPack 1 changed the algorithm for the password file (PWL), password caching can not be accessed by non-Microsoft apllications or clients.	Yes, No	No
`winpopup`	Controls the launching of the Winpopup messaging service when you start the IBM Networks Client. It is better to set this option from the GUI interface by selecting [**Messages** — **Load WinPopup at startup**].	0, 1	1

12.7.9.2 The Domain List Section

IBM Networks Client for Windows 95 keeps track of the domains used for logging on. The domain list is added to the SYSTEM.INI file in the [Domain List] section. You can pre-define the domains listed in the domain list when logging on using the IBM Networks Client for Windows 95 GUI logon window instead of the Windows 95 startup logon window. You can also manually define an unlisted domain to be the logon domain. The following is an example [Domain List] section:

```
[Domain List]
ITSCAUS=
WS_DOM01=
PCSUPPORT=
```

For more information about using the IBM Networks Client for Windows 95 GUI for logging on the domain, see section 9.1, "Common GUI Features and Functions" on page 95.

12.7.10 Installing TCP/IP for Windows 95

To add TCP/IP protocol stack and applications to your Windows 95 system, follow the steps below:

1. Select [**Start** — **Settings** — **Control Panel** — **Network**] to open the Network notebook.

2. Click the **Add** button and select network component type to be **protocol**.

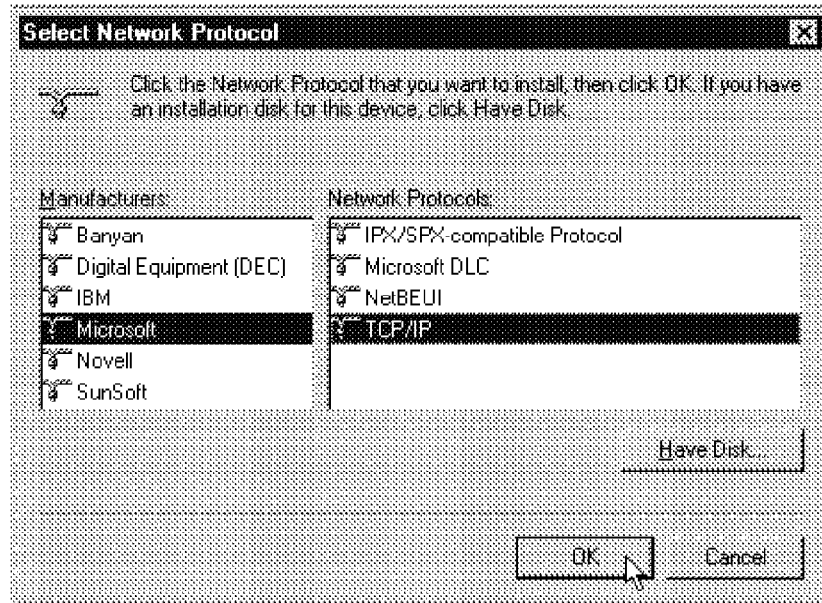3. Select **Microsoft TCP/IP** from the network protocol list (see Figure 160) and select **OK**.

Figure 160. Select the Appropriate Component Type

4. Complete the TCP/IP settings configuration as described in section 12.7.11, "Configuring TCP/IP" and reboot the machine when prompted.

12.7.11 Configuring TCP/IP

To configure the TCP/IP protocol, select **TCP/IP** protocol from the Network notebook's **installed components** list and click the **Properties** button. The TCP/IP Properties notebook is displayed as shown in Figure 161 on page 300.
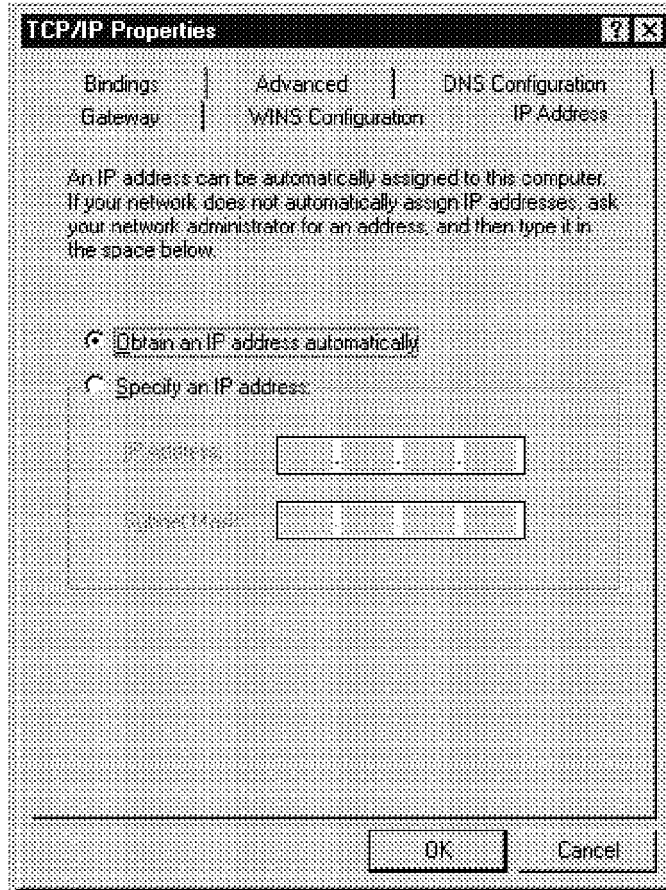
Figure 161. As a Default, the IP Address is Obtained Automatically from DHCP

12.7.11.1 IP Address

There are two ways to configure IP address. If there is a DHCP (Dynamic Host Configuration Protocol) server configured in the network, use it to provide the workstation IP address dynamically. If there is no DHCP server in the network or if the IP address has to be set as non-dynamic, manually define the IP address. The IP address format is xxx.xxx.xxx.xxx, where xxx is a digit between in the range of 0 and 255.

The subnet mask value is used to define the network range of your IP addresses. For example, the default C-class subnet mask is 255.255.255.0 and lets you use up to 254 IP addresses. The highest address is reserved for broadcasting and cannot be used for workstations or servers on the network. For example, if your IP address is 9.3.1.11 and the subnet mask is 255.255.255.0, then 9.3.1.255 is the broadcast address.
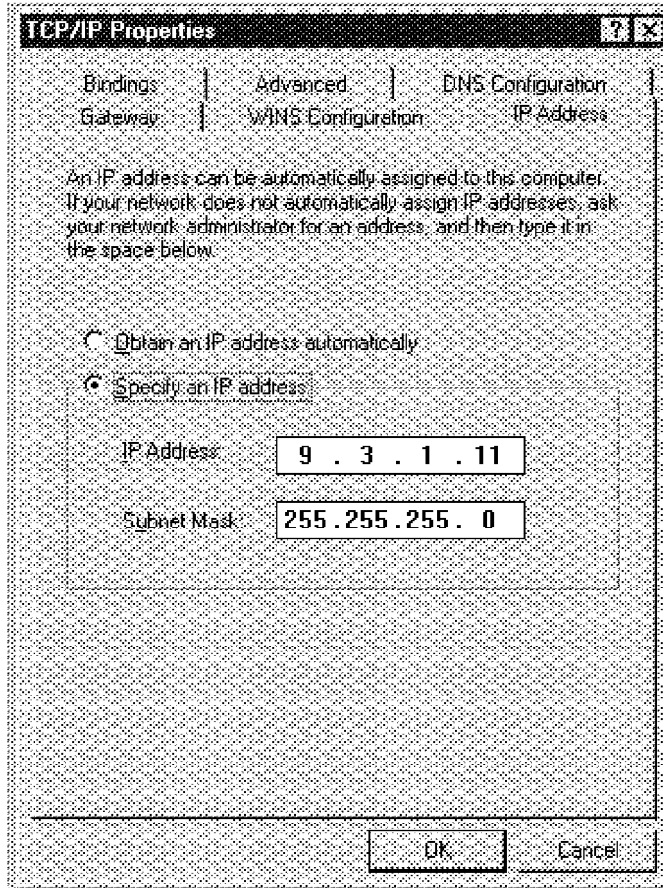
Figure 162. Define Your IP Address Manually if Needed

12.7.11.2 WINS Configuration

WINS (Windows Internet Naming Services) is Microsoft's implementation for NetBIOS name serving. You can also use NTS' Shadow instead of WINS server for dynamic NetBIOS name resolution services. If there is a WINS server or Shadow NBNS server in the network, specify the server IP address here as shown in Figure 163 on page 302. If the address is defined, the NetBIOS names are registered and queried to the NBNS server address and not broadcasted. If the registration or name query fails it is broadcasted. For more information about the Shadow NBNS server, see section 5.1, "The Shadow NetBIOS Name Server" on page 47.
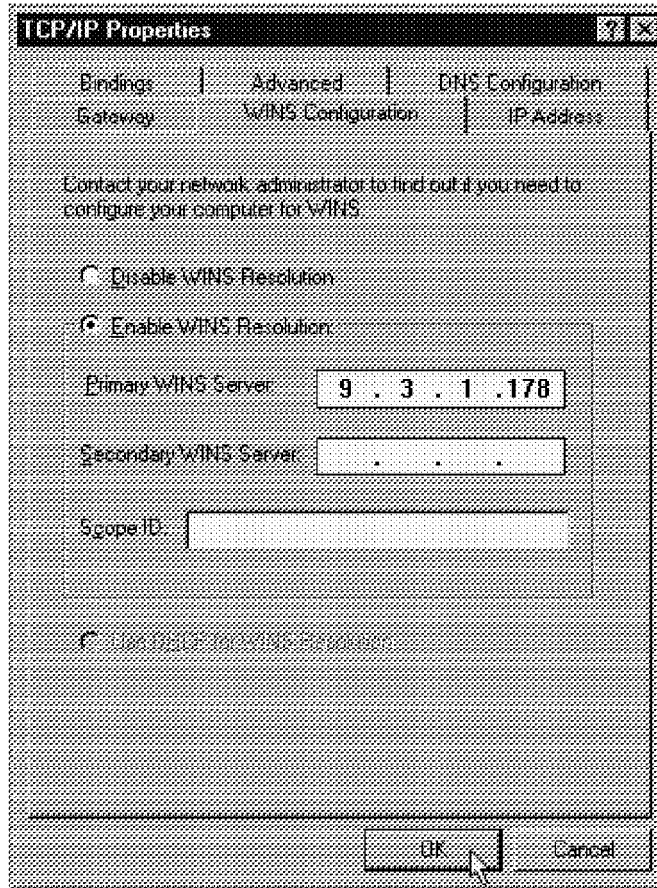
Figure 163. WINS Server Defined

12.7.11.3 Gateway

A gateway is Microsoft's term for an IP router. A router connects IP networks. For example, a LAN (Local Area Network) needs a gateway to connect to the Internet and other IP subnets. You can define up to eight gateways. In the example shown in Figure 164 on page 303, the gateway address is `9.3.1.74`.
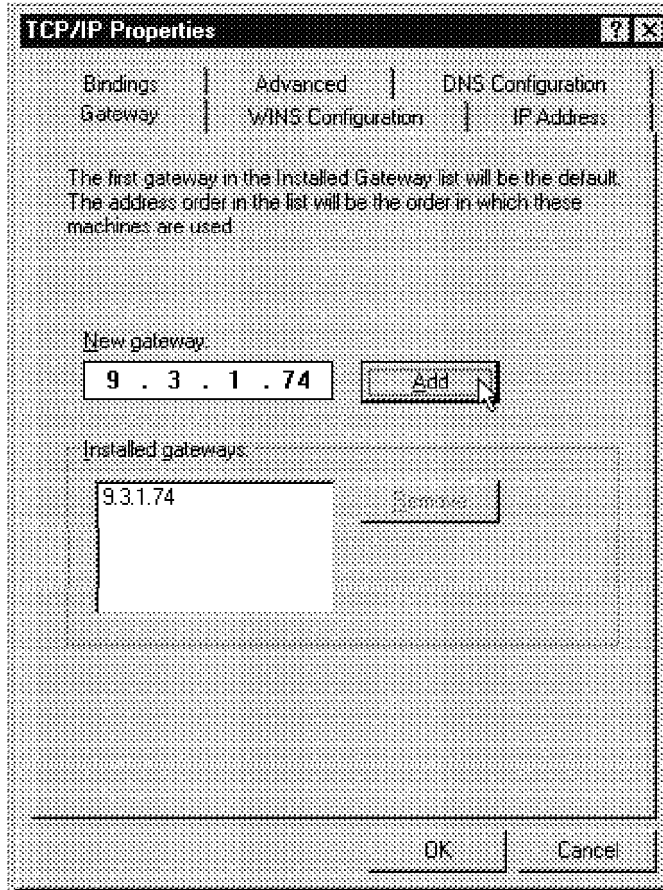
Figure 164. Define Your Gateway(s)

12.7.11.4 DNS Configuration

A Domain Name Server (DNS) identifies your computer's host name on the TCP/IP network. DNS is a server that keeps track of all computer's host names and their corresponding IP addresses and by default, it is used only with native TCP/IP applications; so DNS will not by default resolve NetBIOS names to IP addresses as discussed earlier. The host name does not have to be the same as the computer name. If you use WINS, it is strongly recommended that these two names must match. If the names do not match, the connection between the NetBIOS name and IP address is lost. If DNS is enabled, you can use host names instead of IP addresses to communicate with other TCP/IP computers.

Select the **Enable DNS** radio button to make DNS active. Define your host name and the TCP/IP domain name to which your computer belongs. The domain name is stuctured from one organization unit and one suffix. The suffixes used include `com`, `net`, `org`, or country codes such as `ar` (Argentina), `fi` (Finland) and `se` (Sweden). For example, the domain name for the

University of Helsinki is `helsinki.fi`. The domain name could be, for example, `ibm.com` or the domain can consist of more detailed organization structure like `itsc.austin.ibm.com` or `cc.helsinki.fi`. It is recommended that you use only small letters and no other special characters except a dash or underscore in the host or domain name (see Figure 165).

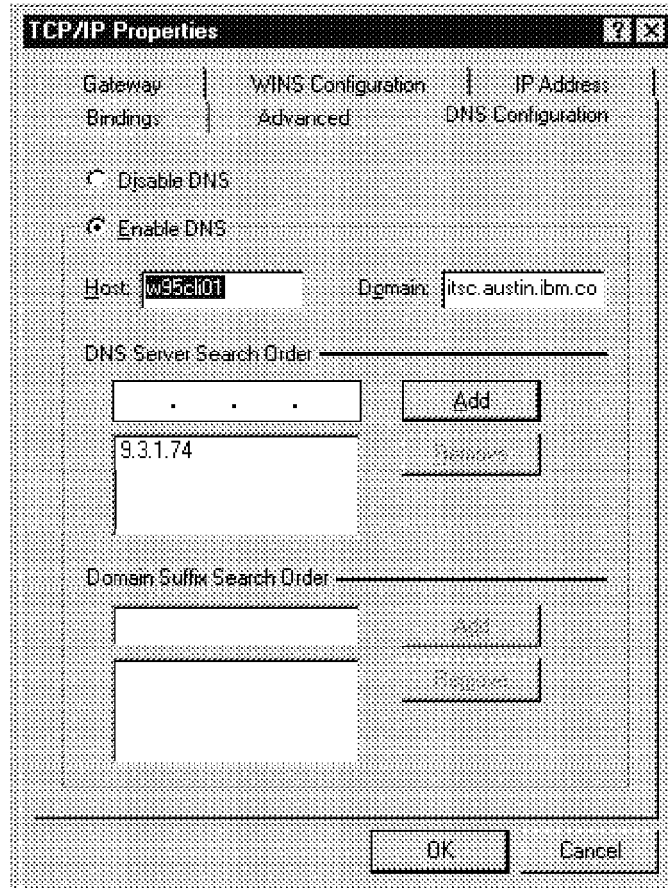*Figure 165. You Can Define Up to Three Name Servers*

12.7.11.5 Advanced Options

There are no entries in the TCP/IP Advanced options list. Under the list there is a check box that allows you to set the TCP/IP protocol to be the default protocol. In Windows 95 the only way to set priorities between different protocols is to set one protocol to be the default protocol (see Figure 166 on page 305).
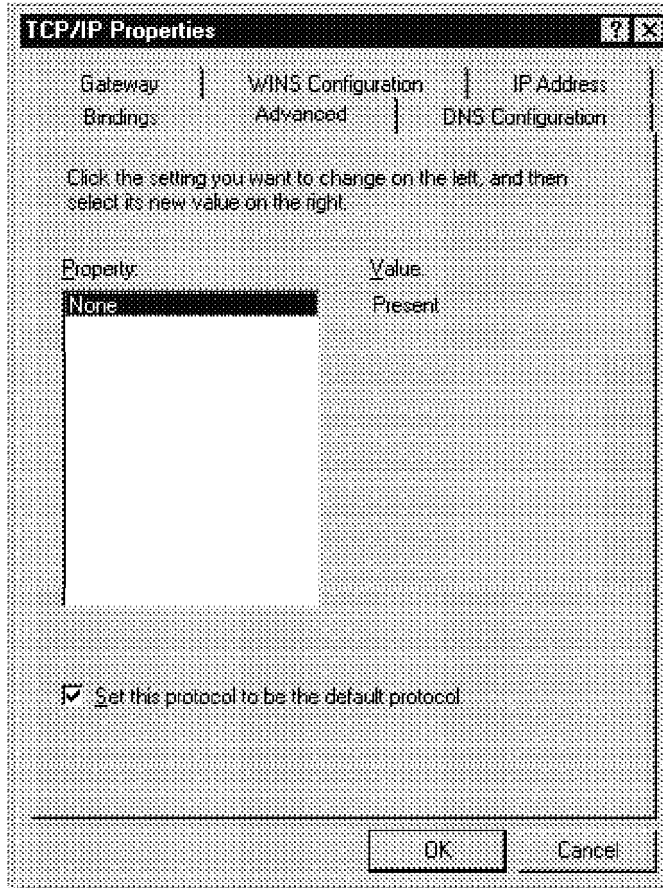
Figure 166. TCP/IP Does Not Have Advanced Options

If users use network clients configured with TCP/IP and NetBEUI, the default
protocol is the one that is used for primary network communications. If you
want to use NetBEUI for LAN traffic and TCP/IP for WAN or Internet access,
open the **NetBEUI Advanced options** and mark the box that says "Set this
protocol to be the default protocol". In Windows 95, the default protocol is
the first protocol that answers all network requests. If the NetBEUI protocol
is set to the default protocol, it reads all the traffic from the network. If the
frame read is not a NetBEUI frame, it passes the frame on to the next
protocol. This means that if you are running NetBEUI and TCP/IP protocols,
where NetBEUI is the default protocol, and NetBIOS and TCPBEUI are
configured on your OS/2 Warp Server, NetBEUI is the protocol used in LAN
traffic. If you do not want to use NetBEUI remove the protocol from the
network configuration or remove bindings from the network clients to use
the protocol stack only.

12.7.11.6 Bindings
To congigure bindings in the TCP/IP properties is done in the same way
how NetBEUI bindings are configured. You can bind the protocol to one or

more network clients or run the native protocol stack only (see Figure 167 on page 306).

If you do not want to use TCP/IP with IBM Networks Client for Windows 95, unselect all the clients from the bindings list.
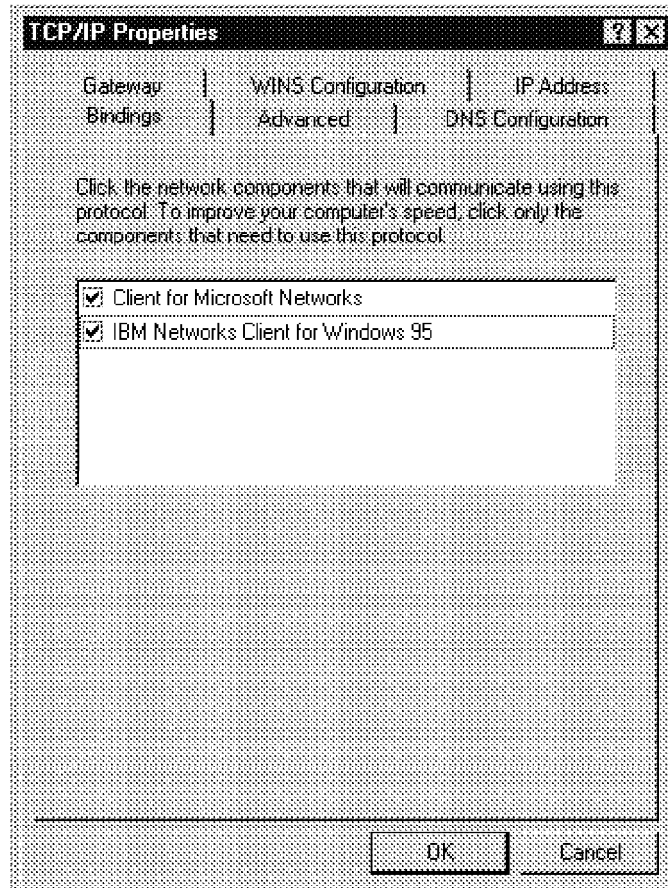

Figure 167. The Bindings Page Options

Tip

To get more detailed information about TCP/IP configuration select [**Start — Run...**], enter the command `WINIPCFG` and select the **OK** button. The IP Configuration program shows used IP address, gateway, DHCP server, and other information. Other informative commands are `NETSTAT` and `NBTSTAT`.

12.8 Windows 95 Dial-Up Networking

Windows 95 Dial-Up Networking is used to connect to another computer or network, even if your computer is not on the network. Windows 95 supports three connection types:

- NRN (NetWare Connect)
- PPP (Point-to-Point Protocol)
- Windows for Workgroups and Windows NT

Only the PPP connection protocol is discussed here.

Windows 95 Dial-Up Networking makes your modem look like a network adapter card connected to the network. All the settings and configuration considerations discussed earlier apply to Dial-Up Networking as well. The main difference is that a low-speed modem link is used instead of a high-speed LAN connection.

12.8.1 Installing Dial-Up Networking

The first step when using Dial-Up Networking is to install and configure the modem. If the modem is a Plug-and-Play modem, Windows 95 installs the necessary drivers when the modem is detected. If the modem cannot be detected automatically, install and configure it from the Control Panel. Modem settings are found by selecting [**Start** — **Settings** — **Control Panel**] and double-clicking the **Modems** icon. For more information about installing modems, refer to the *Microsoft Windows 95 Users Guide*.

To add a new Dial-Up Networking connection, follow the steps below:

1. Double-click on the **My Computer** icon on the desktop and the double-click on the **Dial-Up Networking**. The Dial-Up Networking window is displayed as shown in Figure 168.
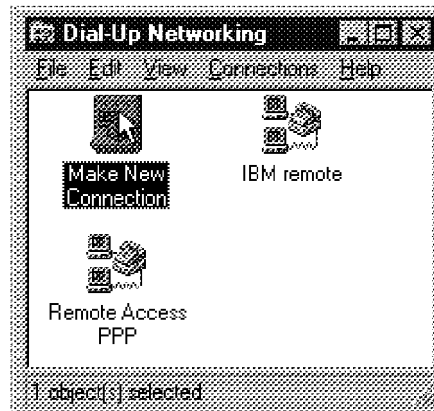

Figure 168. The Dial-Up Networking Connections Window

2. Double-click on the **Make New Connection** icon to create a new connection profile.

3. In the Make New Connection window, enter a name for the connection, select the modem used for this connection, as shown in Figure 169, and click the **Next** button.
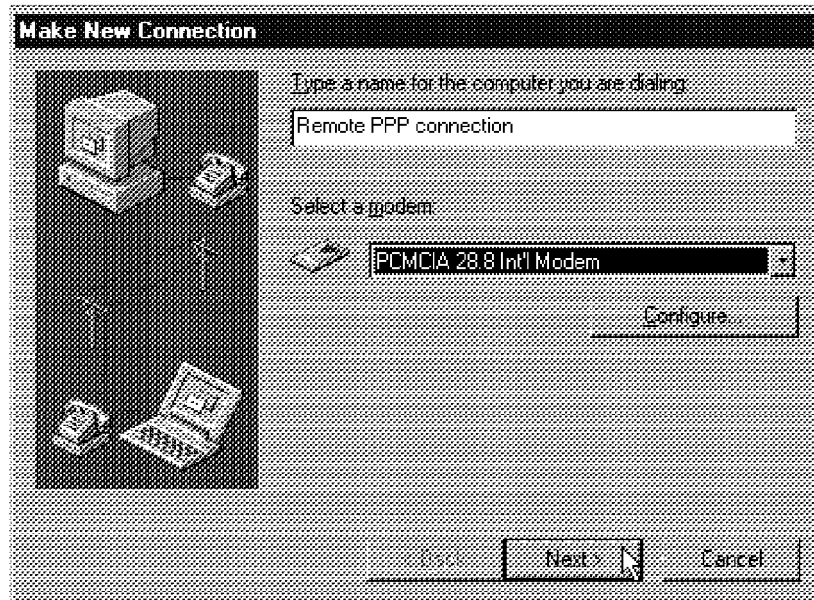
Figure 169. The Make New Connection Window

4. Enter the telephone number dialed for the connection, select the country as prompted in the next window and select the **Next** button to continue.

5. Click the **Finish** button to complete the installation process.

Windows 95 adds a new adapter called Dial-Up Adapter to your network configuration if not already present. The protocol stacks and client products are loaded over the Dial-Up Adapter interface.

12.8.2 Configuring the Dial-Up Networking

The Dial-Up Networking configuration is split into two parts. The networking part includes protocol stack settings and bindings and the connection settings part includes the telephone number to be dialed, advanced options and allowed protocols.

12.8.2.1 The Network Notebook Settings

When the connection profile is created, you must configure the Dial-Up Adapter protocols and bindings from the Control Panel and Network notebook as shown in Figure 170 on page 309. Install the required protocols and client products as described above. You can run different

protocols on a LAN adapter and Diap-Up Adapter. The Dial-Up Adapter has the same functional status as a normal LAN adapter.
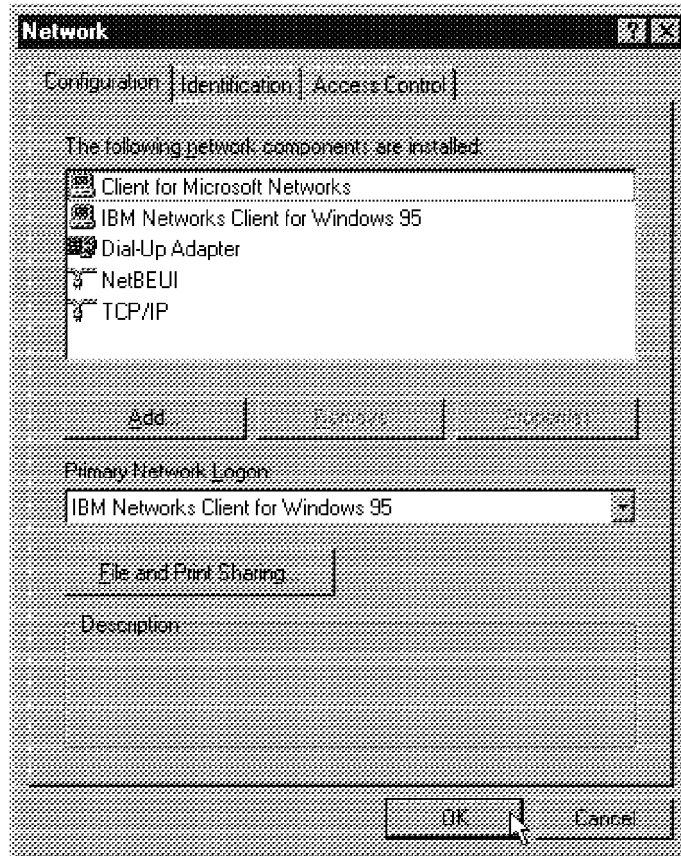
Figure 170. The Dial-Up Adapter is Considered as a Network Adapter

12.8.2.2 The Connection Dependant Settings

To configure the connection profile, right mouse click on the connection icon you created in the previous step and select **Properties** from the pop-up menu. The Remote PPP connection properties notebook is displayed as shown in Figure 171 on page 310. Edit the telephone number to be dialed and other modem settings from here.
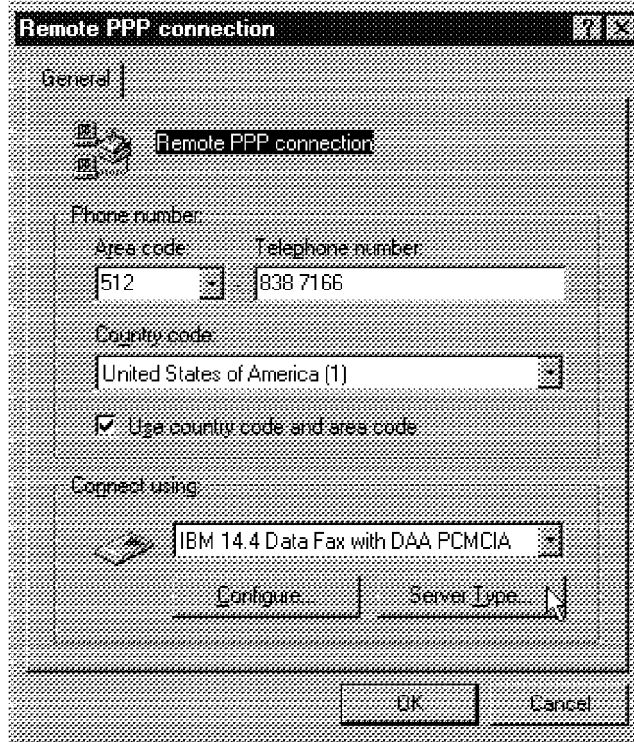
Figure 171. The Dial-Up Networking Connection Properties Notebook

Select the **Server type** button to display more options. Use the Server Types notebook, as shown in Figure 172 on page 311, to enable and disable protocols for the Dial-Up Networking connection and to set other options. PPP is the most widely used connection protocol. PPP enables you to connect to an IBM Enchanced Remote Access Services for OS/2 Warp Server server, IBM 8235 or to a Windows NT server. If you need a SLIP (Serial Line Internet Protocol) connection, install the protocol from the Windows 95 installation CD-ROM first. For more information about IBM Enchanced Remote Access Services for OS/2 Warp Server, see section 7.1, "The Enhanced Remote Access Server for OS/2 Warp Server" on page 83.
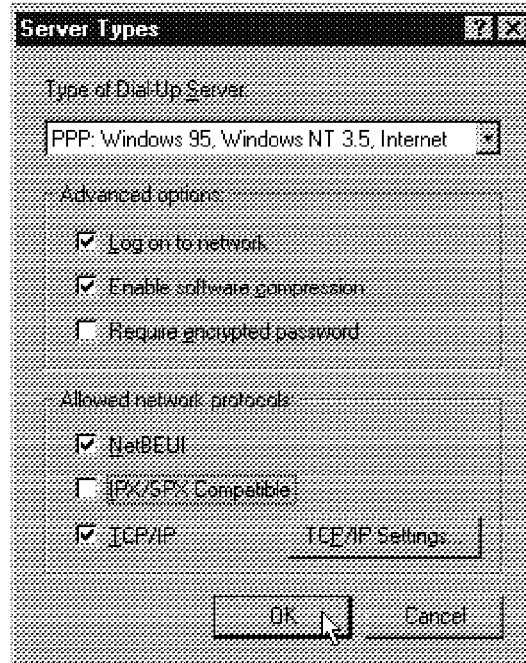
Figure 172. The Server Type Notebook

Options used in the Server Types notebook and their descriptions are listed in Table 18 on page 312.

To connect to IBM Enchanced Remote Access Services for OS/2 Warp Server or to an IBM 8235, select the connection type **PPP**, mark the **Log on to network** check box, and allow at least one protocol. You need to allow either NetBEUI or TCP/IP to log on to the network.

You can use software compression and encryption, but these settings must be set on in the both ends. If the PPP server does not support password encryption, the settings have no effect. If software compression is enabled, the client and the PPP server negotiate the compression type, if any.

When using the configuration shown in Figure 172, the corresponding network setup using the LAN and Dial-UP networking connection is shown in Figure 173 on page 312.
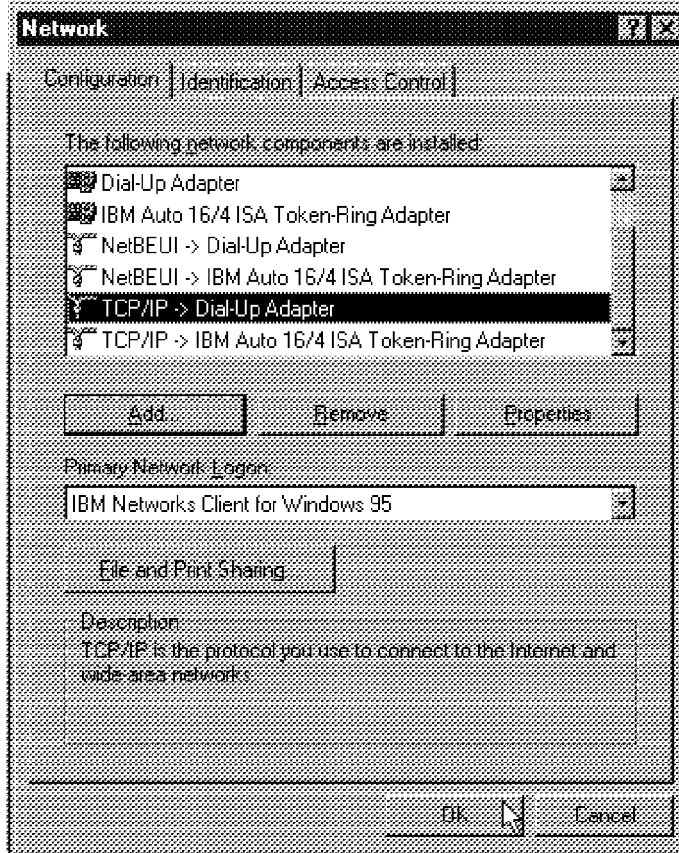
Figure 173. Network Connection Configured with LAN Adapter and Dial-Up Adapter

Depending on the server configuration, you may need to change some settings. All settings in the Server-types notebook are listed in Table 18.

Table 18 (Page 1 of 2). The Server-Types Notebook Options	
Option	**Description**
NRN: NetWare Connect	-
PPP: Windows 95, Windows NT 3.5, Internet	Point-to-Point protocol enables you to make modem connections, for example, to IBM Enchanced Remote Access Services for OS/2 Warp Server or IBM 8235 or to another Windows 95 machine and Windows NT. Almost every Internet provider offers PPP connection for Internet access.
Windows for Workgroups and Windows NT 3.1	-

Table 18 (Page 2 of 2). The Server-Types Notebook Options	
Option	**Description**
Log on to network	If selected, Windows 95 tries to log on the network after the modem connection has been established.
Enable software compression	Specifies whether the information sent or received is packed. Compression is enabled only if both ends support the same type of software compression.
Require encrypted password	If checked, the logon password is sent encrypted over the connection. Valid only if both ends support password encrypting.
NetBEUI	Has to be checked if the NetBEUI protocol is needed. The protocol has to be configured in the Network notebook.
IPX/SPX Compatible	Has to be checked if the IPX/SPX protocol is needed. The protocol has to be configured in the Network notebook.
TCP/IP	Has to be checked if the TCP/IP protocol is needed. The protocol has to be configured in the Network notebook. Use TCP/IP settings button to set configuration if using multiple Dial-Up Networking connections with different IP settings, as described in section 12.8.2.3, "The TCP/IP Settings for the Connection" on page 313.

Note: The PPP server configuration can be set to not allow certain protocols like IPX/SPX or NetBEUI. Make sure that the selected protocol is actually enabled on the server.

12.8.2.3 The TCP/IP Settings for the Connection

The TCP/IP settings must be configured if you are using more than one Dial-Up Networking connection with different IP settings. There can be only one Dial-Up adapter in the network setup meaning that only one IP setting can be defined there. The default behavior for a Dial-Up Networking connection is to read the TCP/IP configuration information from the PPP server. If the server cannot provide this information the configuration is read from the network setup. If you access the LAN and the Internet, you probably need different configurations for the two connections.

Open the TCP/IP Settings notebook as shown in Figure 174 on page 314 by clicking the **TCP/IP settings** button in the Server-Types notebook.
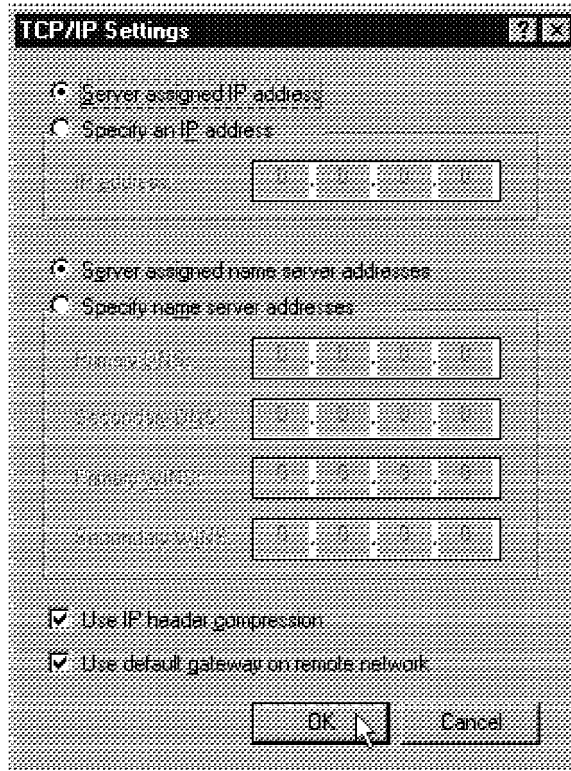
Figure 174. The TCP/IP Settings for the Dial-Up Networking Connection

If you select the Server assigned IP address radio button the IP address is
obtained from the PPP server. If PPP server does not offer an IP addresses,
then the address configured in the network setup for Dial-Up adapter is
used. If you want to set the address manually, select the **Specify an IP
address** button and fill in the IP address to be used.

If you select the Server assigned name server addresses radio button the
DNS and WINS server addresses are obtained from the PPP server. If the
PPP server is not able to provide these addresses, the addresses configured
in the network setup are used. To specify addresses manually, select
Specify name server addresses and fill in the needed addresses. If you do
not configure these settings properly, your TCP/IP connection may fail.

Mark the **Use IP header compression** check box to enable compression for
this connection. You can get more detailed IP status after the connection
has been established by running the WINIPCFG command and selecting the
Dial-Up adapter from the drop-down list.

> **IBM Enchanced Remote Access Services**
>
> The IBM Enchanced Remote Access Services for OS/2 Warp Server
> supports only supports the TCP/IP protocol. If you want to get Internet
> and LAN access, enable NetBIOS over TCP/IP on the OS/2 Warp Servers
> to which you want to have remote access.

If you cannot get the connection to work, start with the modem configuration.
Test and configure your modem by selecting [**Start** — **Settings** — **Control
Panel** — **Modems**]. Select the **Diagnostics** tab, select the modem to be
tested, and click the **More Info...** button. If the modem fails to answer,
check the hardware settings mentioned in the list below:

- Is the port that the modem is using free?
- Is the installed modem driver the right one?
- Is a special initialization string required?
- Is the modem connected to the telephone line correctly?
- Do you have a valid user account on the PPP server?
- Are you running the protocols that are allowed against the server?

If the modem is working correctly but the connection is not established,
check if you have installed and enabled all the necessary protocols to make
the connection. In many situations you need to provide the logon
information for the PPP server to start the connection. The PPP server user
ID and password may be different from your LAN user ID and password.

12.8.2.4 Logging on Using Dial-Up Networking

If you log on to a Windows NT domain using the Dial-Up Networking, you get
the standard Windows Network logon window. Log on as if you were
connected to the network with a network adapter.

If you are using the IBM Networks Client for Windows 95, you must use the
GUI interface to log on the network. After the connection is established,
follow the list below to complete the logon:

1. Select [**Start** — **Programs** — **IBM Networks Client** — **IBM Networks
   Client**] to open the GUI screen.

2. Click on the **Logon** button or use the menu command [**User** — **Log on...**]
   to get the logon window.

3. At the logon window, enter your user ID and password and select the
   domain name to log on to. Click the **OK** button when ready.

The logon process is much slower compared to logon with a network
adapter. All the NetBIOS name registrations, logon assignment handling,

system policy download and profile file execution are executed over a relatively slow telephone line.

Windows 95 Prompting for Network Logon When Remote?

If the IBM Networks Client for Windows 95 is installed, you are prompted for IBM Networks logon every time you start the machine, even if not connected to the network. You can select **Cancel** and make a local Windows 95 logon. This way you can get your personal Windows 95 settings, if the feature is enabled.

12.9 The OEM Service Release 2 of Windows 95

Many PC manufacturers offering pre-installed Windows 95 machines have started using the new OSR-2 version of Windows 95. The new Windows 95 version is available only from OEM vendors on new PC computers.

Identify the Windows 95 version by right-clicking on the **My Computer** icon on the desktop and selecting **Properties** from icon's the pop-up menu. The OSR-2 version version number is `4.00.950B`, the shipping Windows 95 retail version number is `4.00.950`. If you apply the command `VER` from the command line, the corresponding version numbers are `9.00.1111` and `9.00.950`.

The IBM Networks Client for Windows 95 was tested on the OSR-2 version of Windows 95 and the test results were good. An interesting feature of the OSR-2 version is that the NetBIOS API in the TCP/IP tab is now visible to the user and not hidden in the TCP/IP protocol as it used to be.

Go to to the Network Properties notebook and select the **TCP/IP** protocol from the installed component list. As shown in Figure 175 on page 317, the notebook has one extra tab than the earlier release of Windows 95. Networking functions, however, are the same as the earlier release.
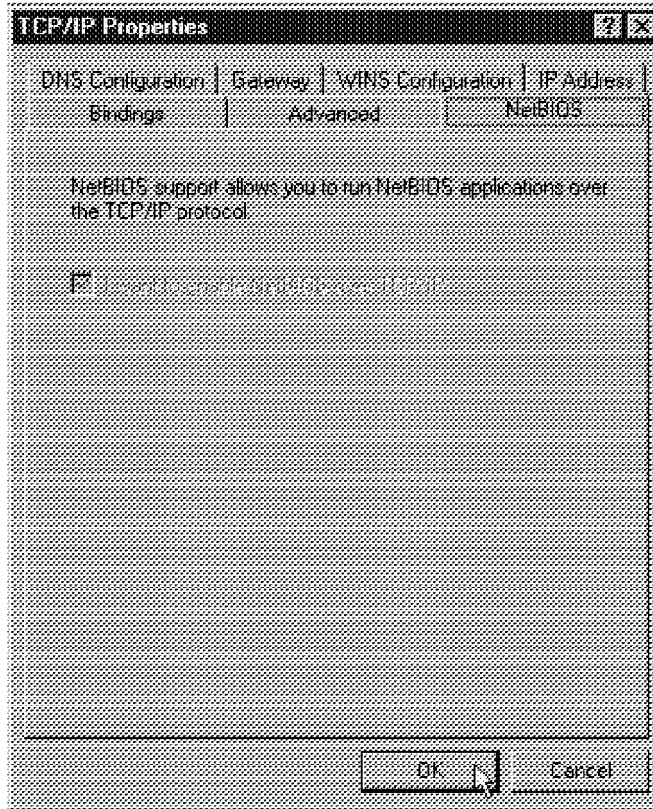
Figure 175. The NetBIOS over TCP/IP Tab

12.10 Dynamic IP Client for Windows 95

IBM recently introduced a new product called the IBM Dynamic IP Client for Windows 95. Dynamic IP integrates the Dynamic Host Configuration Protocol (DHCP) and the Dynamic Domain Name Server (DDNS).

To use IBM Dynamic IP Client for Windows 95, install and configure a network adapter and the TCP/IP protocol. TCP/IP should be configured to use DHCP service to get an IP dynamic address. To see how to install and configure TCP/IP, see section 12.7.5, "The Windows 95 TCP/IP Protocol" on page 284.

DHCP is a client/server protocol that enables you to centrally locate and dynamically distribute configuration information, including IP addresses. If you are not using DHCP, you must define a unique IP address for every computer using the TCP/IP protocol. DHCP makes it possible to pre-define a range of IP addresses, and a DHCP client fetches the configuration information at startup time. This system makes the TCP/IP configuration

much easier because you can centralize the settings to the DHCP server, and avoid most of the manual DNS configuration.

DHCP is based on the Bootstrap Protocol (BOOTP), and it adds the capability of automatically allocating reusable network addresses and distributing additional host configuration options.

DDNS is a protocol that defines extensions to the Domain Name Server (DNS) to enable DNS servers to accept requests to update the DNS database dynamically and securely. These extensions define mechanisms for adding and deleting names and associated resource records.

A DHCP and DDNS server installation and configuration is discussed in detail in the IBM redbook SG24-4602, titled *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*. A brief illustration can be found in 6.1, "Dynamic TCP/IP in OS/2 Warp Server" on page 61.

12.10.1 Dynamic IP Client for Windows 95 Installation

To install Dynamic IP Client for Windows 95, follow the steps below:

1. Insert the Dynamic IP Client for Windows 95 Diskette 1 in drive A:.

2. Select [**Start** — **Run...**].

3. Enter A: SETUP.EXE in the Run dialog box and select **OK** to display the Setup window.

4. Select **OK** in the Information dialog window.

5. Select **Next** in the Welcome window to begin the installation process.

6. Insert the Dynamic IP Client for Windows 95 Diskette 2 when prompted.

7. You can select to view the readme file when the installation is completed.

8. Select **OK** in the Installation is finished window.

9. In the Dynamic IP Information window, enter your computer's host name, TCP/IP domain name and the Primary domain name server name (see Figure 176 on page 319).
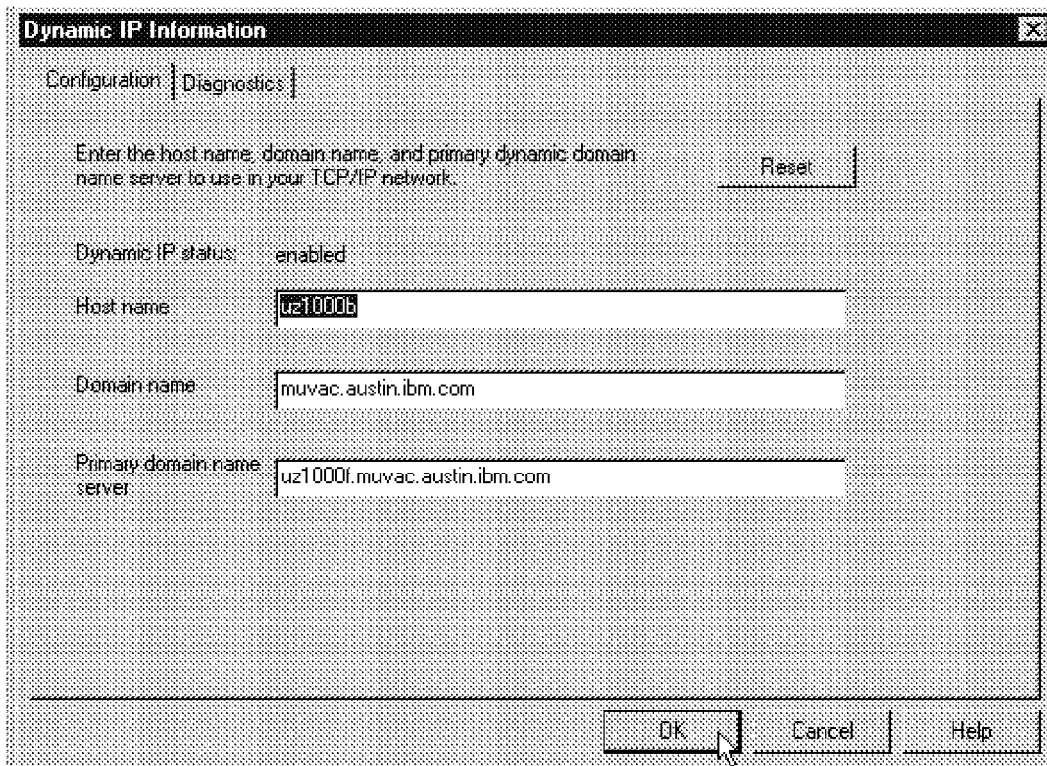
Figure 176. Enter the Host and Domain Names

10. Select **OK** when the settings are somplete and reboot the computer when prompted.

You can change the settings anytime if you select [**Start** — **Programs** — **Dynamic IP Client** — **Settings**]. The menu command gives you the same configuration screen as the installation program.

12.10.2 Removing Dynamic IP Client for Windows 95

The Dynamic IP Client for Windows 95 product can be removed from the Windows 95 configuration at any time. To remove the component, follow the steps below:

1. Select [**Start** — **Settings** — **Control Panel** — **Add/Remove Programs**].

2. Select the **Dynamic IP Client for Windows 95** from the list.

3. Click the **Add/Remove** button.

4. Follow the instructions.

5. Reboot the machine when prompted.

12.10.3 Problem Determination

The IBM Networks Client for Windows 95 is a fully integrated 32-bit Network Provider to the Windows 95 client. If you encounter a problem using IBM Networks Client for Windows 95, the following tests will help you determine if the problem lies in Microsoft code or the IBM code:

1. It should be investigated by Microsoft if:

   a. You can recreate the problem without the IBM Networks Client installed.

   b. The problem is with a network protocol.

   c. The application calls a network API not serviced by the IBM Networks Client for Windows 95.

2. It should be investigated by IBM if it is one of the six IBM unique functions, such as:

   a. Home directories

   b. Logon assignments

   c. Aliases

   d. Shared applications

   e. Directory limits (DASD limits)

   f. LAN Server administration

Chapter 13. IBM Networks Client for Windows NT

This chapter describes the installation and configuration of the IBM Networks Clients for Windows NT:

- IBM Networks Coordinated Logon Client for Windows NT 4.0
- IBM Networks Primary Logon Client for Windows NT 4.0

in a plain NetBEUI and TCP/IP environment, dynamic TCP/IP:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Server (DNS)
- NetBIOS Names Server (NBNS) / Windows Internet Name Server (WINS)

and Remote Access Services using the Point-to-Point (PPP) protocol dialing in to an OS/2 Warp Server Remote Connection Server.

13.1 Client Overview

There are two OS/2 Warp Server clients available for Windows NT Workstation:

- IBM Networks Coordinated Logon Client for Windows NT 4.0

- IBM Networks Primary Logon Client for Windows NT 4.0

The differences between the two clients are summarized in Table 19:

Table 19 (Page 1 of 2). IBM Network Clients for Windows NT — Summary	
Primary Logon Client	**Coordinated Logon Client**
OS/2 Warp Server domains	Windows NT Workstation clients, Windows NT Server and OS/2 Warp Server domains.
NetBEUI, NetBT	NetBEUI, NetBT

Table 19 (Page 2 of 2). IBM Network Clients for Windows NT — Summary	
Primary Logon Client	**Coordinated Logon Client**
OS/2 Warp Server domain	Windows NT Workstation clients or Windows NT Server, OS/2 Warp Server domain.

Note:

1. NetBT is Microsoft's abbreviation for NetBIOS over TCP/IP (TCPBEUI).

2. There is no need for a Windows NT Server to validate a logon request. The logon request can be validated by the user's Windows NT Workstation, and should always do so in a OS/2 Warp Server network.

13.2 IBM Networks Coordinated Logon Client for Windows NT 4.0

The IBM Networks Coordinated Logon Client is intended for Windows NT workstations in a mixed LAN environment, consisting of Windows NT and OS/2 Warp Server domains. A separate logon validation on the OS/2 Warp Server domain is performed, in addition to the normal Windows NT logon validation.

This section describes the installation procedure for the IBM Networks Coordinated Logon Client for Windows NT 4.0, but most of the installation steps also apply to the IBM Networks Primary Logon Client (specifics for the latter are discussed in section 13.3, "IBM Networks Primary Logon Client for Windows NT 4.0" on page 332). Basic GUI features and functions are covered in the GUI sections, 9.1, "Common GUI Features and Functions" on page 95 and 13.6, "Client-Specific Features and Functions" on page 346.

13.2.1 Installation

Both Windows NT clients are shipped together as a ZIP file downloadable from the IBM Software Web site mentioned in the Preface of this book. Unpack it with an appropriate tool to an empty 1.44MB diskette or to a directory. We discuss two methods of installation.

> **Tip**
>
> The README files (README.1ST and README.2ND) contain all information needed for installing the appropriate Windows NT client. Therefore, we recommend having a print-out of it handy when installing.

13.2.1.1 Requirements

Ensure that the following components are installed and activated:

- The Microsoft Workstation service

- An appropriate network adapter device driver

- A supported protocol (NetBEUI or TCP/IP)

Verify this by opening the **Network** icon in the Control Panel. Select the **Services** and **Protocol** tabs respectively and view the installed components. If no protocol of the above is installed, add those now.

13.2.1.2 Installing from Diskette

```
┌─ Tip ─────────────────────────────────────────────────────────┐
│                                                                │
│  Online help is available in this setup stage; press F1 while the cursor is │
│  in an entry field.  Help text for that field is displayed.    │
│                                                                │
└────────────────────────────────────────────────────────────────┘
```

Unpack the ZIP file to an empty 1.44MB diskette, then proceed as follows:

1. Log on to the system as a user with administrator privileges.

2. Click on [**Start** — **Settings** — **Control Panel** — **Network**]. The Network notebook is displayed, as shown in Figure 177.
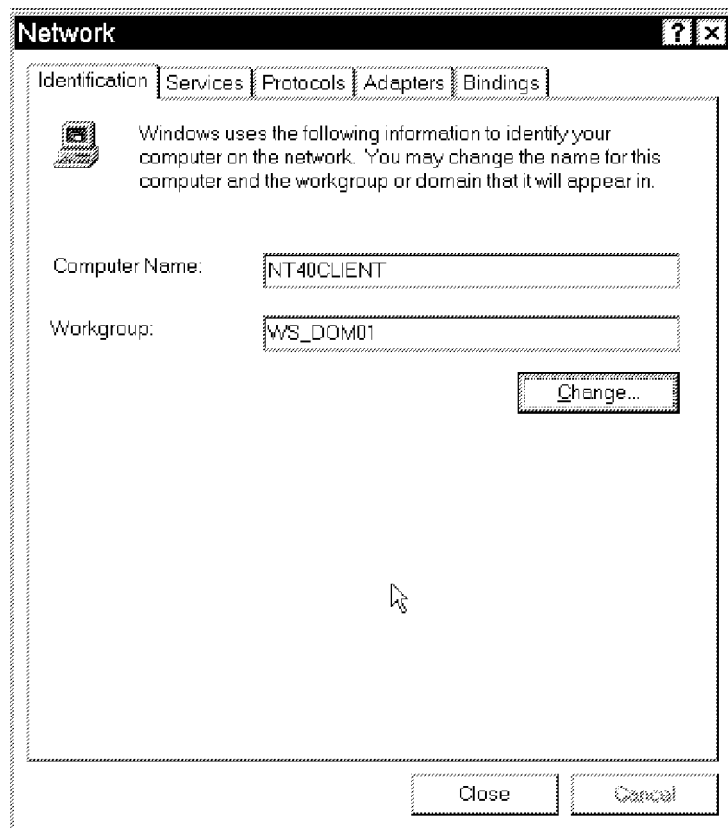
Figure 177. The Network Configuration Menu

3. Click on the **Services** tab.

4. Click on the **Add...** button. The Select Network Service window is displayed, as shown in Figure 178 on page 324.

Figure 178. Selecting Network Services to Install

5. Click on the **Have Disk...** button. The Insert Disk window is displayed.

6. Insert the **IBM Networks Coordinated Logon Client for Windows NT** diskette in the A drive, then click **OK**. The OEM Option window is displayed, as shown in Figure 179 on page 325.
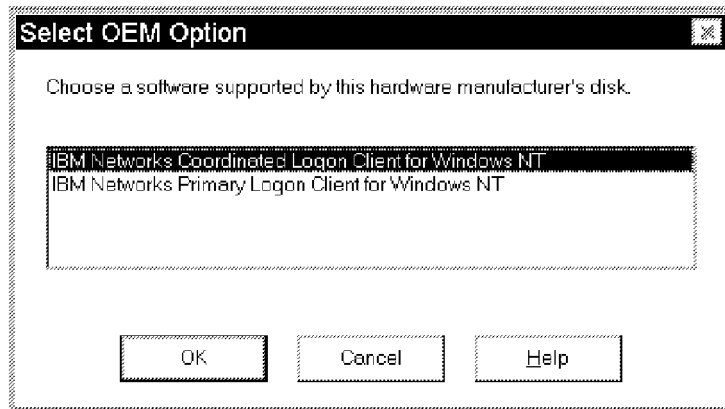
Figure 179. Selecting the OEM Option

7. Select **IBM Networks Coordinated Logon Client for Windows NT** and then click **OK**. The files are copied and the Properties notebook is displayed, as shown in Figure 180.

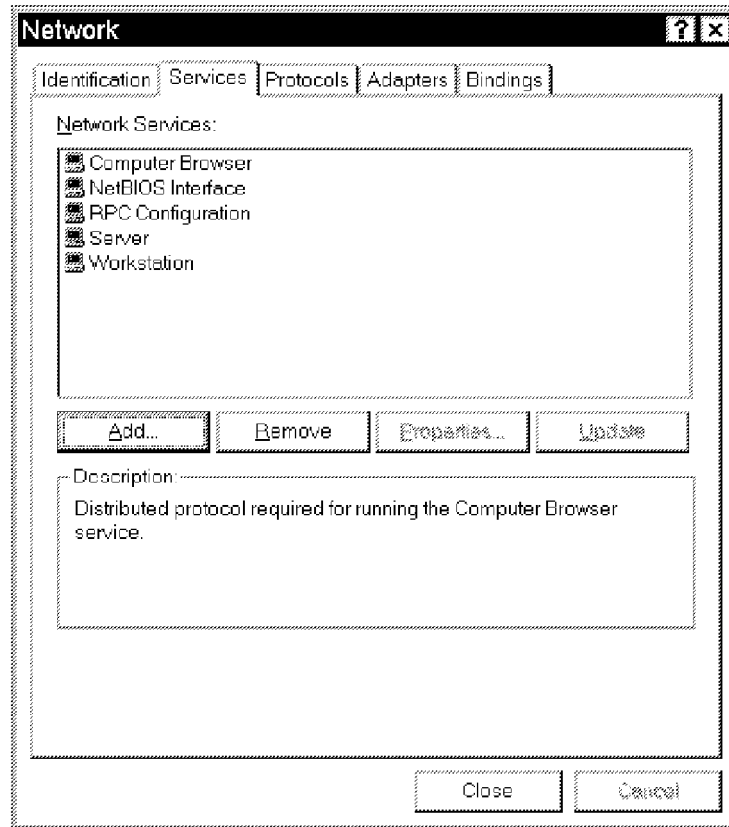8. Click on the **General** tab.
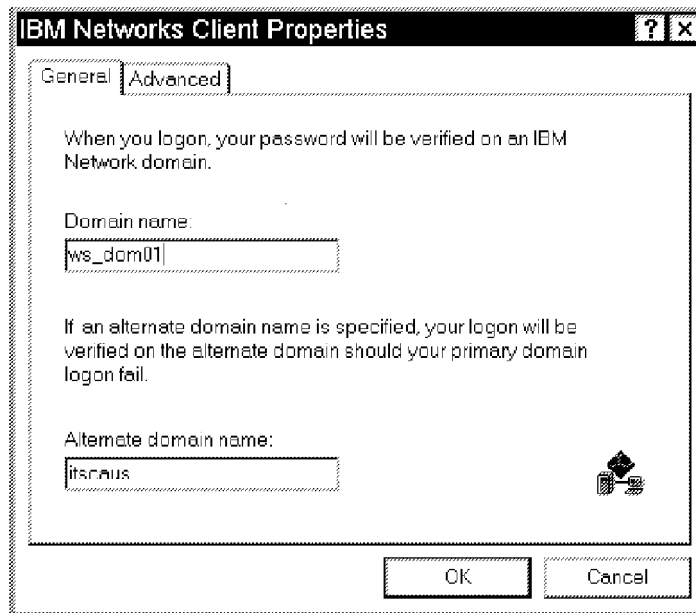
Figure 180. The Network Configuration Menu

9. In the Domain name field, type the name of the default logon IBM OS/2 Warp Server domain.

10. If you want to use an alternate domain, type the name of the alternate domain in the Alternate domain name field. The logon vill be validated on this domain if the default domain is unavailable.

Note: Entry fields are case-sensitive in Windows NT. Check with the LAN Adminstrator if uppercase or lowercase should be used.

11. Click on the **Advanced** tab. The IBM Networks Client Properties - Advanced window is displayed, as shown in Figure 181.
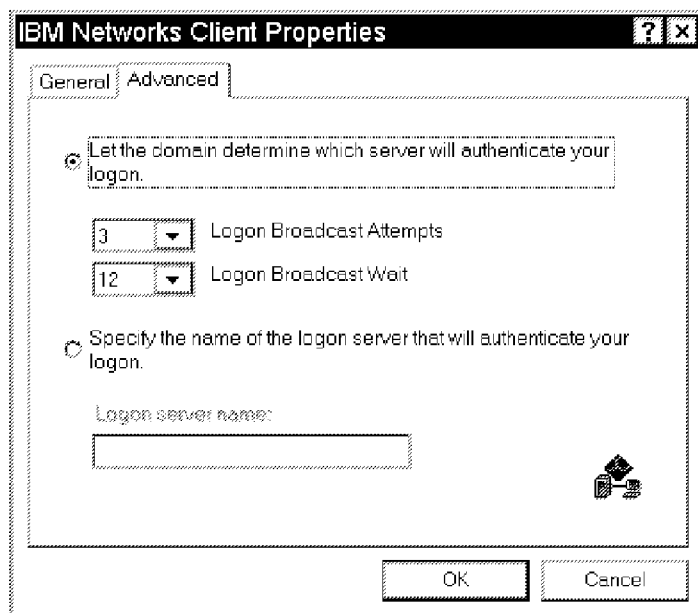
Figure 181. The Network Configuration Menu

12. If you select the button to allow the domain to determine which server will validate the logon, the following settings are affected:

   • Logon Broadcast Attempts

     - Indicates the number of logon broadcast attempts made when trying to connect to the logon server.

   • Logon Broadcast Wait

     - Indicates the number of seconds this client waits for a response after broadcasting a logon request.

13. If you select the button to specify the name of the logon server, enter the NetBIOS name of the logon server.

14. Click **OK**. The Network notebook is displayed, as shown in Figure 182 on page 327.
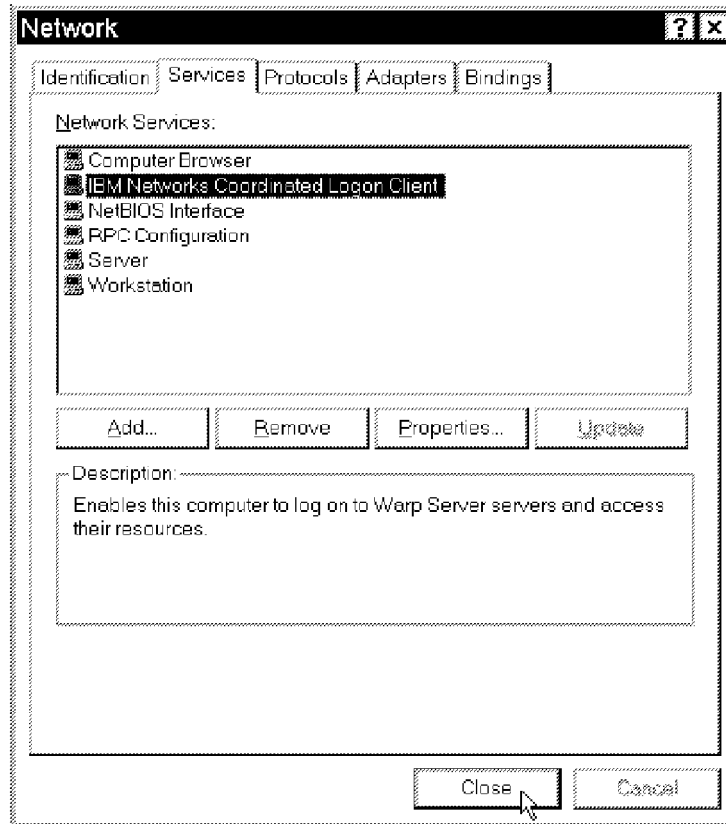
Figure 182. The Network Menu after Installation

15. Select **Close** and a setup message is displayed stating that the user account must be synchronized on the Windows NT and OS/2 Warp Server domains, as shown in Figure 183. Press **OK** to continue.
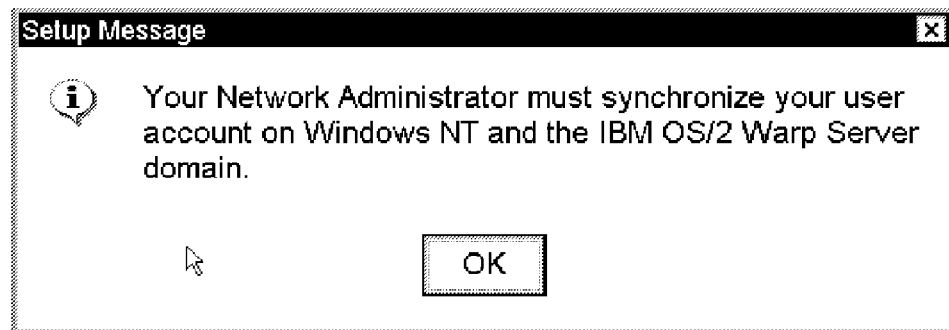
Figure 183. Setup Message Information

Check that the user ID and password are identical on both domains. Again, be aware of the case-sensiveness of Windows NT; ensure that the password is entered correctly. If in doubt, contact the LAN Administrator for assistance.

16. You are prompted to restart the system. Click **Yes**.

17. Click [**Start** — **Programs** — **IBM Networks Client (Common)** — **IBM Network Client**]. The GUI is displayed as shown in Figure 184.
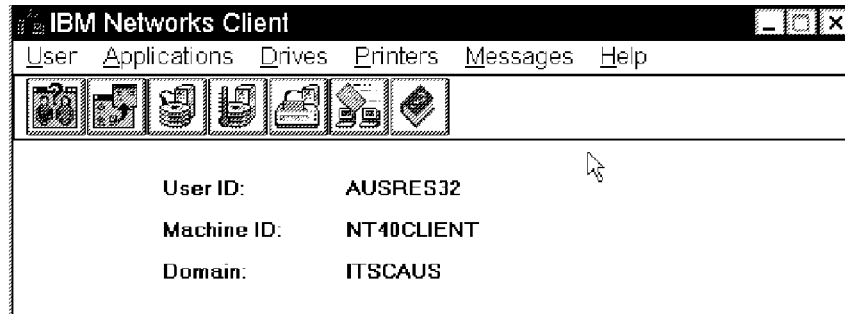
Figure 184. IBM Networks Client Graphical User Interface

> ─ **Tip** ─
>
> It is useful to add the client's GUI to the Windows NT desktop for the sake of convenience. Open **Desktop properties**, select [**New** — **Shortcut**], enter WDLS.EXE in the entry field and click [**Next** — **Finish**]. Now the IBM Networks Client GUI is an object on the desktop.

13.2.1.3 Installing over a Network or from a Local Drive

Instead of unpacking the ZIP file to a diskette, unpack it to a directory of your choice. The source directory can be located on your local hard drive or on a network drive.

Basically, this installation method is really the same. The only difference is in item 6 on page 324. Here, type the path to the source directory instead of inserting a diskette into the A: drive (See Figure 185). Alternatively, you can use a UNC name without a drive letter.
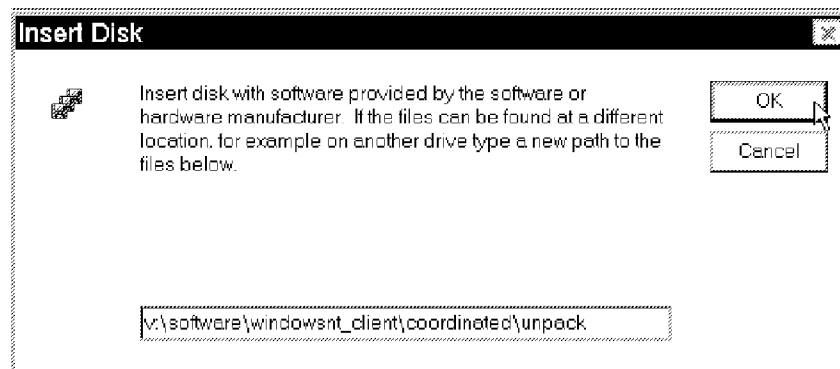
Figure 185. Specifying a Source for Installing the Client

13.2.2 Configuring IBM Networks Coordinated Logon Client for Windows NT 4.0

During installation, the IBM Networks Coordinated Logon Client is configured for NetBEUI use (see 13.2.1.2, "Installing from Diskette" on page 323, steps 9 to 13). To use additional protocols, further configuration is needed.

13.2.2.1 TCP/IP Support

Normally, you also select TCP/IP support when setting up Windows NT. This prompts you to provide the necessary TCP/IP configuration parameters during the setup stage of the Windows NT installation. To change the initially entered information, open [**My Computer** — **Control Panel** — **Network** — **Protocols** — **TCP/IP Protocol** — **Properties**], as shown in Figure 186.
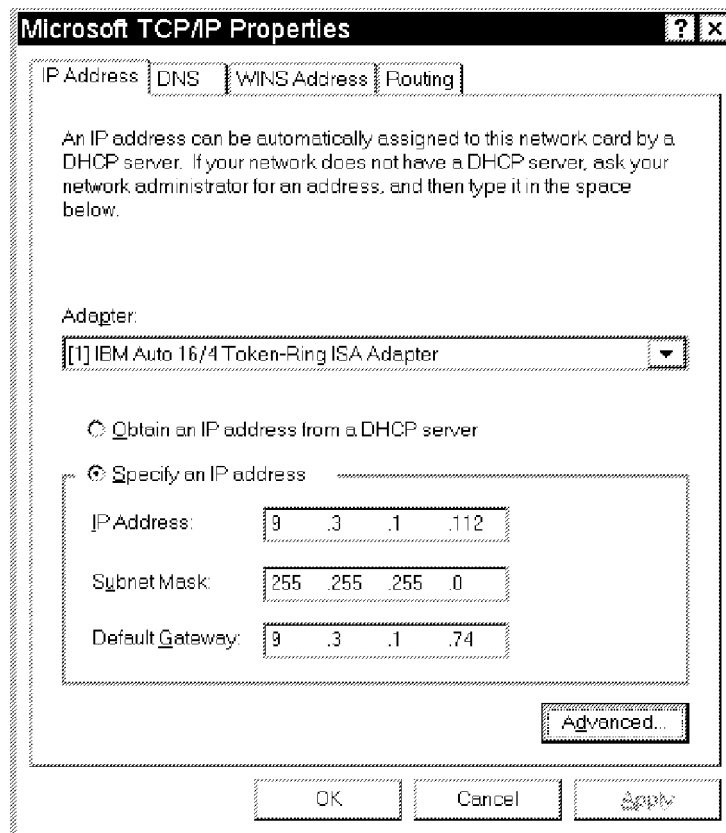
Figure 186. TCP/IP Properties

There are a few alternatives to consider, for example:

- Use of static or dynamic IP address

- Use of WINS protocol

These options are common to Windows NT and Windows 95. They are discussed in detail in sections 12.7.5, "The Windows 95 TCP/IP Protocol" on page 284 and 12.7.11, "Configuring TCP/IP" on page 299. To configure Windows NT to use dynamic IP addresses from an OS/2 Warp Server DHCP/DDNS, see section 13.4, "LAN Connection with Dynamic IP Address" on page 340.

13.2.3 Applying Windows NT Service Packs

Before applying a service pack on a Windows NT workstation that has the IBM Networks Coordinated Logon Client installed, do the following:

- Remove the client (see section 13.2.4, "Removing the IBM Networks Coordinated Logon Client" for details).

- Install the service pack on Windows NT.

- Install the client again.

13.2.4 Removing the IBM Networks Coordinated Logon Client

To remove the IBM Networks Coordinated Logon Client for Windows NT 4.0, follow the steps below:

1. Logon locally to the system using a user ID with administrator privileges.

2. Click [**Start** — **Settings** — **Control Panel** — **Network**].

3. Select the **Services** tab and click **IBM Networks Coordinated Logon Client**. See Figure 187 on page 331.

Figure 187. Removing the IBM Networks Coordinated Logon Client

4. Click **Remove**, then confirm and close. See Figure 188.

Figure 188. Confirmation Window

5. Shut down and reboot. Logon to the system using the same user ID as
   in step 1 on page 330 to complete the removal of the IBM Networks
   Coordinated Logon Client. The Windows NT Registry is updated and the
   product files are removed.

Note: Failure to log on a second time with administrator privileges causes a "File not found" error message to be displayed every time the system is booted. This is c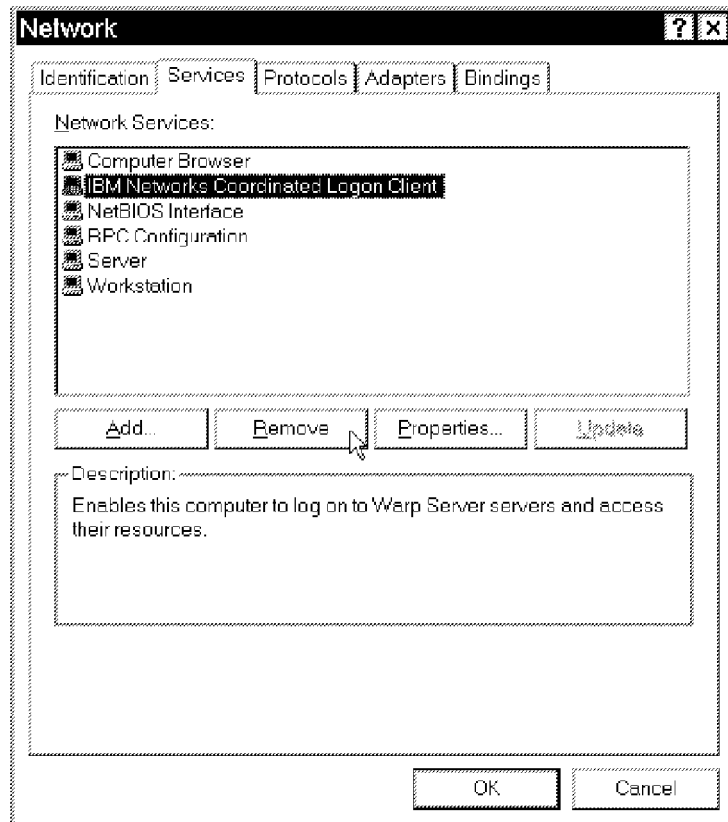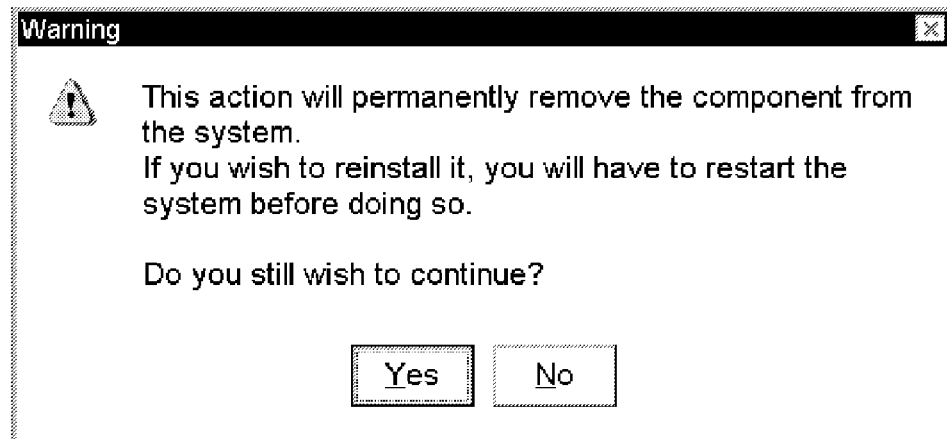aused by Registry entries and can not be properly cleared . Log on on with a user name that has administrator privileges to clear this error message for subsequent reboots.

13.3 IBM Networks Primary Logon Client for Windows NT 4.0

The IBM Networks Primary Logon Client has the same GUI functions as the IBM Networks Coordinated Logon Client. The main difference is in how it handles the logon process. This client is recommended for Windows NT workstations operating in a LAN environment consisting of OS/2 Warp Server domains only. If there are Windows NT domains also, the IBM Networks Coordinated Logon Client (discussed in chapter 13.2, "IBM Networks Coordinated Logon Client for Windows NT 4.0" on page 322) should be considered.

Note: The IBM Networks Primary Logon Client requires Version 4.0 of Windows NT. Version 3.x is not supported.

13.3.1 Preparing the System

The IBM Networks Primary Logon Client implements a vital change to the Windows NT Registry, discussed in section 13.3.3, "Logging on to a OS/2 Warp Server Domain" on page 336, item 2. If the user is allowed to make unrestricted local configuration changes, you need to ensure that a local user ID with administrator privileges exists on the Windows NT workstation, prior to installing the IBM Networks Primary Logon Client. If this is not the case, you must create one.

13.3.2 Installation

The installation procedure is similar to the IBM Networks Coordinated Logon Client (discussed in section 13.2.1, "Installation" on page 322). Here, we focus on the differences in configuring the client during installation. We recommend having a print-out of the README.2ND handy while installing.

Note: If any prior version of the IBM Networks Primary Logon Client exists on the target system, it must be removed before installing this version. For detailed instructions, see section 13.3.8, "Removing the IBM Networks Primary Logon Client" on page 339.

13.3.2.1 Configuring IBM Networks Primary Logon Client

After the initial installations steps, you are prompted to configure the IBM Networks Primary Logon Client as discussed below.

> **Tip**
>
> Online help information is available, just press **F1** when needed.

1. Select the **General** tab, as shown in Figure 189. Type the name of either:

   - the OS/2 Warp Server domain that validates the logon.

   - the cell that validates the logon. This is the only method to designate the authentication cell. For domains, this option can be used also.

     Note: The network discovery is done as part of the configuration process. No user action is required to initiate this. The list contains all SMB type domains discovered. It does not discover DCE cells.
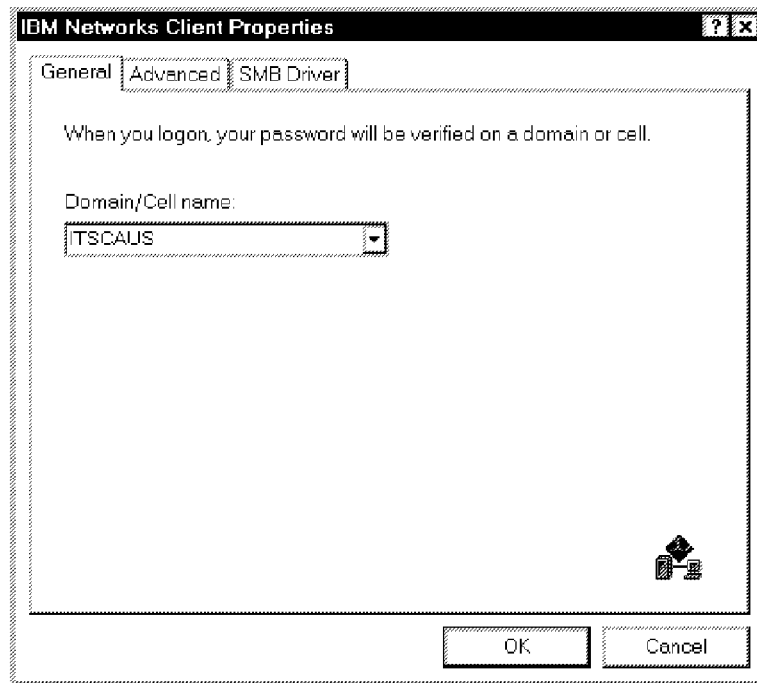
Figure 189. Specifying a Logon Domain/Cell

   Note: Case-sensitivity applies, check with the LAN Administrator.

2. Select **Advanced**; add other domains and/or cells that might be selected, see the example in Figure 190 on page 334. You can also customize the logon panel by enabling/disabling:

   - Domain name searching (allows you to browse the network for available OS/2 Warp Server domains).

- Domain name entry (allows you to type the name of a specific OS/2 Warp Server domain in the entry field; again, mind the case-sensivity).

If both options are disabled, the user can only select the alternatives shown in the logon panel's list box.
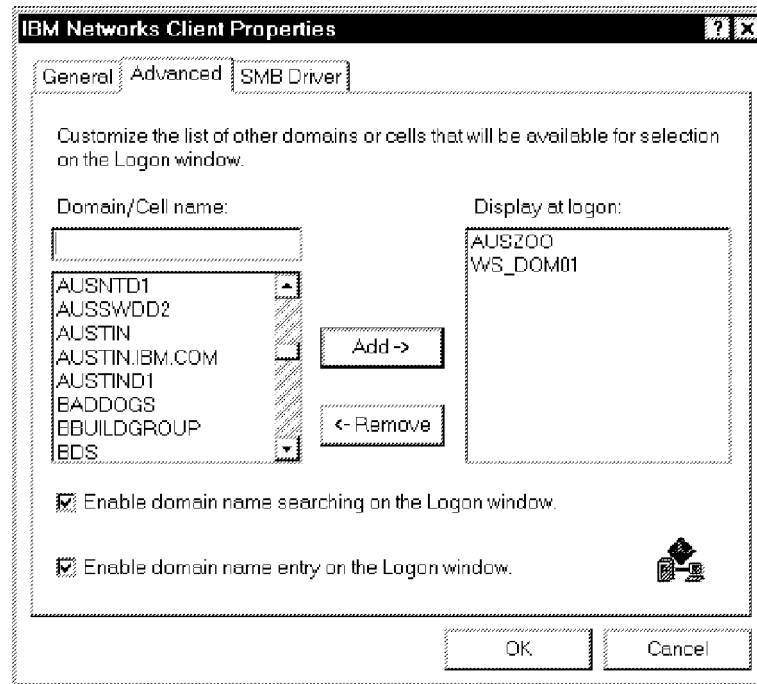
Figure 190. Advanced Configuration Options

3. Select **SMB Driver**; here, a secondary logon validation can be enabled, see Figure 191 on page 335. It is performed if the default logon domain is unavailable. When enabling this option, the warning message shown in Figure 192 on page 335 is displayed. Press **OK**.
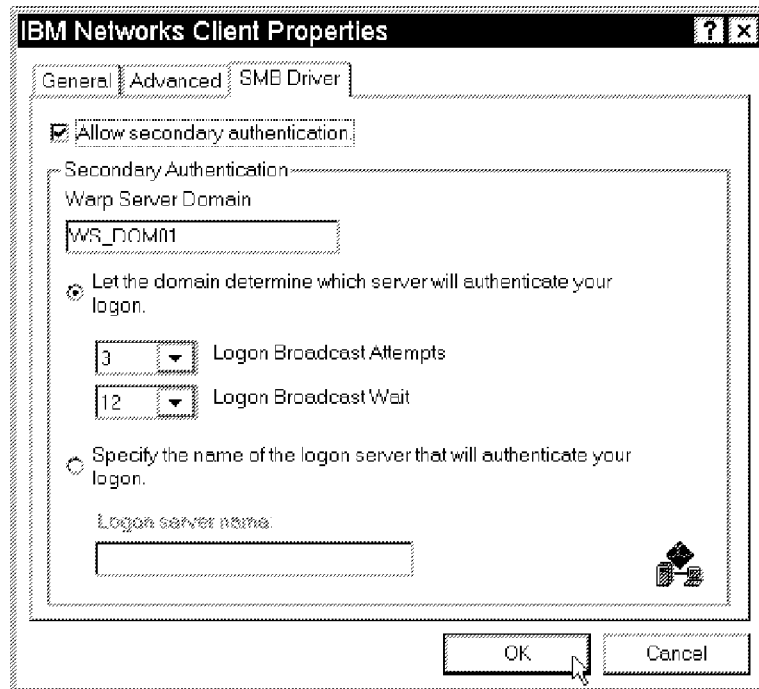
Figure 191. Enabling Secondary Logon Validation
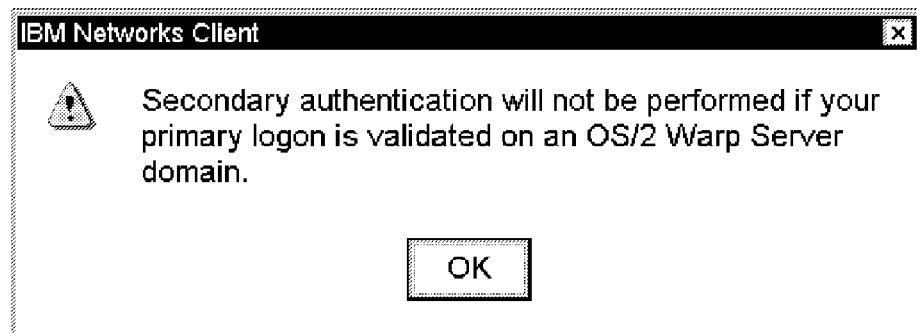
Figure 192. The Secondary Logon Validation Dialog Box

Notes:

a. If the Let the domain determine which server authenticate your logon radio button is selected, the Logon Broadcast Attempts and Logon Broadcast Wait can be configured. Note that setting these values too low can result in the logon not having enough time to complete.

b. If the Specify the name of the logon server that will authenticate your logon radio button is selected, this value overrides the domain values configured on the General tab.

13.3.3 Logging on to a OS/2 Warp Server Domain

The IBM Networks Primary Logon Client will brings a few changes to the Windows NT Registry. The most obvious change pertains to the logon process. The logon sequence and related security issues are discussed below.

13.3.3.1 The Logon Sequence

There is a new group, Roaming Users, created to allow the IBM Networks Primary Logon Client to control how user accounts are handled during logon. For accounts in the Roaming Users group (accounts created dynamically by the IBM Networks Primary Logon Client are automatically added to this group) the following applies:

- They are removed from any groups they are a member of prior to logon (except for the RoamingUsers group).

- They are added to their domain or cell groups.

- Their password is automatically synchronized with their network password during the logon process (if necessary).

For accounts that are not in the Roaming Users group:

- The IBM Networks Primary Logon Client does not modify their group membership.

- Their passwords are not synchronized with their network passwords if they become unsynchronized.

Installing the IBM Networks Primary Logon Client does not migrate user accounts to become Roaming Users accounts. If resource access is based on local group membership, access rights must be changed to include the domain or cell groups of which the user is a member.

Post-configuration is done by the client the next time the system starts up after installing the IBM Networks Primary Logon Client:

1. An OS/2 Warp Server logon panel is displayed instead of the normal Windows NT logon panel. Provide the necessary logon information and press **Enter**. The logon is validated by the OS/2 Warp Server domain controller, and appropriate access is granted. The Windows NT Desktop is now available.

   Note: The appearance and functionality of the logon panel is dependant on how it is customized during installation. See topic 13.3.2.1, "Configuring IBM Networks Primary Logon Client" on page 332, step 2.)

2. The previous privileges of the user ID are replaced by privileges defined in the OS/2 Warp Server domain, that is, all local privilege definitions for this user ID are changed. The implications of this are discussed in section 13.3.1, "Preparing the System" on page 332.

13.3.4 Group Mapping

Group mapping allows you to configure the IBM Networks Primary Logon Client for Windows NT 4.0 to add members of a domain group to a specified local group during logon. To add a group mapping, follow these steps:

1. Add the "GroupMapping" key to the workstation's registry if it is not already present.

   a. Start REGEDT32.EXE.

   b. Select the **HKEY_LOCAL_MACHINE** window.

   c. Double-click on **SYSTEM**.

   d. Double-click on **Services**.

   e. Double-click on **IBMNeTNT**.

   f. From the Edit menu, click on **Add Key**.

   g. Set the key name to **GroupMapping**.

   h. Click on the **OK** button.

2. Click on the **GroupMapping** key.

3. From the Edit menu, click on **Add Value**.

4. Set the value name to the name of the domain group. For example, WSDOM_ADMINS is the name of the ADMINS group in domain WSDOM.

5. Data type should be REG_SZ.

6. Click on the **OK** button.

7. In the String Editor dialog, enter the name of the local group that you want members of the domain group to be added to. For example, Administrators would give members of the WSDOM_ADMINS group local administrator rights.

8. Click on the **OK** button.

9. Close REGEDT32.

The next time someone performs a logon, ADMINS from the WSDOM domain will have administrative rights on the local workstation (based on our example). No reboot is required for changes to the GroupMapping key to take effect.

Note: Steps 2-8 can be followed to add new group mappings at any time.

13.3.5 How to Change Passwords

The method for changing the password is as follows:

1. Press Ctrl-Alt-Del on the Windows NT desktop. The Windows NT Security window is displayed.

2. Click on **Change Password...**.

3. In the Change Password window, select the server name and domain you want to change the password.

4. Type the old, new and confirm passwords and click **OK**.

This changes the password at the authentication location (server at which you were authenticated). No actions are required on the dynamically created local NT user account.

13.3.6 Logon Error Messages

If you see the following message, a timeout occurred processing the logon request:

```
Logon failed (rc = 258)
```

If you see the following message:

```
The system could not log you on.  Your network account and password
are correct, but your local account password is out of sync.  Contact
your system administrator to synchronize your passwords.
```

The local account is not marked as a roaming user (see 13.3.3.1, "The Logon Sequence" on page 336). This message occurs if:

- the local password is not the same as the network password
- the local account has expired or been disabled
- the local password has expired

To correct the problem, the OS/2 Warp Server Administrator must either:

1. Include the user ID to the Roaming User group.
2. Synchronize the network and local password for the user, or reenable the account.

13.3.7 Applying Windows NT Service Packs

Before applying a service pack on a Windows NT workstation that has the IBM Networks Primary Logon Client installed, do the following:

1. Remove the IBM Networks Primary Logon Client (see section 13.3.8, "Removing the IBM Networks Primary Logon Client" on page 339).

2. Install the service pack on Windows NT.

3. Reinstall the IBM Networks Primary Logon Client.

   Note: One reason for reinstalling the IBM Networks Primary Logon
   Client is that Microsoft Service Packs usually replace the
   NET.EXE file (that is IBM's NET.EXE file; Microsoft's NET.EXE file
   was renamed to NETNT.EXE by the IBM Networks Client
   installation program).

13.3.8 Removing the IBM Networks Primary Logon Client

Follow these steps in order to remove the IBM Networks Primary Logon
Client:

1. Logon locally to the system, using an use ID with adminstrator privileges
   (otherwise, access is not granted to the appropriate system files).

2. Click [**Start** — **Settings** — **Control Panel**], open **Network** and select the
   Services tab.

3. Select **IBM Networks Primary Logon Client** and click **Remove** as
   indicated in Figure 193.
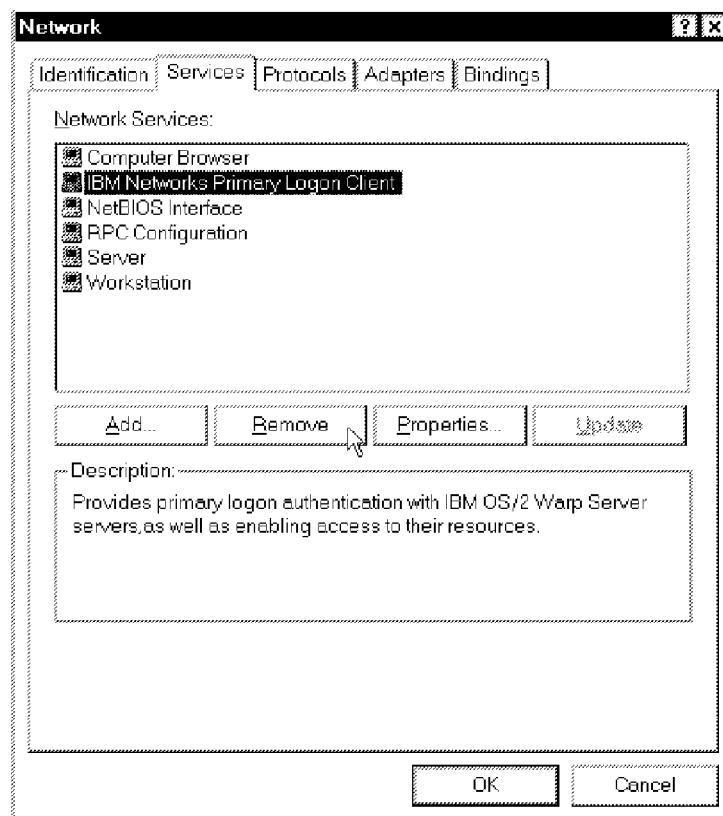
Figure 193. Removing the IBM Networks Primary Logon Client

4. Click the **Yes** button on the confirmation panel, then close the Network window.

5. Restart the workstation and log on to the system using the same user ID as in step 1 on page 339. The IBM Networks Primary Logon Client files are removed and the Windows NT Registry is updated.

13.4 LAN Connection with Dynamic IP Address

Windows NT can work with the DHCP servicer that comes with the OS/2 Warp Server product. Setting up a Windows NT Workstation for use in OS/2 Warp Server DHCP environments is a fairly straight-forward operation. To begin, change the Windows NT TCP/IP configuration as follows:

1. Logon locally to your system, using an user ID with administrator privileges.

2. Click [**Start** — **Settings** — **Control Panel**] and double-click **Network**.

3. Select [**Protocols** — **TCP/IP Protocol**] and click on the **Properties** button; the panel shown in Figure 194 is displayed:
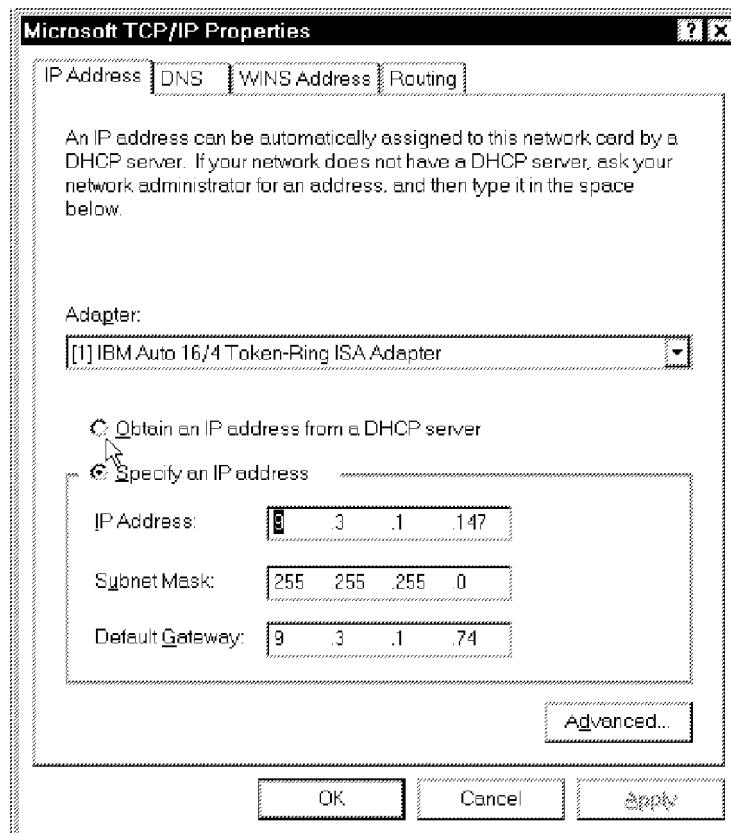
Figure 194. TCP/IP Properties — Changing the Configuration

4. Select Obtain an IP address from a DHCP server radion button. A warning message is displayed, as shown in Figure 195 on page 341. Click **Yes**.
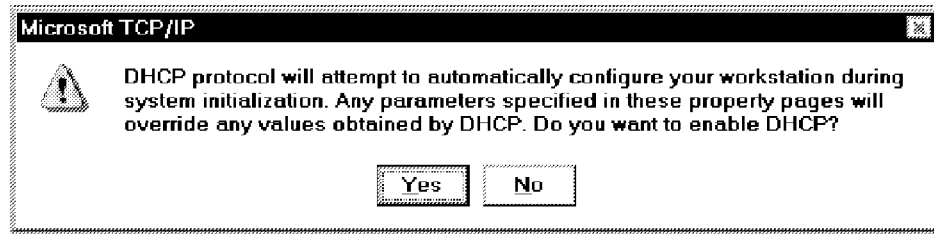
Figure 195. Microsoft TCP/IP — Warning Message

5. Provide other parameter values as instructed by your OS/2 Warp Server administrator and press **OK** when done. You are now set for using a dynamic IP address provided by an OS/2 Warp Server.

13.4.1 Name Resolution through NetBIOS Name Serving

There are a couple of issues to deal with when setting up Windows NT TCPBEUI clients in an OS/2 Warp Server LAN. The general concepts are covered in section 12.7.5.1, "NetBIOS Over TCP/IP" on page 285. Set up your Windows NT client by changing the TCP/IP configuration as follows:

1. Click [**Start** — **Settings** — **Control Panel**] and open **Network**.

2. Select [**Protocols** — **TCP/IP Protocol**] and click **Properties**.

3. Select the **WINS Address** tab and type the IP address of the WINS or NTS' Shadow (see 5.1, "The Shadow NetBIOS Name Server" on page 47) server to be used, as indicated in Figure 196 on page 342.
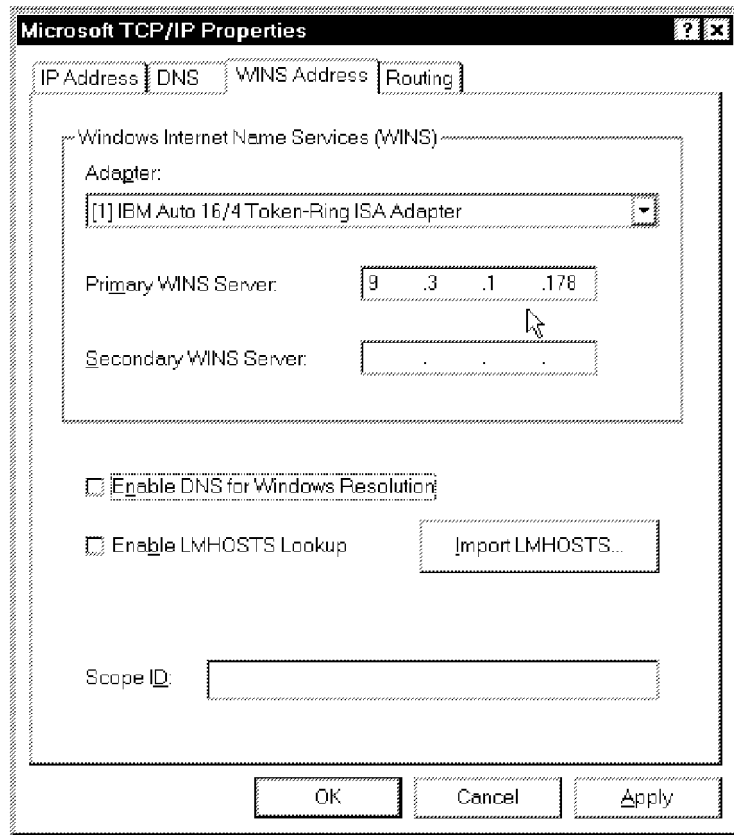
Figure 196. TCP/IP Properties — Changing the Configuration

4. When complete, save your changes. Exit and restart your system.

13.4.1.1 NetBIOS Names Resolution Order B-Node

If Windows NT 4.0 is configured for B-node operation, that is, no WINS configuration is done at your client, NetBIOS name resolution is achieved in the following order:

1. NetBIOS name cache

2. NetBIOS name server

3. IP subnet broadcast

4. Static LMHOSTS file

5. Static HOSTS file

6. DNS server

13.5 LAN Connection through Point-to-Point Protocol

This section describes how to set up your Windows NT Workstation for remote LAN connection through Point-to-Point Protocol (PPP) to an OS/2 Warp Server domain.

13.5.1 Overview

There are quite a few steps to go through to set up a workstation for communicating through PPP, including install and configuring the Remote Access Support (RAS). A properly set-up IBM Enhanced Remote Access Services Connection Server for OS/2 Warp Server (see 7.1, "The Enhanced Remote Access Server for OS/2 Warp Server" on page 83 for more details) must be available for connection.

13.5.1.1 Prerequisites

If you did not select RAS when installing the Windows NT Workstation, you must add it now; before proceeding ensure that the following items are installed/configured:

- An approved modem
- TCP/IP support
- A valid user ID on the OS/2 Warp Server Remote Connection Server
- A valid user ID on the OS/2 Warp Server domain you want to use

13.5.2 Configuring the Workstation

Assuming that RAS was not selected at installation time, the list below details installing and setting up RAS:

1. Ensure that your:

   - Modem is connected and configured
   - Windows NT CD/Install directory is accessible

2. Open **My Computer**, select **Dial-Up Network** and press **Enter**.

3. The installation programs starts and required files are copied from the Windows NT CD/Install directory. You are then prompted to provide relevant input parameters on the following windows, see examples below (Windows NT online help is available throughout).
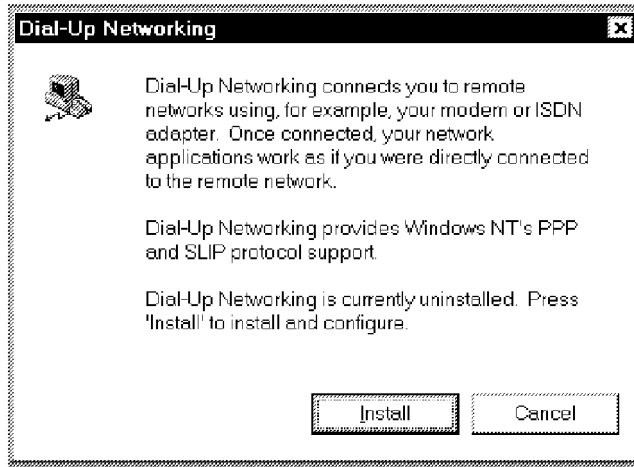
Figure 197. Dial-Up Networking — Installing
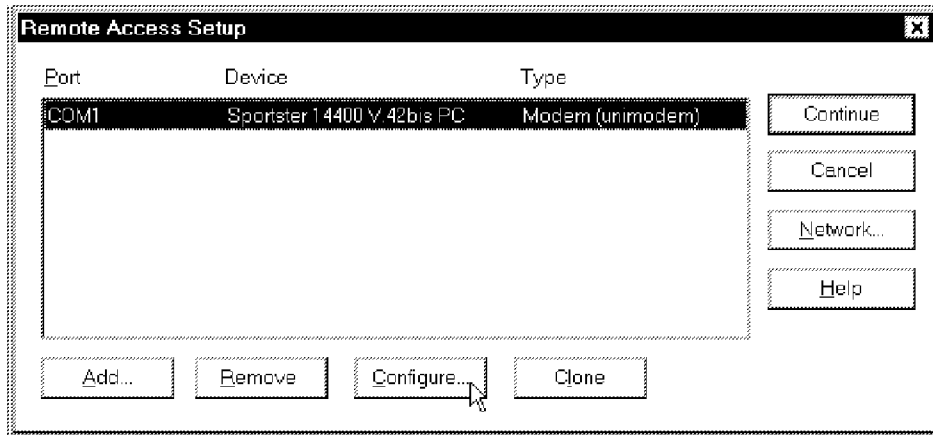
Figure 198. Remote Acess Setup — Configuring the Modem
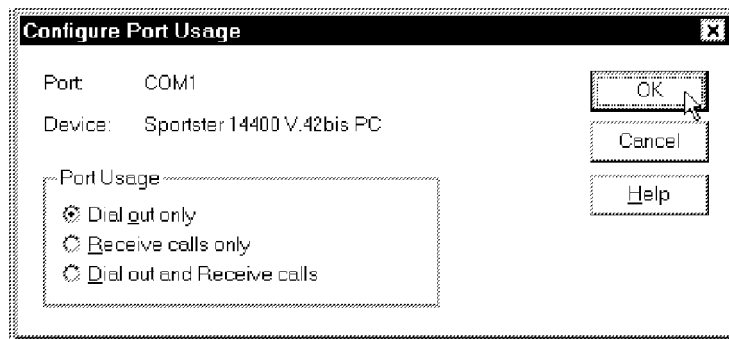
Figure 199. Configure Port Usage — Selecting a Dial Mode
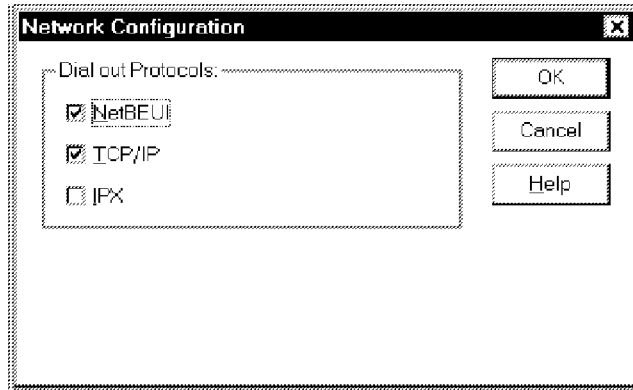
Figure 200. Network Configuration — Selecting Network Protocols
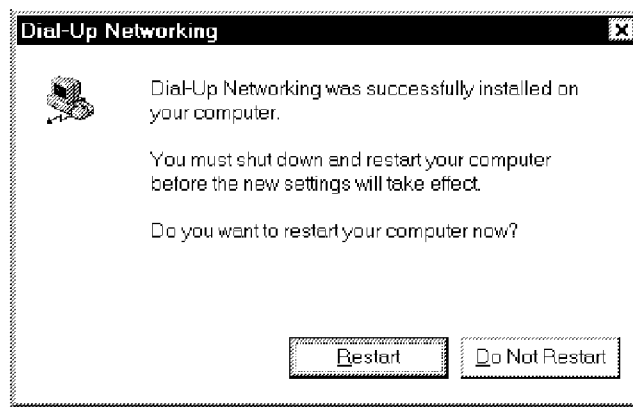
Figure 201. Dial-Up Networking — Installation Done

13.5.3 Connecting through Dial-Up

In Windows NT, we have to deal with an ironic situation when using Dial-Up connections;. Since you are prompted to log on at system startup, you will of course not be validated anywhere but locally — you cannot start your Dial-Up connection before having access to the system, which means that you have to do a local logon. This implies that it is necessary to have a local user ID that is identical to the OS/2 Warp Server domain user ID, even if using the IBM Networks Primary Logon Client.

Once this is sorted out and you are up and running, start your dial-ip session as follows:

1. Open **My Computer**, select **Dial-Up Network**, provide your identification data and press **Dial**, see example in Figure 202 on page 346.
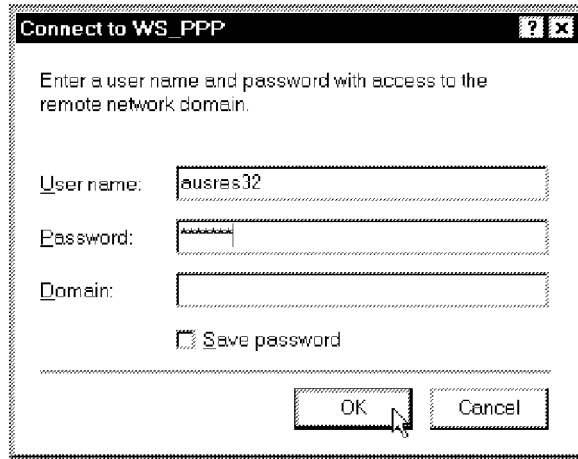
Figure 202. The Dial-Up Logon Panel

2. A monitor pop-up is displayed, indicating the progress (see monitor panels below); when your logon is authenticated, it disappears.
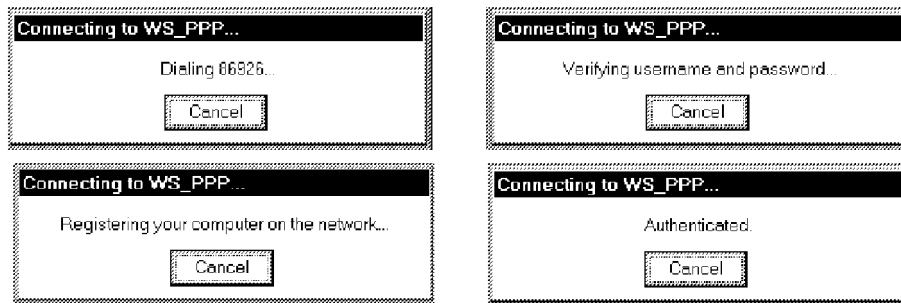
3. You are now able to connect to your OS/2 Warp Server domain resources, as shwown in Figure 203.
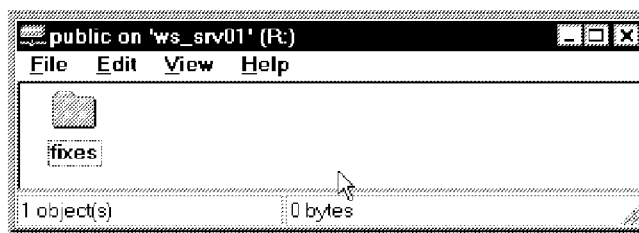
Figure 203. My Computer — Connected Network Directory

13.6 Client-Specific Features and Functions

This section is a NT-specific extension to section 9.1, "Common GUI Features and Functions" on page 95.

13.6.1 User Profiles Support

This feature enables loading unique profiles for each Windows NT user from an OS/2 Warp Server server. Thus, multiple users can obtain their customized desktops, regardless of what Windows NT machine they are using. Here is how it works:

In an OS/2 Warp Server environment, user profiles can be stored in the home directory under the PROFILES subdirectory that is defined at the OS/2 Warp Server to which you log on. If you do not have a home directory defined or you cannot access the home directory, the user profile can be loaded and stored either on your local workstation or a designated UNC path location that points to the server. The default is to utilize the user's home directory.

Note: User profiles are not supported on FAT partitions. The directory that stores the user profile must be defined on a HPFS or HPFS386 partition of a server. The user must have all permissions (`RWCXDAP`) to the directory.

To define a path other than the PROFILES subdirectory or the default local workstation, proceed as follows:

1. Log on using an user ID with administrator privileges; click [**Start** — **Programs** — **Administrative Tools** — **User Manager**].

2. Double-click on the user whose profile location you want to change. The user's Property page is displayed.

3. Click **Profiles** and the User Environment Profile window is displayed, see Figure 204.
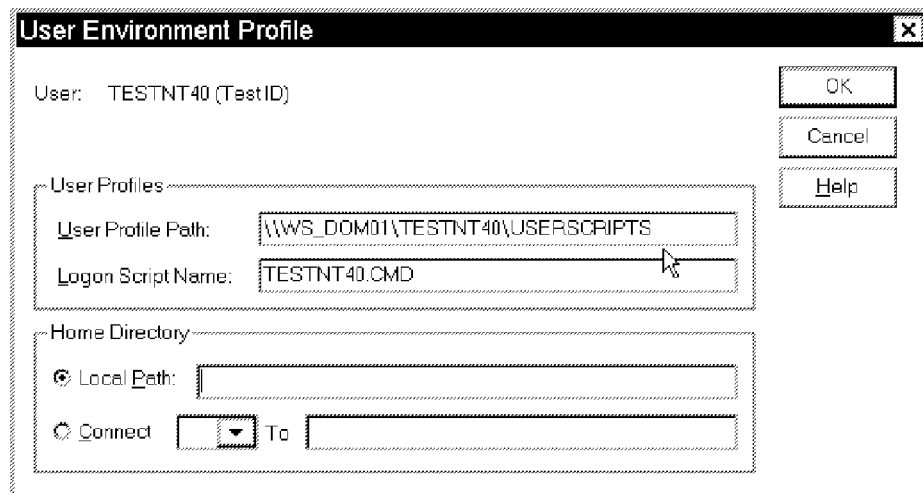
Figure 204. Customizing the User Environment Profile

> **Tip**
>
> Check out the online help; it is available by pressing **F1** or by clicking on the **Help** button.

4. In the User Profile Path entry field, type the UNC path and file name. Use the format of:

   `\\WarpServer\ShareName\ProfileDir`

   where:

   WarpServer Is the NetBIOS name of the server
   ShareName Is the name of the shared resource
   ProfileDir   Is the location where you want the user profile loaded during logon and saved at logoff.

   (An example is given in Figure 204 on page 347.)

5. In the Logon Script Name entry field, type the name of the command file.

6. Click **OK**

7. From the User Properties page, Click **OK** and close the User Manager application.

Note: This procedure overrides the roaming or local profile on this workstation.

13.6.2 Shared Application Support

OS/2 Warp Server is greatly suited to be set up as an application server. In this example we illustrate installing OS/2 Warp Server as an Microsoft Office 97 application server. Follow the steps as described below:

1. Configuring the server:

   a. Define an application group:

      1) From the OS/2 Warp Server desktop, double-click on the **LAN Server Administration** icon and log on with an user ID with administrator privileges.

      2) When the LAN Server Administration - Icon View appears, double-click on the domain icon that respresents your domain name.

      3) Define a group for the application by double-clicking on the groups icon and right mouse button click on the group template icon and drag it to an open space in the window.

      4) Fill in the group name of your choice and provide description information as desired.

5) Click on the **Users** tab and click the **Add** button. and select all users for that group.

6) Click the **Add** button and click the **General** tab and fill in the title for the group.

7) Click the **Create** button and close the window.

b. Define an alias:

1) In the domain icon view window, double-click on the **Resources** icon.

2) In the Resource Definitions window, create a directory alias by clicking the right mouse button on the directory template and dragging it to an open space within the window.

3) In the Directory Alias - Create screen, fill in all required information on the identify tab. For example:

   Alias: `WINAPPS`
   Description: `Office 97`
   Server Name: `SERVER01`
   Path: `D:\WINAPPS`

4) Select the **General** tab and fill in the Title field to name the alias, then click on the **Create** button.

5) When the Access Control Profile does not exist window appears, select **OK** to create a new profile.

6) In the Access Control Profile - Settings View window, select the permissions tab, then click the **Add** button. Select the names and/or 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 [C], read [R], and execute [X]).

7) After permissions have been given, click on the **Create** button.

8) When the Propagate Access Profile to sub directories window appears, click **OK**.

9) When the Setting View window reappears, click the **Set** button. Close the Resource Definitions window.

2. Install the program from a Windows NT workstation:

   This phase requires a workstation that has Windows 95 or Windows NT 4.0 installed and a CD-ROM drive.

a. From a Windows 95 or Windows NT 4.0 desktop, log on as an administrator and connect to the alias you created on the server using the IBM Networks Client GUI.

b. Start the IBM Networks Client from the desktop, click on the icon that represents a hard disk and connect to the alias that you previously created and close the window when completed.

c. From the Windows 95 or Windows NT 4.0 desktop, insert the Microsoft Office 97 CD-ROM in the drive. Click [**Start** — **Run...**] When the Run window appears, type in the drive letter of the CD-ROM drive and type in the command to install the program with the `/A` parameter:

```
X:\SETUP.EXE /A
```

where `X:` is the CD-ROM drive letter. The `/A` parameter indicates the program is to run in administrative mode. This switch is only available from original media.

d. Click the **OK** button.

e. When the Microsoft Office Setup window appears, click **Continue** and read the information on the remaining setup windows before continuing with each step.

f. Fill in the Organization Name field, click **OK** and confirm the organization name by clicking **OK**.

g. Type in the CD KEY # and click **OK**.

h. Click **OK** to verify the information in the Product ID window. The folowing window asks which folder the program will be installed.

i. Click on the **Change Folder** button and select the alias that was previously accessed, then click **OK**.

j. On the following 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 on the users home directory.

n. Select what paper format and language type you want to use and click **OK**. The installation progress bar screen appears while the

program installs. The installation usually takes approximately 45 minutes to complete.

   o. Click **OK** on the Setup Completed Successfully window to exit the installation program.

3. The following are instructions for installing Microsoft Office 97 client on a Windows 95/NT 4.0 workstation from a Warp Server Domain. From a Windows 95/NT 4.0 Workstation desktop, perform the following steps:

   a. Click [**Start** — **Programs** — **IBM Networks Client**] and start the IBM Networks Client.

   b. When the IBM Networks Client GUI appears, click on the drives icon and click the find button.

   c. Select the alias where the program is located and click **OK**.

   d. Click on the **Connect** button and click **Close**.

   e. Close the IBM Networks Client window.

   f. Double-click on **My Computer** icon.

   g. Double-click on the alias drive icon. The Alias directory window will display two folders in the sub directory, MSOFFICE and MSAPPS.

   h. Double-click on the **MSOFFICE** folder icon.

   i. Double-click on the **Setup** icon.

   j. Select **Continue** from the Microfot Office 97 Setup window.

   k. Fill in Name Information window and click **OK** and click **OK** to confirm the information.

   l. Click **OK** when the Microsoft Office Setup Product ID window appears.

   m. Select the product installation path. If desired, set to the user's home directory or set to the local hard drive.

   n. Select **OK**. Select the location for shared files installation. We recommend putting them on the server.

   o. Click on the **Run From Network Server** button. The installation progress bar screen appears while the program installs.

   p. Click **OK** on the Setup Completed Successfully window to exit the installation program.

   q. Close all open windows and restart system.

13.6.2.1 Adding Shared DOS Applications to Program Groups

If you are logged on to a OS/2 Warp Server domain, you can add shared applications to Windows NT program groups on your workstation:

1. From the menu bar, click [**Applications** — **Shared Applications**]. The Shared Application Installation window is displayed, as shown in Figure 205.
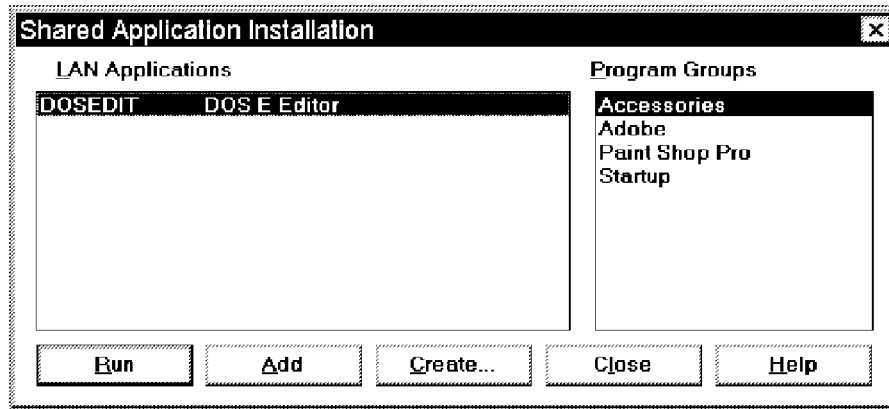
Figure 205. Shared Application Installation

2. From the LAN Applications list, select the applications you want to add. You can make multiple selections.

3. Do one of the following:

   • If the program group is listed, select the program group to which you want to add the applications.

   • If the program group is not listed:

      a. Click **Create**; the Program Group Properties window is displayed.
      b. In the Description entry field, type the title of the group you want to create (an example is given in Figure 206) and click **OK**.
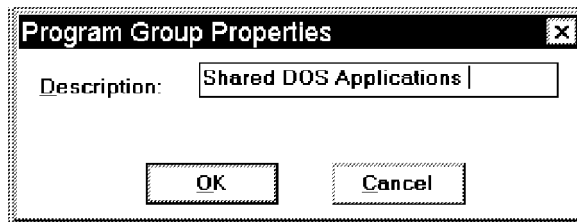
Figure 206. Program Group Properties

Note: When adding LAN applications to a program group, you can select only one program group at a time. To adding LAN applications to

more than one program group, you must add them separately to each group.

4. From the Shared Application Installation window, click **Add**.

5. Click **Close** to exit this window.

When you add shared applications, an application icon is created for each application and the icon is added to the program group you selected.

13.6.2.2 Running a Shared Application
There are two ways to run shared applications defined on an OS/2 Warp Server domain:

1. From the IBM Networks Client GUI

   a. From the menu bar, click [**Applications** — **Shared applications**]. This option is available only if you are currently logged on. The Shared Application Installation window is displayed.

   b. From the LAN Application list, double-click on the desired application.

2. From the Windows NT 4.0 desktop

   a. Click [**Start** — **Programs**], and then select the program group that contains the shared application.

   b. Click on the name of the shared application.

13.6.3 Home Directory
In the case of the IBM Networks Coordinated Logon Client, the home directory on the OS/2 Warp Server domain does not affect the home directory definition in the Windows NT domain. The home directories can coexist.

13.6.4 Storing Windows NT System Policies on OS/2 Warp Server
System policies allow administrators to restrict user access to system configuration changes. In other words, an administrator can restrict which icons and menu options are available on a user's desktop. For more information on system policies, see the Windows NT documentation and help texts. This section describes how to set up a Windows NT workstation to use system policies stored on an OS/2 Warp Server domain.

Note: To perform the following task, you need to either access the System Policy Editor (POLEDIT) that is included in the Windows NT Server product, or let your Windows NT administrator do this for you.

13.6.4.1 Remote System Policies Setup Procedure

To set up your system to use system policies stored on an OS/2 Warp Server domain, proceed as follows:

1. Log on to a Windows NT workstation using an ID with administrator privileges.

2. Start the System Policy Editor; from the File menu, click **Open Registry**. The Local Computer and Local User icons are displayed, as shown in Figure 207:
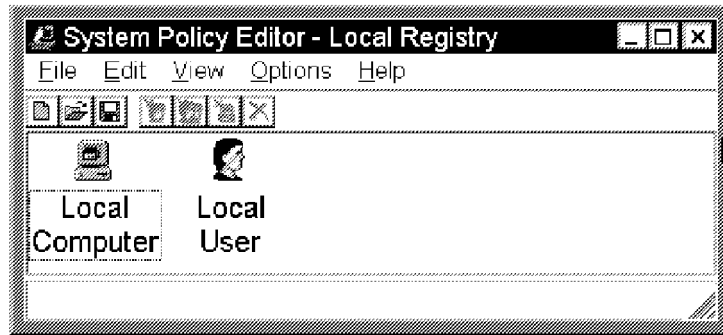
Figure 207. The Windows NT System Policy Editor

3. Double-click **Local Computer**. The Local Computer Properties page is displayed, see Figure 208 on page 355:
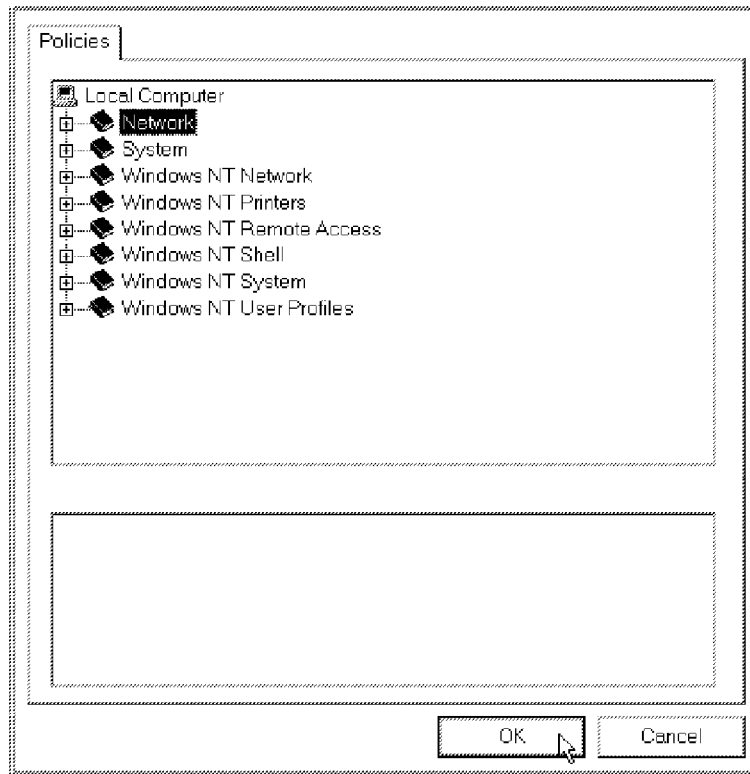
Figure 208. System Policy Editor - Local Computer Properties

4. Open [**Network** — **System Policies Update** — **Remote Update**] and expand the **Update mode** list box. Select **Manual (use specific path)**.

5. In the Path for manual update entry field, type the UNC path and file name. For example:

   `\\WarpServer\NETLOGON\MyConfig.POL`

   where:

   WarpServer Is the NetBIOS name of the server
   Netlogon Is the name of the NETLOGON share
   NTConfig.pol Is the name of the system policy you want to load during logon

   An example is shown in Figure 209 on page 356.
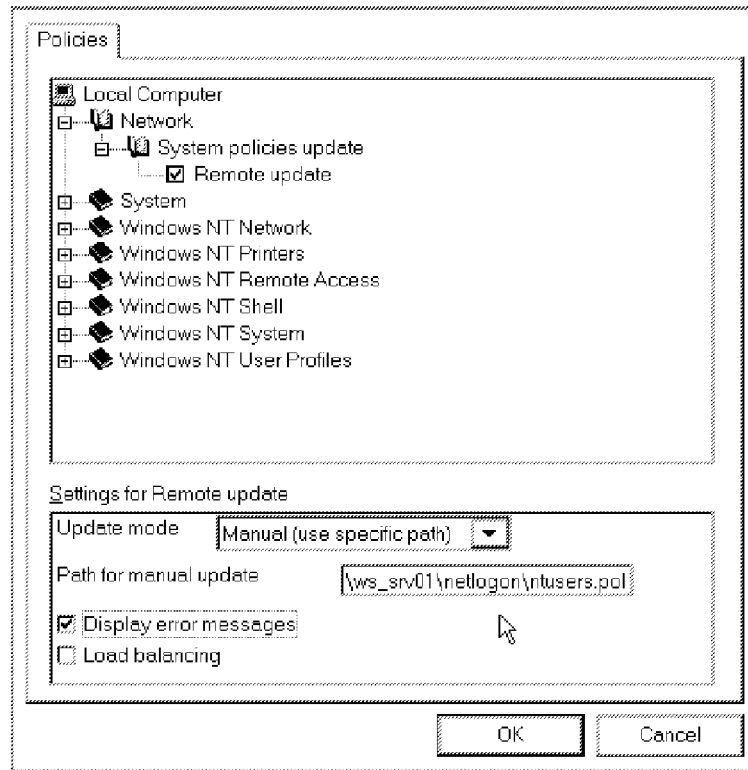
Figure 209. Local Computer Properties - Settings for Remote Update

6. Click **OK**; save your changes, close the system policy editor and restart your system. It is now prepared to use system policies stored on the OS/2 Warp Server domain.

Note: When multiple logon servers are used, the system policy file must be present on each logon server.

13.6.5 Managing Dynamic Local Accounts

Three options exist for dynamically created local NT user accounts. The local user account is created after the user is succesfully authenticated on the remote logon server. Using the logoff policy (as described in section 13.6.5.1, "Enabling the Logoff Policy" on page 357), the product gives the following options for managing the accounts:

• The account can be deleted when the user logs off. This is the default.

• The account can be disabled when the user logs off. This prevents local logon with the network user ID and password.

• The account can be kept when the user logs off.

13.6.5.1 Enabling the Logoff Policy

To set the logoff policy follow these steps:

1. Use the REGEDT32 tool located on the Windows NT machine, to set the logoff policy. The policy is located at:

```
HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\IBMNETNT\LOGOFFPOLICY\DELET
```

Figure 210. Windows NT Registry: Logoff Policy

2. Edit the entry using one of the following settings:

   0　　　　　Keeps the account

   1　　　　　Deletes the account

   2　　　　　Disables the account

3. Save the changes and exit the REGEDT32 tool.

13.6.6 NET Commands for the IBM Networks Client for Windows NT

The OS/2 Warp Server NET commands are accessed using the NET command. This functionality supplements the Microsoft NET commands. The IBM Networks Client for Windows NT (both Primary and Coordinated Logon Client) supports the following commands using the NET command line interface:

- NET ADMIN

- NET ALIAS

- NET DASD

- NET HELP

  - only on ADMIN, ALIAS, DASD, SEND, USE, or WHO

- NET SEND

- NET USE [alias]

- NET WHO

When the IBM Networks Client for Windows NT is installed, the Microsoft NET.EXE program is renamed to NETNT.EXE. The IBM NET.EXE executes the commands mentioned above. If the command is not one of the above it sends the command to Microsoft's NETNT.EXE program to be processed.

13.6.7 Problem Determination

The IBM Networks Client for Windows NT is a fully integrated 32-bit network provider to the Windows NT client. If you encounter a problem using the IBM Networks Client for Windows NT, the following tests help you determine if the problem lies in Microsoft code or the IBM code.

It should be investigated by Microsoft if:

1. You can recreate it without the IBM Networks Client installed.

2. The problem is with a network protocol.

3. The application calls a network API not serviced by the IBM Networks Client for Windows NT.

It should be investigated by IBM if it is one of the six IBM unique functions, such as:

1. Home directories

2. Logon assignments

3. Aliases

4. Shared applications

5. Directory limits (DASD limits)

6. LAN Server administration

If you encounter problems using the NET command line interface, try the same command directly through the renamed Microsoft NETNT command processor. For example, if the following command causes a trap:

```
NET USE X: \\Server\Share
```

try this command:

```
NETNT USE X: \\Server\Share
```

13.7 IBMGina and Other Special Items

A Windows NT service called IBMGina is installed and configured as part of the installation of the Primary Logon Client. The service is used to authenticate the user during the dynamic creation of the local user account. The service is configured to automatically start when Windows NT boots up.

The service uses an IBMGina user account that is also created during the installation process and has administrator privileges. This account must be present on the local NT system.

A Roaming Users group is created during the installation process. Membership in this group causes the user's accounts to be managed by the primary logon client.

Chapter 14. Apple Macintosh Clients

This chapter describes how to enable Apple Macintosh users to take part in OS/2 Warp Server's file and print services. We focus on two choices:

- Using the Macintosh's built-in AppleTalk protocol. With an additional IBM product called OS/2 LAN Server for Macintosh, OS/2 Warp Server can be enhanced to provide the AppleTalk protocol.

- Using NetBIOS over TCP/IP by extending Apple's MacTCP with the NetBIOS protocol. Thursby's software DAVE offers such a kind of solution.

14.1 File and Print Services with OS/2 LAN Server for Macintosh

The easiest way to enable Macintosh clients to work with OS/2 Warp Server is by installing OS/2 LAN Server for Macinstosh (LSM) on top of OS/2 Warp Server. LSM provides the AppleTalk protocol Macintosh users use most often for file and print. No additional software has to be installed on the Macintosh clients. The next paragraphs describe OS/2 LAN Server for Macinstosh functions.

14.1.1 Sharing Files

OS/2 LAN Server for Macintosh (LSM) enables Macintosh users and other workers on an AppleTalk network to access files that reside on an OS/2 LAN/Warp Server, and to share files and folders (directories) with PC users. Files stored on an OS/2 LAN / Warp Server hard disk drive can be accessed by both Macintosh and PC users. However, LSM does not provide OS/2 and DOS users with the ability to access Macintosh hard drives.

LSM turns an OS/2 LAN / Warp Server into an AppleShare file server. The server is displayed to Macintosh users just like an AppleShare server. This enables Macintosh users to gain access to OS/2 LAN Server shared file resources with the standard Chooser interface.

Similarly, networked PC users can see Macintosh files on the LSM server and work with Macintosh data as if it were on a local drive. PC users access files using their standard DOS LAN Services (DLS) or OS/2 LAN Requester interface, or the OS/2 Warp Connect and OS/2 Warp 4 File and Print Resource Browser.

14.1.2 Sharing Print Resources

LSM acts as an intermediary between the workstations and PostScript printers on a network while enabling the sharing of printers by Macintosh and PC users. Shared printers can be attached to OS/2 servers that are running LSM or they can be on the AppleTalk network.

LSM acts as a print spooler for Macintosh users. Up to nine AppleTalk LaserWriters can be associated with OS/2 print queues along with any of the PostScript printers attached to the OS/2 LAN /Warp Server. This enables Macintosh users to spool jobs to printers attached to the OS/2 LAN / Warp Server, while OS/2 and DOS users can send jobs to printers on the AppleTalk network. Note that the data from PC users must be preformatted into a PostScript data stream before it is sent to an AppleTalk printer.

Macintosh users who set background printing can print jobs and return to their applications immediately. LSM takes care of printing the jobs, freeing up the Macintosh workstations for other tasks. Network administrators can manage queues using the OS/2 interface.

14.1.3 Automatic Application Launching for PC Files

DOS and OS/2 data files on the server are displayed to Macintosh users with appropriate Macintosh icons. An LSM administrator sets up mappings between DOS and OS/2 file extensions and Macintosh program names. When a Macintosh user double-clicks on a PC file with a known extension, the Macintosh Finder invokes its associated Macintosh program automatically, just as if the file resided on the Macintosh.

14.1.4 Security

LSM provides security features that are consistent with both LAN/Warp Server and AppleShare security. The network administrator defines security for Macintosh folders and volumes on the server according to standard AFP privileges. OS/2 privileges also remain in effect, taking precedence over Macintosh privileges.

Additional security is provided by passwords at the user and administrator levels. Users can maintain their own passwords.

An optional audit trail keeps track of logins and file activity. Intruders can be locked out after a definable threshold of incorrect login attempts. Two OS/2 LAN / Warp Server parameters control these activities:

- Auditing
- Logon alert

14.1.5 Administration

LSM can be administered from any OS/2 workstation running OS/2 LAN Requester where an administrator is logged on and the LSM Administration Utility is installed.

14.1.6 Naming Files

The Macintosh operating system differs from the DOS and OS/2 operating systems in the way it names files and folders (subdirectories). Macintosh file and folder names can be up to 31 characters long and can use all the keyboard characters except the colon (:). PC users name their files and folders (subdirectories) according to one of the two file systems that are being used on the OS/2 LAN / Warp Server:

- File Allocation Table (FAT)

  File names under the FAT naming scheme are restricted to 8 characters with a 3-character extension. When this type of naming scheme is used on a server, Macinstosh files may be shortened. To designate names that have been shortened, the exclamation point symbol (!) is added to the beginning of the name.

- High Performance File System (HPFS); 16-bit and 32-bit versions

  HPFS allows file names up to 255 characters. File names longer than 31 characters are not seen by Macintosh users. Macintosh files are stored on HPFS drivers without changing the lenght of the name. Because DOS users are restricted to 8.3 FAT conventions, they are not able to see HPFS files longer than 11 characters. LSM provides an option that can restrict HPFS to short name conventions for files stored by Macintosh users.

  If your PC user base consist of all OS/2 users, you may want to use the HPFS or HPFS386 file system so that you can maintain consistent name matching of folders and files between the Macintosh and OS/2 environments.

Both of these file systems have more naming restrictions than the Macintosh. LSM changes some characters in Macintosh file names to a hyphen (-) when creating the OS/2 file name.

14.1.6.1 Macintosh File Forks

Another difference between Macintosh and OS/2 files is that Macintosh files contain two forks:

- Data Fork
- Resource Fork

When Macintosh files are stored ona OS/2 LAN / Warp Server hard disk drive, each fork is stored as a separate OS/2 file. On a FAT format drive, the resource fork will begin with a pound symbol (#). On an HPFS format drive, the resource fork will have a suffix of &perod.#Res. LSM maintains the additional file structure information AFP (AppleTalk Filing Protocol) requires to keep track of each fork under OS/2.

DOS and OS/2 users should be cautioned not to delete any file starting with the pound symbol (#) or ending with &perod.#Res and having a size greater than zero.

14.1.7 Printing Service

LSM acts as an intermediary between the workstations and printers on a network, while enabling the sharing of printer resources by both Macintosh and PC users. LSM enables network users to share many diffrent printers. These printers can be attached to OS/2 servers that are running LSM, or they can be on the AppleTalk network.

All printers configured to be used through LSM must process Postscript data. This is the default for most AppleTalk printers, but PC printers can have different data streams, such as PCL.

Network printers are shared by many different users. which means one printer might have several jobs to it at once. The LSM Print Server minimizes waiting time by permitting several users to simultaneously send documents to be printed.

14.1.7.1 Using LSM Printers

LSM shared printers are accessed by Macintosh users through the standard Macintosh Chooser. Users simply select the appropriate printer icon, usually LaserWriter, from the Chooser screen. They can then select form the list of available printers.

A printer is selected by clicking on it with the mouse. After that, all futer print jobs will be sent to that print device until a different device is selected.

Users handle printing in the usual fashion, by selecting **Print** from the File pull-down meny. The LSM Print Queue Service passes all print jobs to the OS/2 spooler, which manages the jobs in the print queue.

14.1.8 Administration Utility

The configuration of LSM is performed by a Presentation Manager (PM) application known as the Administration Utility. The network administrator can use this program to configure LSM from any OS/2 workstation that is logged in to the OS/2 LAN / Warp Server. The Administration Utility has the

same look and feel as the OS/2 LAN / Warp Server User Profile Management utility, providing network administrators with a familiar interface.

The LSM Administration Utility interacts with the LSM services via OS/2 named pipes. Each LSM service has a named pipe to communicate before the Administration Utility can be used for a particular server.

Menus within the Administration Utility allow the network administrator to perform the followng tasks:

- Pause and resume logons
- Shut down the file service
- Cancel the file service shutdown request
- Show active session information for the file service or share
- Configure Macintosh user alias names
- Change passwords
- Define file extension mapping
- Define print queues for use by Macintosh users
- Define AppleTalk printers to be accessed through LSM

14.1.9 Installing OS/2 LAN Server for Macintosh

The installation is initiated by enetering the following command assuming the OS/2 LAN Server for Macintosh diskette is in drive A:

```
A: LSMINST
```

The installation program automatically installs all required files and updates the CONFIG.SYS, PROTOCOL.INI and IBMLAN.INI files.

In the IBMLAN.INI file, which also reflects new LAN Server services, the following entries are added:

```
[server]
  SRVSERVICES = NETLOGON,LSSERVER,TIMESOURCE,DCDBREPL,LSMFILE,LSMPRINTIN,LSMPRINT

[services]
  lsmfile=services\lsmfile.exe
  lsmprintin=services\lsmpin.exe
  lsmprintout=services\lsmpout.exe

[lsmfile]
  syspath=C:\ibmlan\lsm
  allowsavepassword=true
  maxopenfiles=40
  encryptedlogin=false
```

```
[lsmprintin]
   syspath=C:\ibmlan\lsm

[lsmprintout]
   syspath=C:\ibmlan\lsm
```

Start LSM Services separately throught the Command Line

LSM installation adds all LSM services to automatically start with the
startup of LAN services. However, ee recommend starting LSM services
separately from an OS/2 command line (STARTUP.CMD):

```
NET START LSMFILE    to start the LSM server
NET START LSMPRINTIN       to start the print services
NET START LSMPRINTOUT       to start the print redirector services
```

In the PROTOCOL.INI file, which also reflects new protocols, the following
entries are added:

```
[IBMLXCFG]
   ATALK_nif = ATALK.NIF


[ATALK_nif]

   drivername = ATALK$
   bufs = 64
   zone = *
   bindings = IBMMPC_nif
```

14.1.10 Using an Apple Macintosh on a LSM Server Network

The information in this section is mostly standard for Macintosh AppleShare
users. The basics are presented here for the benefit of OS/2 LAN/Warp
Server administrators, who may not be familiar with the Macintosh
operating system. It is assumed that the Macintosh is properly configured
through the Network Control Panel to use a LAN connection where LSM is
available either directly or through a router. For additional information,
refer to the Macintosh user guides.

This section also includes information about how a LSM server differs from
an Apple AppleShare server. This information may be helpful to all
Macintosh users.

To successfully log in to OS/2 LAN/Warp Server, proceed with the following
steps:

  1. Click on the Apple icon and then select **Chooser** from the pull-down
     menu. The Chooser presents a window with an AppleShare server icon,

along with icons representing all other available resources, such as printers.

2. Select the **AppleShare** server icon to display the file servers currently available on the network. In case the AppleTalk Zones window is present, click on the zone in which the desired server is located, for example, click on **Token-Ring 1**.

3. From the file server list, double-click on the server you want to access resources. You are presented with a logon window.

4. In the logon window, select the type-of-user radio button. If you are a defined user at the OS/2 Warp Server domain, select the **Registered User** radio button. Provide user ID and password information and click **OK** You are presented with a available shares window.

5. From the item list that represents available shares at the OS/2 Warp Server select the share name (alias) you want to access. Mark the item's check box if you want to get access to the desired resource while logging on to the domain.

6. Select **OK** when done selecting. If the connection is successful, a new icon that indicates the resource is available on the desktop.

To disconnect from a resource, drag the icon to Trash icon.

Note: Doing so will not delete files.

14.2 File and Print Services for the Macintosh Using NetBIOS over TCP/IP

Thursby's software titled DAVE sets up a Macintosh to run an IBM or Microsoft TCP/IP network client under either NTS's NetBIOS Name Server Shadow or NT's Windows Internet Name Server (WINS) services. Doing so allows a Macintosh to access as many or few folders on the server as necessary, on an entire hard disk or on as many drives as you have available.

DAVE goes a needed step beyond a server's file and print services for Macintosh to provide full file serving, print serving, and simple messaging by thoroughly integrating Macintosh clients into an OS/2 Warp Server or NT Server-based network.

DAVE uses a custom NetBIOS service on the Macintosh side and the NetBIOS support built into OS/2 Warp Server or Windows NT, running TCP/IP as the main communications protocol. Because of this combination, it is advantageous to have a NetBIOS Name Server like NTS' Shadow or Microsoft's WINS service set up before you use DAVE. The product uses the

H-node as the required default. If no NetBIOS Name Server is available, B-node is used instead.

The DAVE software consists of a NetBIOS control panel used to record the server IP address, the name of the Macintosh workstation and its workgroup name and a secondary IP server address if needed. Apple's TCP/IP services run under either MacTCP or Open Transport; DAVE uses Apple's TCP/IP control panel with its own software to define the addresses you need to get networking up and running. DAVE directly supports Open Transport, that, with Apple's release of the new Open Transport Version 1.1.1, is finally a (barely) functional TCP/IP solution.

We found DAVE relatively simple to set up. In a corporate context, Macintosh users need to get the server's IP address and have a specific IP address assigned to their Macintosh workstation.

Hint

The router address in the TCP/IP panel should be the same as the primary server address you give the NetBIOS panel.

After running the NetBIOS control panel, ensuring that the NetBIOS Name Server (NBNS) was running, we quickly logged the Macintosh onto the server.

You can stipulate which drives and folders should load upon restarting. It is the administrator's responsibility to choose the file and print resources to which a Macintosh user has access. We were able to mount both of the server's hard drives to the Macintosh desktop and browse through their folders without a problem.

Our benchmark tests of file transfers didn't show a major performance boost over the AppleTalk-based Services for Macintosh that we used. DAVE's print-serving functions quickly detected the HP Laserjet connected to our OS/2 Warp Server.

For more information please visit the Thursby Software Systems, Inc. Web site at:

`http://www.thursby.com`

or contact Thursby Software Systems, Inc.:

Phone: (817) 478-5070; Fax: (817) 561-2313; Email: sales@thursby.com

14.2.1 Installing DAVE

To install DAVE, follow these installation steps:

1. After downloading DAVE, put the extracted folder named 'Disk 1' on your Macintosh desktop. Most Web browsers do this for you automatically.

   Note: If you have DAVE on diskette, insert the diskette in the Macintosh's diskette drive. A folder that represents the diskette appears on the desktop. Double-click on the folder to open it.

2. Double-click on the **Readme** file. This file contains important information that will save you time and effort. Please read it.

3. Make sure your Macintosh is booted with your TCP/IP software (MacTCP or Open Transport) active. DAVE will not install if you boot with TCP/IP extensions turned off. It is also a good idea to turn off any anti-virus software before installing.

4. Make sure TCP/IP is configured properly and you can ping other machines on your network. If you use a web browser, you probably have TCP/IP configured already. It is easier to make sure TCP/IP is working before installing DAVE.

5. Install DAVE by double-clicking on the **Installer** in the Disk 1 folder. Remember that the Disk 1 folder must be on your desktop. If you see a message that DAVE cannot install, be sure you have selected a disk with a valid system folder on it.

6. After your Macintosh reboots, select [**Apple Icon** — **Control Panel** — **NetBIOS**]. You are prompted to enter your name, organization and the license key that was e-mailed to you. You should copy and paste the key into this dialog, so you may want to copy the key before you open the NetBIOS control panel.

7. Next, you need to enter a NetBIOS name and workgroup (domain name) for your Macintosh. The name you pick must be unique - no other computer in your NetBIOS network should use this name. The workgroup/domain name you pick should be a workgroup or domain that you use often. If you are not sure what workgroup to use, leave this field blank.

8. Click the **Set** button on the NetBIOS control panel. You are ready to begin using DAVE.

9. Connect to the server resources by selecting **DAVE Client** from the Chooser. It will browse your network for available servers.

```
┌─ IBM Neighborhood Browser Enabler ──────────────────────────┐
│                                                              │
│  We recommend having the IBM Neighborhood Browser Enabler    │
│  installed on your OS/2 Warp Server domain controller.  By default, │
│  DAVE first looks for the master browser.  If there is no master │
│  browser installed on your network, unmark the Browse Services │
│  check box in the DAVE Setup window to avoid the NetBIOS Error #5 │
│  error pop-up window.  If the Error pop-up window appears, click OK │
│  to continue.                                                 │
│                                                              │
└──────────────────────────────────────────────────────────────┘
```

14.2.2 Using an Apple Macintosh with DAVE

The information in this section is mostly standard for Macintosh AppleShare
users. The basics are presented here for the benefit of the Macintosh user.
It is assumed that the Macintosh's TCP/IP and NetBIOS panels are properly
configured.

DAVE uses the standard Apple Chooser to mount servers and PostScript
printers just like AppleTalk. You don't have to learn any new.

1. Click on the Apple icon and then select **Chooser** from the pull-down
   menu. The Chooser presents a window with an DAVE Client icon, along
   with icons representing all other available resources, such as printers.

2. Click on **DAVE Client** to display the servers currently available on the
   network.

3. From the server list, double-click on the server you want to access
   resources. You are presented with a logon window.

4. Apply your user ID, password and domain name to access resources on
   your server network. DAVE works with your OS/2 Warp Server security.
   You can tell DAVE what OS/2 Warp Server domain your user ID is in.

5. When logged on, click on the volumes you want to use. Each one gets
   mounted and is available on your desktop. If you want DAVE to
   remember to mount your volume again when you reboot your
   Macintosh, just check the box to the right of the volume name.

   Note: You can also choose a printer if you like.

6. Click the **OK** button and the server appears on your desktop. Now it is
   exactly like an additional hard drive sitting right next to your Macintosh.

At the time this redbook was written, DAVE clients could not access OS/2
Warp Server resources on HPFS386 partitions. Contact Thursby Software
Systems, Inc. to get the latest status on this issue.

Appendix A. Windows 95 Logon Traces to Illustrate SMB Flows

The following traces are taken to give a deeper view of the network traffic between the workstation and server during the logon process and to show that there is no native TCP/IP traffic but rather NetBIOS over TCP/IP traffic, thus Windows 95 only mentions TCP/IP when dealing with requesters and LAN resources.

These traces are not meant to be exact protocol traces but to illustrate what happens during the logon process, proving that both IBM and Microsoft use SMB (Server Message Block) protocol to communicate between the server and workstation. On the other hand, these traces prove that you get all the logon assignments, PROFILE.BAT execution and system policies you get using Windows NT domain and even more. Your home directory and file aliases are assigned directly from the OS/2 Warp Server domain. You can also see the actual logon sequence from the traces.

The traces are taken from a real production network in the International Technical Support Organization, Austin Center. The traced network traffic was filtered to the server and client addresses only. The actual MAC addresses were replaced by the symbolic names to make it easier to read the trace. IP addresses are kept as they are.

The following server and workstation configurations are used:

Server configuration:

- OS/2 Warp 4 base operating system with OS/2 Warp 4 FixPak 1
- OS/2 Warp Server with FixPak IP08260
- Both NetBIOS and NetBIOS over TCP/IP configured
- IP address `9.3.1.140`

Workstation configuration:

- Microsoft Windows 95, no service packs
- IBM Networks Client for Windows 95 installed and configured
- IP address `9.3.1.11`, when IP used

A.1 The NetBEUI Logon with System Policy Download

The following trace was taken with IBM DataGlance using only the NetBEUI protocol on the Windows 95 workstation. The system policy download and user-dependent desktop and Start menu settings were enabled.

Notes:

1. NetBIOS names are registered. The following 16th byte values are used (also see Table 12 on page 271):
   - `Win95Cli01`   [00h] for workstation service
   - `Win95Cli01`   [03h] for messenger service
   - `WS_DOM01`   [00h] for domain name
2. The logon name is added as a messenger name with the 16th-byte of [03h] and the domain controller server name is queried and found from the network.
3. A NetBIOS session is established and confirmed. From now on, the main traffic is SMB (Server Message Block) traffic. Only one NetBIOS session is opened and all the resource assignments and data transfers to and from the server are over this connection. If more resources are assigned from other servers, one NetBIOS session is opened against every server.
4. The user's home directory is assigned.
5. Logon assignments are applied for aliases CD-ROM, DATA, PUBLIC, and TRANSFER.
6. There is no PROFILE.BAT defined for the user; so the file cannot be run.
7. The USER.DAT file equals to HKEY_CURRENT_USER in the Windows 95 registry database. USER.DAT includes all the user's settings and restrictions. USER.DAT is downloaded only if the user profiles function is enabled in Windows 95.
8. CONFIG.POL file is opened and read in.
9. User's desktop, Start menu, Network Neighborhood, and recent documents list are read from the home directory.

This is the complete trace:

```
Number Destination Source      Size  Delta Time (msec) Interpretation
 192 NetBIOS    Warp Server    194   6582.364770 SMB C Transaction \MAILSLOT\NET\NETLOGON
 193 9.3.1.255  9.3.1.140      265      5.183630 SMB C Transaction \MAILSLOT\NET\NETLOGON

SECTION 1 (SEE NOTE 1)
 713 NetBIOS    Win95Cli01      63  13936.938270 NETBIOS Check name W95CLI01
 714 NetBIOS    Win95Cli01      63      1.094550 NETBIOS Check group WS_DOM01
 715 NetBIOS    Win95Cli01      63      1.090360 NETBIOS Check name W95CLI01       <03>
 738 NetBIOS    Win95Cli01      63    930.309760 NETBIOS Check name W95CLI01       <03>
 739 NetBIOS    Win95Cli01      63      0.972190 NETBIOS Check group WS_DOM01
 740 NetBIOS    Win95Cli01      63      0.958780 NETBIOS Check name W95CLI01
 759 NetBIOS    Win95Cli01      63    890.552980 NETBIOS Check name W95CLI01       <03>
 760 NetBIOS    Win95Cli01      63      0.959620 NETBIOS Check group WS_DOM01
 761 NetBIOS    Win95Cli01      63      3.616390 NETBIOS Check name W95CLI01
1174 NetBIOS    Win95Cli01     204  12995.301630 SMB C Transaction \MAILSLOT\NET\NETLOGON
1175 NetBIOS    Warp Server    172     37.036320 SMB C Transaction \MAILSLOT\TEMP\NETLOGON
1176 9.3.1.11   9.3.1.140       52      2.118710 ARP Prot=IP Request PA=9.3.1.11

SECTION 2 (SEE NOTE 2)
1177 NetBIOS    Win95Cli01      63      0.707350 NETBIOS Check name W95TEST1       <03>
1178 NetBIOS    Win95Cli01      61      2.938370 NETBIOS Find name WS_SRV01
1179 Win95Cli01 Warp Server     61      0.414860 NETBIOS Name WS_SRV01        recognized
1180 Warp Server Win95Cli01     17      0.870780 LLC D=F0 S=F0 C U SABME P
1181 Win95Cli01 Warp Server     17      0.337750 LLC D=F0 S=F0 R U UA F
1182 Warp Server Win95Cli01     18      0.606780 LLC D=F0 S=F0 C S RR NR=0 P
1183 Win95Cli01 Warp Server     18      0.291660 LLC D=F0 S=F0 R S RR NR=0 F

SECTION 3 (SEE NOTE 3)
1184 Warp Server Win95Cli01     32      0.676340 NETBIOS D=31 S=06 Session initialize
1185 Win95Cli01 Warp Server     18      0.341940 LLC D=F0 S=F0 R S RR NR=1 F
1186 Win95Cli01 Warp Server     32      0.261490 NETBIOS D=06 S=31 Session confirm
1187 Warp Server Win95Cli01     18      0.894250 LLC D=F0 S=F0 R S RR NR=1
1188 Warp Server Win95Cli01    186      0.975550 SMB C Negotiate Protocol PC NETWORK PROGRAM 1.0 (more)
1189 Win95Cli01 Warp Server     18      0.507050 LLC D=F0 S=F0 R S RR NR=2
1190 Warp Server Win95Cli01    110      1.925110 SMB R Negotiated Protocol 3
1191 Warp Server Win95Cli01     18      0.931960 LLC D=F0 S=F0 R S RR NR=2
1192 Warp Server Win95Cli01    179      3.862790 SMB C Session Setup and X Account W95TEST1  Windows 4.0 Windows 4.0
1193 Win95Cli01 Warp Server     18      0.447540 LLC D=F0 S=F0 R S RR NR=3
1194 Win95Cli01 Warp Server    115     12.677050 SMB R Session Established and X OS/2 2.40IBM LAN Server 4.0
1195 Warp Server Win95Cli01     18      1.009910 LLC D=F0 S=F0 R S RR NR=3
1197 Warp Server Win95Cli01    202      3.422790 SMB C Transaction \PIPE\LANMAN
1198 Win95Cli01 Warp Server     18      0.515430 LLC D=F0 S=F0 R S RR NR=4
1199 Win95Cli01 Warp Server     32     31.711900 NETBIOS D=06 S=31 Data ACK
1200 Warp Server Win95Cli01     18      0.750940 LLC D=F0 S=F0 R S RR NR=4
1201 Win95Cli01 Warp Server    195     15.487180 SMB R Transaction Completed
1202 Warp Server Win95Cli01     18      0.988120 LLC D=F0 S=F0 R S RR NR=5
1204 Warp Server Win95Cli01    155      6.823780 SMB C Transaction \PIPE\LANMAN
1205 Win95Cli01 Warp Server     18      0.481070 LLC D=F0 S=F0 R S RR NR=5
1206 Win95Cli01 Warp Server    257      2.074290 SMB R Transaction Completed
1207 Warp Server Win95Cli01     18      1.011580 LLC D=F0 S=F0 R S RR NR=6
1208 Warp Server Win95Cli01    198     36.202420 SMB C Transaction \PIPE\LANMAN
1209 Win95Cli01 Warp Server     18      0.478550 LLC D=F0 S=F0 R S RR NR=6
1210 Win95Cli01 Warp Server     92      3.728690 SMB R Transaction Completed
1211 Warp Server Win95Cli01     18      0.863240 LLC D=F0 S=F0 R S RR NR=7
```

Figure 211 (Part 1 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
SECTION 4 (SEE NOTE 4)
1212 Warp Server   Win95Cli01      99     2.432160 SMB C Tree Connect and X Path=\\WS_SRV01\W95TEST1 Device=A:
1213 Win95Cli01    Warp Server     18     0.388040 LLC D=F0 S=F0 R S RR NR=7
1214 Win95Cli01    Warp Server     84     0.345300 SMB R Tree Connected and X Service=A:HPFS386
1215 Warp Server   Win95Cli01      18     0.983930 LLC D=F0 S=F0 R S RR NR=8
1217 Warp Server   Win95Cli01     142    21.420070 SMB C Transaction \PIPE\LANMAN
1218 Win95Cli01    Warp Server     18     0.506210 LLC D=F0 S=F0 R S RR NR=8
1219 Win95Cli01    Warp Server    186     8.738830 SMB R Transaction Completed
1221 Warp Server   Win95Cli01      18     1.210210 LLC D=F0 S=F0 R S RR NR=9
1224 NetBIOS       Win95Cli01     191     6.173420 SMB C Transaction \MAILSLOT\NET\NETLOGON
1225 Warp Server   Win95Cli01      32    47.045710 NETBIOS D=31 S=06 Data ACK
1226 Win95Cli01    Warp Server     18     0.370440 LLC D=F0 S=F0 R S RR NR=9 F
1234 NetBIOS       Win95Cli01      63   631.158750 NETBIOS Check name W95TEST1       <03>
1252 NetBIOS       Win95Cli01      63   878.740010 NETBIOS Check name W95TEST1       <03>
1264 Warp Server   Win95Cli01      67   453.198180 SMB C Tree Disconnect T=5800
1265 Win95Cli01    Warp Server     18     0.393070 LLC D=F0 S=F0 R S RR NR=10
1266 Win95Cli01    Warp Server     67     0.561520 SMB R Tree Disconnected
1268 Warp Server   Win95Cli01      32    40.130570 NETBIOS D=31 S=06 Data ACK
1269 Win95Cli01    Warp Server     18     0.368760 LLC D=F0 S=F0 R S RR NR=11 F
1395 NetBIOS       Win95Cli01     191  2953.554370 SMB C Transaction \MAILSLOT\NET\NETLOGON
1396 NetBIOS       Win95Cli01     191     2.710400 SMB C Transaction \MAILSLOT\NET\NETLOGON
1398 NetBIOS       Win95Cli01     191     2.661790 SMB C Transaction \MAILSLOT\NET\NETLOGON
1400 NetBIOS       Warp Server    167    13.951790 SMB C Transaction \MAILSLOT\NET\GETDC000
1401 9.3.1.11      9.3.1.140       52     2.364270 ARP Prot=IP Request PA=9.3.1.11
1403 Warp Server   Win95Cli01      96    20.941520 SMB C Tree Connect and X Path=\\WS_SRV01\IPC$ Device=IPC
1405 Win95Cli01    Warp Server     18     0.616840 LLC D=F0 S=F0 R S RR NR=12
1406 Win95Cli01    Warp Server     77     0.573260 SMB R Tree Connected and X Service=IPC
1407 Warp Server   Win95Cli01     150     1.433980 SMB C Transaction \PIPE\LANMAN
1408 Win95Cli01    Warp Server     18     0.441680 LLC D=F0 S=F0 R S RR NR=13
1409 Win95Cli01    Warp Server   2144     7.008160 SMB R Transaction Completed

SECTION 5A (SEE NOTE 5)
1410 Warp Server   Win95Cli01      97     5.148430 SMB C Tree Connect and X Path=\\WS_SRV01\CD-ROM Device=A:
1411 Win95Cli01    Warp Server     18     0.426590 LLC D=F0 S=F0 R S RR NR=14
1412 Win95Cli01    Warp Server     81     4.146900 SMB R Tree Connected and X Service=A:CDFS
1414 Warp Server   Win95Cli01     148     7.433080 SMB C Transaction \PIPE\LANMAN
1415 Win95Cli01    Warp Server     18     0.446710 LLC D=F0 S=F0 R S RR NR=15
1416 Win95Cli01    Warp Server   2144     6.292430 SMB R Transaction Completed

SECTION 5B (SEE NOTE 5)
1417 Warp Server   Win95Cli01      95     5.407400 SMB C Tree Connect and X Path=\\WS_SRV01\DATA Device=A:
1418 Win95Cli01    Warp Server     18     0.576610 LLC D=F0 S=F0 R S RR NR=16
1421 Win95Cli01    Warp Server     84     0.835580 SMB R Tree Connected and X Service=A:HPFS386
1422 Warp Server   Win95Cli01     150     3.929840 SMB C Transaction \PIPE\LANMAN
1423 Win95Cli01    Warp Server     18     0.450060 LLC D=F0 S=F0 R S RR NR=17
1424 Win95Cli01    Warp Server   2144     6.705610 SMB R Transaction Completed

SECTION 5C (SEE NOTE 5)
1426 Warp Server   Win95Cli01      97     5.162670 SMB C Tree Connect and X Path=\\WS_SRV01\PUBLIC Device=A:
1427 Win95Cli01    Warp Server     18     0.530510 LLC D=F0 S=F0 R S RR NR=18
1428 Win95Cli01    Warp Server     84     0.235510 SMB R Tree Connected and X Service=A:HPFS386
1429 Warp Server   Win95Cli01     152     3.893800 SMB C Transaction \PIPE\LANMAN
1430 Win95Cli01    Warp Server     18     0.450060 LLC D=F0 S=F0 R S RR NR=19
1431 Win95Cli01    Warp Server   2144     6.409760 SMB R Transaction Completed

SECTION 5D (SEE NOTE 5)
1433 Warp Server   Win95Cli01      99     5.278330 SMB C Tree Connect and X Path=\\WS_SRV01\TRANSFER Device=A:
1434 Win95Cli01    Warp Server     18     0.529680 LLC D=F0 S=F0 R S RR NR=20
1435 Win95Cli01    Warp Server     84     0.553140 SMB R Tree Connected and X Service=A:HPFS386
1437 Warp Server   Win95Cli01      98     7.680320 SMB C Tree Connect and X Path=\\WS_SRV01\IBMLAN$ Device=A:
1438 Win95Cli01    Warp Server     84     0.527160 SMB R Tree Connected and X Service=A:HPFS386
```

Figure 211 (Part 2 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
SECTION 6 (SEE NOTE 6)
1439 Warp Server   Win95Cli01      130      2.288000 SMB C Open and X \DCDB\USERS\W95TEST1\PROFILE.BAT
1440 Win95Cli01    Warp Server      67      0.541410 SMB R Open and X Failed (File not found)
1441 Warp Server   Win95Cli01      129      3.123580 SMB C Transaction \PIPE\LANMAN
1442 Win95Cli01    Warp Server      18      0.909330 LLC D=F0 S=F0 R S RR NR=23
1444 Win95Cli01    Warp Server     110      6.095480 SMB R Transaction Completed
1445 Warp Server   Win95Cli01       67      2.337450 SMB C Tree Disconnect T=D0BB
1446 Win95Cli01    Warp Server      18      0.395580 LLC D=F0 S=F0 R S RR NR=24
1447 Win95Cli01    Warp Server      67      0.328530 SMB R Tree Disconnected
1449 Warp Server   Win95Cli01       32     21.285140 NETBIOS D=31 S=06 Data ACK
1450 Win95Cli01    Warp Server      18      0.582480 LLC D=F0 S=F0 R S RR NR=25


SECTION 7 (SEE NOTE 7)
1451 Warp Server   Win95Cli01       78      4.643050 SMB C Get File Attributes \USER.MAN
1452 Win95Cli01    Warp Server      67      0.498670 SMB R Get File Attributes Failed (File not found)
1454 Warp Server   Win95Cli01       78     21.337100 SMB C Get File Attributes \USER.DAT
1455 Win95Cli01    Warp Server      87      0.502860 SMB R Got File Attributes
1456 Warp Server   Win95Cli01      107      1.986290 SMB C Open and X \USER.DAT
1457 Win95Cli01    Warp Server      97      0.552300 SMB R Opened and X F=0046
1459 Warp Server   Win95Cli01       73      1.993830 SMB C Close File F=0046
1460 Win95Cli01    Warp Server      67      0.497830 SMB R Closed File
1463 Warp Server   Win95Cli01       32     36.143750 NETBIOS D=31 S=06 Data ACK
1464 Win95Cli01    Warp Server      18      0.330210 LLC D=F0 S=F0 R S RR NR=30


SECTION 8 (SEE NOTE 8)
1472 Warp Server   Win95Cli01      102     91.121200 SMB C Tree Connect and X Path=\\WS_SRV01\NETLOGON Device=?????
1473 Win95Cli01    Warp Server      84      0.529680 SMB R Tree Connected and X Service=A:HPFS386
1474 Warp Server   Win95Cli01       80      1.392920 SMB C Get File Attributes \CONFIG.POL
1475 Win95Cli01    Warp Server      87      0.502860 SMB R Got File Attributes
1476 Warp Server   Win95Cli01       98      1.853030 SMB C Set File Attributes \CONFIG.POL
1477 Win95Cli01    Warp Server      67      0.528000 SMB R Set File Attributes Failed (Access denied)
1478 Warp Server   Win95Cli01      109      1.976230 SMB C Open and X \CONFIG.POL
1479 Win95Cli01    Warp Server      97      0.532190 SMB R Opened and X F=0047
1481 Warp Server   Win95Cli01       83      1.701340 SMB C Read Block Raw F=0047 4096 at 0
1482 Win95Cli01    Warp Server    4076      2.986140 NETBIOS D=06 S=31 Data, 232 bytes
1483 Win95Cli01    Warp Server      84      0.676340 NETBIOS D=06 S=31 Data, 52 bytes
1484 Win95Cli01    Warp Server      32      4.524880 NETBIOS D=31 S=06 Data ACK
1485 Win95Cli01    Warp Server      18      0.369600 LLC D=F0 S=F0 R S RR NR=36
1486 Warp Server   Win95Cli01       83      1.796880 SMB C Read Block Raw F=0047 4096 at 4096
1487 Win95Cli01    Warp Server    4076      3.059050 NETBIOS D=06 S=31 Data, 232 bytes
1489 Win95Cli01    Warp Server      84      0.942020 NETBIOS D=06 S=31 Data, 52 bytes
1490 Win95Cli01    Warp Server      32      4.344690 NETBIOS D=31 S=06 Data ACK
1491 Win95Cli01    Warp Server      18      0.370440 LLC D=F0 S=F0 R S RR NR=38
1496 Warp Server   Win95Cli01       98     64.601320 SMB C Set File Attributes \CONFIG.POL
1497 Win95Cli01    Warp Server      67      0.556500 SMB R Set File Attributes Failed (Access denied)
1499 Warp Server   Win95Cli01       32     21.205520 NETBIOS D=31 S=06 Data ACK
1501 Win95Cli01    Warp Server      18      0.635280 LLC D=F0 S=F0 R S RR NR=40
1519 Warp Server   Win95Cli01      127    580.029000 SMB C Transaction \PIPE\LANMAN
1520 Win95Cli01    Warp Server      18      0.438330 LLC D=F0 S=F0 R S RR NR=41
1521 Win95Cli01    Warp Server     987      1.862250 SMB R Transaction Completed
1523 Warp Server   Win95Cli01      127     10.749430 SMB C Transaction \PIPE\LANMAN
1524 Win95Cli01    Warp Server      18      0.436650 LLC D=F0 S=F0 R S RR NR=42
1525 Win95Cli01    Warp Server     987      1.833760 SMB R Transaction Completed
1526 Warp Server   Win95Cli01       32     19.235990 NETBIOS D=31 S=06 Data ACK
1527 Win95Cli01    Warp Server      18      0.368760 LLC D=F0 S=F0 R S RR NR=43
1528 Warp Server   Win95Cli01      127      7.029120 SMB C Transaction \PIPE\LANMAN
1529 Win95Cli01    Warp Server      18      0.414860 LLC D=F0 S=F0 R S RR NR=44
1530 Win95Cli01    Warp Server     987      1.940190 SMB R Transaction Completed
1532 Warp Server   Win95Cli01       32     26.581070 NETBIOS D=31 S=06 Data ACK
1533 Win95Cli01    Warp Server      18      0.367920 LLC D=F0 S=F0 R S RR NR=45
1534 Warp Server   Win95Cli01      127     50.766860 SMB C Transaction \PIPE\LANMAN
1535 Win95Cli01    Warp Server      18      0.439160 LLC D=F0 S=F0 R S RR NR=46
1536 Win95Cli01    Warp Server     987      1.658590 SMB R Transaction Completed
1539 Warp Server   Win95Cli01       32     47.809220 NETBIOS D=31 S=06 Data ACK
1540 Win95Cli01    Warp Server      18      0.367920 LLC D=F0 S=F0 R S RR NR=47
```

Figure 211 (Part 3 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
SECTION 9 (SEE NOTE 9)
1542 Warp Server   Win95Cli01      77     40.411340 SMB C Get File Attributes \DESKTOP
1543 Win95Cli01    Warp Server     18      0.389710 LLC D=F0 S=F0 R S RR NR=48
1544 Win95Cli01    Warp Server     87      0.386360 SMB R Got File Attributes
1545 Warp Server   Win95Cli01     123      4.011130 SMB C Transact2 Find First \DESKTOP\*.*
1546 Win95Cli01    Warp Server    448      0.970520 SMB R Transact2 Completed
1547 Warp Server   Win95Cli01     136      7.071860 SMB C Transact2 Find First \DESKTOP\MY BRIEFCASE\*.*
1548 Win95Cli01    Warp Server     18      0.364570 LLC D=F0 S=F0 R S RR NR=50
1549 Win95Cli01    Warp Server    156      0.394740 SMB R Transact2 Completed
1550 Warp Server   Win95Cli01     113      2.164800 SMB C Transact2 Find Next
1551 Win95Cli01    Warp Server     95      0.535540 SMB R Transact2 Failed (No more files)
1552 Warp Server   Win95Cli01      69      1.885720 SMB C Find Close F=20A3
1553 Win95Cli01    Warp Server     67      0.397260 SMB R Find Closed
1555 Warp Server   Win95Cli01     143      8.161380 SMB C Transact2 Find Next
1556 Win95Cli01    Warp Server    137      0.570740 SMB R Transact2 Completed
1557 Warp Server   Win95Cli01     125      3.651590 SMB C Transact2 Find Next
1558 Win95Cli01    Warp Server     95      0.539730 SMB R Transact2 Failed (No more files)
1559 Warp Server   Win95Cli01      69      1.712230 SMB C Find Close F=20A2
1560 Win95Cli01    Warp Server     67      0.394740 SMB R Find Closed
1561 Warp Server   Win95Cli01      77     23.174210 SMB C Get File Attributes \DESKTOP
1562 Win95Cli01    Warp Server     87      0.920230 SMB R Got File Attributes
1563 Warp Server   Win95Cli01     123      3.972580 SMB C Transact2 Find First \DESKTOP\*.*
1564 Win95Cli01    Warp Server    448      0.833070 SMB R Transact2 Completed
1565 Warp Server   Win95Cli01     136      5.439250 SMB C Transact2 Find First \DESKTOP\MY BRIEFCASE\*.*
1566 Win95Cli01    Warp Server    156      0.582480 SMB R Transact2 Completed
1567 Warp Server   Win95Cli01     113      2.058370 SMB C Transact2 Find Next
1568 Win95Cli01    Warp Server     95      0.538060 SMB R Transact2 Failed (No more files)
1569 Warp Server   Win95Cli01      69      1.654400 SMB C Find Close F=20A5
1570 Win95Cli01    Warp Server     67      0.397260 SMB R Find Closed
1571 Warp Server   Win95Cli01     143      4.990030 SMB C Transact2 Find Next
1572 Win95Cli01    Warp Server    137      0.550630 SMB R Transact2 Completed
1573 Warp Server   Win95Cli01     125      1.960310 SMB C Transact2 Find Next
1574 Win95Cli01    Warp Server     95      0.543920 SMB R Transact2 Failed (No more files)
1575 Warp Server   Win95Cli01      69      1.580650 SMB C Find Close F=20A4
1576 Win95Cli01    Warp Server     67      0.522130 SMB R Find Closed
1578 Warp Server   Win95Cli01      32     41.959300 NETBIOS D=31 S=06 Data ACK
1579 Win95Cli01    Warp Server     18      0.332730 LLC D=F0 S=F0 R S RR NR=64
1580 Warp Server   Win95Cli01     127      6.425690 SMB C Transaction \PIPE\LANMAN
1581 Win95Cli01    Warp Server     18      0.542250 LLC D=F0 S=F0 R S RR NR=65
1582 Win95Cli01    Warp Server    987      1.576460 SMB R Transaction Completed
1584 Warp Server   Win95Cli01     127     29.305720 SMB C Transaction \PIPE\LANMAN
1585 Win95Cli01    Warp Server     18      0.539730 LLC D=F0 S=F0 R S RR NR=66
1586 Win95Cli01    Warp Server    987      1.892420 SMB R Transaction Completed
1588 Warp Server   Win95Cli01      32     41.064210 NETBIOS D=31 S=06 Data ACK
1589 Win95Cli01    Warp Server     18      0.296690 LLC D=F0 S=F0 R S RR NR=67
1590 Warp Server   Win95Cli01     127     31.197300 SMB C Transaction \PIPE\LANMAN
1591 Win95Cli01    Warp Server     18      0.473530 LLC D=F0 S=F0 R S RR NR=68
1592 Win95Cli01    Warp Server    987      1.561370 SMB R Transaction Completed
1593 Warp Server   Win95Cli01      32     36.950840 NETBIOS D=31 S=06 Data ACK
1594 Win95Cli01    Warp Server     18      0.408150 LLC D=F0 S=F0 R S RR NR=69
1596 Warp Server   Win95Cli01      76    122.829750 SMB C Get File Attributes \RECENT
1597 Win95Cli01    Warp Server     18      0.527160 LLC D=F0 S=F0 R S RR NR=70
1598 Win95Cli01    Warp Server     87      0.974710 SMB R Got File Attributes
1600 Warp Server   Win95Cli01     122     29.601570 SMB C Transact2 Find First \RECENT\*.*
1601 Win95Cli01    Warp Server    412      1.217750 SMB R Transact2 Completed
1602 Warp Server   Win95Cli01     127     15.602840 SMB C Transact2 Find Next
1603 Win95Cli01    Warp Server     18      0.404800 LLC D=F0 S=F0 R S RR NR=72
1604 Win95Cli01    Warp Server    407      0.477710 SMB R Transact2 Completed
1605 Warp Server   Win95Cli01     125     19.019760 SMB C Transact2 Find Next
1606 Win95Cli01    Warp Server    137      0.607620 SMB R Transact2 Completed
```

Figure 211 (Part 4 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
1607 Warp Server   Win95Cli01    125      4.085720 SMB C Transact2 Find Next
1608 Win95Cli01    Warp Server    95      0.493640 SMB R Transact2 Failed (No more files)
1609 Warp Server   Win95Cli01     69      1.633450 SMB C Find Close F=20A6
1610 Win95Cli01    Warp Server    67      0.416530 SMB R Find Closed
1611 Warp Server   Win95Cli01     76     22.331080 SMB C Get File Attributes \RECENT
1612 Win95Cli01    Warp Server    87      0.595890 SMB R Got File Attributes
1613 Warp Server   Win95Cli01    122      4.279320 SMB C Transact2 Find First \RECENT\*.*
1614 Win95Cli01    Warp Server   412      0.818820 SMB R Transact2 Completed
1615 Warp Server   Win95Cli01    127      3.937380 SMB C Transact2 Find Next
1616 Win95Cli01    Warp Server   407      0.822170 SMB R Transact2 Completed
1617 Warp Server   Win95Cli01    125      3.989340 SMB C Transact2 Find Next
1618 Win95Cli01    Warp Server   137      0.591700 SMB R Transact2 Completed
1619 Warp Server   Win95Cli01    125      2.234370 SMB C Transact2 Find Next
1620 Win95Cli01    Warp Server    95      0.461790 SMB R Transact2 Failed (No more files)
1621 Warp Server   Win95Cli01     69      1.567240 SMB C Find Close F=20A7
1622 Win95Cli01    Warp Server    67      0.426590 SMB R Find Closed
1627 Warp Server   Win95Cli01     32     41.511760 NETBIOS D=31 S=06 Data ACK
1628 Win95Cli01    Warp Server    18      0.344460 LLC D=F0 S=F0 R S RR NR=82
1629 Warp Server   Win95Cli01    127      9.746220 SMB C Transaction \PIPE\LANMAN
1630 Win95Cli01    Warp Server    18      0.445870 LLC D=F0 S=F0 R S RR NR=83
1631 Win95Cli01    Warp Server   987      1.724800 SMB R Transaction Completed
1632 Warp Server   Win95Cli01     32     35.382760 NETBIOS D=31 S=06 Data ACK
1633 Win95Cli01    Warp Server    18      0.346970 LLC D=F0 S=F0 R S RR NR=84
1634 Warp Server   Win95Cli01    127     10.809770 SMB C Transaction \PIPE\LANMAN
1635 Win95Cli01    Warp Server    18      0.409830 LLC D=F0 S=F0 R S RR NR=85
1636 Win95Cli01    Warp Server   987      2.238560 SMB R Transaction Completed
1637 Warp Server   Win95Cli01     32     23.358590 NETBIOS D=31 S=06 Data ACK
1638 Win95Cli01    Warp Server    18      0.350320 LLC D=F0 S=F0 R S RR NR=86
1641 Win95Cli01    Warp Server   127     61.895100 SMB C Transaction \PIPE\LANMAN
1642 Win95Cli01    Warp Server    18      0.525490 LLC D=F0 S=F0 R S RR NR=87
1643 Win95Cli01    Warp Server   987      1.635130 SMB R Transaction Completed
1644 Warp Server   Win95Cli01     77     17.702270 SMB C Get File Attributes \NETHOOD
1645 Win95Cli01    Warp Server    18      0.425750 LLC D=F0 S=F0 R S RR NR=88
1646 Win95Cli01    Warp Server    87      0.383010 SMB R Got File Attributes
1647 Warp Server   Win95Cli01    123      5.119930 SMB C Transact2 Find First \NETHOOD\*.*
1648 Win95Cli01    Warp Server   156      0.670480 SMB R Transact2 Completed
1649 Warp Server   Win95Cli01    113      2.099430 SMB C Transact2 Find Next
1650 Win95Cli01    Warp Server    18      0.627730 LLC D=F0 S=F0 R S RR NR=90
1651 Win95Cli01    Warp Server    95      0.236340 SMB R Transact2 Failed (No more files)
1652 Warp Server   Win95Cli01     69      1.780120 SMB C Find Close F=20A8
1653 Win95Cli01    Warp Server    67      0.416530 SMB R Find Closed
1654 Warp Server   Win95Cli01     77     20.498160 SMB C Get File Attributes \NETHOOD
1655 Win95Cli01    Warp Server    87      0.467660 SMB R Got File Attributes
1656 Warp Server   Win95Cli01    123      5.056240 SMB C Transact2 Find First \NETHOOD\*.*
1657 Win95Cli01    Warp Server   156      0.600080 SMB R Transact2 Completed
1658 Warp Server   Win95Cli01    113      1.979580 SMB C Transact2 Find Next
1659 Win95Cli01    Warp Server    95      0.605940 SMB R Transact2 Failed (No more files)
1660 Warp Server   Win95Cli01     69      1.550480 SMB C Find Close F=20A9
1661 Win95Cli01    Warp Server    67      0.397260 SMB R Find Closed
1662 Warp Server   Win95Cli01    127     32.698340 SMB C Transaction \PIPE\LANMAN
1663 Win95Cli01    Warp Server    18      0.430780 LLC D=F0 S=F0 R S RR NR=96
1664 Win95Cli01    Warp Server   987      1.678710 SMB R Transaction Completed
1666 Warp Server   Win95Cli01     32     39.654540 NETBIOS D=31 S=06 Data ACK
1667 Win95Cli01    Warp Server    18      0.372950 LLC D=F0 S=F0 R S RR NR=97
1668 Warp Server   Win95Cli01    127      8.227590 SMB C Transaction \PIPE\LANMAN
1669 Win95Cli01    Warp Server    18      0.433300 LLC D=F0 S=F0 R S RR NR=98
1670 Win95Cli01    Warp Server   987      1.734860 SMB R Transaction Completed
1672 Warp Server   Win95Cli01     32     30.386030 NETBIOS D=31 S=06 Data ACK
1673 Win95Cli01    Warp Server    18      0.376310 LLC D=F0 S=F0 R S RR NR=99
1678 Warp Server   Win95Cli01    127    111.378000 SMB C Transaction \PIPE\LANMAN
```

Figure 211 (Part 5 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
1679 Win95Cli01   Warp Server    18     0.439160 LLC D=F0 S=F0 R S RR NR=100
1680 Win95Cli01   Warp Server   987     1.663620 SMB R Transaction Completed
1688 Warp Server  Win95Cli01     32    47.763120 NETBIOS D=31 S=06 Data ACK
1689 Win95Cli01   Warp Server    18     0.367920 LLC D=F0 S=F0 R S RR NR=101
1715 Warp Server  Win95Cli01     80  1037.783910 SMB C Get File Attributes \START MENU
1716 Win95Cli01   Warp Server    18     0.458440 LLC D=F0 S=F0 R S RR NR=102
1717 Win95Cli01   Warp Server    87     0.377980 SMB R Got File Attributes
1718 Win95Cli01   Warp Server   126    23.211920 SMB C Transact2 Find First \START MENU\*.*
1719 Win95Cli01   Warp Server   192     0.704840 SMB R Transact2 Completed
1720 Warp Server  Win95Cli01    135     2.764040 SMB C Transact2 Find First \START MENU\PROGRAMS\*.*
1721 Win95Cli01   Warp Server    18     0.419890 LLC D=F0 S=F0 R S RR NR=104
1722 Win95Cli01   Warp Server   391     0.542250 SMB R Transact2 Completed
1723 Warp Server  Win95Cli01    147     3.031390 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\*.*
1724 Win95Cli01   Warp Server   413     0.784460 SMB R Transact2 Completed
1726 Warp Server  Win95Cli01    153     7.879780 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\GAMES\*.*
1727 Win95Cli01   Warp Server   318     0.919390 SMB R Transact2 Completed
1729 Warp Server  Win95Cli01    124    14.722840 SMB C Transact2 Find Next
1730 Win95Cli01   Warp Server    95     0.475200 SMB R Transact2 Failed (No more files)
1731 Warp Server  Win95Cli01     69     1.744080 SMB C Find Close F=20AD
1732 Win95Cli01   Warp Server    18     0.391390 LLC D=F0 S=F0 R S RR NR=108
1733 Win95Cli01   Warp Server    67     0.480230 SMB R Find Closed
1734 Warp Server  Win95Cli01    162    12.338460 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\PAINT SHOP PRO\*.*
1735 Win95Cli01   Warp Server   257     0.776920 SMB R Transact2 Completed
1736 Warp Server  Win95Cli01    136     8.153000 SMB C Transact2 Find Next
1737 Win95Cli01   Warp Server    95     0.512920 SMB R Transact2 Failed (No more files)
1738 Warp Server  Win95Cli01     69     1.614170 SMB C Find Close F=20AE
1739 Win95Cli01   Warp Server    67     0.367090 SMB R Find Closed
1740 Warp Server  Win95Cli01    125     8.123670 SMB C Transact2 Find Next
1741 Win95Cli01   Warp Server   211     0.576610 SMB R Transact2 Completed
1742 Warp Server  Win95Cli01    160     4.653110 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\SYSTEM TOOLS\*.*
1743 Win95Cli01   Warp Server   343     0.774400 SMB R Transact2 Completed
1745 Warp Server  Win95Cli01    135    14.030570 SMB C Transact2 Find Next
1746 Win95Cli01   Warp Server    95     0.491120 SMB R Transact2 Failed (No more files)
1747 Warp Server  Win95Cli01     69     1.637640 SMB C Find Close F=20AF
1748 Win95Cli01   Warp Server    67     0.575770 SMB R Find Closed
1749 Warp Server  Win95Cli01    122    11.103100 SMB C Transact2 Find Next
1750 Win95Cli01   Warp Server    95     0.469330 SMB R Transact2 Failed (No more files)
1752 Warp Server  Win95Cli01     69     1.837110 SMB C Find Close F=20AC
1753 Win95Cli01   Warp Server    67     0.351160 SMB R Find Closed
1754 Warp Server  Win95Cli01    145     9.137770 SMB C Transact2 Find First \START MENU\PROGRAMS\DOCUMENTS\*.*
1755 Win95Cli01   Warp Server   156     0.741720 SMB R Transact2 Completed
1756 Warp Server  Win95Cli01    113     2.281300 SMB C Transact2 Find Next
1757 Win95Cli01   Warp Server    95     0.490290 SMB R Transact2 Failed (No more files)
1758 Warp Server  Win95Cli01     69     1.636800 SMB C Find Close F=20B0
1759 Win95Cli01   Warp Server    67     0.417370 SMB R Find Closed
1760 Warp Server  Win95Cli01    155    10.344620 SMB C Transact2 Find First \START MENU\PROGRAMS\IBM NETWORKS CLIENT\*.*
1761 Win95Cli01   Warp Server   250     0.673830 SMB R Transact2 Completed
1762 Warp Server  Win95Cli01    126     8.243520 SMB C Transact2 Find Next
1763 Win95Cli01   Warp Server    95     0.566550 SMB R Transact2 Failed (No more files)
1765 Warp Server  Win95Cli01     69     1.946900 SMB C Find Close F=20B1
1766 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
1768 Warp Server  Win95Cli01    140     8.721230 SMB C Transact2 Find First \START MENU\PROGRAMS\MAIN\*.*
1769 Win95Cli01   Warp Server   378     0.800380 SMB R Transact2 Completed
1771 Win95Cli01   Warp Server   131    13.998730 SMB C Transact2 Find Next
1772 Win95Cli01   Warp Server    95     0.512080 SMB R Transact2 Failed (No more files)
1773 Warp Server  Win95Cli01     69     1.622550 SMB C Find Close F=20B2
1774 Win95Cli01   Warp Server    67     0.420720 SMB R Find Closed
1775 Warp Server  Win95Cli01    143    11.352860 SMB C Transact2 Find First \START MENU\PROGRAMS\STARTUP\*.*
1776 Win95Cli01   Warp Server   156     0.670480 SMB R Transact2 Completed
1777 Warp Server  Win95Cli01    113     2.070940 SMB C Transact2 Find Next
```

Figure 211 (Part 6 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
1778 Win95Cli01   Warp Server    95     0.457600 SMB R Transact2 Failed (No more files)
1779 Warp Server  Win95Cli01     69     1.640150 SMB C Find Close F=20B3
1780 Win95Cli01   Warp Server    18     0.415700 LLC D=F0 S=F0 R S RR NR=1
1781 Win95Cli01   Warp Server    67     0.368760 SMB R Find Closed
1782 Warp Server  Win95Cli01    118     6.177610 SMB C Transact2 Find Next
1783 Win95Cli01   Warp Server   143     0.527160 SMB R Transact2 Completed
1784 Warp Server  Win95Cli01    131     5.375550 SMB C Transact2 Find Next
1785 Win95Cli01   Warp Server    95     0.709870 SMB R Transact2 Failed (No more files)
1786 Warp Server  Win95Cli01     69     1.840460 SMB C Find Close F=20AB
1787 Win95Cli01   Warp Server    67     0.832230 SMB R Find Closed
1788 Warp Server  Win95Cli01    119    11.257310 SMB C Transact2 Find Next
1789 Win95Cli01   Warp Server    95     0.568230 SMB R Transact2 Failed (No more files)
1790 Warp Server  Win95Cli01     69     1.687930 SMB C Find Close F=20AA
1791 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
1793 Warp Server  Win95Cli01     32    43.260870 NETBIOS D=31 S=06 Data ACK
1794 Win95Cli01   Warp Server    18     0.349490 LLC D=F0 S=F0 R S RR NR=7
1796 Warp Server  Win95Cli01     80   127.912800 SMB C Get File Attributes \START MENU
1797 Win95Cli01   Warp Server    87     0.530520 SMB R Got File Attributes
1799 Warp Server  Win95Cli01    126    27.482860 SMB C Transact2 Find First \START MENU\*.*
1800 Win95Cli01   Warp Server   192     0.641980 SMB R Transact2 Completed
1802 Warp Server  Win95Cli01    135     2.878020 SMB C Transact2 Find First \START MENU\PROGRAMS\*.*
1803 Win95Cli01   Warp Server   391     0.812950 SMB R Transact2 Completed
1804 Warp Server  Win95Cli01    147     2.995360 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\*.*
1805 Win95Cli01   Warp Server   413     0.916880 SMB R Transact2 Completed
1806 Warp Server  Win95Cli01    153     3.895470 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\GAMES\*.*
1807 Win95Cli01   Warp Server   318     0.901790 SMB R Transact2 Completed
1809 Warp Server  Win95Cli01    124     3.449610 SMB C Transact2 Find Next
1810 Win95Cli01   Warp Server    95     0.490290 SMB R Transact2 Failed (No more files)
1811 Warp Server  Win95Cli01     69     1.806940 SMB C Find Close F=20B7
1812 Win95Cli01   Warp Server    67     0.525490 SMB R Find Closed
1813 Warp Server  Win95Cli01    162     8.249380 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\PAINT SHOP PRO\*.*
1814 Win95Cli01   Warp Server   257     0.921910 SMB R Transact2 Completed
1815 Warp Server  Win95Cli01    136     2.919090 SMB C Transact2 Find Next
1816 Win95Cli01   Warp Server    95     0.490290 SMB R Transact2 Failed (No more files)
1817 Warp Server  Win95Cli01     69     1.701330 SMB C Find Close F=20B8
1818 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
1819 Warp Server  Win95Cli01    125     7.986220 SMB C Transact2 Find Next
1820 Win95Cli01   Warp Server   211     0.771890 SMB R Transact2 Completed
1821 Warp Server  Win95Cli01    160     2.848690 SMB C Transact2 Find First \START MENU\PROGRAMS\ACCESSORIES\SYSTEM TOOLS\*.*
1822 Win95Cli01   Warp Server   343     0.776080 SMB R Transact2 Completed
1823 Warp Server  Win95Cli01    135     3.553530 SMB C Transact2 Find Next
1824 Win95Cli01   Warp Server    95     0.492800 SMB R Transact2 Failed (No more files)
1825 Warp Server  Win95Cli01     69     1.634290 SMB C Find Close F=20B9
1826 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
1828 Warp Server  Win95Cli01    122     9.033000 SMB C Transact2 Find Next
1829 Win95Cli01   Warp Server    95     0.468500 SMB R Transact2 Failed (No more files)
1830 Warp Server  Win95Cli01     69     2.029870 SMB C Find Close F=20B6
1831 Win95Cli01   Warp Server    67     0.417370 SMB R Find Closed
1832 Warp Server  Win95Cli01    145     9.356510 SMB C Transact2 Find First \START MENU\PROGRAMS\DOCUMENTS\*.*
1833 Win95Cli01   Warp Server   156     0.603430 SMB R Transact2 Completed
1834 Warp Server  Win95Cli01    113     2.044120 SMB C Transact2 Find Next
1835 Win95Cli01   Warp Server    95     0.492800 SMB R Transact2 Failed (No more files)
1836 Warp Server  Win95Cli01     69     1.700500 SMB C Find Close F=20BA
1837 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
1838 Warp Server  Win95Cli01    155    10.541580 SMB C Transact2 Find First \START MENU\PROGRAMS\IBM NETWORKS CLIENT\*.*
1839 Win95Cli01   Warp Server   250     0.687240 SMB R Transact2 Completed
1840 Warp Server  Win95Cli01    126     2.744770 SMB C Transact2 Find Next
1841 Win95Cli01   Warp Server    95     0.486930 SMB R Transact2 Failed (No more files)
1842 Warp Server  Win95Cli01     69     1.768380 SMB C Find Close F=20BB
1843 Win95Cli01   Warp Server    67     0.418210 SMB R Find Closed
```

Figure 211 (Part 7 of 8). Windows 95 Logon Traces to Illustrate SMB Flows

```
1844 Warp Server  Win95Cli01    140    8.406110 SMB C Transact2 Find First \START MENU\PROGRAMS\MAIN\*.*
1845 Win95Cli01   Warp Server   378    0.893410 SMB R Transact2 Completed
1846 Warp Server  Win95Cli01    131    6.283210 SMB C Transact2 Find Next
1847 Win95Cli01   Warp Server    95    0.490290 SMB R Transact2 Failed (No more files)
1848 Warp Server  Win95Cli01     69    1.636800 SMB C Find Close F=20BC
1849 Win95Cli01   Warp Server    67    0.417370 SMB R Find Closed
1850 Warp Server  Win95Cli01    143   15.227370 SMB C Transact2 Find First \START MENU\PROGRAMS\STARTUP\*.*
1851 Win95Cli01   Warp Server   156    0.541410 SMB R Transact2 Completed
1852 Warp Server  Win95Cli01    113    2.051660 SMB C Transact2 Find Next
1853 Win95Cli01   Warp Server    95    0.567390 SMB R Transact2 Failed (No more files)
1854 Warp Server  Win95Cli01     69    1.626750 SMB C Find Close F=20BD
1855 Win95Cli01   Warp Server    67    0.415700 SMB R Find Closed
1856 Warp Server  Win95Cli01    118    6.002450 SMB C Transact2 Find Next
1857 Win95Cli01   Warp Server   143    0.530510 SMB R Transact2 Completed
1858 Warp Server  Win95Cli01    131    2.064230 SMB C Transact2 Find Next
1859 Win95Cli01   Warp Server    95    0.488610 SMB R Transact2 Failed (No more files)
1860 Warp Server  Win95Cli01     69    1.898290 SMB C Find Close F=20B5
1861 Win95Cli01   Warp Server    18    0.419050 LLC D=F0 S=F0 R S RR NR=38
1862 Win95Cli01   Warp Server    67    0.370440 SMB R Find Closed
1864 Warp Server  Win95Cli01    119   11.187750 SMB C Transact2 Find Next
1865 Win95Cli01   Warp Server    95    0.502020 SMB R Transact2 Failed (No more files)
1866 Warp Server  Win95Cli01     69    1.635960 SMB C Find Close F=20B4
1867 Win95Cli01   Warp Server    67    0.424080 SMB R Find Closed
1869 Warp Server  Win95Cli01     32   27.116610 NETBIOS D=31 S=06 Data ACK
1870 Win95Cli01   Warp Server    18    0.318480 LLC D=F0 S=F0 R S RR NR=41
1872 Warp Server  Win95Cli01     67   81.659930 SMB C Tree Disconnect T=6000
1873 Win95Cli01   Warp Server    18    0.396420 LLC D=F0 S=F0 R S RR NR=42
1874 Win95Cli01   Warp Server    67    0.560690 SMB R Tree Disconnected
1877 Warp Server  Win95Cli01     32   50.162590 NETBIOS D=31 S=06 Data ACK
1878 Win95Cli01   Warp Server    18    0.334400 LLC D=F0 S=F0 R S RR NR=43
```

Figure 211 (Part 8 of 8). Windows 95 Logon Traces to Illustrate SMB Flows. MAC Addresses are Replaced by Symbolic Names.

Appendix B. Windows 95 Logon Traces to Illustrate NetBIOS Flows in MS TCP/IP

In the TCP/IP trace, it is interesting to see that the NetBIOS session is established over TCP/IP and no native IP is used. Another interesting feature is that NetBIOS names with 16th-byte hex values [1Bh] and [1Ch] are queried. These values are not supported by OS/2 Warp Server by default and because the names could not be resolved by broadcasting, queries are made to DNS as shown in the trace. NetBIOS names' 16th-byte values are displayed in the trace as ASCII characters, the corresponding hex values are declared in Table 20.

Note: If you install the Neighborhood Browser Enabler on the domain controller, the values [1Bh] and [1Ch] are recognized and answered by the domain controller.

Table 20. 16th-Byte Hex Values in the TCP/IP Trace			
ASCII Character	**ASCII Value in Hex**	**Used With Name**	**Corresponding Service**
(null)	00h	Computer name & domain name	Workstation service & domain name
	03h	Computer name & logon name	Messenger service
¬	1Bh	Domain name	Domain Master Browser
	1Ch	Domain name	Domain Controllers

Here is the TCP/IP trace and its explanation. No system policy download included in the trace and logon assigments handling is skipped this time as well to make the trace a bit shorter and easier to read.

Notes:

1. Name registrations begin. Workstation, domain and messenger services are registrated.
2. The user name registration as a messenger name is started.
3. Quering for the domain controller machine's NetBIOS names. The query is send to address 9.3.1.255, which is this subnet's broadcast address.
4. A NetBIOS session is opened to the server.
5. Domain controllers and domain master browser are queried. No answer, because OS/2 Warp Server does not recognize the [1Bh] and [1Ch] values by default.
6. Logon assigments are run like using NetBEUI.

379

7. Still quering for the domain controller machine's NetBIOS names. Retry count is exceeded and no more queries are broadcasted for the names.
8. Name queries are sent to the DNS address 9.3.1.74. This follows the NetBIOS name resolution flow order as described in section 12.7.5.1, "NetBIOS Over TCP/IP" on page 287.

```
Number Destination Source      Size  Delta Time (msec) Interpretation
 444 OS2Merlin   Warp Server    42  12197.723730 NETBIOS Session alive
 694 NetBIOS     Warp Server   194   7837.601200 SMB C Transaction \MAILSLOT\NET\NETLOGON
 696 9.3.1.255   9.3.1.140     265      4.280160 SMB C Transaction \MAILSLOT\NET\NETLOGON
1141 9.3.1.11    9.3.1.11       52   9836.371710 ARP Prot=IP Request PA=9.3.1.11

SECTION 1 (SEE NOTE 1)
1164 9.3.1.255   9.3.1.11      120   1056.944470 NetBIOS C ID=0 Registration Name=W95CLI01
1165 9.3.1.255   9.3.1.11      120      2.264540 NetBIOS C ID=1 Registration Name=WS_DOM01
1166 9.3.1.255   9.3.1.11      120      1.124720 NetBIOS C ID=2 Registration Name=W95CLI01
1177 9.3.1.255   9.3.1.11      120    749.438470 NetBIOS C ID=2 Registration Name=W95CLI01
1178 9.3.1.255   9.3.1.11      120      1.253790 NetBIOS C ID=1 Registration Name=WS_DOM01
1179 9.3.1.255   9.3.1.11      120      1.923430 NetBIOS C ID=3 Registration Name=W95CLI01
1195 9.3.1.255   9.3.1.11      120    751.650210 NetBIOS C ID=3 Registration Name=W95CLI01
1196 9.3.1.255   9.3.1.11      120      1.261340 NetBIOS C ID=1 Registration Name=WS_DOM01
1197 9.3.1.255   9.3.1.11      120      1.208530 NetBIOS C ID=2 Registration Name=W95CLI01
1215 9.3.1.255   9.3.1.11      120    752.859590 NetBIOS C ID=2 Registration Name=W95CLI01
1216 9.3.1.255   9.3.1.11      120      1.392080 NetBIOS C ID=1 Registration Name=WS_DOM01
1217 9.3.1.255   9.3.1.11      120      1.323360 NetBIOS C ID=3 Registration Name=W95CLI01
1431 9.3.1.255   9.3.1.11      275   7777.756080 SMB C Transaction \MAILSLOT\NET\NETLOGON
1434 NetBIOS     Warp Server   172     40.278080 SMB C Transaction \MAILSLOT\TEMP\NETLOGON
1435 9.3.1.11    9.3.1.140     243      2.172350 SMB C Transaction \MAILSLOT\TEMP\NETLOGON

SECTION 2 (SEE NOTE 2)
1436 9.3.1.255   9.3.1.11      120      3.376690 NetBIOS C ID=5 Registration Name=AUSRES07

SECTION 3 (SEE NOTE 3)
1437 9.3.1.255   9.3.1.11      102      3.629800 NetBIOS C ID=6 Query Name=WS_SRV01
1438 9.3.1.11    9.3.1.140     114      1.120530 NetBIOS R ID=6 Query OK
1440 9.3.1.140   9.3.1.11       50      1.452420 ARP Prot=IP Request PA=9.3.1.140
1441 9.3.1.11    9.3.1.140      50      0.486930 ARP Prot=IP Reply HA=_Win95Cli01
1442 9.3.1.140   9.3.1.11       66      0.792000 TCP S=1025 D=139 SEQ=29150 SYN WIN=8192
1443 9.3.1.11    9.3.1.140      66      0.943700 TCP S=139 D=1025 SEQ=3462396929 ACK=29151 SYN WIN=28672
1444 9.3.1.140   9.3.1.11       62      0.900120 TCP S=1025 D=139 SEQ=29151 ACK=3462396930 WIN=8760

SECTION 4 (SEE NOTE 4)
1445 9.3.1.140   9.3.1.11      134      0.825530 NetBIOS Session request Called name=WS_SRV01        Calling name=W95CLI01
1446 9.3.1.11    9.3.1.140      66      2.769070 NetBIOS Positive session response
1447 9.3.1.140   9.3.1.11      220      1.787660 SMB C Negotiate Protocol PC NETWORK PROGRAM 1.0 (more)
1448 9.3.1.11    9.3.1.140     144      3.406030 SMB R Negotiated Protocol 3
1449 9.3.1.140   9.3.1.11      213      4.829110 SMB C Session Setup and X Account AUSRES07  Windows 4.0 Windows 4.0
1450 9.3.1.11    9.3.1.140     149     16.436750 SMB R Session Established and X OS/2 2.40IBM LAN Server 4.0
1451 9.3.1.140   9.3.1.11      236      4.172880 SMB C Transaction \PIPE\LANMAN
1454 9.3.1.11    9.3.1.140     229     53.774790 SMB R Transaction Completed
1455 9.3.1.140   9.3.1.11      189      7.578070 SMB C Transaction \PIPE\LANMAN
1456 9.3.1.11    9.3.1.140     266      4.518180 SMB R Transaction Completed
1457 9.3.1.140   9.3.1.11      176     26.114250 SMB C Transaction \PIPE\LANMAN
1458 9.3.1.11    9.3.1.140      62      4.327090 TCP S=139 D=1025 SEQ=3462397474 ACK=29947 WIN=28672
1459 9.3.1.11    9.3.1.140     220      8.649990 SMB R Transaction Completed
```

Figure 212 (Part 1 of 2). Windows 95 Logon Traces to Illustrate NetBIOS Flows in MS TCP/IP

```
SECTION 5 (SEE NOTE 5)
1460 9.3.1.255    9.3.1.11      102     6.516200 NetBIOS C ID=8 Query Name=WS_DOM01
1464 9.3.1.140    9.3.1.11       62   131.309610 TCP S=1025 D=139 SEQ=29947 ACK=3462397632 WIN=8058
1474 9.3.1.255    9.3.1.11      120   467.103030 NetBIOS C ID=5 Registration Name=AUSRES07
1476 9.3.1.255    9.3.1.11      102   150.980570 NetBIOS C ID=8 Query Name=WS_DOM01
1491 9.3.1.255    9.3.1.11      120   604.167850 NetBIOS C ID=5 Registration Name=AUSRES07
1498 9.3.1.255    9.3.1.11      102   150.967160 NetBIOS C ID=8 Query Name=WS_DOM01
1518 9.3.1.140    9.3.1.11      101   274.948460 SMB C Tree Disconnect T=5000
1519 9.3.1.11     9.3.1.140     101     1.921750 SMB R Tree Disconnected
1520 9.3.1.140    9.3.1.11       62     1.351850 TCP S=1025 D=139 SEQ=29986 ACK=3462397671 FIN WIN=8019
1521 9.3.1.11     9.3.1.140      62     0.871620 TCP S=139 D=1025 SEQ=3462397671 ACK=29987 WIN=28672
1522 9.3.1.11     9.3.1.140      62     0.590860 TCP S=139 D=1025 SEQ=3462397671 ACK=29987 FIN WIN=28672
1523 9.3.1.140    9.3.1.11       62     0.874970 TCP S=1025 D=139 SEQ=29987 ACK=3462397672 WIN=8019
1552 9.3.1.255    9.3.1.11      120   323.604990 NetBIOS C ID=5 Registration Name=AUSRES07
1556 OS2Merlin    Warp Server    28    34.470910 LLC D=F0 S=F0 R S RR NR=108
1566 9.3.1.74     9.3.1.11       50   116.763610 ARP Prot=IP Request PA=9.3.1.74
1568 9.3.1.74     9.3.1.11      104     1.672840 DNS ID=8 Query    WS_DOM01.itsc.austin.ibm.com
1625 OS2Merlin    Warp Server    42  1034.554720 NETBIOS Session alive
1631 9.3.1.74     9.3.1.11      104   473.958660 DNS ID=8 Query    WS_DOM01.itsc.austin.ibm.com
1647 9.3.1.255    9.3.1.11      102  1237.544210 NetBIOS C ID=10 Query Name=WS_DOM01
1648 9.3.1.255    9.3.1.11      102     2.717110 NetBIOS C ID=12 Query Name=WS_DOM01
1649 9.3.1.255    9.3.1.11      262     3.027200 SMB C Transaction \MAILSLOT\NET\NETLOGON
1651 NetBIOS      Warp Server   167    11.730000 SMB C Transaction \MAILSLOT\NET\GETDC000
1652 9.3.1.11     9.3.1.140     236     2.680230 SMB C Transaction \MAILSLOT\NET\GETDC000
1653 9.3.1.140    9.3.1.11       66    22.847350 TCP S=1026 D=139 SEQ=34351 SYN WIN=8192
1654 9.3.1.11     9.3.1.140      66     1.165790 TCP S=139 D=1026 SEQ=3462998529 ACK=34352 SYN WIN=28672
1656 9.3.1.140    9.3.1.11       62     1.145680 TCP S=1026 D=139 SEQ=34352 ACK=3462998530 WIN=8760

SECTION 6 (SEE NOTE 6)
1668 9.3.1.140    9.3.1.11      131     2.871320 SMB C Tree Connect and X Path=\\WS_SRV01\CD-ROM Device=A:
1669 9.3.1.11     9.3.1.140     115     5.041990 SMB R Tree Connected and X Service=A:CDFS
1696 9.3.1.11     9.3.1.140     144     8.787440 SMB R Transaction Completed
...
1697 9.3.1.140    9.3.1.11      101     2.572960 SMB C Tree Disconnect T=D0BB
1698 9.3.1.11     9.3.1.140     101     1.709720 SMB R Tree Disconnected

SECTION 7 (SEE NOTE 7)
1702 9.3.1.74     9.3.1.11      104    66.412440 DNS ID=8 Query    WS_DOM01.itsc.austin.ibm.com
1705 9.3.1.140    9.3.1.11       62   107.308200 TCP S=1026 D=139 SEQ=35815 ACK=3463007604 WIN=8488
1716 9.3.1.255    9.3.1.11      102   394.662160 NetBIOS C ID=12 Query Name=WS_DOM01
1717 9.3.1.255    9.3.1.11      102     1.913370 NetBIOS C ID=10 Query Name=WS_DOM01
1732 9.3.1.255    9.3.1.11      102   743.362280 NetBIOS C ID=10 Query Name=WS_DOM01
1733 9.3.1.255    9.3.1.11      102     1.243730 NetBIOS C ID=12 Query Name=WS_DOM01
1738 9.3.1.140    9.3.1.11      101   259.639790 SMB C Tree Disconnect T=5800
1739 9.3.1.11     9.3.1.140     101     1.894940 SMB R Tree Disconnected
1742 9.3.1.140    9.3.1.11       62   121.268370 TCP S=1026 D=139 SEQ=35854 ACK=3463007643 WIN=8449

SECTION 8 (SEE NOTE 8)
1748 9.3.1.74     9.3.1.11      104   406.566490 DNS ID=12 Query    WS_DOM01.itsc.austin.ibm.com
1750 9.3.1.74     9.3.1.11      104     7.707970 DNS ID=10 Query    WS_DOM01.itsc.austin.ibm.com
1794 9.3.1.74     9.3.1.11      104  1490.847990 DNS ID=12 Query    WS_DOM01.itsc.austin.ibm.com
1797 9.3.1.74     9.3.1.11      104     6.661190 DNS ID=10 Query    WS_DOM01.itsc.austin.ibm.com
1887 9.3.1.74     9.3.1.11      104  1495.421480 DNS ID=12 Query    WS_DOM01.itsc.austin.ibm.com
1889 9.3.1.74     9.3.1.11      104    11.741730 DNS ID=10 Query    WS_DOM01.itsc.austin.ibm.com
```

*Figure 212 (Part 2 of 2). Windows 95 Logon Traces to Illustrate NetBIOS Flows in MS TCP/IP.
System Policy Download and Logon Assignments Not Included.*

Appendix C. Windows 95 Slow Network Performance

The following traces show performance problems that might occur with Windows 95 clients.

C.1 Microsoft Windows 95 Redirector Code

Although IBM's Network Client for Windows 95 enhances Windows 95 to log on to an OS/2 Warp Server domain, the Windows 95 client still is responsible for API calls to the protocol and redirector code supplied in Windows 95. IBM Network Client for Windows 95 allows the customer to get logon assignments added at logon.

C.1.1 Slow Network Performance Sympton

Some customers might see an unreasonable delay in the logon sequence. In comparison to a 13 second logon time with a like number of logon assignments with OS/2 Warp, you might see a up to a three minute logon time. This of course is unacceptable.

We share traces with you that allow you to compare OS/2 logon sequence against Windows 95 logon sequence. You see when you compare the two traces (one of a logon using OS/2 and one using the Windows 95 code) that OS/2 makes one NetBIOS name query, which is responded to immediately. Under the Windows 95 logon you see a series of four NetBIOS name queries, the first three with no routing information and the fourth with the requested routing information. The user is forced to time out three times for each resource they are connecting to. This adds up to a long logon time.

C.1.2 Comparing Sniffer Traces Windows 95 with OS/2

Comparing the SNIFFER traces:

1. Windows 95 logon with NetBIOS only (approx 51 seconds)

   User TBMTEST2 is used in both instances to logon to domain DOM4. Investigation shows Windows 95 making repeated `NETBIOS Find Name` queries that appear to be timing out. The following are examples from Windows 95 trace:

```
Frame  msec  cmd
21     1     NETBIOS Find name DOM4DC01
24     877   NETBIOS Find name DOM4DC01
26     877   NETBIOS Find name DOM4DC01
27           NETBIOS Name DOM4DC01 recognized
58     15    NETBIOS Find name DOM4DB02
61     853   NETBIOS Find name DOM4DB02
```

```
63    661   NETBIOS Find name DOM4DB02
64          NETBIOS Name DOM4DB01 recognized
```

This pattern of NetBIOS timing out is repeated througout the Windows 95 trace for each `NETBIOS Find name` query.

2. OS/2 logon with NetBIOS only (approx 13 seconds)

In the IBM OS/2 trace for the first grouping of `NetBIOS Find name` queries `DOM4DC01`:

```
Frame  msec  cmd
9     182   NETBIOS Find name DOM4DC01
10          NETBIOS Name DOM4DC01 recognized
```

3. Additionally, comparing the sequences of the two traces: (editing `DOM4` from each of the `NetBIOS Find name` query)

```
OS/2                 Win95
Logon                Logon
NETBIOS Find DC01    NETBIOS Find DC01
NETBIOS Find DB02    NETBIOS Find DB02
NETBIOS Find FS04    NETBIOS Find DC01
NETBIOS Find FS01    NETBIOS Find DC01
NETBIOS Find PS04    NETBIOS Find PSO4
NETBIOS Find DC01    NETBIOS Find DC01
                     NETBIOS Find FS04
                     NETBIOS Find DC01
                     NETBIOS Find DB03
                     NETBIOS Find DC01
                     NETBIOS Find FS09
                     NETBIOS Find FS01
```

Where:

```
ID    Role
DC01 - Domain Controller
DB03 - Network group drive
DB02 - Network home directory
FS09 - Network directory
FS04 - Network directory
FS01 - Network directory
FS04 - Print Server
```

Not only are there more `NETBIOS Find Name` queries on the Windows 95 side, each one takes much longer because of the repeated `NETBIOS Find name` queries. This scenario adds up to a significantly longer logon time for Windows 95.

Note: The repeated `NETBIOS find name` query for `DC01` after each connection to the other servers. Quick logon was enabled.

4. Further research on the trace:

   With the multiple `NETBIOS Find Name` queries:

   • IBM OS/2 NetBIOS: (typically)

   ```
   NETBIOS Find name (routing information)
   NETBIOS Name recognized
   ```

   • Windows 95 NetBIOS: (typically)

   ```
   NETBIOS Find name (no routing info) (timeout)
   NETBIOS Find name (no routing info) (timeout)
   NETBIOS Find name (no routing info) (timeout)
   NETBIOS Find name (broadcast all routes?)
   NETBIOS Name recognized
   ```

C.1.3 Resolution of the Slow Network Performance

From Microsoft you can get an updated version of the NETBEUI.VXD file that resolves this problem. The version number of this file is NETBEUI.VXD Version 4.00.951

When you are using NetBEUI on a token-ring network, a NameQuery packet is broadcast several times without the source routing field set. If there is no response to half the possible name query requests, remaining requests are resubmitted with the source routing field set. This behavior was designed to reduce network traffic on the LAN. If a program repeatedly establishes connections and disconnects from servers across a source routing bridge, network performance is greatly reduced.

This update recognizes a registry entry that enables the source routing information on all NameQuery packets. The default is to send the first four NameQuery requests without the source routing information. To enable source routing information on all NameQuery packets, add the string value:

`QueryAlwaysUsesSourceRouting`

to the registry under:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VXD\Netbeui`

If the value is 1, NetBEUI uses source routing information in all NameQuery packets. The default value is 0, which broadcasts half of the NameQuery packets on the local ring first without source routing information.

Appendix D. PCMCIA Configuration Files for DOS with Windows for Workgroups

The following examples show configuration information for PCMCIA-based machines.

D.1 DOS LAN Services Configured for PCMCIA Machines

This section shows example files how an IBM ThinkPad 750C was configured to work with PC-DOS 7.0, Windows for Workgroups, and DOS LAN Services with TCPBEUI (Real-Mode) support.

Notes:

1. IBM PC-DOS 7 is the only DOS version available with integrated PCMCIA support. PCMCIA support can be installed with the `PCMDINST` command.

2. For IBM ThinkPads later than 750, you need to use PC Card Director rather than the PCMCIA support of PC-DOS 7.

After the full redirector was loaded with the TCPBEUI (Real-Mode) network driver and a logon was successfully completed, the amount of available base memory was 390 kB. All PCMCIA drivers can be loaded into upper memory yet leaving not many upper memory blocks available for other drivers.

D.1.1 CONFIG.SYS with PCMCIA and VESA Support

Following example shows a PC-DOS 7 CONFIG.SYS file with PCMCIA and VESA support enabled:

```
DEVICE = C:\DOS\PCM\CNFIGNAM.EXE /DEFAULT
DEVICE = C:\DOS\HIMEM.SYS
DEVICE = C:\DOS\EMM386.EXE NOEMS RAM X=A000-BFFF I=C000-D3FF X=D400-F7FF
DOS=HIGH,UMB
FILES=42
BUFFERS=16
DEVICEHIGH = C:\IBMVESA\VESA.EXE
DEVICEHIGH = C:\DOS\PCM\PCMSS.EXE
DEVICEHIGH = C:\DOS\PCM\PCMCS.EXE
DEVICEHIGH = C:\DOS\PCM\PCMRMAN.SYS
DEVICEHIGH = C:\DOS\PCM\PCMSCD.EXE
STACKS=9,256
SHELL=C:\DOS\COMMAND.COM C:\DOS\ /E:512 /P
LASTDRIVE=Z
SWITCHES=/W
DEVICEHIGH = C:\NET\PROTMAN.DOS /i:C:\NET
DEVICEHIGH = C:\NET\IBMTOKCS.DOS
DEVICEHIGH = C:\NET\NTSTS.DOS
DEVICEHIGH = C:\NET\DLSHELP.SYS
```

Figure 213. CONFIG.SYS File with PCMCIA and VESA Support

D.1.2 AUTOEXEC.BAT with NET Support

Following example shows a PC-DOS 7 AUTOEXEC.BAT file with DOS LAN
Services support enabled:

```
@ECHO OFF
SET PATH=C:\NET;C:\NWDBPATH;C:\WINDOWS;C:\;C:\DOS;C:\DOS\PCM;
SET TEMP=C:\TEMP
SET TCPHELP=C:\NET
SET ETCDIR=C:\ETC
LH C:\DOS\KEYB.COM US,,C:\DOS\KEYBOARD.SYS
LH C:\DOS\MOUSE.COM
LH C:\DOS\DOSKEY.COM
LH C:\DOS\SHARE.EXE
CLS
C:\NET\NET START
C:\WINDOWS\WIN
```

Figure 214. AUTOEXEC.BAT File with NET Support of DOS LAN Services

D.1.3 PROTOCOL.INI with TCPBEUI (Real-Mode)

Following example shows a DLS PROTOCOL.INI file with TCPBEUI
(Real-Mode) loaded:

```
[network.setup]
version=0x3100
netcard=IBM_TRCC,1,IBM_TRCC
transport=nts$ntsts,NTS$NTSTS
lana0=IBM_TRCC,1,nts$ntsts

[NTS$NTSTS]
DNSAddr=[9.53.249.2]
GatewayAddr=[9.53.62.129]
NetSubNetMask=[255.255.255.128]
IPAddr=[9.53.62.187]
NodeType=H-Node
NBNSAddr=[9.3.1.81]
NBDGAddr=[9.3.1.81]
Token-Ring
DriverName=ntsts$
VCs=16
VCReceiveLarge=6
VCSends=6
RcvWindow=2920
UseMemory=UMB
BINDINGS=IBM_TRCC
LANABASE=0
[protman]
DriverName=PROTMAN$
PRIORITY=nts$ntsts

[IBM_TRCC]
DriverName=IBMTOK$
MAXTRANSMITS=6
RECVBUFS=2
RECVBUFSIZE=256
XMITBUFS=1
XMITBUFSIZE=2040
RINGSPEED=16
```

Figure 215. PROTOCOL.INI File with TCPBEUI (Real-Mode)

D.1.4 SYSTEM.INI with PCMCIA, Audio, Video, and Network Support

Following example shows a Windows for Workgroups SYSTEM.INI file with
PCMCIA, Network, Video, and Audio support loaded:

```
[boot]
386grabber=v7vga.3gr
oemfonts.fon=vgaoem.fon
fixedfon.fon=vgafix.fon
fonts.fon=vgasys.fon
display.drv=vgac24.drv
shell=progman.exe
network.drv=dlsnet.drv
mouse.drv=mouse.drv
language.dll=
drivers=mmsystem.dll power.drv
sound.drv=mmsound.drv
comm.drv=comm.drv
keyboard.drv=keyboard.drv
system.drv=system.drv

[keyboard]
subtype=
type=4
keyboard.dll=
oemansi.bin=

[boot.description]
aspect=100,96,96
displayinf=OEM0.INF
display.drv=SVGA(WD90C24)  640x480 256 colors small fonts
keyboard.typ=Enhanced 101 or 102 key US and Non US keyboards
mouse.drv=Microsoft, or IBM PS/2
language.dll=English (American)
system.drv=MS-DOS System with APM
codepage=437
woafont.fon=English (437)
network.drv=IBM DOS LAN Services
secondnet.drv=No Additional Network Installed
```

Figure 216 (Part 1 of 4). SYSTEM.INI File with PCMCIA, Network, Video, and Audio Support

```
[386Enh]
network=vnetbios.386,vnetsup.386,vredir.386
device=tpaudvxd.386
device=MonoUMB.386
display=vddc24.386
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
VDDFreeB000=No
EnableVESABIOS=Yes
device=*vpd
mouse=*vmd
device=vpowerd.386
ebios=*ebios
woafont=dosapp.fon
keyboard=*vkd
netheapsize=36
device=*vpicd
device=*vtd
device=*reboot
device=*vdmad
device=*vsd
device=*v86mmgr
device=*pageswap
device=*dosmgr
device=*vmpoll
device=*wshell
device=*PAGEFILE
device=*BLOCKDEV
device=*vfd
device=*parity
device=*biosxlat
device=*vmcpd
device=*combuff
device=*cdpscsi
device=vtdapi.386
device=vpmtd.386
device=vcomm.386
device=serial.386
device=lpt.386
device=ifsmgr.386
device=vcache.386
device=vshare.386
local=CON
FileSysChange=off
COM3Irq=4
COM3Base=03E8
COM4Irq=3
COM4Base=02E8
Paging=0
device=C:\DOS\PCM\PCMVCD.386
COM3BASE=3E8
EmmExclude=DF00-DFFF
```

Figure 216 (Part 2 of 4). SYSTEM.INI File with PCMCIA, Network, Video, and Audio Support

```
[NonWindowsApp]
localtsrs=dosedit,ced
CommandEnvSize=512

[vcache]
minfilecache=512

[mci]
WaveAudio=mciwave.drv
Sequencer=mciseq.drv
CDAudio=mcicda.drv

[drivers]
timer=timer.drv
midimapper=midimap.drv
wave=ibmmme.drv
midi=ibmmme.drv
aux=ibmmme.drv

[DDEShares]
CHAT$=winchat,chat,,31,,0,,0,0,0
SCHAT$=winchat,chat,,31,,0,,0,0,0
CLPBK$=clipsrv,system,,31,,0,,0,0,0
HEARTS$=mshearts,hearts,,15,,0,,0,0,0

[Network]
domain=ITSCAUS
lanroot=C:\NET
computername=THINKPAD750UZ
winnet=nonet
multinet=nonet
FileSharing=No
PrintSharing=No
NibTableSize=7

[network drivers]
devdir=C:\WINDOWS
LoadRMDrivers=No
```

Figure 216 (Part 3 of 4). SYSTEM.INI File with PCMCIA, Network, Video, and Audio Support

```
[VGAC24]
CursorColor=Normal
CursorSize=Small
HWLineDraw=Yes
HWBitBlt=Yes
HWCursor=Yes
FontCache=Yes
ResourceSize=Small
GrayScale=No
DynamicResolutionChange=No
VirtualScreen=No
Resolution=640x480
[PCMCIA]
COM03=TRUE
```

Figure 216 (Part 4 of 4). SYSTEM.INI File with PCMCIA, Network, Video, and Audio Support

Appendix E. Special Notices

This publication is intended to help Network adminstrators in enabling various clients, such as OS/2 Warp 4, DOS with or without Windows, Windows 95, Windows NT, and Apple Macintosh to work with OS/2 Warp Server 4.0, including the enhancements made to OS/2 Warp Server since its roll-out in October 1995. It also helps end-users to work more efficiently with their clients in a networked environment.

The information in this publication is not intended as the specification of any programming interfaces that are provided by products described in this book.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

DatagLANce	IBM
LAN Distance	LANStreamer
Operating System/2	OS/2
ServicePac	ThinkPad
WIN-OS/2	Workplace Shell

The following terms are trademarks of other companies:

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

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

395

Other company, product, and service names may be trademarks or service marks of others.

EtherLink	3COM Corporation
1-2-3, Lotus, Freelance, Freelance Graphics, Word Pro	Lotus Development Corporation

Appendix F. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

F.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How To Get ITSO Redbooks" on page 399.

- *Inside OS/2 Warp Server, Volume 1: Explore the Core Components*, SG24-4602

- *Inside OS/2 Warp Server, Volume 2: System Management, Backup/Restore, Advanced Print Services*, SG24-4702

- *OS/2 Warp Server, Windows NT, and NetWare: A Network Operating System Study*, SG24-4786

- *OS/2 Warp Server Functional Enhancements, Part 1*, SG24-2008 (in press)

F.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

F.3 Other Publications

These publications are also relevant as further information sources:

- *Getting to Know OS/2 Warp 4*, SG24-4758-00, ISBN 0-13-842147-1

- *Prepare for OS/2 Engineer Certification*, SG24-4869-00, ISBN 9-655-61119-1

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.ibmlink.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.ibmlink.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.

399

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	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **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.ibmlink.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.ibmlink.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 _____

O Invoice to customer number _____

O 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.

Glossary

AppleTalk.   A protocol family developed by Apple Computer to implement LANs serving Macintoshes.

Bridge.   A network "relay" which reads, buffers, and sends data to relay it from one data link to another, but makes the two data links appear as one to levels higher than the data link layer.

Broadcast.   A message (such as packet or frame) sent to all the nodes on a network.

Dialup Modem.   Modem used over ordinary dial-up telephone lines as opposed to private or leased lines.

Ethernet.   LAN data-link protocol developed by a consortium of vendors, later standardized as IEEE 802.3 with a few modifications. For many applications, users have not adopted all the IEEE 802.3 differences. Ethernet/802.3 now can be run on two types of coaxial cable as well as on multi-mode fiber and unshielded twisted-pair cables. The raw rate of data transmission is 10 megabits/second.

Fast Ethernet.   A nickname for the 100 Mbps version of IEEE 802.3.

FTP.   Protocol in the TCP/IP family for copying files from one computer to another. Stands for "File Transfer Protocol".

IEEE.   Institute of Electrical & Electronic Engineers

IEEE 802.   The set of IEEE standards for the definition of LAN protocols. A story goes that a long time ago, IEEE and ANSI decided that IEEE would get the slow protocols and ANSI would get the fast ones, thus IEEE defined the 802 protocols and ANSI defined FDDI. Presumably, IEEE saw limited application for FDDI at the time. Also, the IEEE standards-making committees associated with these standards.

IEEE 802.2.   An IEEE standard for the portion of LAN data-link protocols that is the same for all

flavors of IEEE LAN protocols, such as 802.3 and 802.5. Sometimes not used.

IEEE 802.3.   An IEEE standard for LANs--their "improved" version of Ethernet. See Ethernet.

IEEE 802.5.   An IEEE standard for token-ring-based LANs. There are two types: 4 Mbps and 16 Mbps. See also "Token Ring".

IETF.   "Internet Engineering Task Force" — A group responsible for defining protocols in the TCP/IP family for use on the Internet.

IP.   "Internet Protocol" — The basic protocol of TCP/IP and the Internet.

IPX.   Novell's protocol used by NetWare. Utilizes part of XNS. A router with "IPX routing" purports to interconnect LANs so that Novell NetWare clients and servers can talk through the router.

ISDN.   "Integrated Services Digital Network" — A recent development in telephone/data communications that offers the subscriber digitized voice service and/or 64 Kbps data service.

LAN.   "Local Area Network"

Protocol.   The "rules" by which two network elements trade information in order to communicate. Must include rules about a lot of mundane detail as well as rules about how to recover from a lot of unusual communication problems. Thus, they can be quite complicated.

RFC.   "Request For Comments" — The name is a real red herring when it comes to Internet RFCs. Some really are "Requests For Comments," but all Internet protocol documents are stamped with an RFC number that they never shake; so the acronym RFC generally refers to documents that describe protocols in the TCP/IP family.

Router.   A network "relay" that uses a protocol beyond the data-link protocol to route traffic between LANs and other network links.

Routing Protocol.   A protocol sent between routers by which routers exchange information own how to route to various parts of the network. The TCP/IP family of protocols has a bunch, such as RIP, EGP, BGP, OSPF, and dual IS-IS.

SNMP.   "Simple Network Management Protocol" — Originally developed to manage IP-based network equipment like routers and bridges, now extended to wiring hubs, workstations, toasters, jukeboxes, etc. SNMP for IPX and AppleTalk under development. Widely implemented.

TCP/IP.   "Transmission Control Protocol/Internet Protocol" — Literally, two protocols developed for the Defense Data Network to allow their ARPANET to attach to other networks relatively transparently. The name also designates the entire family of protocols built out of IP and TCP. The Internet is based upon TCP/IP.

Token Ring.   People often use the term "Token Ring" to designate IEEE 802.5. In the more general sense of the phrase, a token ring is a type of LAN that has stations wired in a ring, where each station constantly passes a special message (a "token") on to the next. Whoever has the token can send a message.

WAN.   "Wide Area Network" — A term for state/country/worldwide networks developed to parallel the term LAN for "Local Area Network".

List of Abbreviations

ACL	Access Control List	**HPFS**	High Performance File System
API	Application Programming Interface	**HPFS386**	High Performance File System (32-bit)
AppleTalk	A networking protocol used to interconnect Apple Computer, Inc. devices	**HTTP**	Hypertext Transmission Protocol
		IBMGINA	Generic INteractive Application from IBM
BDC	Backup Domain Controller	**IETF**	Internet Engineering Task Force
BootP	Bootstrap Protocol	**IEEE**	Institute of Electrical and Electronics Engineers
CSD	Corrective Service Disk		
DASD	Direct Access Storage Device	**IFS**	Installable File System
DAVE	Macintosh software developed by Thursby Software Systems, Inc.	**IBM**	International Business Machines Corporation
DC	Domain Controller	**IP**	Internet Protocol
DCDB	Domain Controller Database	**IPX**	Internetwork Packet eXchange
DDE	Dynamic Data Exchange	**IPX/SPX**	Internetwork Packet eXchange/Sequenced Packet eXchange
DDNS	Dynamic Domain Name System (also Dynamic Domain Name Server)	**ISDN**	Integrated Dervices Digital Network
DES	Data Encryption Standard/System	**ITSO**	International Technical Support Organization
DHCP	Dynamic Host Configuration Protocol	**LAA**	Locally Administered Address (network adapter cards)
DLL	Dynamic Link Library		
DLS	DOS LAN Services	**LAN**	Local Area Network
DNS	Domain Name System (also Domain Name Server)	**LAPS**	LAN Adapter and Protocol Support
EMS	Expanded Memory Specification (DOS, PC, PS/2)	**LLC**	Logical Link Control (LAN, top sublayer of layer 2, IEEE 802.2)
FAT	File Allocation Table	**LM10**	LAN Manager 1.0 interface
GA	General Availability		
GUI	Graphical User Interface	**LPR**	Line Printer Requester

LSM	OS/2 LAN Server for Macintosh	**OSI**	Open Systems Interconnection
MAC	Medium Access Control (LAN, bottom sublayer of layer 2, IEEE 802.3 - 802.6)	**OT**	Open Transport (networking selection/parameters controller)
MACOS	Macintosh Operating System	**PDC**	Primary Domain Controller
MACTCP	Macintosh TCP/IP	**PIF**	Program Information File
MD5	Message Digest 5 (Rivest-Shamir-Aleman alogorithm)	**PM**	Presentation Manager
		PPP	Point-to-Point Protocol
MPTS	Multiple Protocol Transport Services (replacement for LAPS - LAN Adapter and Protocol Support)	**RAS**	Remote Access Services
		RCD	Remote Connection Server
NBDD	NetBIOS Datagram Distributor	**RFC**	Request for Comments
NBNS	NetBIOS Name Server	**RIPL**	Remote Initial Program Load
NC	Network Computing	**RSA MD5**	Rivest-Shamir-Aleman alogorithm Message Digest 5
NCB	Network Control Block		
NDIS	Network Driver Interface Specification	**SLIP**	Serial Line Interface Protocol
NetBEUI	NetBIOS Extended User Interface	**SMB**	Server Message Block
NetBIOS	Network Basic Input/Output System	**SMP**	Symmetric MultiProcessors/MultiProcessing
NetBT	Microsoft's NetBIOS over TCP/IP	**SMTP**	Simple Mail Transfer Protocol
NIC	Network Interface Card	**SNA**	Systems Network Architecture (IBM)
NOS	Network Operating System	**SNMP**	Simple Network Management Protocol
NTS	Network TeleSystems Corporation	**SPX**	Sequenced Packet eXchange
ODI	Open Datalink Interface	**TCP**	Transmission Control Protocol
OEM	Original Equipment Manufacturer	**TCP/IP**	Transmission Control Protocol/Internet Protocol
OSF	Open Software Foundation		
OS/2	Operating System/2		

TCPBEUI	TCP NetBIOS Extended User Interface (IBM's implementation of NetBIOS over TCP/IP)
TSR	Terminate and Stay Resident
UBF	Use-Based Feature
UDP	User Datagram Protocol
UMB	Upper Memory Block
UNC	Universal Naming Convention
UPM	User Profile Management
URL	Universal Resource Locator
VDM	Virtual DOS Machine
WAN	Wide Area Network
WFW	Windows for Workgroups
WINS	Windows Internet Name Service
WPS	Workplace Shell
WWW	World Wide Web
X/OPEN	A group (Bull, DEC, Ericsson, ICL, Nixdorf, Olivetti, Philips, Siemens, Unisys) to create a standard interface between software packages and UNIX (portability)
XMS	eXtended Memory Specification (DOS, PC, PS/2)

Index

Numerics

A

B

C

D

U

UBF   4
unique name   29
Use-Based Feature   4
Use-Based Pricing   3
User level   34
User profiles   95, 98, 347, 370
Users, Roaming   265, 336

V

Verification, Logon   138

W

WAN   33
WDLS.EXE   209
WDLS.INI   102
Windows   16
Windows 95   16, 32, 83, 107, 266
   Configuring DNS   303
   Configuring TCP/IP   299
   Configuring WINS/NBNS   301
   Dial-Up Networking   307
   Dynamic IP Client for Windows 95   317
   Group Policies   293
   How to Change Passwords   266
   IBM Networks Client for Windows 95   249
   Increasing Network Browsing
    Performance   274
   Installing a Network Printer   267
   Installing IBM Networks Client for Windows
    95   250
   Installing TCP/IP   298
   LMHOSTS   287, 289
   Logging on   264
   NetBEUI   281
   NetBIOS 16th-Byte Values   271
   NetBIOS Names Resolution Order
    B-Node   287
   NetBIOS over TCP/IP   285
   NetBIOS/NetBEUI   284
   Password Caching   266, 298
   Problem Determination   320
   Quick Logon   264
   Roaming User   265

Windows 95 *(continued)*
   System Policies   258, 292
   SYSTEM.INI   296, 297
   TCP/IP   284
   Uninstall IBM Networks Client for Windows
    95   262
Windows for Workgroups   32
Windows NT   17, 32, 83
   Adding Shared Applications to Program
    Groups   352
   Client Overview   321
   DHCP   341
   Dynamic Local Accounts   356
   Dynamic TCP/IP   340
   Group mapping   337
   Home directory   353
   How to Change Passwords   338
   IBM Networks Coordinated Logon Client for
    Windows NT 4.0   322
   IBM Networks Primary Logon Client for
    Windows NT 4.0   332
   IBMGINA   358
   Logoff Policy   357
   Logon authentication   335
   NetBIOS Name Resolution   341
   PPP   343
   Remote Access   343
   Roaming Users   336
   System Policies   353
   System Policy Editor   354
   User Profiles   347
   WINS/NBNS   341
WINS   41, 47, 60, 301, 329, 365
Workgroup   23, 289

ITSO Redbook Evaluation

Network Clients for OS/2 Warp Server: OS/2 Warp 4, DOS/Windows, Windows 95/NT, and Apple Macintosh
SG24-2009-00

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!)**

_____

_____

_____

_____

_____

IBML®

Printed in U.S.A.