Integrating Microsoft Windows for Workgroups with Microsoft LAN Manager 2.2

Glen Clark
Microsoft Technical Resource Group

Created: November 1992

Overview

This document discusses integrating workstations running the Microsoft® Windows™ for Workgroups operating system with integrated networking with Microsoft LAN Manager. We will examine both adding LAN Manager servers into existing Windows for Workgroups environments, and adding workstations running Windows for Workgroups into existing LAN Manager environments. All major aspects of the integration will be discussed:

- Installation considerations
- Installation of multiple protocols
- Security considerations
- Domain member issues

Note This document is not intended to supersede the information found in the *Windows for Workgroups Installation* or *User Guides*. If questions arise, please refer to those documents for the authoritative answer.

Product Highlights

Advantages of a Mixed Network

Microsoft has a scalable, modular family of network solutions, designed to address a range of information-sharing needs. If you are in a medium-sized to large organization you probably want the best in ease of installation, ease of use, and high productivity for all users at their desktops, combined with the heterogeneous connectivity, client-server solutions, and advanced management and security of a full-featured, high-end, server-based LAN. We believe the answer that meets both sets of needs is to combine the Windows for Workgroups operating system with integrated networking version 3.1 and Microsoft LAN Manager local area network software version 2.2.

What Is Windows for Workgroups?

Windows for Workgroups extends the popular, easy-to-use Windows operating system from the individual desktop to the workgroup. The information-sharing functionality of Windows for Workgroups is tightly integrated into the Windows interface, making it easy to share information and resources, such as printers, among desktops. In addition, your workgroup productivity needs for electronic mail and group scheduling have been addressed with the integration of customized versions of Microsoft Mail and Microsoft Schedule+ into the Windows for Workgroups interface. Windows for Workgroups is also the platform for future workgroup applications from Microsoft and other software vendors.

Providing networking within an organization increases communication among members of a

workgroup. This improved communication in turn raises productivity by avoiding duplication of effort and increasing synergy among workers. Windows for Workgroups makes it possible to share resources from each workstation, cutting down on duplication of data and administration of servers. In a sense, each member of the workgroup becomes the administrator of his or her own machine, which empowers workers to take ownership and place value in the data residing on their PCs.

Windows for Workgroups may meet all your information-sharing needs. Or, you may choose to use Windows for Workgroups as an excellent network desktop connected into your organization's broader network.

What Is LAN Manager?

LAN Manager is advanced, full-featured network server software designed for multiple-server networks. LAN Manager makes it easy for users with Windows-based desktops to access and use information and resources that are scattered, often on a mix of PC, minicomputer, and mainframe platforms, throughout medium-sized to large organizations. To help manage the multiple-server network, LAN Manager includes advanced tools to centrally manage security, backup, and monitoring.

Microsoft LAN Manager is also the premier client-server platform. You can use the LAN Manager server to run powerful, server-based applications such as Microsoft SQL Server; centralized document management or image management systems; or powerful vertical applications for payroll, transaction processing, inventory, manufacturing control, insurance claims management, or other functions. Client-server computing efficiently distributes the processing load between powerful servers and "client" PCs, delivering excellent price/performance benefits.

Why Combine Windows for Workgroups and LAN Manager?

Quite simply, Windows for Workgroups is the best network desktop software. It is easy to install and use, and has integrated group productivity tools.

What LAN Manager adds to the Windows for Workgroups-based network is connectivity to other platforms outside the workgroup, a way to add advanced security and centralized administration, plus the server platform needed for client-server computing.

Desktops running Windows for Workgroups can access LAN Manager servers, and LAN Manager servers can administer and monitor access rights and privileges for users of Windows for Workgroups.

Connectivity Beyond the Windows for Workgroups LAN

Users on a Windows for Workgroups-based network can access resources from the following sources: other machines running Windows for Workgroups, LAN Manager servers, NetWare servers, and servers running Windows NT. The following PCs can also access resources of Windows for Workgroups: any MS-DOS®–based machines running LAN Manager or other Microsoft-compatible client software.

If users of Windows for Workgroups in your organization will need information or resources on platforms other than those listed above, you may want to add a LAN Manager server. Once you add a LAN Manager server to a Windows for Workgroups-based LAN, all desktops running Windows for Workgroups on that LAN have access to the broad range of LAN Manager connectivity options. Using Microsoft LAN Manager Services for Macintosh® on a LAN Manager server, you can connect Apple® Macintosh PCs to your network. You can also use Microsoft LAN Manager Remote Access to allow users to dial in to the network from home or while traveling. LAN Manager 2.2 also provides connectivity to IBM® SNA networks either as a

platform for the DCA® Microsoft Communications Server, an SNA gateway, or by using the Microsoft Data Link Control protocol for the MS-DOS and Windows operating systems.

LAN Manager was designed to be network-protocol independent. This allows you to run virtually any transport, such as TCP/IP, native, without a layer of tunneling or translation at the server. Using the TCP/IP included with LAN Manager 2.2, all clients can access any TCP/IP resource directly, including servers with LAN Manager for UNIX®.

All the connectivity options explained above are available to the user of a Windows for Workgroups-based desktop. You can install the LAN Manager Remote Access Service version 1.1 client software onto a desktop running Windows for Workgroups and dial in to a LAN Manager server. You'll even find special instructions for installing the TCP/IP or DLC transports included in the LAN Manager 2.2 package onto desktops running Windows for Workgroups. For customers who require TCP/IP or DLC but don't require LAN Manager servers, Microsoft is planning to introduce separate protocol packages for Windows for Workgroups in the first quarter of 1993.

Sharing Information with Character-Based Desktops

You may have older machines in your organization that are only capable of running the MS-DOS operating system. Or, you may need network connectivity for desktops running the OS/2® 1.3 or 2.0 operating systems. Or you may have diskless PCs that need to be remotely booted from the server, a feature that is not available for the first release of Windows for Workgroups.

To address all these needs, Microsoft will continue to offer client software based on the previous LAN Manager clients. This client software can run on machines with the MS-DOS, Windows, or OS/2 operating systems and is included in the LAN Manager 2.2 server package. To obtain the right to copy this software onto a desktop, you need one LAN Manager 2.2 Client MLP (Microsoft License Pack) for each desktop. This license pack contains only a license, no software.

To summarize: The recommended LAN Manager client, if you have Windows, is Windows for Workgroups. The recommended client for MS-DOS, OS/2, and remote-boot desktops is the client software in the LAN Manager server package.

Security

Combining desktops running Windows for Workgroups with LAN Manager servers gives you a number of security options. Windows for Workgroups has "workgroup-level" security built in. Individuals using Windows for Workgroups can "share" some of the directories on their PCs and set passwords for access to those directories. Access to printers attached to PCs works the same way. It is convenient, allowing a workgroup to share files without posting them to a central server. And it does not require an administrator.

In both Windows for Workgroups and LAN Manager, passwords are protected using the government's data encryption standard (DES). Passwords cannot be traced over the network. Windows for Workgroups also encrypts Microsoft Mail files and folders, as well as messages in transit.

LAN Manager offers much greater control over security, but requires that an individual be designated as an administrator to set access rights for others. LAN Manager offers two security models. The first is share-level security, which sets passwords for protected resources. The stricter user-level security is more centralized. A user logs onto the network with a single password, and a central database contains that person's access rights to a range of network servers, shares, directories, files, printers, or other resources. This means that when you hire, transfer, or dismiss an employee, you need to make only one change, rather than distributing or changing an array of passwords. LAN Manager also allows you to easily assign expiration dates to access privileges for temporary employees, or to control the hours when a user can access

the network. Features such as Groups and Account Cloning highly automate the setting of access rights for groups such as accountants or payroll administrators.

You can allow workgroups to share their own information with the convenience of the built-in "workgroup-level" security of Windows for Workgroups, while keeping sensitive information or resources on the more tightly controlled LAN Manager servers. Or you may decide to eliminate the desktop-based file- and print-sharing capabilities of Windows for Workgroups and rely entirely on the central LAN Manager security settings. In this case, all shared information or resources will be stored on LAN Manager servers or accessed through secure gateways based on LAN Manager servers. Eliminating the file- and print-sharing capabilities of Windows for Workgroups networks will not affect the users' abilities to access LAN Manager or NetWare servers, only the ability to share files and printers directly from the desktop PC.

You may choose to allow some departments to set their own shares and passwords, while other groups, such as payroll, may need that feature disabled. The security policy you choose will depend on your organization's needs.

Central Administration

In addition to enhanced security, other LAN Manager administration features, such as login scripts, can be used with desktops running Windows for Workgroups. File replication/synchronization allows you to change program or data files on multiple LAN Manager servers in your network. You can also perform centralized and scheduled backups to LAN Manager servers.

Tools in LAN Manager and the LAN Manager resource kit also enable you to monitor and set alerts for failed login attempts, keep an audit trail of network use, and monitor network utilization.

Running Client-Server Applications

LAN Manager was designed for client-server applications. Typically, these applications are based on company-wide or departmental data. Examples of client-server applications include a customer order-entry system, a personnel management system, or a company-wide daily sales update. Often the data required is on larger systems such as a minicomputer or mainframe. The processing application runs at the LAN Manager server, with bridges or gateways to needed data. Client-server applications are often critical to the competitive success of your organization: if the application fails, the result is expensive downtime or missed opportunities.

The larger, shared-data, "server-side" of these applications can run on a LAN Manager server. The user running Windows for Workgroups at the desktop can use the client or "front-end" side of these applications. Often, this front-end is a familiar application, such as Microsoft Excel or Microsoft Word for Windows, sometimes with special commands added to the menus or other customizations. Sometimes this front-end is an application built with tools such as the Microsoft Visual Basic™ programming system. There are also numerous turnkey applications available for a variety of industries and functions.

What makes a LAN Manager server an ideal platform for client-server applications? A LAN Manager server was designed to run multiple applications simultaneously. With it, you can combine the tasks of login and validation of users with database server applications, gateways, and other needed applications. You can also run applications that simultaneously serve multiple users performing disparate tasks.

Fail-Safe or Fault-Tolerance Features

LAN Manager is designed to guard against downtime and data loss. It supports uninterruptible power supply (UPS), disk mirroring (in case the hard disk fails), and disk duplexing (in case the

drive controller fails). If you introduce a LAN Manager server into a Windows for Workgroups-based LAN, you add a more secure place for especially sensitive data or operations.

Availability of Server Applications and Tools

More than 100 client-server applications for LAN Manager are currently shipping. For a free directory, call Microsoft inside sales at 800-227-4679.

Convenience of a Windows for Workgroups-Based "Front-End"

A client-server system is designed to solve an entire task—for example, creating, tracking, and processing customer claims. To accomplish this task, many client-server systems combine data from different sources or even use multiple back-end server applications. The desktop user wants an easy-to-use interface that hides the complexity behind the scenes. On a Windows for Workgroups-based network, the user can log in once to a LAN Manager server and be confirmed and validated on the LAN Manager network. With user-level security, an application from this desktop may be accessing different resources in a secure manner (even using different transports), without the user being prompted for new passwords or disrupted in any other way.

Summary: From the Workgroup to the Department or Enterprise

How we share information with our immediate coworkers is often different from the way other departments, such as legal, payroll, or manufacturing, manage information. The combination of Windows for Workgroups and LAN Manager can create a wonderfully flexible system that meets both needs. For more detailed information, please see the Microsoft Windows for Workgroups Resource Kit.

Architectural Overview of Windows for Workgroups

Windows for Workgroups offers technical advantages:

- Automatic network card detection simplifies network client installation.
- Virtual, protected-mode drivers free more MS-DOS memory at the desktop.
- The Windows for Workgroups package contains all the client code a user needs to access servers running Novell® NetWare®, Microsoft LAN Manager, Windows for Workgroups, and Windows NT™, all from one unified interface.

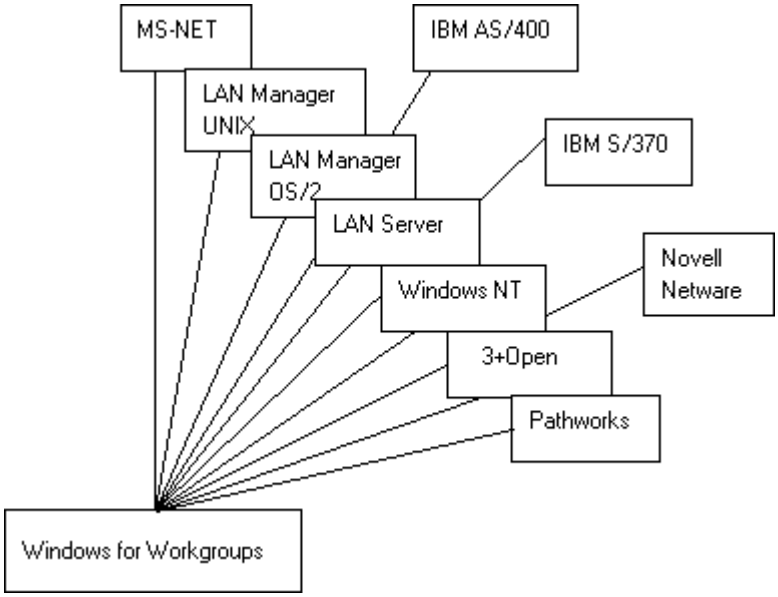

Figure 1. Interoperability of Windows for Workgroups with SMB-based products

Figure 1 describes the major existing LAN products with which Windows for Workgroups interoperates. All these products share the SMB (server message block) protocol as their means of passing operating system commands across the network. Windows for Workgroups can communicate with AS/400®s and IBM® mainframes using either the DLC protocol or SNA gateways. Although Windows for Workgroups can also interoperate with Novell NetWare, this feature is beyond the scope of this document. Please see the Microsoft Windows for Workgroups Resource Kit for more information.

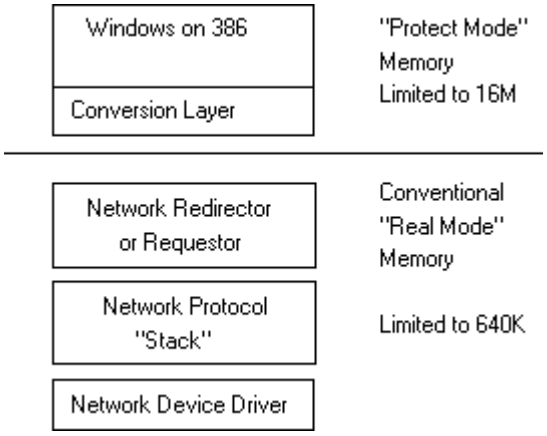

Figure 2. Windows and networks on 386 machines

Windows has been capable of using networks since its initial release. These solutions allowed Windows to use the networking facilities originally developed for the MS-DOS operating system. Figure 2 shows the active components of Windows running on a 386-class machine. There is nothing technically "wrong" with this solution; we shall see it repeated for Windows for Workgroups running on 286-class machines. It does not, however, allow the networking components to take advantage of 386 protected-mode memory. Each time Windows makes a request of the Redirector or the Protocol Stack, the microprocessor must be "context switched." Context switching involves "reprogramming" the microprocessor to use the different memory model. Each time the processing flows between real mode and protected-mode memory, a context switch occurs. Context switching cannot always be avoided, but reducing the number of context switches can increase performance.

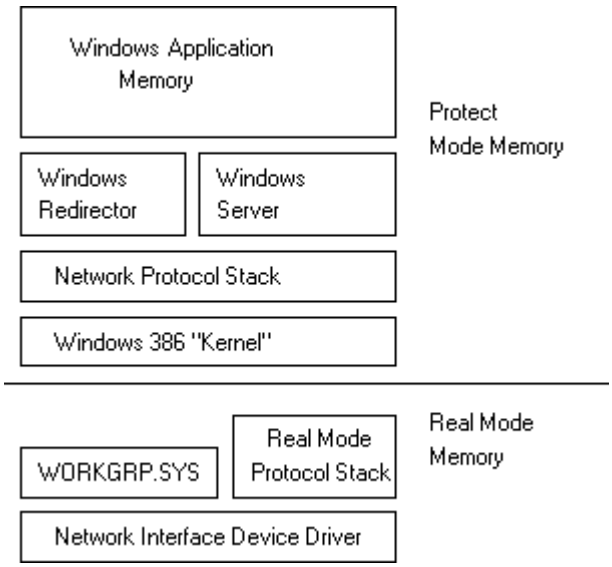

Figure 3. Windows for Workgroups and networks on 386 machines

As Figure 3 shows, Windows for Workgroups moved as many of the networking components into protected mode as possible. This decreases the number of context switches needed during network activity. Available memory in virtual MS-DOS command screens is also increased. It also provides a more stable environment for the networking components. Components in real mode can be susceptible to rogue programs (applications, terminate-and-stay-resident programs, or TSRs, or other device drivers) overwriting memory owned by others. This can cause network failures or even system freezes. Components in protected mode have their own logical memory space and cannot directly be damaged by "unfriendly" activity of other components in protected-mode memory or real-mode memory.

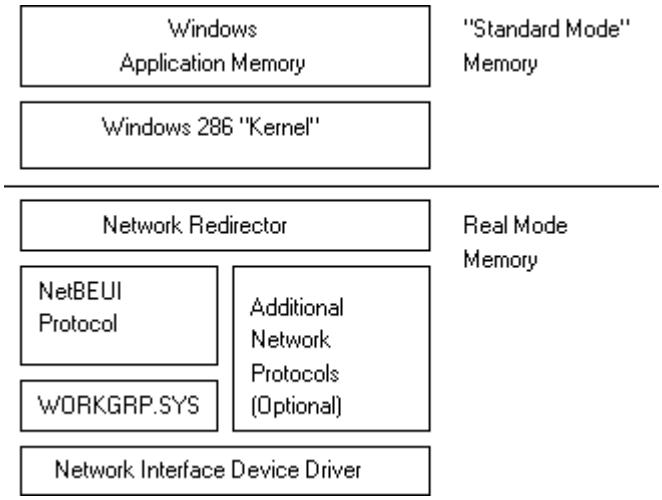

Figure 4. Windows for Workgroups and networks on 286 machines

When running on 286-class machines, Windows for Workgroups looks very much like Windows today. The 286 microprocessor does not support the 386-style protected mode. The 286 does support a form of protected-mode memory used by Windows for Workgroups. However, the protected mode redirector and server used when running on a 386 cannot execute in the 286 "standard-mode" memory environment.

Note Windows for Workgroups can be executed on a 286-class machine. It can also participate on the network using the real mode redirector. It cannot participate on the network as a Windows for Workgroups-based server, or as a Windows Mail Post Office workstation. It can

participate as a Network DDE-based client, but cannot act as a Network DDE server.

The remainder of this paper will focus on Windows for Workgroups in the 386 environment.

Installation Over MS-DOS-Based Workstations on LAN Manager Networks

Note This paper will not discuss installing Windows for Workgroups on a MS-DOS-based workstation that is not already running LAN Manager. This installation procedure is discussed in the *Windows for Workgroups Installation Guide*.

Figure 5 shows the configuration of the machine prior to the installation of Windows for Workgroups. The machine used during the development of this paper was a 386SX-class machine, with 10 MB of memory, a 60-MB hard disk, and a 3Com® EtherLink II® card (IRQ 5, IO 300, External Transceiver). Figure 6 is a memory map of the installation. We can see that all components were loaded into low memory or UMBs (upper memory blocks). This leaves approximately 500K of memory for applications to execute.

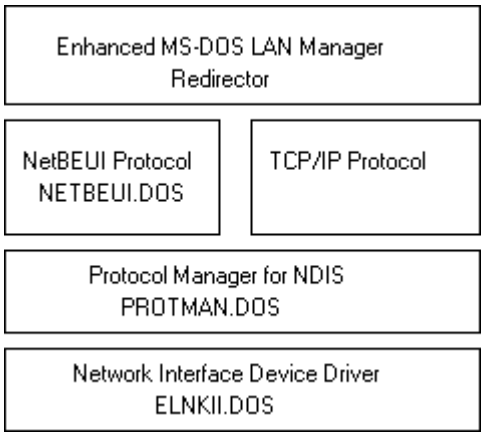

Figure 5. Enhanced LAN Manager components

```
Conventional Memory :
  Name                Size in Decimal       Size in Hex
-------------      ---------------------   -------------
  MSDOS              16000      ( 15.6K)        3E80
  SETVER               400      (  0.4K)         190
  HIMEM               1184      (  1.2K)         4A0
  EMM386              8512      (  8.3K)        2140
  PROTMAN             6208      (  6.1K)        1840
  ELNKII             14528      ( 14.2K)        38C0
  TCPDRV              1040      (  1.0K)         410
  NEMM                 400      (  0.4K)         190
  COMMAND             2624      (  2.6K)         A40
  UMB                  256      (  0.3K)         100
  NETBEUI            37104      ( 36.2K)        90F0
  TCPTSR             63504      ( 62.0K)        F810
  TINYRFC              256      (  0.3K)         100
  FREE                  64      (  0.1K)          40
  FREE                 144      (  0.1K)          90
  FREE              502768      (491.0K)       7ABF0
Total  FREE :       502976      (491.2K)
Upper Memory :
  Name                Size in Decimal       Size in Hex
-------------      ---------------------   -------------
```

```
  SYSTEM             163840      (160.0K)      28000
  UMB                   672      (  0.7K)        2A0
  TINYRFC             15328      ( 15.0K)       3BE0
  MINSES               1888      (  1.8K)        760
  NETWKSTA            93456      ( 91.3K)      16D10
  ENCRYPT              2112      (  2.1K)        840
  MSRV                10512      ( 10.3K)       2910
  NETPOPUP            18976      ( 18.5K)       4A20
  FREE                  128      (  0.1K)         80
  FREE                20608      ( 20.1K)       5080
Total  FREE :         20736      ( 20.3K)
Total bytes available to programs (Conventional+Upper) :
      523712   (511.4K)
Largest executable program size :      502768   (491.0K)
Largest available upper memory block :  20608   ( 20.1K)
```

Figure 6. Memory map of enhanced MS-DOS installation

Figure 7 shows the arrangements of components under Windows for Workgroups. Notice that on a 386-class machine the redirector and protocol components are located in protected-mode memory. Figure 8 shows the amount of conventional memory saved, roughly 100K (after compensating for the lack of TCP/IP).

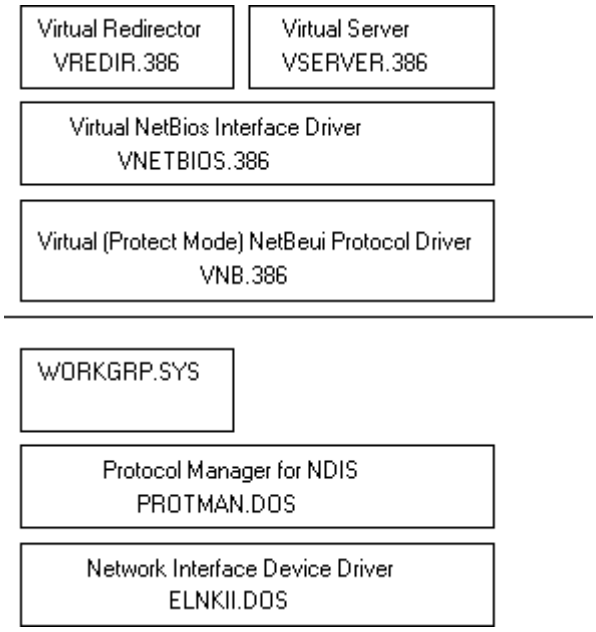

Figure 7. Components of Windows for Workgroups

```
Conventional Memory :
  Name                Size in Decimal       Size in Hex
-------------      ---------------------   ------------
  MSDOS               17152      ( 16.8K)       4300
  SETVER                400      (  0.4K)        190
  HIMEM                1072      (  1.0K)        430
  EMM386               3232      (  3.2K)        CA0
  PROTMAN               112      (  0.1K)         70
  WORKGRP              4352      (  4.3K)       1100
  ELNKII              14528      ( 14.2K)       38C0
  COMMAND              2624      (  2.6K)        A40
  FREE                   64      (  0.1K)         40
  FREE                611552      (597.2K)      954E0
Total  FREE :         611616      (597.3K)
Upper Memory :
  Name                Size in Decimal       Size in Hex
```

```
-------------       ---------------------    -------------
  SYSTEM             167472      (163.5K)       28E30
  SMARTDRV            28304      ( 27.6K)        6E90
  FREE                   32      (  0.0K)          20
  FREE               131808      (128.7K)       202E0
Total  FREE :        131840      (128.8K)
Total bytes available to programs (Conventional+Upper) :
    743456   (726.0K)
Largest executable program size :      611440   (597.1K)
Largest available upper memory block : 131808   (128.7K)
```

Figure 8. Memory map of real memory using Windows for Workgroups

Installation of Windows for Workgroups on an existing MS-DOS-based workstation on a LAN Manager network is almost as straightforward as installation on a fresh machine. Windows for Workgroups can be installed while LAN Manager is running. The Setup program for Windows for Workgroups attempts to identify the type of network hardware running, its settings for IRQ and IO base, and other settings. Although Setup attempts to determine the correct configuration, it does allow for modifications and potential corrections.

During the installation in this environment, Setup located a network protocol for which it did not have a protected-mode memory solution. The VREDIR, VNB, VSERVER, and so on, are not the same components as their real mode counterparts in LAN Manager, but are new 32-bit versions coded as Windows Virtual Device Drivers (VxDs). The TCP/IP protocol stack has not been ported as a Virtual Device Driver. The Setup program detected this and displayed a MessageBox explaining that this protocol would not be available when Windows for Workgroups started. (This is not to say it is not available! Please continue to the next section.)

The Setup process installed the Windows for Workgroups code as well as made several modifications to the system control files (CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI). Figure 9 is a comparison of the files before and after the installation of Windows for Workgroups. Notice that, where possible, Windows for Workgroups replaces existing MS-DOS and LAN Manager drivers with its own. This ensures you are running the most up-to-date version. In the case of the ELNKII.DOS driver, the Windows for Workgroups and the LAN Manager drivers are the same. Windows for Workgroups also moves the active PROTOCOL.INI file from the MS-DOS directory of LAN Manager (LANMAN.DOS) to the Windows directory. PROTOCOL.INI is the most modified of the three files. The new section added at the top associates binding paths to NetBIOS LANA (local area network adapter) numbers. The redirector and server will use the LANA numbers when communicating to each of the bind paths. Because of the new section, the PROTMAN.DOS that shipped with Windows for Workgroups is newer than the PROTMAN.DOS that shipped with LAN Manager.

Figure 9. Comparison of CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI

Figure 10 discusses the new modules found in Windows for Workgroups. Notice there is still a need for real-mode modules to accomplish the communications with the device driver. Also notice the modules from LAN Manager, which seem to be missing.

Figure 10. New modules in Windows for Workgroups

Figure 11 discusses where a LAN Manager function for MS-DOS moved to in Windows for Workgroups. Of importance is the lack of support for the LAN Manager messaging system. Though the CHAT function and Microsoft Mail provide functionality superior to "net send," existing LAN Manager systems (such as the Alerter) cannot use the advanced functionality of Windows for Workgroups. Special consideration is given to this topic later in this paper.

Figure 11. MS-DOS LAN Manager components map

Special Installation Considerations

Windows for Workgroups is designed to meet the user's growing need to share information freely. In providing this functionality it also provides a technically superior networked Windows-based workstation environment. However, some aspects of Windows for Workgroups are not desired in all installations. This section discusses two of these situations.

Removing the Server Component of Windows for Workgroups

Highly security-conscious organizations may not desire each user to have access to the resources of all machines. Windows for Workgroups does not attempt to implement or rely on any centralized security system, like the LAN Manager domain security system. Windows for Workgroups allows for these concerns by allowing Windows for Workgroups to install without the server component. With the server component removed, Windows for Workgroups may still use resources on other server machines (either LAN Manager or Windows for Workgroups that still have the server component) but will not be able to share resources (files, printers, server-side Network DDE, or Workgroup Mail Post Office). The two steps for removing the server component of Windows for Workgroups are outlined below, followed by an image of the completed SYSTEM.INI file.

- Step 1: Delete (or rename) the two files used by the server.

  In the \WINDOWS\SYSTEM directory delete or rename the following files:

  - VSERVER.386
  - VBROWSE.386

  Note If the files are renamed, it may be possible for the user to reconstruct the server component by reversing the steps in this section. To ensure that the server cannot be run without additional software, the files should be deleted.

- Step 2: Edit the \WINDOWS\SYSTEM.INI file to remove the server.

  Remove the references to "vserver.386" and "vbrowse.386" from the network line in the [386Enh] section of the SYSTEM.INI file.

  A copy of a modified SYSTEM.INI file is provided. The modified line is marked in **bold.** Also note that the original value for the line was retained but commented out. This was done for

clarity and is optional.

Note Notice that the Enablesharing value is still set to 1 (enabled). The user still has the ability to select and deselect this option for the Network section of Control Panel. However, once the above modifications are made, this value is ignored, and no sharing can be accomplished.

The final \WINDOWS\SYSTEM.INI file:

```
[boot]
shell=progman.exe
mouse.drv=mouse.drv
network.drv=wfwnet.drv
language.dll=
sound.drv=mmsound.drv
comm.drv=comm.drv
keyboard.drv=keyboard.drv
system.drv=system.drv
386grabber=vga.3gr
oemfonts.fon=vgaoem.fon
286grabber=vgacolor.2gr
fixedfon.fon=vgafix.fon
fonts.fon=vgasys.fon
display.drv=vga.drv
drivers=mmsystem.dll

[keyboard]
subtype=
type=4
keyboard.dll=
oemansi.bin=

[boot.description]
keyboard.typ=Enhanced 101 or 102 key US and Non US keyboards
mouse.drv=Microsoft, or IBM PS/2
network.drv=Microsoft Windows for Workgroups (3.1)
language.dll=English (American)
system.drv=MS-DOS System
codepage=437
woafont.fon=English (437)
aspect=100,96,96
display.drv=VGA

[386Enh]
32BitDiskAccess=OFF
device=*int13
device=*wdctrl
mouse=*vmd
netheapsize=20
network=vnetbios.386,vnetsup.386,vredir.386
; network=vnetbios.386,vnetsup.386,vredir.386,vserver.386,vbrowse.386
ebios=*ebios
woafont=dosapp.fon
display=*vddvga
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
keyboard=*vkd
device=vtdapi.386
device=vcd.386
device=vshare.386
device=vpicd.386
```

```
device=vpd.386
device=*vtd
device=*reboot
device=vdmad.386
device=*vsd
device=*v86mmgr
device=*pageswap
device=*dosmgr
device=*vmpoll
device=*wshell
device=*BLOCKDEV
device=*PAGEFILE
device=*vfd
device=*parity
device=*biosxlat
device=*vmcpd
device=*combuff
device=*cdpscsi
local=CON
FileSysChange=off
transport=vnb.386

[standard]

netheapsize=8
[NonWindowsApp]
localtsrs=dosedit,ced

[mci]
WaveAudio=mciwave.drv
Sequencer=mciseq.drv
CDAudio=mcicda.drv

[drivers]
timer=timer.drv
midimapper=midimap.drv

[DDEShares]
CHAT$=winchat,chat,,31,,0,,0,0,0
CLPBK$=clipsrv,system,,31,,0,,0,0,0
HEARTS$=mshearts,hearts,,31,,0,,0,0,0


[network]
ComputerName=GLENC3
Workgroup=CNSMKTG
UserName=glenc3
multinet=lanman
logonvalidated=yes
AutoLogon=Yes
Comment=
EnableSharing= 1
cachethispassword=yes
reshare=yes

[Password Lists]
*Shares=C:\WINDOWS\Shares.PWL
GLENC3=C:\WINDOWS\GLENC3.PWL
```

Removing Mail and Scheduling Components from Windows for Workgroups

Some organizations may not want to use the mail or scheduling systems included in Windows for Workgroups. Disabling this functionality is very simple. If a Workgroup Post Office is not created within a defined workgroup, the mail systems will not be able to send mail to others because there is no post office to act as clearinghouse for the mail. If disk space is at a premium on the workstations, the Mail and Schedule+ programs may also be removed. The Microsoft Mail programs are MSMAIL.EXE, MSMAIL.HLP, and MSMAIL.INI. The Microsoft Schedule+ programs are SCHDPLUS.EXE, SCHDPLUS.HLP, and SCHEDMSG.DLL. All files are located in the \WINDOWS directory.

Multiple Protocol Environments

As noted above, not all network protocols currently supported by LAN Manager have been ported to run in 386 protected mode (as VxDs). Therefore it may be necessary to install real mode protocol stacks to communicate with an existing environment. The three protocols that are currently not supported as VxDs in Windows for Workgroups are the TCP/IP protocol, DLC protocol, and Remote Access Service protocol. Microsoft provides TCP/IP and Microsoft's DLC in the LAN Manager 2.2 product offering ready for installation on Windows for Workgroups-based workstations. Other protocol stacks, such as Remote Access Service, can be used on Windows for Workgroups-based workstations, but must be installed manually. We will look at the installation of TCP/IP, MS-DLC, and Remote Access Service.

In general, installing multiple protocol stacks is quite simple. The network interface device driver (NDIS driver) remains in real memory. The VNETBIOS driver can be informed as to which NetBIOS driver to route commands to based on the LANA number.

Installing and Configuring TCP/IP

LAN Manager 2.2 provides the TCP/IP protocol in a format ready to install on Windows for Workgroups. The WFWPROT disk contains the needed installation files and device drivers.

To install the device driver, start the Control Panel program from the Main group in the Program Manager. From the Control Panel start Networks. At the bottom of the Networks panel is a row of command buttons. Select the Adapter command button. If more than one adapter is present in the workstation, make sure the adapter that is to support TCP/IP is selected. Once the adapter is selected, press the Setup command button on the right of the panel. From the Setup panel select the Protocols command button. From the Available Protocols list select Unlisted or Updated Protocol, and press OK.

The installer will now ask for a diskette for drive A. Place the WFWPROT disk in the appropriate drive, and press OK. Once the installation program has read the configuration information from the disk, the TCP/IP and DLC protocols will be added to the Available Protocols list. Select the TCP/IP protocol, and move it to the Protocols in Use list by pressing the Add button.

Once TCP/IP has been moved to the Protocols in Use list, select it and press the SETTINGS... command button. A panel of parameters needed by the TCP/IP protocol is presented. A list of parameters appears at the top of the panel, and an area below appears in which to enter the needed value. To change a value, select a parameter from the list, move to the entry field and set the value, then press the **Set** command button.

Figure 12 discusses the parameters for TCP/IP. Of special note is the use of "space delimited" address notation instead of the more common "dot decimal" format.

TOCOL.INI").

TOCOL.INI").

sly connect to this node for server services.

ROTOCOL.INI")

Figure 12. TCP/IP parameters

Once the protocol has been completely configured, use the OK command button to "walk" back though the various panels. At the last network panel you will be prompted to restart your computer to load the appropriate device drivers.

Figure 13 details the active components of the TCP/IP installation. Notice that the NMTSR.EXE is an optional component and is only used with the PING utility. It is not installed but is on the WFWPROT disk and can be added manually to the AUTOEXEC.BAT file immediately after the TINYRFC launch.

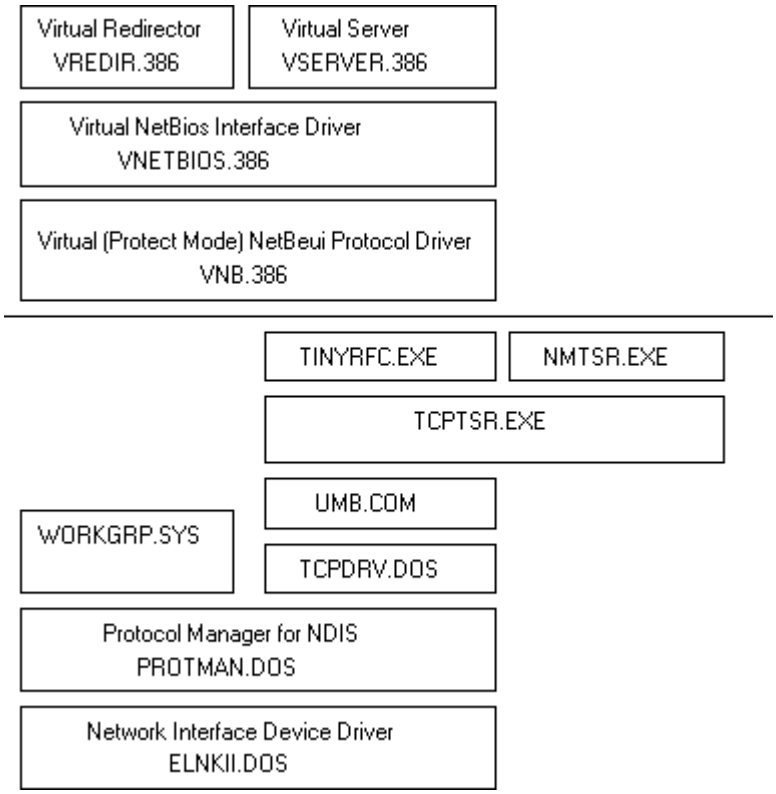

Figure 13. Active components in a NetBEUI and TCP/IP installation

Additional notes

Two parameters in the \WINDOWS\SYSTEM.INI file may need to be adjusted in the event of problems, specifically if Windows for Workgroups hangs during startup.

- After the [386Enh] section header, add the following line:

  ```
  V86ModeLanas=<LANABASE for TCP/IP>
  ```

  This informs the networking components of Windows for Workgroups that this LANA is supported by a real mode protocol stack.

- Increase the **netheapsize** in the [386Enh] section to 28 or 32. This parameter reserves real-mode memory to be used as data transfer buffers between Windows and real-mode protocol stacks. The default of 12 (kilobytes) may not be sufficient.

Installing and Configuring Microsoft DLC

Installation of the Microsoft DLC protocol stack is important for organizations that want their mainframes (either S/370 or AS/400s) to communicate with Windows for Workgroups-based workstations. Using the LAN Manager 2.2 product offering, installation of the DLC protocol stack is very similar to the installation of the TCP/IP stack.

To install the device driver, start the Control Panel program from the Main group in the Program Manager. From the Control Panel start Networks. At the bottom of the Networks panel is a row of command buttons. Select the Adapter command button. If more than one adapter is present in the workstation, make sure the adapter that is to support TCP/IP is selected. Once the adapter is selected, press the Setup command button on the right of the panel. From the Setup panel select the Protocols command button. From the Available Protocols list select Unlisted or Updated Protocol, and press OK.

The installer will now ask for a diskette for drive A. Place the WFWPROT disk in the appropriate drive and press OK. Once the installation program has read the configuration information from the disk, the TCP/IP and DLC protocols will be added to the Available Protocols list. Select the DLC protocol and move it to the Protocols in Use list by pressing the Add button.

Once DLC has been moved to the Protocols in Use list, select it and press the SETTINGS... command button. A panel of parameters needed by the DLC protocol is presented. A list of parameters appears at the top of the panel, and an area below appears in which to enter the needed value. To change a value, select a parameter from the list, move to the entry field, and set the value, then press the Set command button.

Figure 14 discusses the parameters for DLC. Of special note is the DIX or 802.3 parameter.

® III si).

Figure 14. DLC parameters

Once the protocol has been completely configured, use the OK command button to "walk" back though the various panels. At the last network panel you will be prompted to restart your computer to load the appropriate device drivers.

Figure 15 details the active components of the DLC installation.

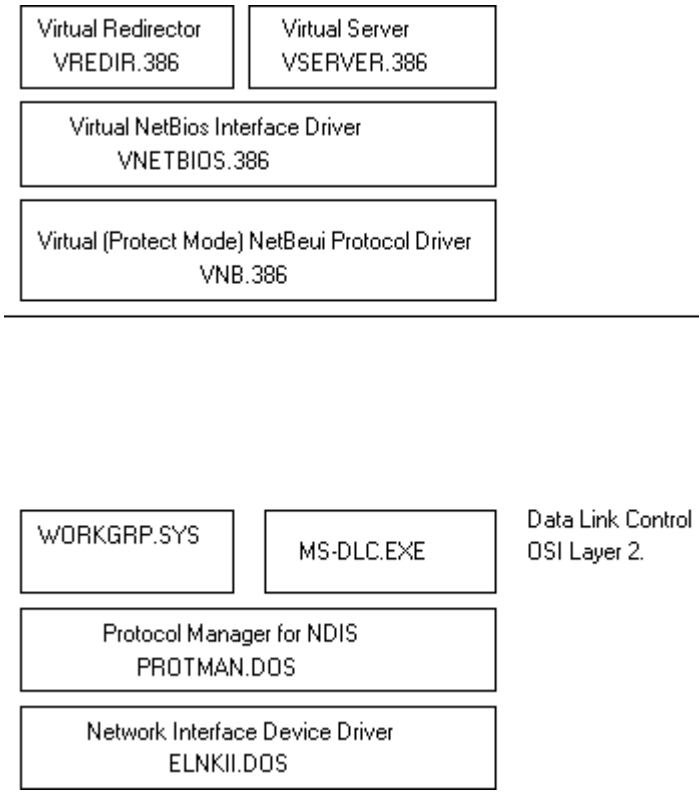

Figure 15. Active components in a NetBEUI and DLC installation

Additional notes

Two parameters in the \WINDOWS\SYSTEM.INI file may need to be adjusted in the event of problems, specifically if Windows for Workgroups fails to start network services.

- After the **[386Enh]** section header add the following line:

  ```
  V86ModeLanas=<LANABASE for DLC>
  ```

  This informs the networking components of Windows for Workgroups that this LANA is supported by a real mode protocol stack.

- After the **[network]** section header add the following line:

  ```
  exclude=<LANABASE for DLC>
  ```

  This informs the networking components of Windows for Workgroups not to attempt to send NBC (NetBIOS commands) to this interface. If this is not coded, the networking components of Windows for Workgroups will not initialize and will report errors.

Installing and Configuring for Remote Access Service

Installation of the Remote Access Service protocol stack involves not only installing the protocol stack, but adding the supportive programs as well. Unlike the installations we have seen above, installation of the Remote Access Service protocol stack does require the manual manipulation of the CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI files. The following steps make the task easier. A completed example of the files has been provided for reference.

- Step 1: Install Remote Access Service on an MS-DOS–based machine on a LAN Manager network.

  Before we start the installation of Remote Access Service we must first get a copy of the files. This is easily done by installing LAN Manager on a single MS-DOS–based machine, then copying the files onto a disk or a file share point for distribution to Windows for Workgroups-based workstations.

  Note Please follow the procedures and installation prompts for installing Remote Access Service. When prompted for the COM Port, modem type, and phone number you may wish to use information for the most common workstation environment. Further manipulation of the MODEM.INF may be needed if this information does not match the workstation's hardware configuration.

- Step 2: Copy the needed files to a floppy disk.

  Copy the following files to a floppy disk:

  C:\LANMAN.DOS\DRIVERS\ASYNC\ASYMAC.DOS
  C:\LANMAN.DOS\DRIVERS\PROTOCOL\ASYBEUI\ASYBEUI.EXE
  C:\LANMAN.DOS\NETPROG\VCOMMIOD.EXE
  C:\LANMAN.DOS\NETPROG\WANTSR.EXE
  C:\LANMAN.DOS\NETPROG\RASADMIN.EXE
  C:\LANMAN.DOS\NETPROG\RASADMIN.HLP
  C:\LANMAN.DOS\NETPROG\RASDIAL.EXE
  C:\LANMAN.DOS\NETPROG\RASHELP.EXE
  C:\LANMAN.DOS\NETPROG\RASPHONE.EXE
  C:\LANMAN.DOS\NETPROG\RASPHONE.HLP
  C:\LANMAN.DOS\NETPROG\RASPHONE.ICO
  C:\LANMAN.DOS\COMDEV.INI
  C:\LANMAN.DOS\MODEM.INF
  C:\LANMAN.DOS\PHONE.INF
  This file may not be present if this is a new installation.
  C:\LANMAN.DOS\RASDIAL.MSG
  C:\LANMAN.DOS\RASHELP.MSG
  C:\LANMAN.DOS\RASPHONE.MSG

- Step 3: Install Windows for Workgroups on a target machine.

- Step 4: Copy the Remote Access Service files from the floppy disk created in step 2 to the \WINDOWS directory (assuming this is the directory where Windows for Workgroups is installed).

- Step 4A: Copy the following Remote Access Service files from the floppy disk created in step 2 to the root directory of the Windows for Workgroups computer (example: C:\):

  COMDEV.INI
  MODEMS.INF
  PHONE.INF
  RASDIAL.MSG
  RASHELP.MSG
  RASPHONE.MSG

- Step 5: In the CONFIG.SYS file, insert the following line immediately *after* the line that installs PROTMAN.DOS:

  ```
  device=c:\windows\asymac.dos
  ```

- Step 6: Make the following modifications to the \AUTOEXEC.BAT file:

  Immediately *before* the net start line add the following line:

  ```
  c:\windows\asybeui.exe
  ```

  Immediately *after* the net start line add the following lines:

```
c:\windows\vcommiod.exe
c:\windows\wantsr.exe
```

- Step 7: Make the following modifications to the \WINDOWS\PROTOCOL.INI file.

  After the last existing netcard line, add the following line:

  ```
  netcard=ms$asymac,1,MS$ASYMAC
  ```

  After the last existing transport line, add the following line:

  ```
  transport=ms$asybeui,MS$ASYBEUI
  ```

  After the last existing LANA number line, add the following line:

  ```
  lana1=ms$asymac,1,ms$asybeui
  ```

  Note The LANA number may be different if you are more than one protocol.

  Add the following lines to the end of the PROTOCOL.INI file:

  ```
  [MS$ASYMAC]
  Drivername=ASYMAC$

  [MS$ASYBEUI]
  DRIVERNAME=ASYBEUI$
  LOAD="ASYBEUI","VCOMMIOD[U]","WANTSR[U]"
  UNLOAD="WANTSR /U[C]","VCOMMIOD /U[C]", "ASYBEUI [DU]"
  LANABASE=1
  BINDINGS="MS$ASYMAC"
  ```

- Step 8: In the \WINDOWS\SYSTEM.INI file, add the following lines to the **[386Enh]** section:

  ```
  V86ModeLANAs=1
  MaintainServerList=No
  ```

  The **V86ModeLANAs** entry identifies the LANA as a real-mode protocol stack. If Remote Access Service has been given a different LANA number it should be used.

  For performance reasons, the **MaintainServerList** entry prevents the remote workstation from being designated as the computer that maintains the list of workgroups or computers on the network.

- Step 9: Reboot the target computer to load the device drivers and TSRs. Once restarted, start RASPHONE to ensure everything is properly installed.

- Step 10: When you are sure everything is installed correctly, add RASPHONE to the Startup group to start automatically each time you start Windows for Workgroups.

  RASPHONE is used to dial in. It cannot be started until after the redirector is started. In 386 enhanced mode, the redirector is VREDIR.386, and it is not started until Windows for Workgroups is started.

  Note In the Program Item that starts RASPHONE, set the Working Directory to \WINDOWS (or the appropriate Windows for Workgroups root directory). RASPHONE uses this path to locate its message files.

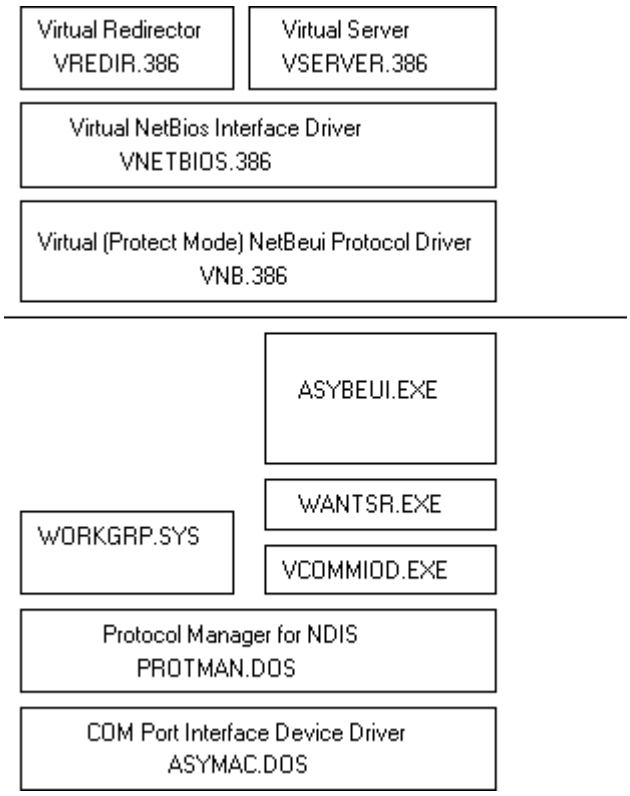

Figure 16. Active components in a NetBEUI and Remote Access Service installation

Figure 16 details the active components of the Remote Access Service installation. The following are the final installation images of CONFIG.SYS, AUTOEXEC.BAT, and PROTOCOL.INI. Areas where manual manipulation was needed have been highlighted in **bold**.

Final \CONFIG.SYS file:

```
DEVICE=C:\DOS\SETVER.EXE
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\WINDOWS\EMM386.EXE NoEMS
DOS=HIGH,UMB
FILES=30
LASTDRIVE=Z

device=C:\WINDOWS\protman.dos /i:C:\WINDOWS
device=c:\windows\asymac.dos
device=C:\WINDOWS\workgrp.sys
device=C:\WINDOWS\elnkii.dos
STACKS=9,256
```

Final \AUTOEXEC.BAT file:

```
C:\WINDOWS\SMARTDRV.EXE
c:\windows\asybeui
C:\WINDOWS\net start
c:\windows\vcommiod
c:\windows\wantsr
@ECHO OFF
PROMPT $p$g
PATH C:\WINDOWS;C:\DOS
SET TEMP=C:\DOS
```

Final \WINDOWS\PROTOCOL.INI file:

```
[network.setup]
version=0x3100
netcard=ms$elnkii,1,MS$ELNKII
netcard=ms$asymac,1,MS$ASYMAC
transport=ms$netbeui,MS$NETBEUI
transport=ms$asybeui,MS$ASYBEUI
lana0=ms$elnkii,1,ms$netbeui
lana1=ms$asymac,1,ms$asybeui

[protman]
DriverName=PROTMAN$
PRIORITY=MS$NETBEUI

[MS$ELNKII]
DriverName=ELNKII$
INTERRUPT=5
IOADDRESS=0x300
MAXTRANSMITS=40
TRANSCEIVER=EXTERNAL

[MS$NETBEUI]
DriverName=netbeui$
SESSIONS=6
NCBS=12
BINDINGS=MS$ELNKII
LANABASE=0

[MS$ASYMAC]
Drivername=ASYMAC$

[MS$ASYBEUI]
DRIVERNAME=ASYBEUI$
LOAD="ASYBEUI","VCOMMIOD[U]","WANTSR[U]"
UNLOAD="WANTSR /U[C]","VCOMMIOD /U[C]", "ASYBEUI [DU]"
LANABASE=1
BINDINGS="MS$ASYMAC"
```

Adding LAN Manager Servers to a Windows for Workgroups Environment

There are a number of very powerful reasons for adding LAN Manager servers into Windows for Workgroup environments. LAN Manager servers provide the server component of a client-server environment. A number of products are available that exploit this type of environment; these products typically centralize a function to make greater use of a valuable resource or specialized environment. Three of these products are Microsoft SQL Server 4.2, DCA/Microsoft Comm Server 1.1, and Microsoft LAN Manager Remote Access Service. Windows for Workgroups can make use of these and other client-server products to help increase the workgroup's functionality.

In addition to being the platform for client-server products, LAN Manager servers can also be used as special security servers. Security can be applied in two directions. The first is logon security, the second is logon scripting facilities. LAN Manager servers also have additional file-sharing security options, which allows LAN Manager to act as a super-secure file platform.

Installing a LAN Manager Server into a Windows for Workgroups Environment

The LAN Manager server is a component of the LAN Manager 2.*x* product. The server requires a

386 machine or better, with 8 MB of memory, and at least 100 MB of hard disk space. The LAN Manager server runs on top of OS/2 1.*x*. Microsoft provides a copy of OS/2 1.3 with LAN Manager.

The installation steps are explained in detail in the *LAN Manager Installation and Configuration Guide.* In general, however, the steps involve installing OS/2 1.3 on the machine, then installing LAN Manager and the required network protocols.

An important decision when installing a LAN Manager server is the type of security the server will implement. LAN Manager servers provide two types of security.

- *Share Security* is very much like the security provided on Windows for Workgroups-based workstations. Anyone who wishes to use a shared resource must know the password. Unlike the password structure of Windows for Workgroups, LAN Manager shares require only one password. Unlike Windows for Workgroups, however, it is possible to have multiple shares defined to the same resource on a LAN Manager server, each with a different password.
- The other form of security LAN Manager servers may provide is *User Security.* This is the much more common form of security used with LAN Manager servers. In this security the password is associated with the user, not the shared resource. Thus a user has a single password to all shared resources on the server. What resources the user may use and the level of access the user has are based on permissions granted by the server's administrator.

The remainder of this discussion assumes the LAN Manager server is executing in User Security mode.

Creating a Server-Based Security Environment

Each user of Windows for Workgroups does not have to be added to the LAN Manager user-security database in order to use resources on the LAN Manager server. LAN Manager has the concept of *Guest* accounts. Users not defined to LAN Manager are allowed to use resources granted to the Guest account. Usually this is a very small set of resources such as a public disk directory.

If a user of Windows for Workgroups is to have more permissions on a server than the guest account, a user account must be created on the server. Note that not all of the user account attributes available from LAN Manager workstations are available from Windows for Workgroups-based workstations.

- LAN Manager has the ability to "age" passwords and set a maximum age for a password. In LAN Manager environments a message would be sent to the user when the password is about to expire. Because Windows for Workgroups does not support messaging the user will not receive the message.
- Windows for Workgroups uses passwords differently than LAN Manager-based workstations do. Users may change their LAN Manager passwords in two ways. First, users may use the MS-DOS console command NET PASSWORD. Users may also change their LAN Manager passwords in the Control Panel. The Set Password option is part of the Networks Setting dialog.

  Note An expired password on the LAN Manager server does not prohibit users from logging onto their workstations, or from using resources shared by other workstations running Windows for Workgroups.
- The LAN Manager server administrator can set an expiration date for a user, or disable a user's account. This will stop the user from using resources on the LAN Manager server. The user will still be able to access resources shared by other Windows for Workgroups-based workstations.
- LAN Manager workstations have access to a facility known as *logon scripts*. This predefined script (batch file) is executed on the LAN Manager workstation once the user's id and

password have been authenticated. Windows for Workgroups-based workstations will execute logon scripts on the local workstation if using the LAN Manager domain logon feature (LAN Manager Settings under the Networks section of Control Panel).

Users on LAN Manager servers can collectively be given access rights to resources through a system known as *groups*. Groups make management of security of a LAN Manager server much easier. A group may be given access permission to a resource, say a file. When a user is added to the group, the user is automatically given access permission to the file. This is a convenient method of giving resource permissions to a workgroup.

A single LAN Manager server may be shared by multiple workgroups. The use of groups is an easy way to control access permissions among various groups. Figure 17 illustrates this situation. The server is likely to have Finance's Chart of Accounts file, the Accounts Payable Ledger file, and so on, as well as Manufacturing's Build Schedule, Current Component Inventories, and Latest Vendor's price sheets. The server administrator would want to establish groups so that a person in finance does not accidentally erase Manufacturing's Build Schedule.

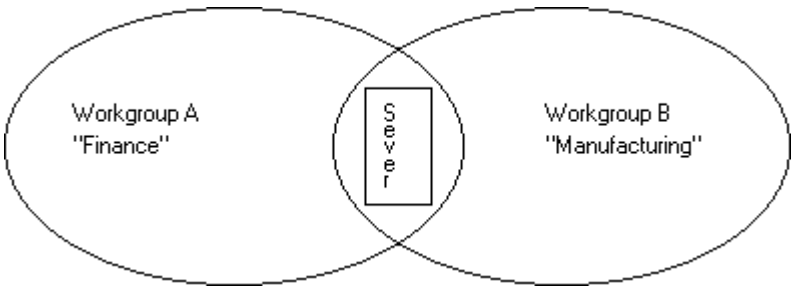

Figure 17. Multiple workgroups sharing a single server

Groups also make adding and moving employees easier. When a person joins the Finance department, the server administrator needs only to create the user's account and add it to the finance group. When an employee is transferred from Finance to Manufacturing, the server administrator moves the user account from one group to another. This avoids the laborious task of adding individual resource permissions.

Once the user accounts for each user in a workgroup have been created and associated with the resources they have access to (either directly or by groups), the user of Windows for Workgroups may use LAN Manager server resources. LAN Manager and Windows for Workgroups share the same underlying NOS (network operating system) protocol, called SMBs (server message blocks). Access to resources is always verified prior to being granted, even to Windows for Workgroups-based workstations.

Tuning Considerations

There are no special tuning considerations on the server when using workstations running Windows for Workgroups versus using workstations on LAN Manager. The server should be tuned according to the number of workstations and type of activities being performed.

One area that does require comment is Microsoft LAN Manager Remote Access Service. This facility allows a workstation to use a standard async modem and telephone line to dial into the server and access resources as if the workstation were connected via the network. The components needed on the workstation side have been examined above. Figure 18 illustrates in general the components in a remote connection.

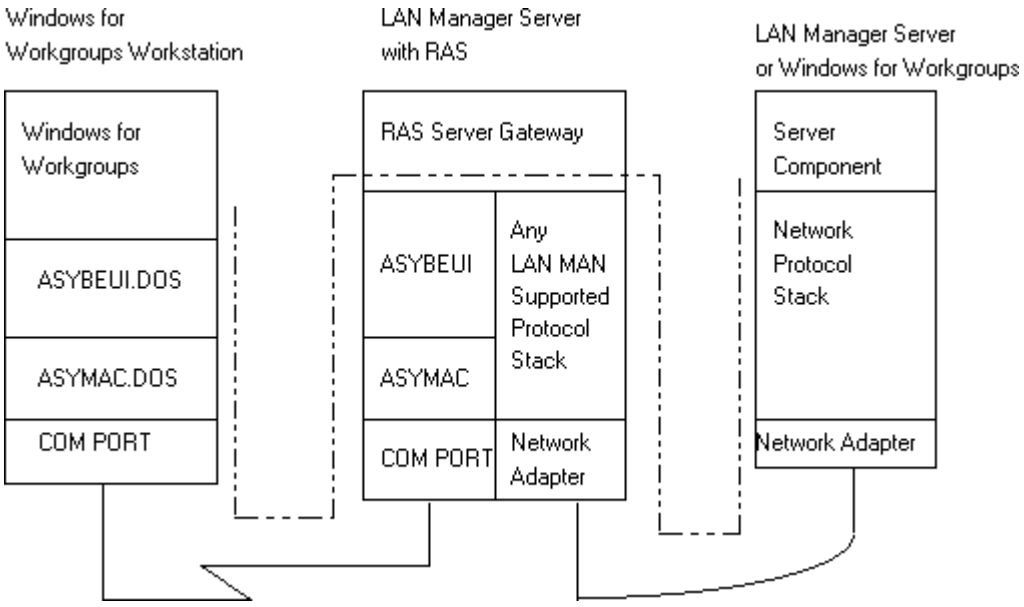

Figure 18. General description of Remote Access Service data flow

The server component acts as a gateway, reading data from the modem and posting it to its LAN protocol stacks. One of the components of the workstation that is communicated over the telephone line is its *name space*. This is the list of names associated with the workstation. A workstation is known by many names on the network: computer name, user name, workgroup name, and so on. A Windows for Workgroups-based workstation has a total of seven different names, which are all added to the network protocol stack when the user establishes a connection via Remote Access Service. The server too must add its names to the network protocol stack. There are from five to nine names used by the server. By default the network protocol stack allows only 17 names to be added to its name space. This limit can be quickly exceeded. Each Remote Access Service server can support up to 16 concurrent remote workstations. Thus 16 times 7 plus 9 creates a need for a maximum of 127 names.

The number of names in a NetBEUI protocol stack is determined by the **names** parameter in the **[netbeui]** section of the PROTOCOL.INI file in the \LANMAN directory on the server. In the TCP/IP protocol stack the parameter is **numnames** in the **[tcpip]** section. Each name does use memory. An accurate estimation of the number of names that will be needed should be done prior to modifying PROTOCOL.INI.

Note In TCP/IP the maximum for the numnames parameter is 127. In NetBEUI it is 256.

Adding Windows for Workgroups to Existing LAN Manager Environments

Windows for Workgroups-based workstations that are installed to use the LAN Manager network interface can immediately gain access to resources shared by LAN Manager servers. Being designed to function in a cooperative environment (without a central authority server), Windows for Workgroups does treat some aspects of networking differently from LAN Manager.

Windows for Workgroups workstations will use "guest" privilege on LAN Manager servers (user-security servers) unless given individual user accounts, the same as LAN Manager workstations. User IDs for Windows for Workgroups can be combined into groups on the server to make resource management easier.

Users of Windows for Workgroups can change their passwords on the LAN Manager server from

their workstations. If password aging is used on the LAN Manager server, the user must use the NET PASSWORD command to change the password stored on the LAN Manager server. The Control Panel Change Password command does not affect the LAN Manager server. The LAN Manager password command and Network settings of Control Panel.

Windows for Workgroups does not support the LAN Manager messaging system. Thus Windows for Workgroups-based workstations will not receive system alerts, print job complete messages, or password expiration messages. Windows for Workgroups does provide the Chat facility for quick person-to-person messaging, and Microsoft Mail for more global messaging.

Windows for Workgroups cannot currently be started using RIPL (remote initial program load). All workstations running Windows for Workgroups must be booted from their own local hard disks.

LAN Manager Domains and Workgroups

Multiple LAN Manager servers and workstations can logically be grouped together to form a *domain*. Servers are the main benefactors of the domain construct. There is one Primary Domain Controller (PDC) in a domain, which is the source server for user security information. Though a user logon request may be satisfied by any domain controller in the domain, the master copy of the security database is maintained on a single server (with updates sent to backup domain controllers [BDCs] as needed). Domains also combine workstations into logical units for broadcast messaging.

The workgroup concept used by Windows for Workgroups is very similar to domains, with a few exceptions. Because there is no concept of centralized security, there is no PDC or BDC concept or replication of security databases. Workgroups primarily organize a group of workstations for messaging.

A feature of Windows for Workgroups is the ability to *browse* a workgroup—that is, to see a list of workstations within a workgroup and a list of workgroups. The ability to browse can be extended to LAN Manager domains by adding a single Windows for Workgroups-based workstation into each domain that is to appear in the browse list.

Note If a LAN Manager domain includes workstations running Windows for Workgroups, that domain will appear in the browse list. This feature cannot be turned off in Windows for Workgroups.

MS-DOS Functions of LAN Manager Not Available in Windows for Workgroups-Based Workstations

Because Windows for Workgroups addresses different networking needs from LAN Manager, not all of the MS-DOS user functions of LAN Manager are available to it. The following is a list of network commands available to the MS-DOS–based workstation on LAN Manager and comments on their availability in Windows for Workgroups.

NET ADMIN

This function allows an MS-DOS–based workstation on LAN Manager to issue commands to administer servers remotely. This function is not available on Windows for Workgroups-based workstations. However, the LAN Manager 2.2 NetAdmin program will allow workstations running Windows for Workgroups to administer LAN Manager servers remotely.

NET CONFIG

In MS-DOS–based workgroups on LAN Manager, this command displays a list of executing services. Under Windows for Workgroups, this command displays the current names of the

workstation, the version number, and the workgroup name.

NET CONTINUE
MS-DOS–based workstations allow the "pausing" of services. The CONTINUE Command reactivates these services. Windows for Workgroups does not allow for the pausing of services, thus does not need the CONTINUE command.

NET COPY
MS-DOS–based workstations on LAN Manager can instruct the server to copy a file from one directory to another on the server without the data first being passed to the workstation. Windows for Workgroups does not implement this command.

NET HELP
This command is available on both MS-DOS–based workstations and Windows for Workgroups.

NET HELPMSG
This command is not implemented under Windows for Workgroups.

NET LOG
Under MS-DOS–based workstations, this command tells users the status of the message logging facility and the current message log file. Windows for Workgroups does not support messaging and therefore does not provide this command.

NET LOGOFF
This command is available on both MS-DOS–based workstations and Windows for Workgroups.

NET LOGON
This command is available on both MS-DOS–based workstations and Windows for Workgroups. Under MS-DOS, however, attempts are made to verify the logon against a centralized logon server. If one is found and a logon script for the user is available, the logon script will be executed on the workstation. Because Windows for Workgroups does not support centralized logon authority, in it NET LOGON simply establishes a local user ID and password.

NET MOVE
This command is very similar to the NET COPY command and is not supported under Windows for Workgroups.

NET NAME
Under Windows for Workgroups the functionality of this command has been moved to NET CONFIG.

NET PASSWORD
This command is supported under both MS-DOS–based workstations on LAN Manager and Windows for Workgroups. This command allows Windows for Workgroups-based workstations to update passwords on a logon server.

NET PAUSE
This command is not supported on Windows for Workgroups. All of the major LAN Manager services for MS-DOS have been moved into the redirector and are not pausable.

NET SEND
Windows for Workgroups does not support the LAN Manager messaging system at this time.

NET START
This command performs a different role under Windows for Workgroups. Its role is to bind the protocol and NDIS device drivers in preparation for network communications.

NET USE
This command is available on both MS-DOS–based workstations and Windows for Workgroups.

NET VERSION
This command is available on both MS-DOS-based workstations and Windows for Workgroups.

NET VIEW
This command is available on both MS-DOS-based workstations and Windows for Workgroups.

NET WHO
This command is not available under Windows for Workgroups.

Access to SQL Server and Comm Server from Windows for Workgroups

No modifications are needed to access SQL Server or Comm Server from a Windows for Workgroups workstation. The client software should be installed as if installing on Windows 3.*x*.